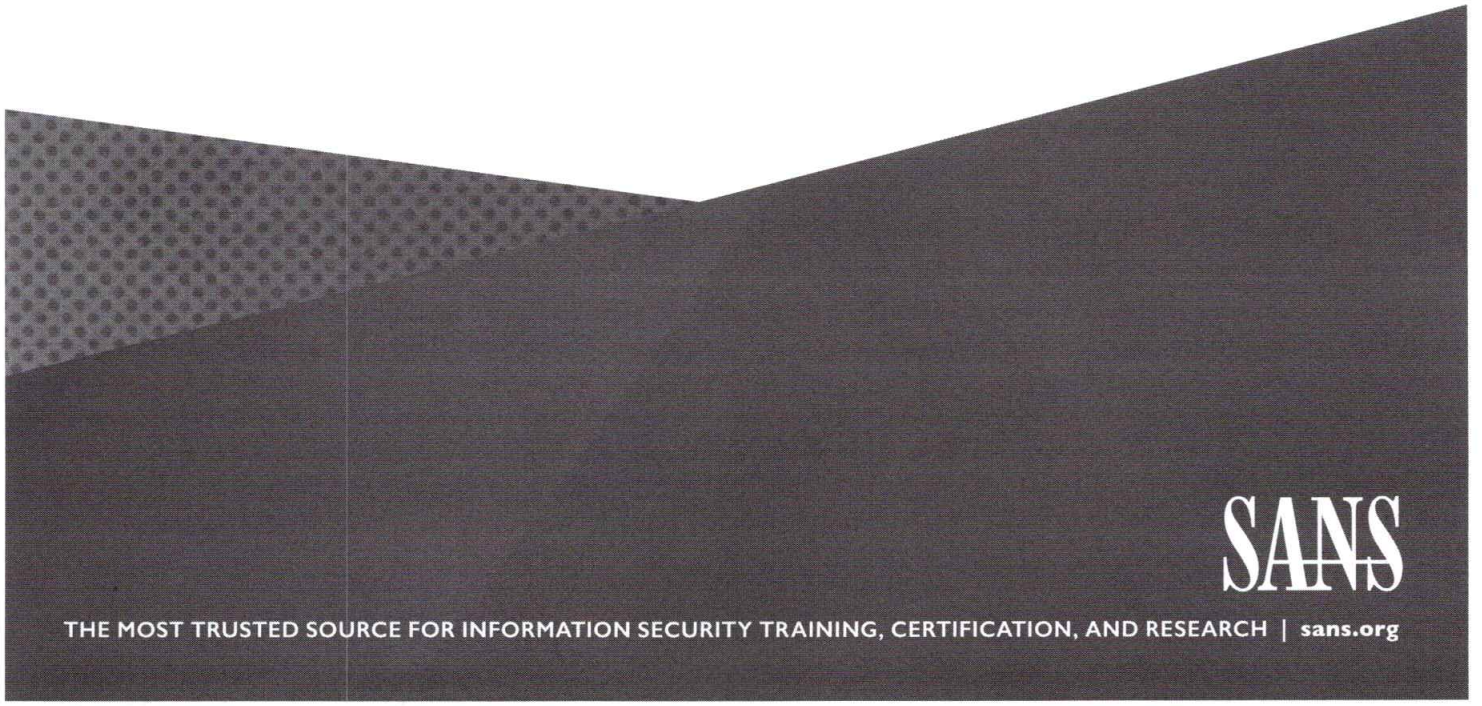
514.2

Strategic Roadmap Development



MGT514.2 | IT Security Strategic Planning, Policy, and Leadership

SANS

Strategic Roadmap Development

This page intentionally left blank.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- *Analyze Current State*
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

How to Analyze Current State

1) Understand where you've been
   - Analyze your organization's history
2) Understand how you operate
   - Determine your values and organizational culture
3) Understand where you are strong and weak
   - Analyze your Strengths, Weaknesses, Opportunities, and Threats (SWOT)

Analyzing your current state is key to developing an effective strategic plan. An understanding of your current state comes from:

1) Understanding where you've been

By analyzing your organization's history, you can better plan for the future.

2) Understanding how you operate

It's not just about *what* has been done in the past. Understanding *how* this was accomplished is key to understanding acceptable working norms. This is done by understanding the organization's values and culture.

3) Understanding where you are strong and weak

By analyzing your Strengths, Weaknesses, Opportunities, and Threats (SWOT), you can determine where you should focus and invest.

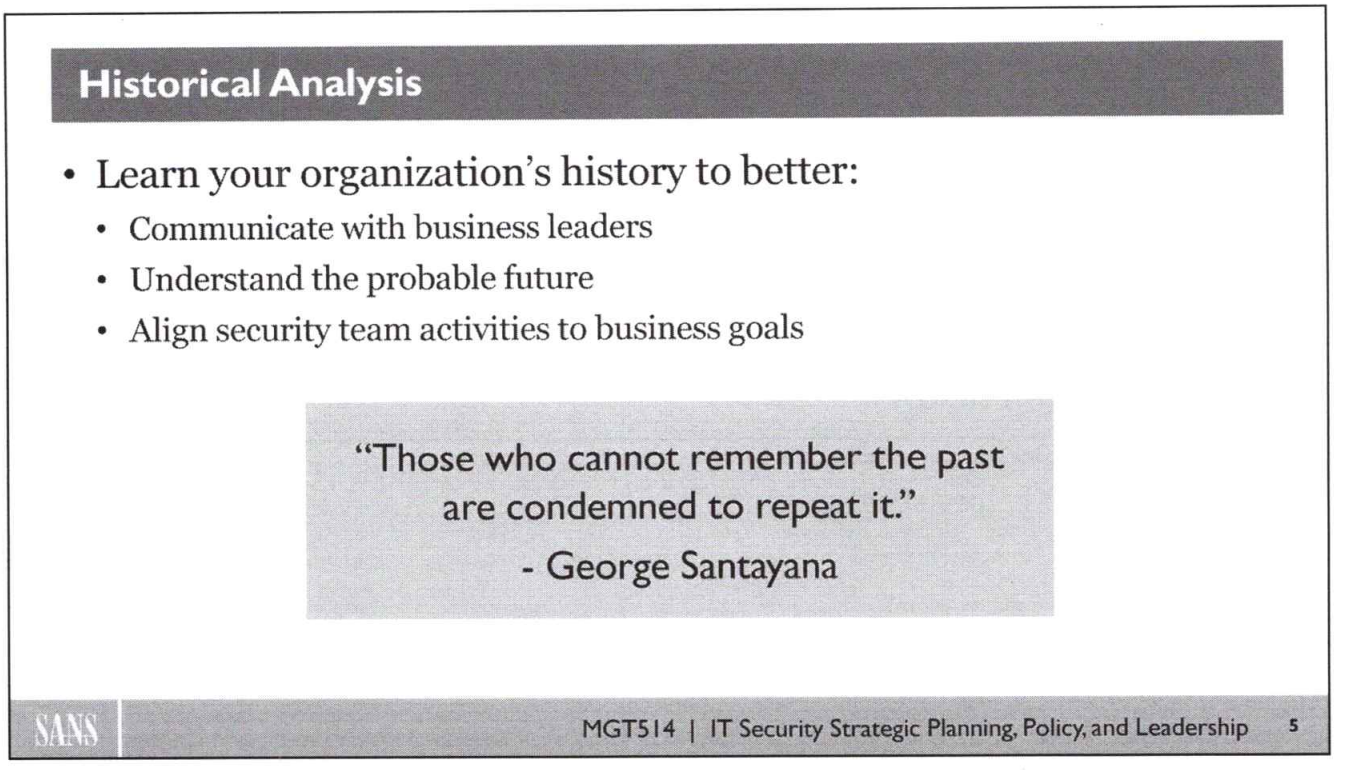
Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - *Historical Analysis*
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.



George Santayana was a philosopher, essayist, poet, and novelist who was born in Spain and raised and educated in the United States. He famously said, "Those who cannot remember the past are condemned to repeat it." This is especially important for strategic planning. Business leaders are aware of an organization's history. If we don't have that same understanding, we will not be able to communicate effectively with those business leaders. Moreover, the past helps us understand the probable future. Instead of being condemned to repeat the past by remembering what has previously occurred, we will be better prepared to align security team activities to business goals.

What Are the Major Periods of Change?

- Identify periods of major change
  - Use archives and interviews
- Are there things you used to do that you should consider doing again?
- Lessons from history
  - Mistakes you do not want to repeat
  - Events that helped shape the culture

To better understand your organization's history, it is useful to identify the major periods of change.

In 1993, Apple introduced the Newton, which was the first Personal Digital Assistant (PDA). It was intended to be a portable computer that would reinvent personal computing. However, it was not commercially successful and was discontinued in 1998. Despite its commercial failure, Apple learned from the Newton and went on to develop the iPhone and iPad. This is an example of a product that was ahead of its time and was worth considering again once technology matured.

It was under the leadership of then Apple CEO John Sculley that the Newton was introduced. John Sculley famously ousted Apple founder Steve Jobs from the company and went on to increase profits from $800 million to $8 billion.[1] He was CEO from 1983 to 1993 and, many argue that by the time of his departure, had shifted the company away from its product-centric culture and focus on "making the best products in the world." This lesson of staying true to the company culture is with Apple to the present day. In 2012, Apple hired John Browett to head the retail business. He was fired after only nine months on the job. Apple and Browett realized very quickly that it wasn't a cultural fit with Browett saying, "The issue is I just didn't fit with the way they ran the business."[2]

References

[1] http://en.wikipedia.org/wiki/John_Sculley

[2] https://gigaom.com/2013/03/15/former-apple-retail-chief-john-browett-admits-he-was-a-bad-fit-at-the-company/

Wayback Machine

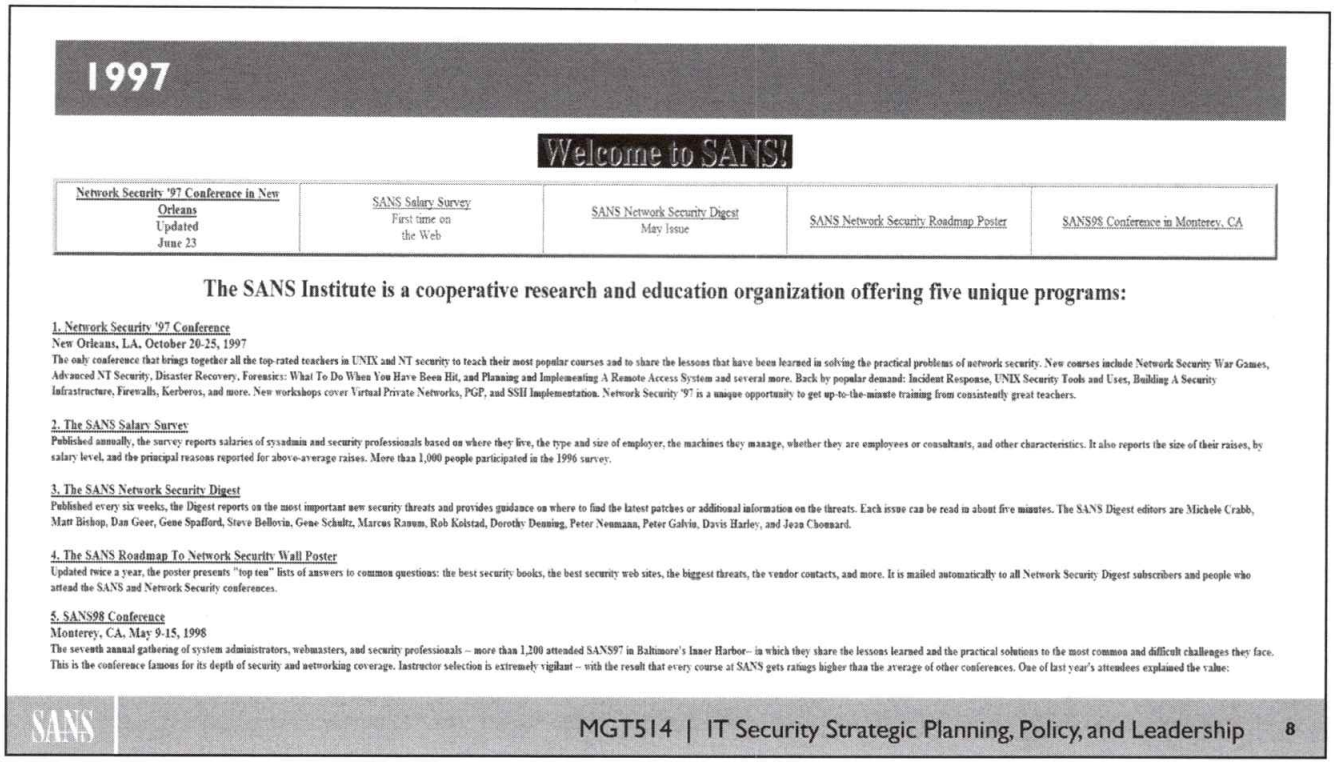
- Wayback Machine
  - From the Internet Archive Project
  - Important tool to model major changes in an organization's history
  - Available at archive.org
- Use it to review sans.org

The Wayback Machine[1] is a tool that captures web pages as they were at a point in time. It is hosted by the Internet Archive, which is a non-profit organization dedicated to providing "universal access to all knowledge." It is fascinating to see websites of old and is very useful for researching and modeling major changes in an organization's history.

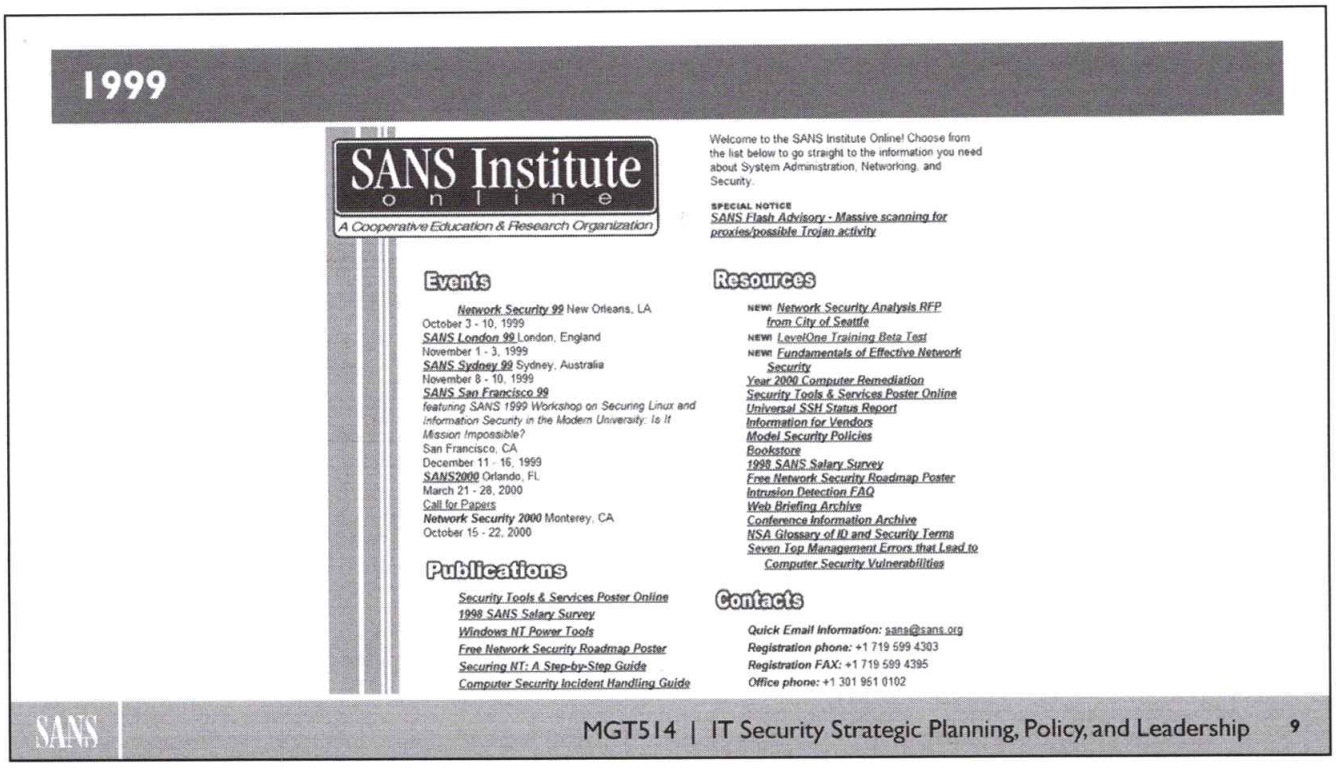
Using images from the Wayback Machine, let's look at the SANS Institute over time.

Reference

[1] https://archive.org/web/

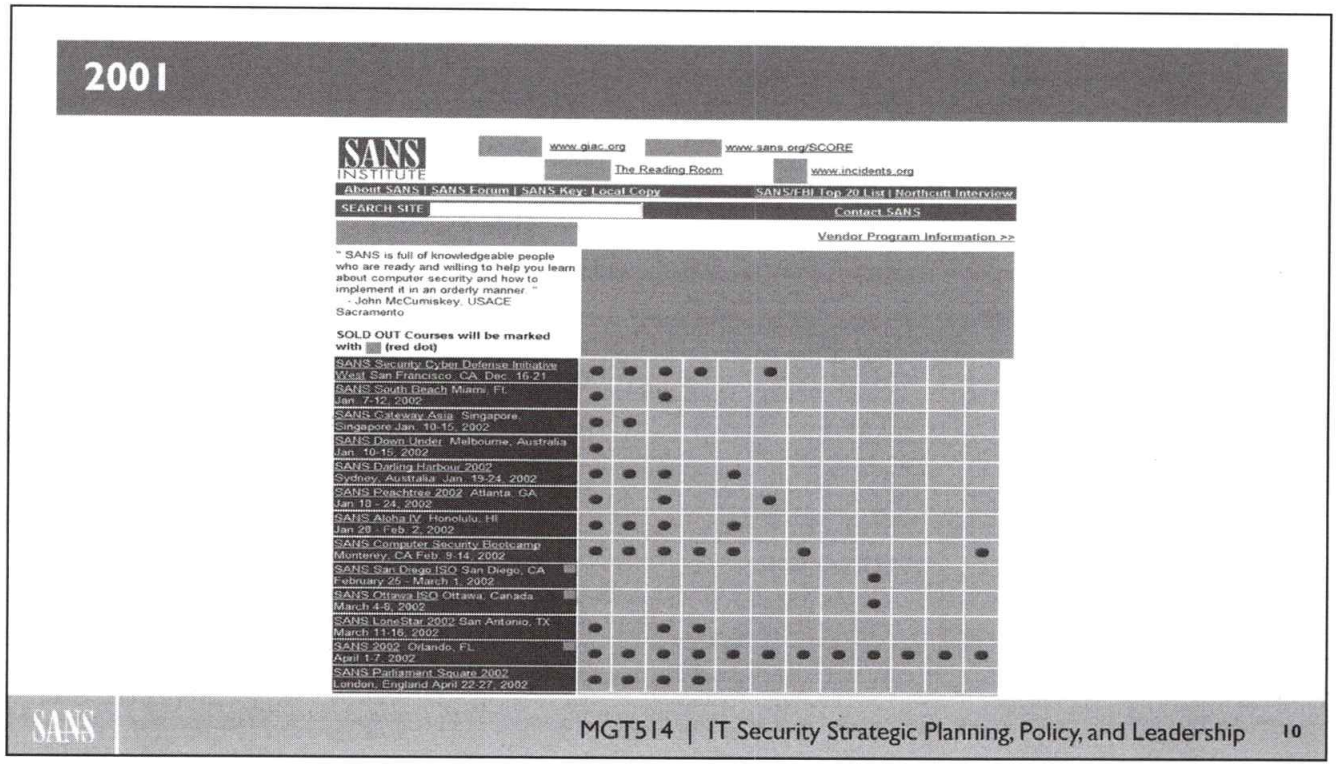


In 1997, SANS had only two events per year, serving 1000-1200 total students. The focus was on two-day technical conference sessions with one-day tutorials. There was a partnership with Usenet/SAGE and, as the screenshot shows, the concept of cooperative research was already in place. In addition to the conference sessions, community resources like the salary survey, security digest, and free posters were already in place.



By 1999, SANS had increased the number of events and went international with events in Sydney and London. The "LevelOne" training, which was a precursor to the popular Security Essentials course, was introduced.

- Amount of security content on web increased
- Published books during this phase
- No mention of Usenet and SAGE
- Forerunner of GIAC was called "SNAP" (System and Network Assurance Program)
- Already using quotes as a primary marketing tool



By 2001, classes were on a "track" system with track one being Security Essentials:

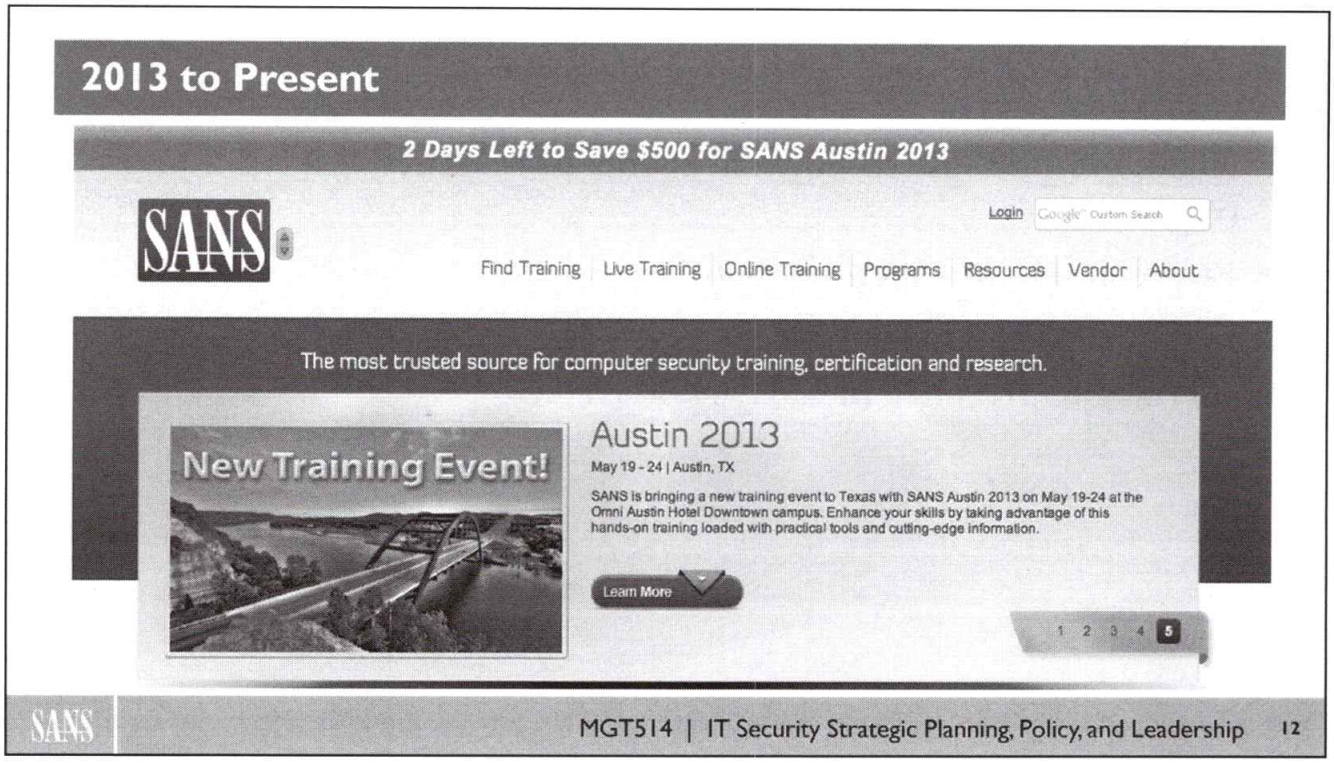
- Twelve tracks plus one-day courses
- GIAC formed
- Six-day courses
- Additional international events (London, Sydney, Ottawa, and Singapore)
- SANS Forum, an early blog that allows user comments, was introduced

2007

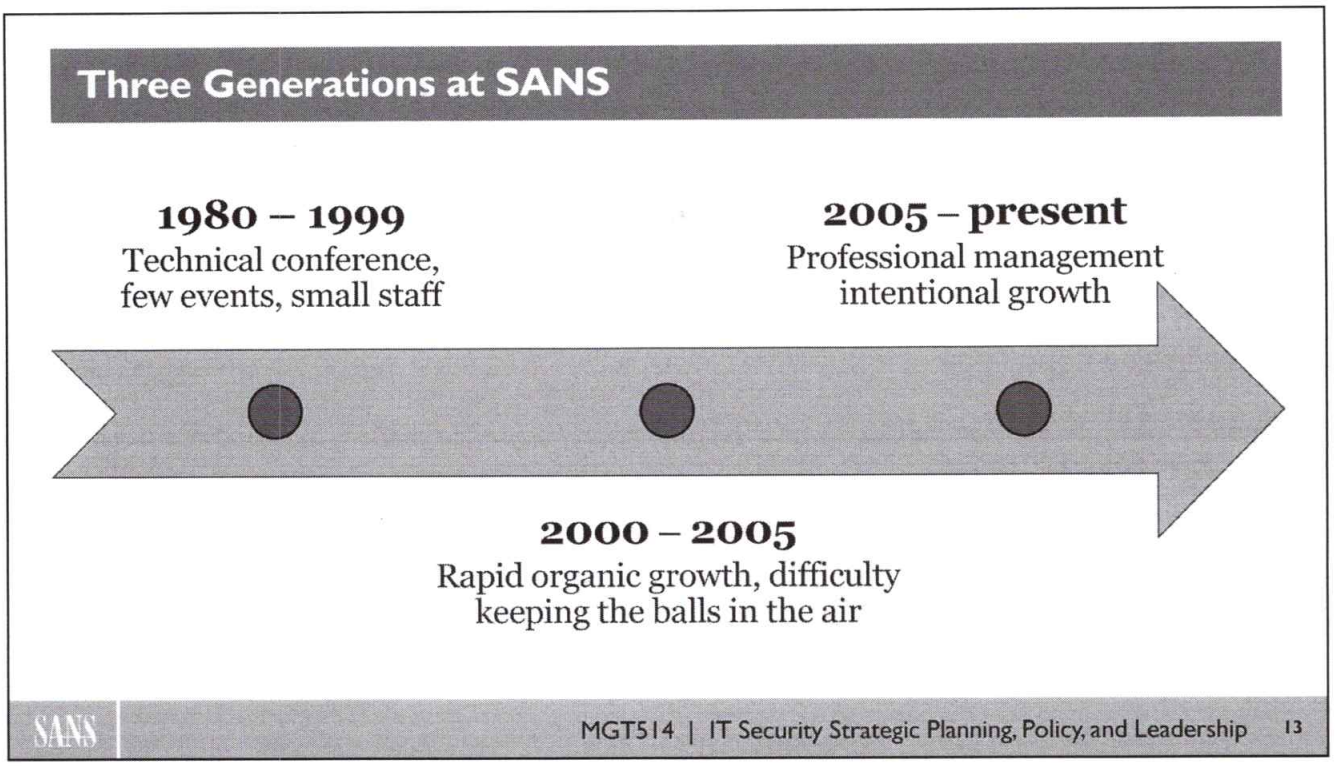
- No longer possible to show all events or resources on the home page
- Professional management team
- Growth beyond live events
- Increasing presence in EMEA and APAC

By 2007, it was no longer possible to show all events on the home page. International events also required different landing pages for areas like EMEA and APAC.

- Community SANS (one or two tracks) growing rapidly
- OnDemand growing and modernizing
- Strong growth in Europe
- The shelf space problem: too much courseware; some had to be retired



By 2013, there was no attempt to present all the information, and the products started to branch out.



SANS has endured two complete "makeovers." Essentially nothing remained from generation 1 to generation 2 programmatically, but many cultural things remained, such as the use of quotes in marketing, the idea of consensus research, and the idea of the gift economy. If you have great free things on your website, the things that must be paid for must be wonderful.

Generation 3 of SANS has a strong, professional management team. There is strategic planning to select opportunities, develop a plan that is measurable, and go after the opportunity.

IBM – A Century of Innovation

- 1911: Three tabulating machine companies merged
- 1914: Thomas Watson Jr. joined company
- 1940: Mark I calculator
- 1964: IBM 360
- 1971: The floppy disk
- 1981: The IBM PC
- 1985: Token ring
- 1993: CEO Gerstner focuses company on consulting
- 1997: Deep Blue
- 2003: zSeries 990, fastest server in the world
- 2005: Z9 mainframe, 13th consecutive year leading patent grantee in the world

IBM is one of the most amazing companies in the history of business. It started as a merger of mechanical tabulating machines. It was there with the first computer, the Mark I. When we get to 1960, it took the lead with mainframes and the IBM 360, and for years, it was the mainframe company. Then, of course, the IBM PC came along and that defined the company for a short period of time, but the competition was intense, margins were tight, and in the 1990s, it moved its focus to services while continuing to make some of the most widely used mainframes in the world.

IBM Strategic Planning – PC

- Change or die
  - World was moving from terminal and mainframe to client/server
- How do you go from a mainframe company to a PC company?
  - What is the roadmap?
- What does this mean to the workforce?
  - Do mainframe skills translate to the PC focus of the company?

We could debate whether there are five major phases at IBM or four (or even six), but the key thing to focus on is that it had a lot of very smart people, great leadership, and the ability to adapt to radical change. In strategic planning sessions, you can almost hear what was said. Environmental forces were acting on IBM. It was a change or die situation; the world was moving from terminal and mainframe to client-server.

How do you go from a mainframe company to a PC company? What is the roadmap? What are the big obstacles? What does this mean to the workforce? Do mainframe skills translate to the PC focus of the company?

IBM Strategic Planning – Services

- The competition for PCs was too high
  - Dell and HP/Compaq were taking market share, and margins were slim
- How do you go from a mainframe/PC company to a services company?
  - What is the roadmap?
  - What are the priorities?

Again, you can almost hear what had to be said in the boardroom, "The margins for PCs are just too small for the company to prosper. We need to take a different path. We think we need to transition the company to a services model. What are the major steps to do that?"

Phases of Computing

Era	Dates (approximate)	Computers (approximate)	Users (approximate)
Mainframe	1950-1965	~100,000	Millions
Mini-computing	1965-1980	~10M	Tens of millions
PC & Client/Server	1980-1995	~100M	Hundreds of millions
Internet	1995-2007	~1B	Billions
Mobile	2007-present	Billions	Billions
Internet of Things (IoT)	Present-?	Tens of billions	Billions

IBM as a company largely parallels the history of computing. In the mainframe era, the cost of computing was high. Only large enterprises could afford the investment, which limited the number of computers and corresponding users. With the mini-computer, costs decreased and more companies could invest in computing resources. However, it wasn't until the PC era ushered in by IBM and Microsoft that the cost of computing decreased enough to reach larger numbers of users. Now everyone could have a PC on his desk and eventually have access to the Internet. With the introduction of mobile devices, computing access has now increased to billions of people. It is estimated that there will soon be almost as many smartphones as there are literate adults in the world. With the Internet of Things (IoT), there is an opportunity to connect even more devices.

Looking back in time, the height of each phase of computing lasted approximately 15 years. Certainly, the older technologies still persist. Mainframes are still widely used today. But, each wave of computing allowed technology to reach more and more people. Recently, starting with the Internet era, the length of time between new technologies seems to be shortening. With the Internet era starting in roughly 1995, it was overtaken by the Mobile era starting in 2007. Has the Internet of Things already started its rise?

The table is based on a Computer World article.[1]

Reference

[1] http://www.computerworld.com/article/2475696/it-transformation/smac-and-the-evolution-of-it.html

Security History

- 1972: Buffer overflow first described
- 1988: Morris Worm exploits buffer overflow
- 1996: Step-by-step guide for exploiting buffer overflow
  - "Smashing the Stack for Fun and Profit" by Aleph One
- 1998: SQL Injection described
  - Article by Rain Forest Puppy in *Phrack* magazine
- 2005: Samy MySpace Worm
- 2006: XSS goes mainstream
  - "Hacking Intranet Websites from the Outside" by Jeremiah Grossman
- 2010: Stuxnet discovered
  - "The World's First Digital Weapon"

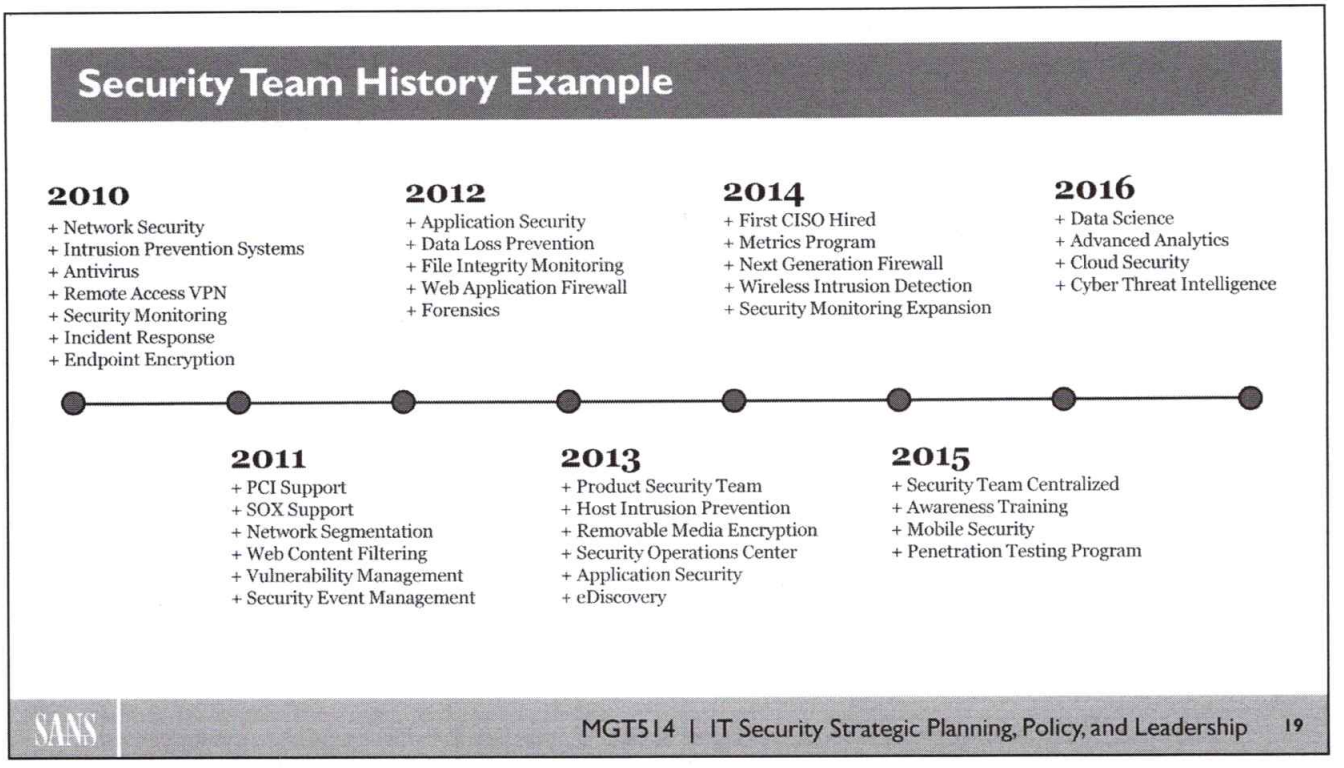
The history of security closely maps to the various phases of computing. The buffer overflow vulnerability was first described in 1972.[1] However, it wasn't until 1988, in the middle of the PC era, that the first large-scale exploit of a buffer overflow occurred. This was the Morris Worm created by Robert Tappan Morris who was a graduate student at Cornell University. It exploited known vulnerabilities in UNIX services, including sendmail, finger, and rsh/exec, and it was the first work to gain significant media attention. *The Cuckoo's Egg*[2] by Cliff Stoll also described the author's efforts at combating the worm. Buffer overflow vulnerabilities still plague many systems today. This is partly due to Aleph One's 1996 paper entitled "Smashing the Stack for Fun and Profit," which provided step-by-step instructions for exploiting buffer overflows.[3]

As the web rose in prominence, so did web application security vulnerabilities. In 1998, Rain Forest Puppy described SQL Injection in *Phrack* magazine.[4] It is still one of the most impactful vulnerabilities that you can have in your application because it allows an attacker to potentially execute any database command. In 2005, Samy Kamkar created the Samy MySpace Worm,[5] which was the first Cross-Site Scripting (XSS) worm. Just one year later in 2006, Jeremiah Grossman gave a talk at BlackHat called "Hacking Intranet Websites from the Outside."[6] This talk helped take knowledge about XSS mainstream and resulted in increased focus on web application security issues.

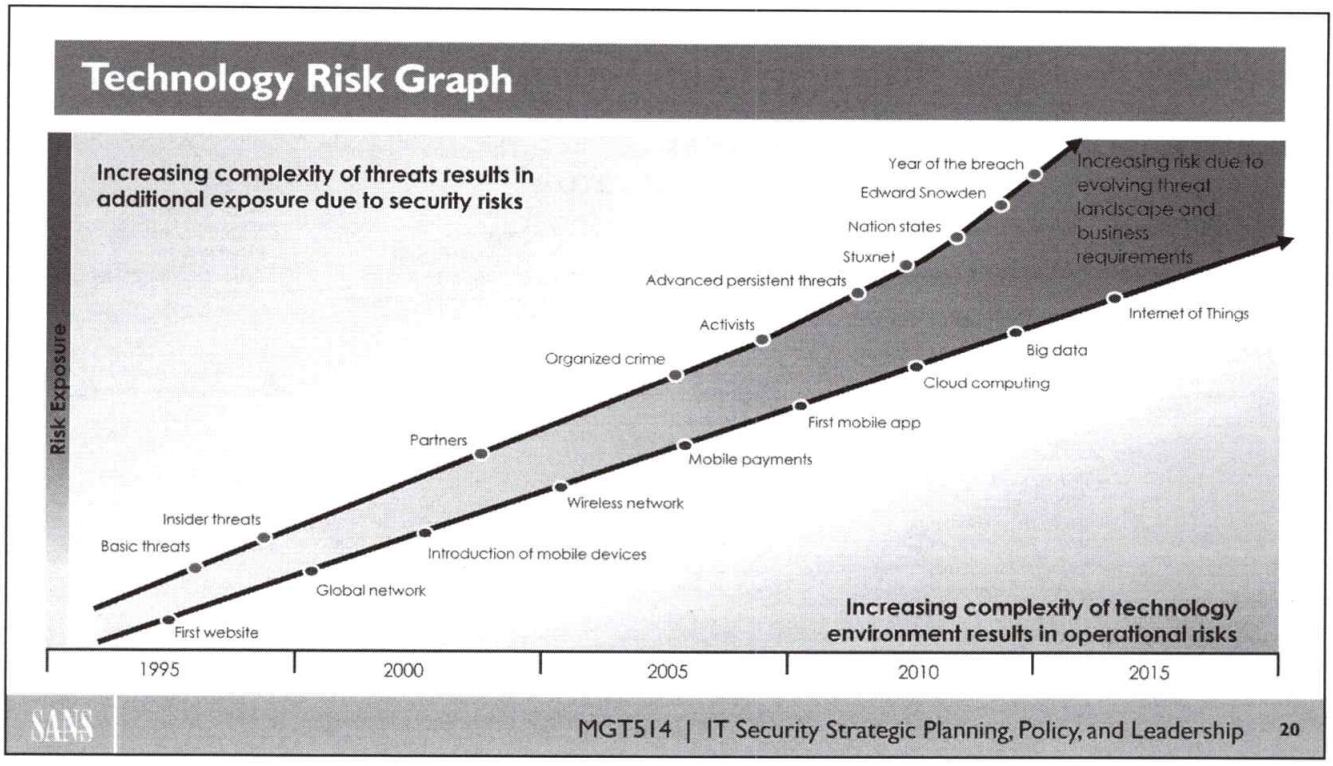
The Internet of Things (IoT) is about connecting increasing numbers of physical objects such as cars, homes, thermostats, and even people to the Internet. The Stuxnet Worm[7] showed how security issues could have huge impact on connected devices. By targeting the Siemens Programmable Logic Controllers (PLC) used in Iranian nuclear facilities, the Stuxnet Worm changed the speed at which centrifuges used to process nuclear materials would spin. This resulted in damage to the nuclear facilities and a delay in Iran's nuclear capabilities.

References

[1] http://csrc.nist.gov/publications/history/ande72.pdf
[2] http://en.wikipedia.org/wiki/The_Cuckoo's_Egg
[3] http://phrack.org/issues/49/14.html
[4] http://phrack.org/issues/54/8.html
[5] http://namb.la/popular/tech.html
[6] https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grossman.pdf
[7] http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/



Just as it's useful to track the history of your company or industry, it is also useful to track the history of your security team. This example shows how the security team improved capabilities over years by focusing on network, host, compliance, incident response, application security, data security, mobile, and many other capabilities. If your team has undertaken major initiatives or projects it is useful to create a timeline like this to remind management of all the work that has been done and celebrate the team for their accomplishments to date.



This graph shows another way that you can visually represent the history of your organization. The lower part of the graph represents the evolution of technology that is used in your company to support various business initiatives. This example has been made generic to include things like "First website," "First mobile app," and "Cloud computing." For your company, you can put even more specific items and systems. This highlights the fact that, over time, the company makes increasing investments in technology to support business goals. This increasing complexity of the technology environment results in increased operational risks. These technology investments coupled with the increasing complexity of the threat landscape as shown in the upper part of the graph result in increasing risk that the organization has to choose how to handle.

In Summary

- Business leaders
  - Understand the history of the organization
  - Where it's been and where it's going
- Security team must:
  - Frame our work within the larger business and technology context
  - Highlight the accomplishments of the team
- Allows us to better:
  - Communicate with business leaders
  - Understand the probable future
  - Align security team activities to business goals

By understanding the history of your industry, company, and department, you can better understand where you've been and where you might want to go. Framing the work or the security team within these larger contexts allows us to better communicate with business leaders. By framing the conversation around risk associated with various business decisions, we can better align security activities with business goals.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - *Values & Culture*
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

Values and Culture

- Learn about core values to:
  - Better understand the culture of your organization
  - Establish acceptable working norms
  - Align security to corporate culture

"Culture eats strategy for breakfast."
- Peter Drucker

The quote, "Culture eats strategy for breakfast," is attributed to famed management guru Peter Drucker. On one hand, it can refer to the fact that a winning culture, one focused on teamwork and delivery, can accomplish anything. On the other hand, it can refer to the fact that every organization has a certain way of doing things and, if you don't conform to those working norms, the culture will eat you alive. As a leader and manager, you have to understand the culture of your organization so that you can establish acceptable working norms. By aligning security to the corporate culture, you can position your team for success.

Purpose of a Value Statement

- Values
  - Help you understand the culture of your org
  - Critical to current state analysis
  - Guiding principles to help you achieve your vision
  - Foundation of organizational culture
- Why are values important for strategic planning?
  - Establish stability and long-term continuity
  - Provide guidance for appropriate employee behavior
  - Describe "how" the work will get done
- Let's look at some value statements
  - Discuss how they help us understand the norms of the org

Organizations are living organisms and, like individuals, they have a personality and organizational culture that are unique. A large part of being a successful executive is understanding your people, and then using that knowledge to build both high-performance teams and superior working relationships. Organizational culture and personality are built on a foundation of values that define the organization.

To establish this understanding and then get people to buy into the fact that you have their best interest at heart while still accomplishing the organizational mission require the executive to demonstrate the values of trust and integrity each and every minute of each and every day. Values must be shown by example and driven top down in alignment with overall corporate direction.

You can also encourage employees to create a personal value statement aligning with the departmental and corporate values. This might add more meaning to the company's value statement for the employee.

Employees will pay more attention to what you *do* instead of what you *say*. Executives must "walk the talk." Too often in the business environment, managers will say the right thing, and then turn around and by their actions demonstrate that they didn't mean what they said. This type of behavior will lead to an environment that lacks trust, and it shows employees the manager is lacking in integrity. Employees can often put up with a lack of competence in some areas, a lack of time management skills, etc., but very few will put up with a lack of trust and integrity for an extended period of time.

Some researchers go as far as to say that in regards to integrity and trust "this competency is…an entry ticket to leadership effectiveness" (Garman, 2006).

Initially designing organizational values is important, but it is just as important for senior management to show—preferably by example—that it embraces and lives the values that have been determined to be of importance to the organization. It is not sufficient to establish values and a value statement, and then take a look at it only every couple of years in order to dust it off and say, "Hey, look what we have." The established organizational values, as defined in the value statement, must be lived by all employees each and every day.

The consumer product giant Procter & Gamble has as one of its values that it will not provide bribes to local, state, or government officials in any country—even if that is the norm for the country in which it is trying to establish a business foot hold. This value is "lived" by every employee so there is never any confusion as to what the right thing to do is when establishing a factory in a third-world country. Conversely, Enron had a fantastic value statement and the results speak for themselves. Enron management clearly did not "walk the talk."

In too many cases in organizations, cynicism and hypocrisy abound among the leadership elite in regards to how well they adopt and embrace organizational values (Urbany, 2005).

The SEC, in its final definition of "Code of Ethics," states, "We continue to believe that ethics codes do, and should, vary from company to company and that decisions as to the specific provisions of the code, compliance procedures, and disciplinary measures for ethical breaches are best left for the company. We strongly encourage companies to adopt codes that are broader and more comprehensive than necessary" (Allen, 2005).

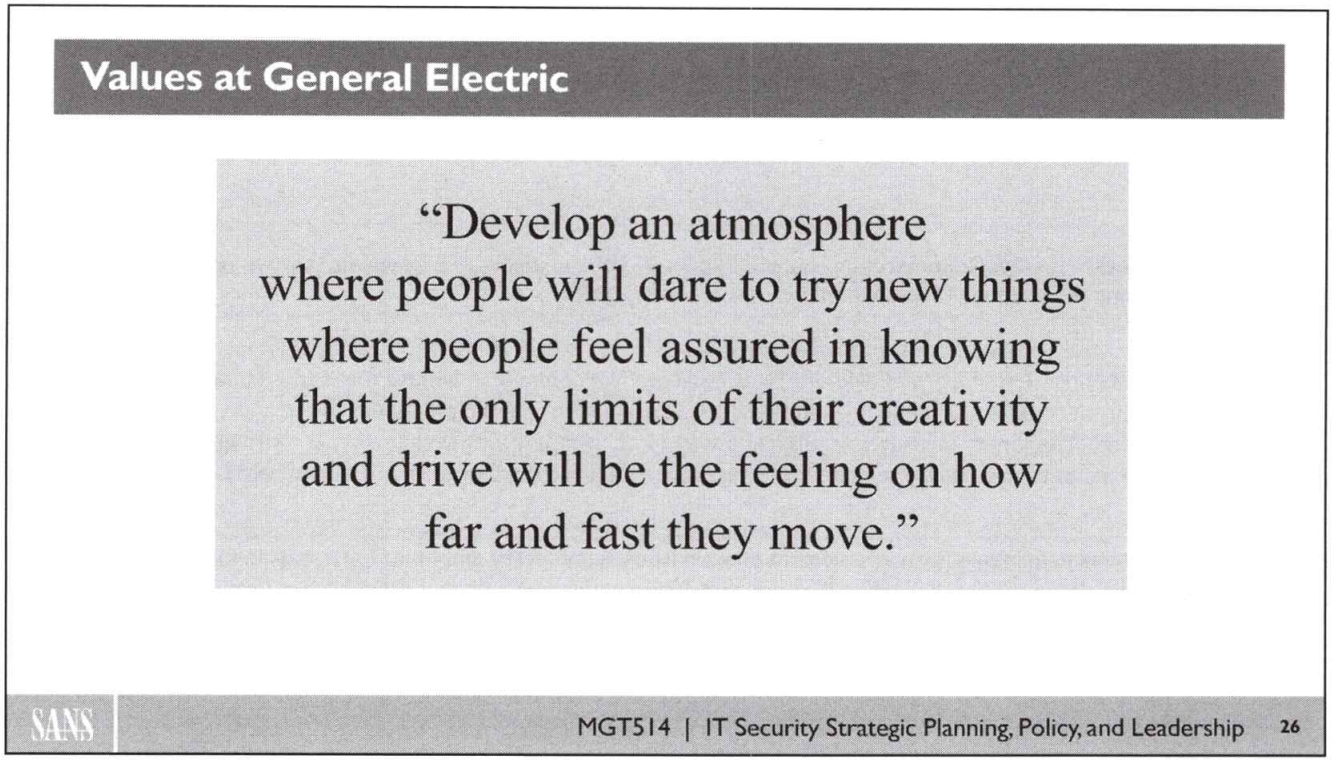
The primary reason to create a value statement is to assist each and every employee in regards to knowing how to act and what decisions to make when they are confronted with a question that requires clarification. For example, I need to build this factory in China and the local mayor is asking for a $10,000 contract kick-back. Is this okay for me to do? What if the employee of a competitor calls me and wants to sell me its new secret product formula? Can I buy it and use it to improve our competitive advantage?

It is vital to an organization that the executives believe in and promote the value statement as a core part of the organization's ethical culture. They must ensure the organization applies resources to provide employee training on the key concepts covered by the value statement and communicate expectations about adhering to these values in all situations.

Consider the famous quote attributed to Machiavelli, "The end justifies the means." Do we want to live like that and work in an organization that thinks like that? Probably not. Value statements balance the mission and vision. We define what we want to achieve and how we want to act in pursuit of those achievements. Both are important.

Reference

http://www.businessdictionary.com/definition/value-statement.html



Jack Welch, of General Electric, made this value statement, and then went on to make internal changes showing that he was serious about having this value embraced.

At GE's training center, procedures on what made a good senior manager had been enshrined in Blue Books. When Welch made his new value statement on creativity, he then had a symbolic Blue Book burning ceremony. This was his way of saying that the old values were not enough and that new values were needed.

In a culture such as this that values innovation, the security team cannot be seen as the team that blocks creativity. In fact, security can thrive in this environment by pushing the envelope on security capabilities and enhancing product security features.

Reference

http://www.ge.com/annual01/values/

Values at Disney

"The Walt Disney Company has entertained and delighted families around the world with extraordinary experiences that expand the limits of imagination and set a new standard of excellence for family entertainment…We believe that doing the right thing for families is the right thing for our business."

Walt Disney spent his life pursuing the idea of clean, wholesome family entertainment. Gord Hotchkiss writes, "The normally affable Walt could quickly become contentious when his values came into debate. He drove the overall moral tone of Disney entertainment with an iron will. The door was open for technical and creative innovation, but heaven help the poor Disney employee who let their moral guard slip, even for an instant."[1]

Disney's values of innovation, quality, community, storytelling, optimism, and decency support the statement, "doing the right thing for families is the right thing for our business."[2]

"At Disney, leadership is not defined by your title—it's defined by your actions."[3]

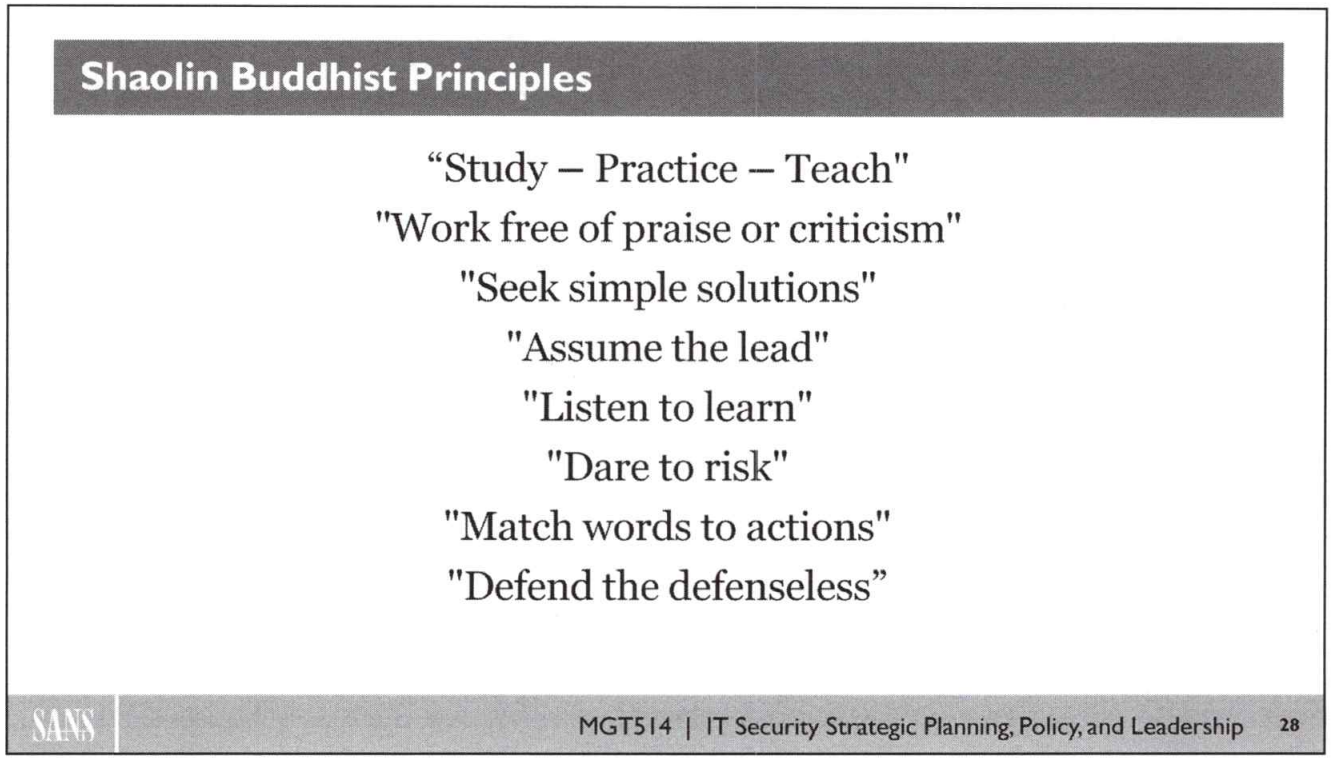
This means that information security at Disney security can succeed by providing a safe environment for families and actors while taking a "do-the-right-thing" approach.

References

[1] http://outofmygord.com/2010/03/15/10-things-i-learned-from-disney-2-values-are-non-negotiable/

[2] http://thewaltdisneycompany.com/sites/default/files/reports/DisneyCitizenshipSummary_FINAL_0.pdf

[3] https://stacycacciatore.wordpress.com/2014/12/30/the-walt-disney-company-reinforcing-culture-and-values-to-employees/



Eric Conrad, SANS author and instructor, wrote an excellent essay titled, "Waking Sleeping Dogs: Information Security Ethics,"[1] where he mentions his former boss, a fifth-degree black belt in Karate, who had a poster of the Shaolin Buddhist principles on his wall. At the time, Conrad was a security manager for a large healthcare provider and recalled analyzing complex issues through the prism of "What is best for the patients? Are we defending the defenseless?"

Quoting his essay:

"In September 2007, we were alerted to an article titled 'Officials: Man Living with Parents Had over 150,000 Child Porn Images.' At that time, the suspect, Matthew Grasso, was an employee of a member facility. HR called to discuss a possible investigation: had a crime occurred on company property? This raised ethical issues:

- Should we investigate? We had no request from law enforcement and had no indication that any crime had occurred on company property.
- If we investigated and discovered evidence of crime, what should we do?
- What if the company suffered bad press from association with a suspected criminal?

My boss and I discussed the issue. We agreed that we should investigate and turn over any evidence to law enforcement. Defend the defenseless."

Conrad's investigation revealed evidence of a crime associated with a webmail account called "grasso666" as well as a second account. He provided the evidence to law enforcement. Later, he saw a news bulletin about the arrests in Europe of eight child pornography suspects. Detective Inspector Stuart Hood "spoke to police in the U.S. about a man who used an e-mail address 'grasso666.'"

"The ethical decisions we make do not occur in a vacuum. We are connected; our decisions make waves. It's important to do the right thing not only on principle, but also because our decisions matter. They echo and reverberate."

Reference

[1] http://www.sans.edu/research/management-laboratory/article/conrad-mgt421

Values at United Parcel Service (UPS)

- Integrity
  - It is the core of who we are and all we do
- Teamwork
  - Determined people working together can accomplish anything
- Service
  - Serving the needs of our customers and communities is central to our success
- Quality and Efficiency
  - We remain constructively dissatisfied in our pursuit of excellence
- Safety
  - The well-being of our people, business partners, and the public is of utmost importance
- Sustainability
  - Long-term prosperity requires our continued commitment to environmental stewardship and social responsibility
- Innovation
  - Creativity and change are essential to growth

United Parcel Service (UPS) has many items that are commonly seen in corporate value statements. Its values are integrity, teamwork, service, quality and efficiency, safety, sustainability, and innovation.

Reference

https://pressroom.ups.com/pressroom/ContentDetailsViewer.page?ConceptType=FactSheets&id=1426321650156-161

Organizational Structure

- Values inform how to navigate in the org
- Where security is situated also informs how to navigate
  - What part does Information Security play in the organization's strategic plan?
  - Where should Information Security report to within the organization?
  - How well does it interface with HR?
- Current reporting lines
  - Advantages and disadvantages of various org structures

Does the information security strategic plan roll up into the organization's overall strategic plan? There should be some linkage. In the past, security was more tolerated than treasured. The target compromise was the watershed event. There had been many breaches before and many breaches after, but this cost the CEO and CIO their jobs. That got the corporate world's attention like no other.

But change is a process and sometimes happens slowly. Does the information security group report to a real decision maker such as the CEO, CFO, or COO, or is it buried? A whitepaper from ISC2 points out the importance of the relationship between HR and Security. In addition, a thought-provoking article from CSOonline points out that the CSO interview process gives a lot of insight into these questions.

References

https://www.isc2.org/uploadedfiles/industry_resources/hrwhitepaper.pdf

http://www.csoonline.com/article/220898/does-the-job-fit-

Tips for Creating Value Statements

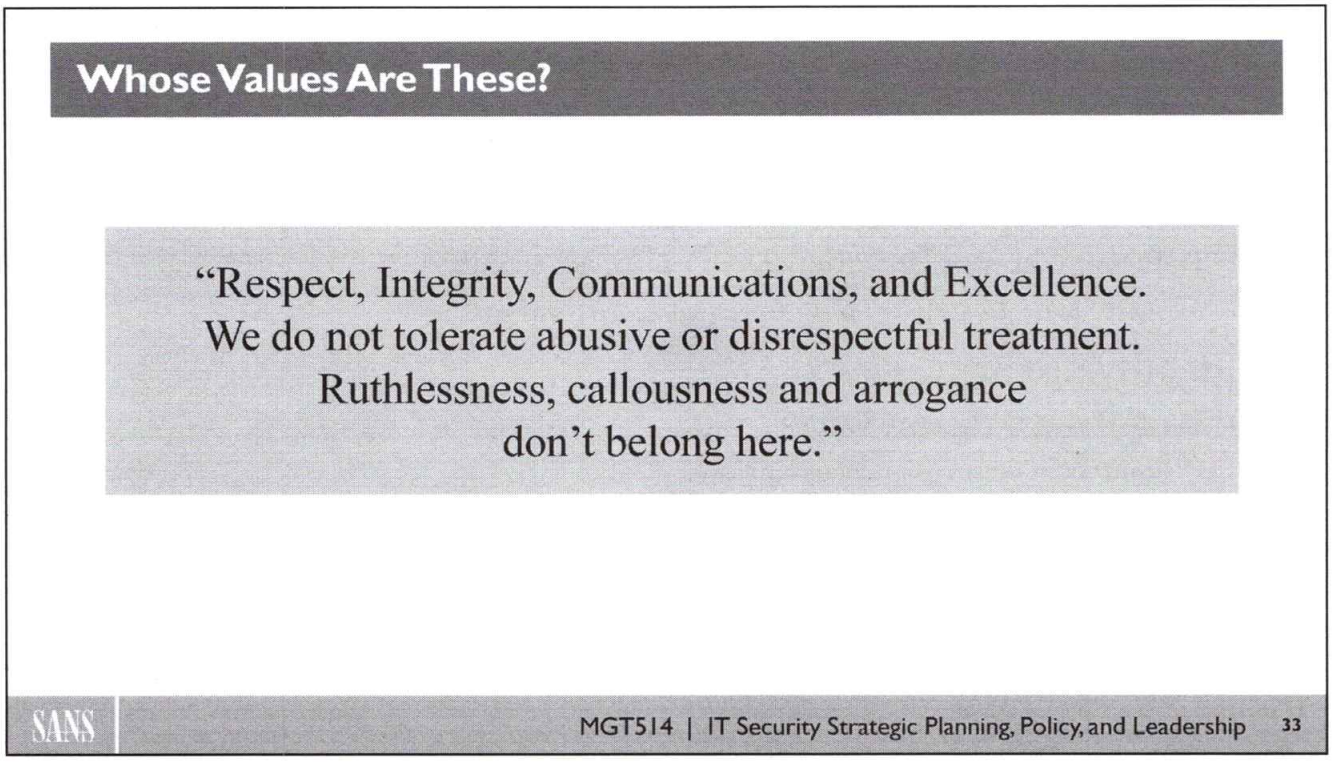
- As a manager and leader, you are expected to:
  - Understand the vision and values of the company
  - Define "how" the work of the team gets done
  - Express the "how" by the values you create and espouse
- Pick a small number of core values around which you can build the team culture and personality
  - Do they provide guidance to employees?
  - Can they be measured and prioritized?
  - Are they stable? They should not change frequently
- Security team culture must align with:
  - Values of stakeholders
  - Culture of the overall organization

As a manager and leader, you are expected to understand the vision and values of the company. These values define how the work gets done in the organization. By defining and living these core values, you create a team culture and personality that help guide employees in the work that they do.

Once you determine a core value, you need to also figure out how you are going to measure the adoption and adherence to that value. For example, if we want to be a people-oriented organization, we can measure employee turnover. Why? So we can compare retention with our peers. Can we put periodic annual checks in place to see how well we are adhering to this value? How are we going to enforce or discipline an employee who is behaving counter to this value?

Values should be stable and tied closely to the vision of the organization. The mission might change due to the changing demands of the market, and the vision might be altered based on the results of strategic planning, but the values, culture, and ethics or your organization should be long-lasting.

Security should not try to change the corporate culture. Security must align with the values and culture of key stakeholders and the overall organization.



This is Enron's value statement. It has common values like respect, integrity, communications, and excellence. However, it then specifically calls out ruthlessness, callousness, and arrogance as not being acceptable to the organization. It is very strange to have such items called out in a value statement. Maybe the leaders at Enron knew something about the culture of their organization and wanted to attention to what employees *do* instead of what they *say*.

Reference

http://www.nytimes.com/2002/01/19/opinion/enron-s-vision-and-values-things.html

Exercise 2.1 – Identifying Core Values

Estimated Time: 20 Minutes

- Goals of this exercise
  - Determine how organizational values impact security
  - Identify how security can display these core values
- Identifying core values
  - Write down three core values
    - From your current or previous employer
  - As a group discuss:
    - How this core value impacts the security team
    - How security can display this core value

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 34

The goal of this exercise is to determine how certain values impact the security team and identify what security can do to display these core values.

Using the next page as a worksheet, follow this process:

1) Write down three core values. These can be from your current or previous employer. Alternatively, you can write down a core value that you want your security team to exhibit.

2) As a group, discuss:
   - How this core value impacts the security team for better or for worse
   - How security can display this core value

Core Values Worksheet

Core value	How does this core value impact the security team?	How can security display this core value?

Use this page to write down three core values at your company.

What Values Should Your Security Department Have?

- Accountability
- Collaboration
- Customer focus
- Efficiency
- Entrepreneurial
- Ethical behavior
- Excellence
- Expertise
- Leadership
- Innovation
- Integrity
- Passion
- Professionalism
- Quality
- Reputation
- Respect
- Transparency
- Trustworthiness

No matter what the overall values of your larger company, you might want to instill a specific set of values specifically for the security team. Some example values are listed here on this slide for reference.

Exercise 2.1 – Core Values Debrief

- Core values are key to:
  - The culture of the organization
  - Establishing acceptable working norms
- Culture is very unlikely to change
  - Must determine how to adapt the security team to the culture of the org

Remember that "culture eats strategy for breakfast." In other words, culture is very unlikely to change. As a manager and leader, you must determine how to adapt the security team to the culture of the larger organization so that it can be successful. This is done by understanding the values of the larger organization and establishing acceptable working norms. This helps guide the team and provides guidelines for *how* the work should get done.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - *SWOT Analysis*
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

SWOT Analysis

- Goals of this section
  - Understand how SWOT analysis is used as part of the strategic planning process
  - Learn how to do a SWOT analysis

When examining the potential for your strategy or your security initiatives, a SWOT analysis can help you determine the likely risks and rewards. As such, the goals of this section are to provide you with an understanding of how SWOT analysis is used as part of the strategic planning process and how to complete a SWOT analysis.

What Is SWOT Analysis?

- A structured discovery and planning tool used:
  - To evaluate strengths, weaknesses, opportunities, and threats
  - For your business initiatives, teams, and/or individuals
- SWOT stands for:
  - **S**trengths
    - Favorable characteristics of the business that are working well
    - These will work to your advantage
  - **W**eaknesses
    - Unfavorable conditions of the business that put you at a disadvantage
    - These should be mitigated as soon as possible
  - **O**pportunities
    - External situations that the organization might leverage to its advantage
  - **T**hreats
    - External factors that might be potential sources of failure

SWOT analysis is a structured discovery and planning tool that is useful in helping you understand your **s**trengths and **w**eaknesses, identify both the opportunities that are open to you, and identify the **t**hreats that you face. This tool can be used for your business initiatives, teams, and/or individuals.

SWOT analysis can be used in a number of decision-making situations. As an example, when used in the business initiative context, it helps you to understand and maintain your niche in your particular market. Used in the team context, it helps you understand how to strengthen and manage high-performing teams. Used in the individual context, it can help identify talent, abilities, and develop career paths. SWOT can also be used in pre-incident/crisis planning and preventive incident/crisis management or used in creating a recommendation during a viability study.

The acronym SWOT stands for:

- **Strengths**: Favorable characteristic of your business that are working well and you can use to your advantage. These are generally internal to your organization.
- **Weaknesses**: Unfavorable conditions of the business that put you at a disadvantage or detract from your ability to achieve your desired goal. These should be mitigated as soon as possible.
- **Opportunities**: External situations that your organization might leverage or propel to your advantage.
- **Threats**: External factors that might be potential sources of failure, place the group's mission or operation at risk, and should be managed or eliminated as soon as possible through contingency planning.

The origins of the SWOT analysis are generally credited to Albert Humphrey, who led a convention at the Stanford Research Institute in the 1960s and 1970s using data from Fortune 500 companies. Humphrey himself does not claim the creation of SWOT, and the origins remain somewhat obscure.

Like PEST and Porter's Five Forces, over the course of time, many variants have been created. Heinz Weihrich, author, management consultant, and a professor of global management and behavioral science at the University of San Francisco, introduced the TOWS Matrix, a conceptual framework that aids in finding the most efficient actions. Weihrich claimed that some users found it difficult to translate the results of the SWOT analysis into meaningful actions that could be adopted within the wider corporate strategy. Comparative SWOT analysis is another variant that facilitates the groups and comparison of competing SWOT analysis such as different projects and/or markets. Finally, there is a SWOT landscape analysis that systematically deploys the relationship between the overall objective and underlying SWOT factors and provides an interactive query-able 3D landscape.

Setting aside the variations of SWOT, the framework you will learn in this section is the most widely recognized and utilized SWOT analysis framework. SWOT should be used as a complimentary tool to PEST and Porter's Five Forces in developing your strategy.

References

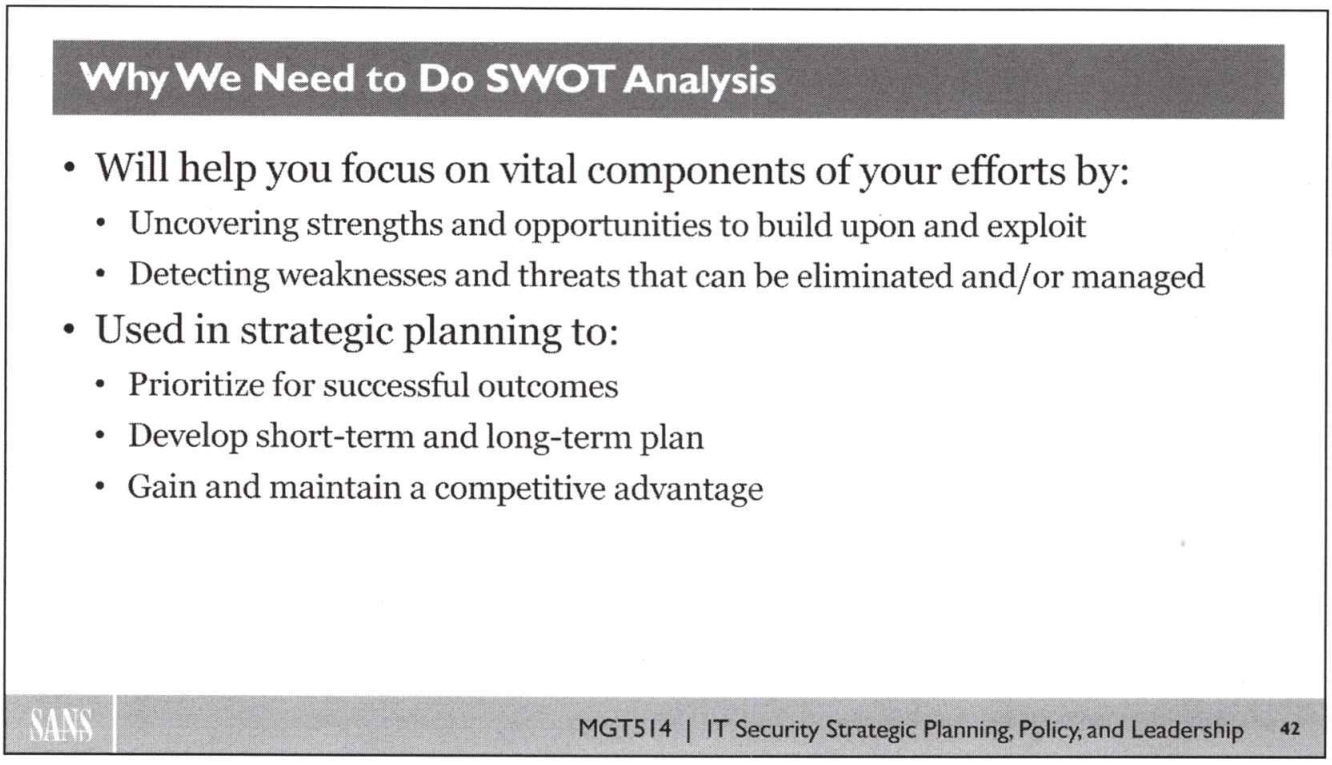
https://en.wikipedia.org/wiki/SWOT_analysis

https://en.wikipedia.org/wiki/Heinz_Weihrich

https://en.wikipedia.org/wiki/Albert_S._Humphrey

http://www.businessnewsdaily.com/4245-swot-analysis.html

http://www.mindtools.com/pages/article/newTMC_05.htm



SWOT analysis highlights the areas in which major strengths and weaknesses are evident. It also highlights opportunities that you may be well positioned to exploit and threats that you would want to manage and eliminate over time. In addition, by looking at yourself and your competitors using the SWOT tool, you can further refine and focus your strategy on vital components that distinguish you from your competitors with a greater likelihood of success.

The SWOT analysis framework is beneficial in so many ways. It can help set objectives by defining what your organization is going to do. It can help you with an environmental scan so you better understand how you are positioned in your particular industry. It can help you see what changes you need to make in your current operations or existing strategies. SWOT analysis helps organizations decide whether or not an objective is obtainable or in exploring avenues for new initiatives. It can also be used as a monitoring mechanism for an initiative underway to determine whether refinement or redirection efforts are needed.

In summary, identification of the SWOT elements is important because it can determine vital steps that should be included in planning to achieve the desired outcome.

References

http://www.washington.edu/research/rapid/resources/toolsTemplates/SWOT_analysis.pdf

http://www.businessnewsdaily.com/4245-swot-analysis.html

SWOT Analysis

- Strengths and Weaknesses are often internal to your org
- Opportunities and Threats are generally external factors

	Helpful	Harmful
Internal	**Strengths**	**Weaknesses**
External	**Opportunities**	**Threats**

Strengths and weaknesses are often internal to your organization, whereas opportunities and threats generally relate to external factors. For this reason, the SWOT analysis is sometimes called "Internal-External (IE) analysis," and the SWOT Matrix is sometimes called the "IE Matrix." It's probably obvious but still worth stating that strengths and opportunities are helpful, whereas weaknesses and threats are harmful.

Strengths are favorable characteristics of your business that are working well and you can use to your advantage. These are internal to your organization. You'll want to consider your strengths from an internal perspective, also from the point of view of your customers, and others in the marketplace as well as your competitors. Think about your strengths in relation to your competitors. For example, if all of your competitors provide high-quality products, and high-quality production processes are not a strength in your organization, it might be a necessity to compete in that specific market.

Weaknesses are unfavorable conditions of the business that put you at a disadvantage or detract from your ability to achieve your desired goal. These should be mitigated as soon as possible. Although this is often internal to your organization, you'll also want to consider looking at this from the eyes of external people as well. For example, do other people outside your organization seem to perceive weaknesses that you possibly don't see, or are your competitors doing better than you? It's best to be brutally honest and realistic in this section and face the unpleasant truths so you have the opportunity to do something about them.

Opportunities are external situations that your organization may leverage or propel to your advantage. Useful opportunities can come from such things as changes in technology and markets on both a broad and narrow scale, or changes in government policy related to your field, changes in social patterns, population profiles, and lifestyles and local events. A useful approach when looking at your opportunities is to look at your strengths and weaknesses and ask yourself whether they open up any opportunities if you leverage your strengths or eliminate threats.

Threats are external factors that might be potential sources of failure or place the group's mission or operation at risk and should be managed or eliminated as soon as possible through contingency planning. You might also want to look at your strengths and weaknesses to determine the threat of successes turning into weaknesses and weaknesses turning into real threats.

References

https://en.wikipedia.org/wiki/SWOT_analysis

http://www.washington.edu/research/rapid/resources/toolsTemplates/SWOT_analysis.pdf

http://www.businessnewsdaily.com/4245-swot-analysis.html

http://www.mindtools.com/pages/article/newTMC_05.htm

PharmaCo Case Scenario

- Cheryl Miller was recently hired as Director of Security Strategy
  - Asked by her boss, the CIO, to create a plan for improving security
    - This includes security operations, threat intelligence, security monitoring, incident response, and anything else she uncovers that needs improvement
- PharmaCo is a large pharmaceutical company
  - Created breakthrough drugs that have helped millions of people lead longer, healthier lives
  - $25 billion in revenue, 70,000 employees around the world
  - Increasing competition—pressure to create new drugs
  - Decentralized operations—including security
  - Recent evidence of intrusions—leaked documents containing sensitive product development plans

Your friend, Cheryl Miller, works for a large pharmaceutical company, PharmaCo. She was recently hired as Director of Security Strategy and has been asked by her boss, the CIO, to create a plan to improve the effectiveness of the organization's security operations. This includes threat intelligence, security monitoring, incident response, and anything else she uncovers that needs improvement. At your monthly dinner, she expresses that she's having a hard time understanding the organization and how to structure her approach to deliver what the CIO has asked for. Cheryl looks to you for guidance and counsel on how she can get her arms around the enormity of this task, and prioritize efforts for an improvement plan.

PharmaCo is a large multinational organization with $25 billion in annual revenue, 70,000 employees, and offices across six continents. At the heart of PharmaCo's culture is a heavy focus on innovation and R&D. In fact, it has created breakthrough drugs for the treatment of cancer and has helped millions of people lead longer, healthier lives. Due to its success, competitors are constantly looking to take market share. There is increasing pressure to speed up the creation of new drugs in the face of this competition and increasingly difficult regulatory environment. At PharmaCo, each individual business unit runs its own research & development and operations functions. As a result, security is currently decentralized across business units. Historically, this has not posed a problem, but recently there has been evidence of intrusions. Sensitive documents about product development plans have been found in the hands of outsiders.

You can clearly see from Cheryl's conversation with you, she has a big job ahead of her, but the good news from your point of view is she has a high level understanding of her company PharmaCo, and more importantly, she has a stated objective from the CIO to create a plan to improve the effectiveness of the organization's security operations.

You explain to Cheryl that the most effective tool, in this case, is a SWOT analysis and the use of this tool should help her identify strengths, weaknesses, opportunities, and threats for the security organization and develop objectives for an improvement plan as the CIO had requested. Because Cheryl had been a participant

only in doing a SWOT analysis for a specific project, she asks you the best approach to lead this effort. You advise her that a SWOT analysis for this particular application is best developed in a group setting with a facilitator to conduct the meeting. You recommend that she pull together key players in the operations, threat intelligence, monitoring, and incident response team and allow the participants to creatively brainstorm, identify obstacles, and strategize possible solutions to the limitations. Not only will this help her understand each of the areas of the SWOT, but it will also facilitate the buy-in and stakeholder management component for these initiatives, because the key players will in effect end up owning these improvement initiatives.

After the brainstorming activity, you'll critically examine each area and distill the content in each area into a few strategic macro issues. You advise her of the common mistakes in SWOT analysis are focusing on the micro level of details. A common mistake to be aware of and avoid is when you look internally, be aware and avoid loyalties or bias towards function that can prevent real areas of concerns from surfacing. This often presents itself as over expressing details. When looking at the external factors, team members might not want to do the work it takes to look outside your company and finally, there is also a common problem of failing to evaluate threats correctly. Opinions swing from "It won't affect us at all" to "It spells instant disaster" for the same threats, which is something you need to be mindful of.

You also recommend that if she hasn't already done a PEST, Porter's Five Forces, she should complete these as well, and you remind her of the importance of a Stakeholder Management Strategy, because it is likely that many cross-functional, cross-organizational initiatives will result from this effort, which is directly in alignment with the CIO's expectations.

Strengths

- Favorable characteristics of the business that are done right and working well
  - These will work to your advantage
- Perspectives to consider
  - Internal
  - Customers' point of view
  - Others in the marketplace
  - Competitors
- Key questions to ask
  - Does your organization have any advantages over others?
  - What do you do better than anyone else?
  - Do you have unique capabilities and/or attributes?
  - How do others in the marketplace view your strengths?
  - Do you have a unique value proposition?

As a reminder, strengths are favorable characteristics of your business that are working well and you can use to your advantage. These are internal to your organization. You'll want to consider your strengths from an internal perspective, from the point of view of your customers, others in the marketplace, and your competitors.

A good place to begin analyzing the strengths is to determine what advantages the organization has: What do you do better than anyone else, what are the unique capabilities and/or attributes you can draw on that others can't, what do other people in your market see as your strengths, and what is your unique value proposition?

Other examples for consideration internally for you are financial resources such as funding availability, sources of income and investment opportunities, physical resources (such as location, facilities, and equipment), human resource elements (such as employees, volunteers, and target audiences), and the role of key staff members. Access to natural resources, trademarks, patents and copyrights, and current processes (such as employee programs, training, etc.) should also be considered. You might also want to look at departmental hierarchies and company culture and image, and don't forget to consider any technology advantage or disadvantage. You can look at operational efficiency and operational potential. These examples could also be considered for the Weakness quadrant.

If you're having difficulty identifying strengths, this is where the brainstorming and the aid of various people can come into play. Begin by writing down a list of your organization's characteristics. Some of these ideas will likely be strengths that you can build on.

References

http://www.businessnewsdaily.com/4245-swot-analysis.html

http://www.mindtools.com/pages/article/newTMC_05.htm

PharmaCo SWOT Analysis

	Helpful	Harmful
Internal	**Strengths** • Business mission to help people lead healthier lives • Culture of innovation and R&D • Ability to create breakthrough new drugs • Decentralized business units allow quick innovation • Strong geographic presence • Access to talent around the world	**Weaknesses**
External	**Opportunities**	**Threats**

Cheryl did exactly as you had recommended. She pulled a meeting together with key players from security operations, threat intelligence, monitoring, and incident response teams. There was no shortage of ideas coming out of the brainstorming session, and after some healthy discussions, the team agreed it had a good prioritized macro list of the strengths of the organization.

The team agreed that the company has many strengths, one being the business mission to help people lead healthier lives. Two additional strengths are a heavy cultural focus on innovation and research and development and the ability to create breakthrough drugs. All of these strengths are apparent and evident by the millions of people it has helped to date and by the recent breakthrough in drugs for the treatment of cancer.

The company has decentralized business units where each individual business runs its own research and development and operations. This allows for quick innovation. Finally, because this company is a large, multinational organization with offices across six continents, it has access to top talent around the world.

Weaknesses

- Unfavorable conditions of the business that put you at a disadvantage
  - It's best to be realistic in this section so you can mitigate risk as soon as possible
- Perspectives to consider
  - Internal
  - Customers' point of view
  - Others in the marketplace
  - Competitors
- Key questions to ask
  - Are there areas that others in your market would likely to see as a weakness?
  - What factors would lose credibility for you?
  - Is there anything my competitors are doing better than me?

As a reminder, weaknesses are unfavorable conditions of the business that put you at a disadvantage or detract from your ability to achieve your desired goal. These should be mitigated as soon as possible. Although this is often internal to your organization, you'll also want to consider looking at this from the eyes of external people. For example, do other people outside your organization seem to perceive weaknesses that you possibly don't see, or are your competitors doing better than you? Don't forget to be brutally honest and realistic in this section.

A good place to begin analyzing the weaknesses is to determine where you can improve, what you can avoid, what people in the market are likely to see as your weaknesses, what factors lose credibility for you, and what your competitors are doing better than you.

Weaknesses can include limited financial resources, constrained physical resources (e.g. location, facilities, and equipment), employees with the wrong skill sets, limited access to natural resources, and a weak patents library. You should also determine whether current processes are broken or non-existent, or if you have inadequate employee programs such as training. You might also want to consider whether departmental hierarchies are detrimental and cause a weakness or whether the company culture or image shows as a weakness. Don't forget to consider any technology disadvantage or any operational inefficiency and lack of operational potential, which are all starting points.

References

http://www.businessnewsdaily.com/4245-swot-analysis.html

http://www.mindtools.com/pages/article/newTMC_05.htm

PharmaCo SWOT Analysis

	Helpful	Harmful
Internal	**Strengths** • Business mission to help people lead healthier lives • Culture of innovation and R&D • Ability to create breakthrough new drugs • Decentralized business units allow quick innovation • Strong geographic presence • Access to talent around the world	**Weaknesses** • No CISO or central security responsibility • Security is decentralized and understaffed • No central threat strategy • Technology is under utilized • Slow deployment of clinical trials • Aging workforce—key thought leaders near retirement
External	**Opportunities**	**Threats**

Cheryl was a bit surprised that the weaknesses came out so easily from the team. In fact, the hard part in this section was agreeing on which handful should be listed because each of the key team members wanted his opinion included here, and at the rate they were heading, this topic could have gone on all day. In the meeting, everyone was quite brutally honest with Cheryl about the pain points, despite the fact that she was the new person on the team.

The team eventually agreed that not having a CISO or central security responsibility was one of the biggest challenges and that it could very well be the root cause as to why security is decentralized and without a threat strategy. Most importantly, each of the team members in the meeting felt his area was critically understaffed. This was obviously a passionate topic, similar to her previous company (at least there was a CISO in place at the other company, though). The team also felt like technology was underutilized not only in the security department, but also across the entire company.

A business article was recently published about the pharmaceutical industry, and one of PharmaCo's top executives was quoted about the industry challenges of slow deployment of clinical trials and the impact that has on the business mission. "The rigor of clinical trials, although necessary, slows the ability to get medicines into the hands of those people who need it most. The pharmaceutical industry must do what it takes to eliminate waste and delays in the process and get the people the right medicine at the right time."

Finally, it was well known at PharmaCo that the aging workforce was a challenge for the company. Many of the key thought leaders from across all business sectors were nearing retirement.

Cheryl also wondered to herself why security was not centralized. She was anxious to learn more.

Opportunities

- External situations that the organization can leverage or exploit to its advantage
- Perspectives to consider
  - Strengths and Weaknesses you've already documented
  - Include output of PEST analysis to ensure you haven't overlook any factors such as demographics, employment trends, etc.
- Key questions to ask
  - What interesting trends are you aware of?
  - Are there any significant changes in technology and markets?
  - What government and/or regulatory policy relate to your field?
  - How can you leverage social patterns such as population profiles, lifestyle changes, etc.?

As a reminder, opportunities are external situations which your organization may leverage or propel to your advantage. Useful opportunities can come from such things as changes in technology and markets on both a broad and narrow scale, or changes in government policy related to your field, changes in social patterns, population profiles, lifestyle changes, and local events.

A useful approach when looking at your opportunities is to look at your strengths and weaknesses and ask yourself if they open up any opportunities if you leverage your strengths or eliminate threats. You may also want to include output of your PEST analysis to ensure you haven't overlooked any factors such as demographics, employment trends etc.

External forces influence and affect every company, organization and individual whether they are directly or indirectly connected to an opportunity or threat. It's important to consider all items that were generated as a result of the brainstorming activities.

References

http://www.businessnewsdaily.com/4245-swot-analysis.html

http://www.mindtools.com/pages/article/newTMC_05.htm

PharmaCo SWOT Analysis

	Helpful	Harmful
Internal	**Strengths** • Business mission to help people lead healthier lives • Culture of innovation and R&D • Ability to create breakthrough new drugs • Decentralized business units allow quick innovation • Strong geographic presence • Access to talent around the world	**Weaknesses** • No CISO or central security responsibility • Security is decentralized and understaffed • No central threat strategy • Technology is under utilized • Slow deployment of clinical trials • Aging workforce—key thought leaders near retirement
External	**Opportunities** • Hire a CISO • Operationalize around the kill chain • Organize personnel to improve security effectiveness (combining physical & info sec) • Leverage global presence to build 24x7 team • Increase staffing levels	**Threats**

It was clear to Cheryl that the key participants she had in her brainstorming meeting were the security thought leaders. When it came to the opportunities quadrant, they wasted little time reaching an agreement on what should be included.

First and foremost, the greatest opportunity was to hire a CISO. The team felt that this role would bring clarity and cohesion to the security teams. The recent evidence of data loss where development plans were found in the hands of outsiders was a clear indication of compromise and rightly so; each and every person in that room along with all the security staff had reason to be alarmed. Based on this evidence, the team found opportunities to operationalize around the kill chain by leveraging its global presence to build a 24x7 security operations team. In addition, the team felt that the security organization needed to be re-organized and possibly centralized to improve the overall effectiveness. This included combining physical security and information security. All of these ideas lead to an opportunity to increase staff in an overall effort to minimize data loss.

Threats

- External factors that can be potential sources of failure or cause trouble for the business
- Perspectives to consider
  - Include output of PEST analysis to ensure you haven't overlooked any factors such as government regulations and technology changes
- Key questions to ask
  - What obstacles do you face?
  - What are your competitors doing?
  - Are quality standards or specifications for your job changing?
  - Is changing technology threatening your position?
  - Does your company have cash-flow problems?
  - Could any of your weaknesses seriously threaten your business?

As a reminder, threats are external factors that can be potential sources of failure or place the group's mission or operation at risk and should be managed or eliminated as soon as possible through contingency planning. For this quadrant, you might also want to include the output of your PEST analysis to ensure you haven't overlooked any critical areas such as government regulations or technology changes.

A good place to start your brainstorming for this quadrant is to look at some of the obstacles you, your organization, and your company face. You'll want to look at what your competitors are doing. If they are doing the same thing better than you, this would certainly be a threat. You'll need to determine whether quality standards and/or specifications for your job are changing. In security, this might be any new regulatory mandate for instance. You should also look at technology and answer, "Is there any threat to your position?" Although in security, that is highly unlikely. You shouldn't, however, discount looking into this question and making sure the answer is as it appears. You should also look at your company and the financial aspect for example, and answer, "Does it have cash-flow problems, and is its credit rating at risk?" And most importantly, you'd like to know whether any of your weaknesses seriously threaten your business as is the case of the development plans have been found in the hands of outsiders. We know from our Porter's Five Forces the importance of understanding competitive rivalry, and should sensitive research and development documents, or sensitive documents related to clinical trials, were to be leaked to the competitors it might be a going-out-of-business event.

PharmaCo SWOT Analysis

	Helpful	Harmful
Internal	**Strengths** • Business mission to help people lead healthier lives • Culture of innovation and R&D • Ability to create breakthrough new drugs • Decentralized business units allow quick innovation • Strong geographic presence • Access to talent around the world	**Weaknesses** • No CISO or central security responsibility • Security is decentralized and understaffed • No central threat strategy • Technology is under utilized • Slow deployment of clinical trials • Aging workforce—key thought leaders near retirement
External	**Opportunities** • Hire a CISO • Operationalize around the kill chain • Organize personnel to improve security effectiveness (combining physical & info sec) • Leverage global presence to build 24x7 team • Increase staffing levels	**Threats** • Insider threat—geographically dispersed workforce and risk of data loss • Competitors—seeking intellectual property • Nation state—seeking to accelerate R&D • Regulatory—increased regulation results in delays getting new drugs to market

At this point, Cheryl is beginning to see hope that an improvement plan can be pulled together for the CIO as requested. The team has worked diligently to complete the SWOT analysis and she feels like this is all beginning to make a lot of sense.

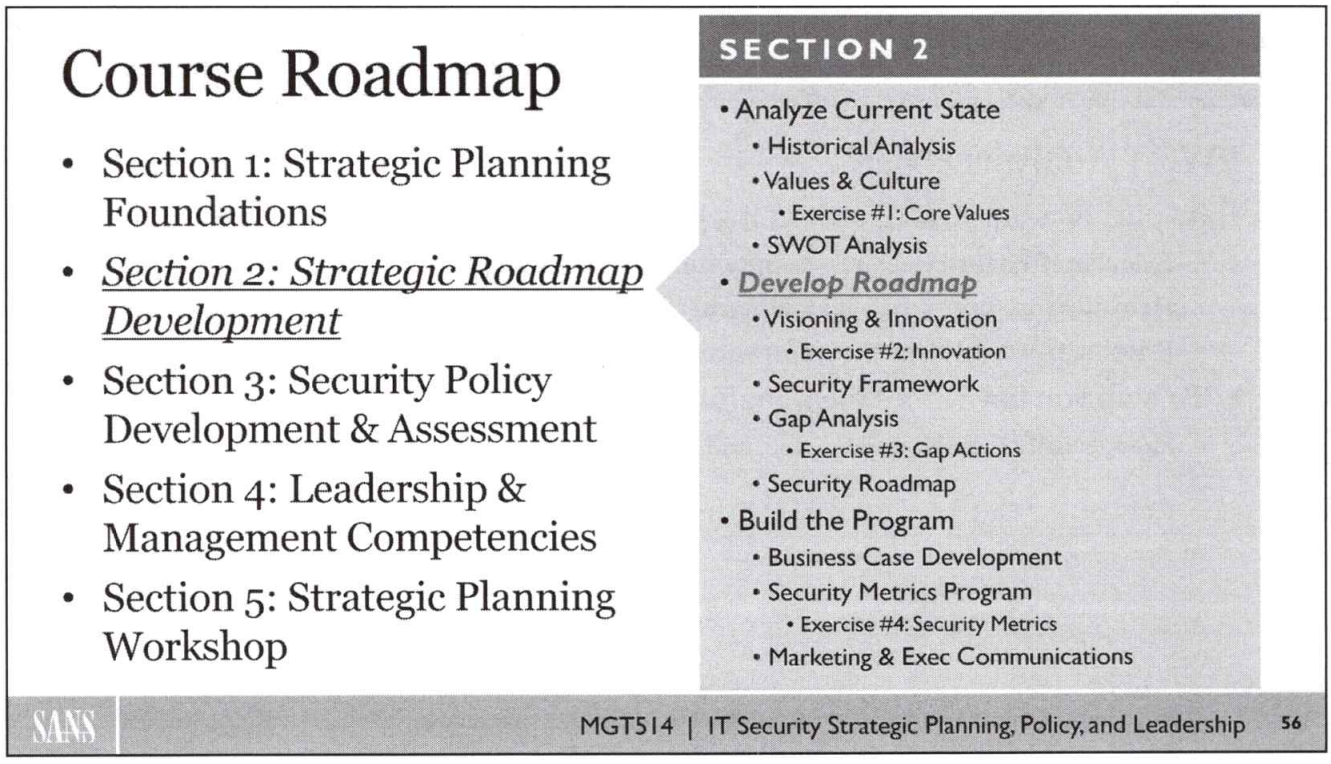
For the threats, the team once again lost no time in coming to consensus about the threats. It must be in the nature of security professionals to identify threats quickly. Insider threats and the risk of data loss is a big problem given the geographically dispersed workforce, and it's not an easy problem to solve. Competitors seeking intellectual property are also a high threat. With all the research and development that PharmaCo does, getting your hands on it would be tremendously valuable as a competitor. Nation states are also looking to accelerate their research and development efforts. PharmaCo is also concerned with the regulatory landscape, which results in delays in getting new drugs to market.

The team and Cheryl take a step back to review their SWOT analysis and find it interesting that this process and this SWOT matrix did indeed help them understand the strengths, define the weaknesses, and clearly outline opportunities the team could leverage for an improvement plan. The threats confirmed what the security team had always known, but now the team feels as though it can have a very different conversation with the CIO.

In Summary

- SWOT Analysis is used:
  - As part of a the strategic planning process
    - Evaluate strengths, weaknesses, opportunities, and threats
    - Help develop short-term and long-term plan
    - Prioritize security investments for successful outcomes
  - To help you have more meaningful dialogue with business leaders
    - How security can respond, enable, and support business goals and market trends

In summary, the SWOT analysis is a structured discovery and planning tool that is useful in helping you understand your strengths, weaknesses, opportunities, and the threats to your business initiatives, teams, and/or individuals. It should be used as part of the strategic planning process to help develop short-term and long-term plans. This will help you prioritize security investments for successful outcomes and most importantly, the results will provide you with the right information to have a more meaningful dialogue with your business leaders and illustrate to them in their terminology how security can respond, enable, and support business goals and market trends.



This page intentionally left blank.

How to Develop the Roadmap

1) Determine where you want to go
   - Create a vision that fosters innovation
2) Create a structure to follow
   - Utilize a security framework
3) Understand what it takes to reach the goal
   - Analyze your gaps
4) Create a plan
   - Develop the roadmap

Developing a roadmap for your security team or program is not just about identifying technical capabilities and tools to deploy. An effective roadmap is developed by:

1) Determining where you want to go

By defining a vision for an improved future state, you as a leader can create an environment that allows people to think in innovative new ways.

2) Creating a structure

It's not just about the grand plan or vision. Making this practical requires following a structure for the security team. This can be done by creating or utilizing a security framework.

3) Understanding what it takes to reach the goal

By understanding the current state and analyzing the resulting gaps, you can identify discrete actions that need to be taken to reach the goal.

4) Creating a plan

With the end goal, program structure, and gaps identified, you can create the roadmap for your team to follow.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - *Visioning & Innovation*
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

Visioning and Innovation

- Goals of this section
  - Incorporate visioning into strategic planning
  - Learn to innovate with the business
    - By solving their "jobs to be done"

> "If I'd asked people what they wanted, they would have said faster horses."
> - Henry Ford

Henry Ford is the famous founder of Ford Motor Company who brought affordable automobiles to the masses by pioneering the assembly line technique of mass production. In a time when automobiles were extremely expensive and reserved for the wealthy, Ford had a vision of providing inexpensive goods and high wages for workers. He was able to envision an alternate future that was not dominated by horses and carriages. This vision led to business process innovation that resulted in solving the problem of affordable and convenient transportation for millions of people around the world.

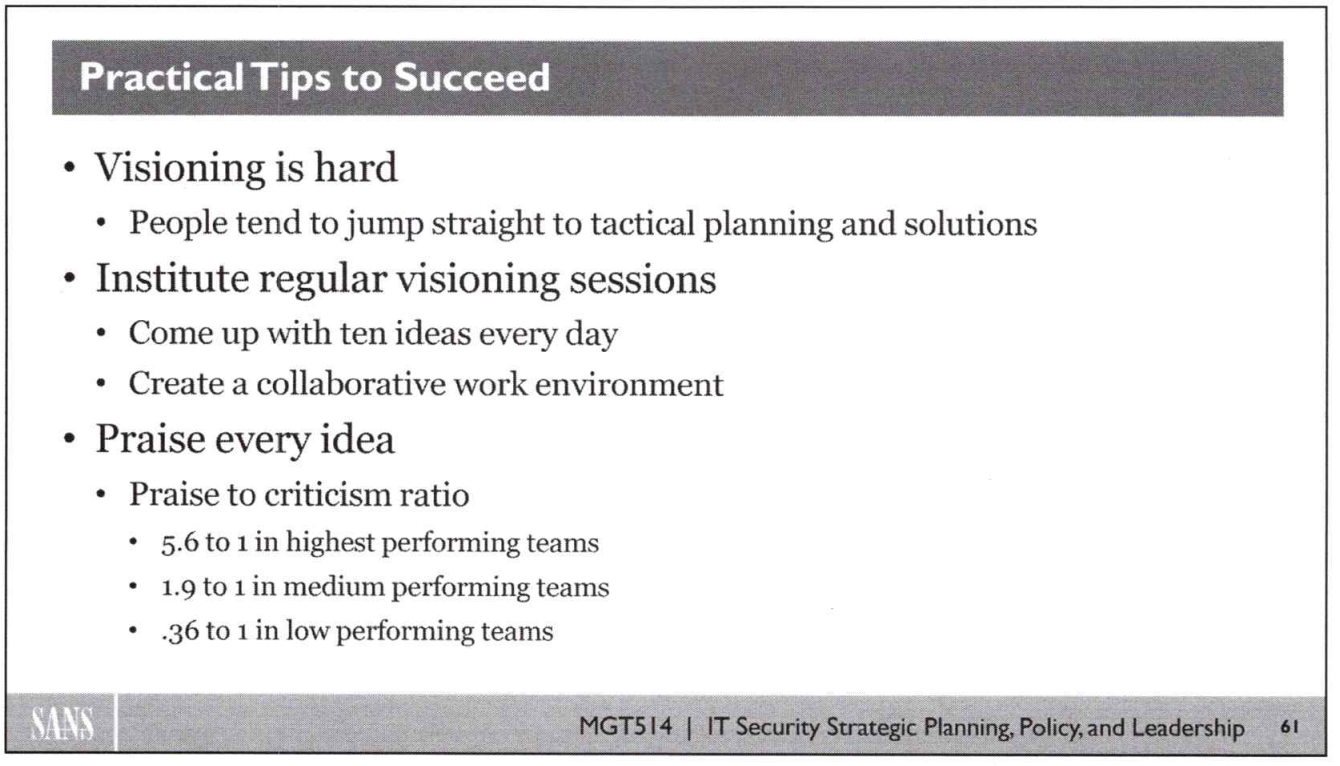
Visioning

- Process of thinking about how the world will be in the future
  - Helps "stretch" strategic planning
- Without the visioning step
  - Will likely end up producing a tactical plan instead of a strategic plan

Visioning is not the same thing as a vision statement. A vision statement is what we want to become and what we aspire to be. Visioning helps us to think about the world we are most likely to face.

Visioning, or futurism, is the process of thinking about what the world will be like 10 or even 20 years from today. It is an invaluable tool in strategic planning because it forces us to think about the unknown world. We tend to be short-term focused in security, partly because we are constantly responding to new threats. We also tend to skip doing things that are hard. What operating system and computing device will your organization use in 5 years? What about 10 years? You don't know and we do not either, but we do expect we will have operating systems and computing devices.

Skipping the visioning process is not recommended. If you do, you will almost certainly end up with a tactical plan.



Visioning is a difficult process. Just as people tend to jump straight into creating solutions when presented with a problem, people tend to jump straight into tactical planning when doing strategic planning.

Often the mind has to be trained to think in innovative ways. James Altucher is an entrepreneur and author who founded StockPickr, sold it to TheStreet.com for $10 million, and lost $15 million in two years on failed investments. This enabled him to re-evaluate his approach to business and life. He has an article titled, "The Ultimate Guide for Becoming an Idea Machine."[1] He says, "It's important to exercise the idea muscle right now. If your idea muscle atrophies, then even at your lowest point, you won't have any ideas." Among other things, he says that you should come up with ten ideas every day. Start the idea muscle working. That's it.

At work, you can institute collaborative work environments that can help with visioning and innovation—perhaps something similar to English coffee houses in the 17th and 18th century that might have contributed to The Enlightenment.[2] No matter how you create these collaborative environments, one thing is clear. You as a manager and leader should praise every idea. You probably can't say "I agree with that" or "That's a great idea" often enough. Research has shown that the highest-performing teams compliment each other up to 15 times more often than the lowest-performing teams.[3] Similar research has shown comparable results when looking at the rate of married couples getting divorced vs. staying together. This can even apply to acts of non-verbal communication such as high fives and fist bumps on sports teams.[4]

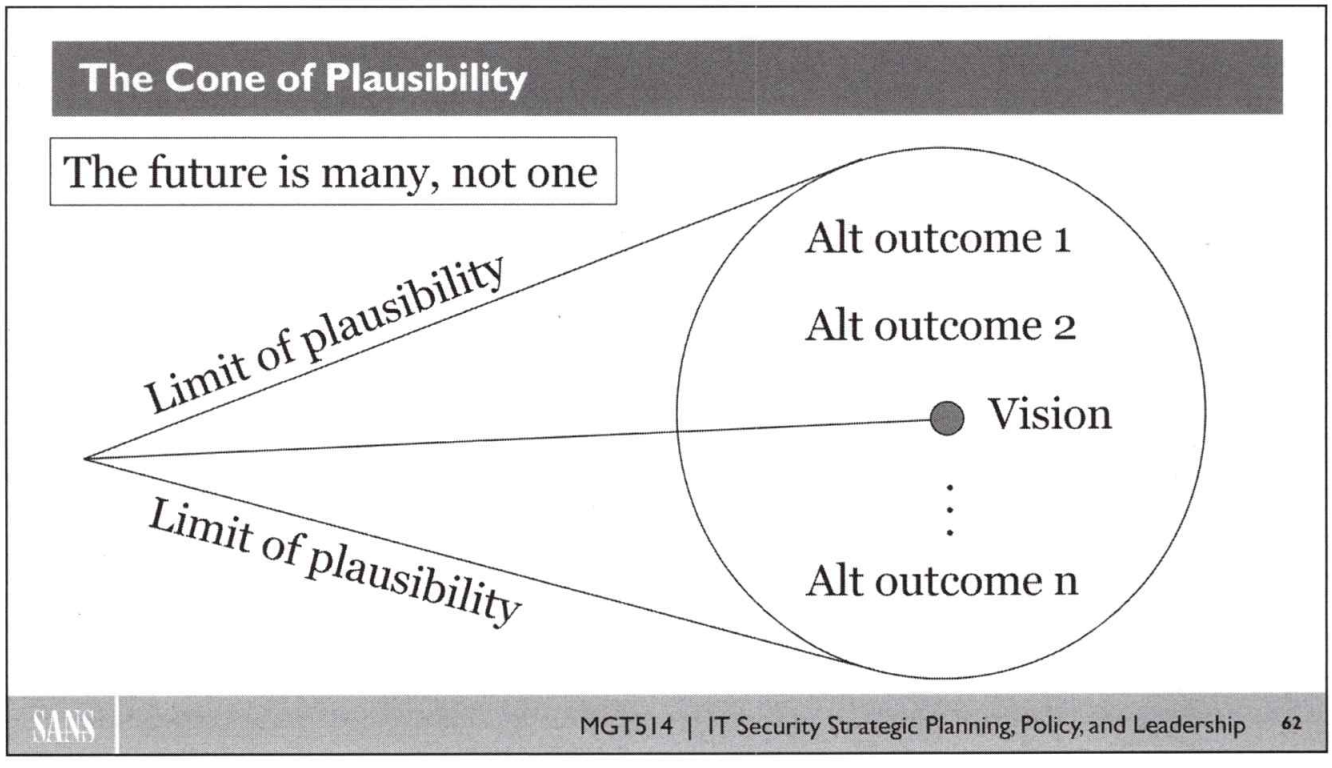
References

[1] http://www.jamesaltucher.com/2014/05/the-ultimate-guide-for-becoming-an-idea-machine/

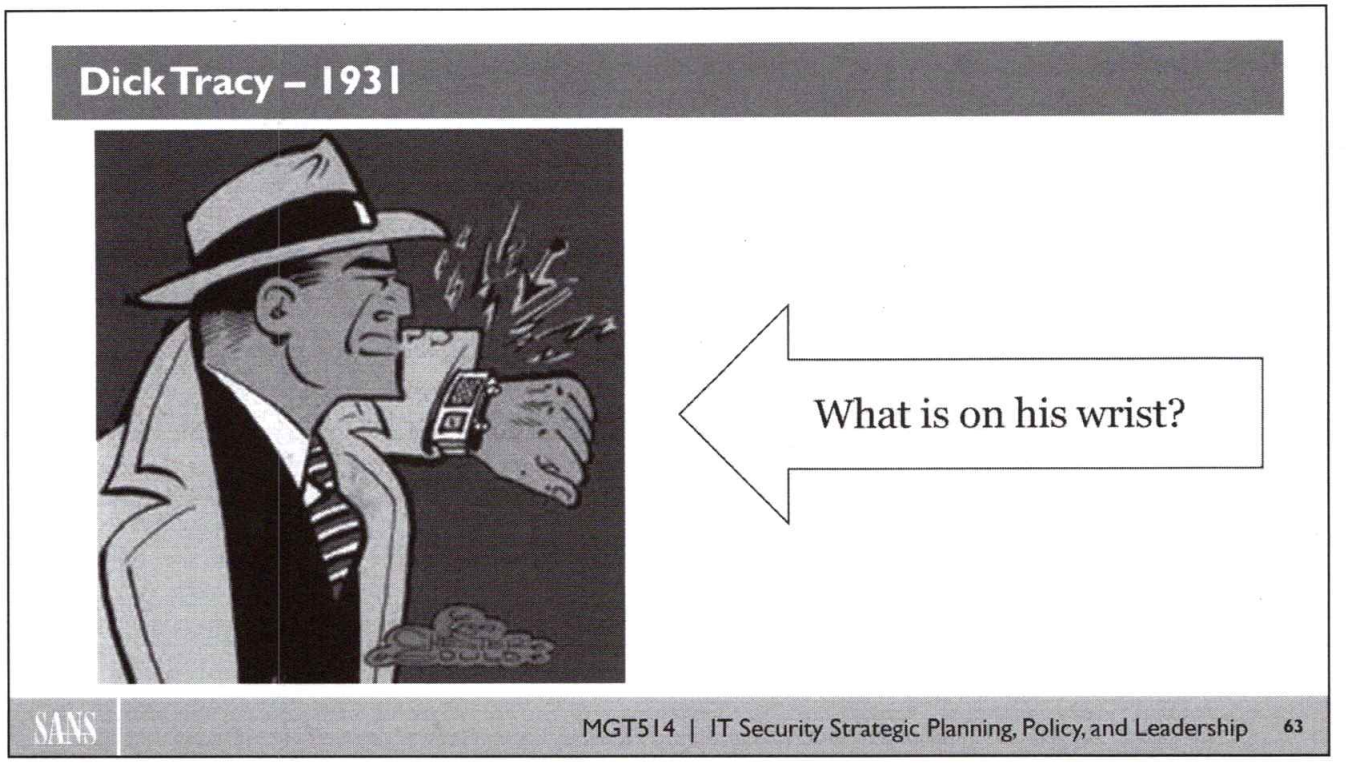
[2] https://en.wikipedia.org/wiki/English_coffeehouses_in_the_17th_and_18th_centuries#The_Enlightenment

[3] https://hbr.org/2013/03/the-ideal-praise-to-criticism/

[4] http://espn.go.com/blog/truehoop/post/_/id/13761/study-good-players-arent-afraid-to-touch-teammates



Even if you implement regular visioning sessions and create a nurturing environment for innovative ideas, visioning is still very hard. The good news is that we do not have to be pin point accurate to gain benefits from visioning. As long as we respect the limits of plausibility (in the next ten years, faster than light travel, cold fusion, world peace, etc., are not within the limits of plausibility), we have a good chance of being close enough to position our organization to what actually happens to take advantage of perceived opportunity.

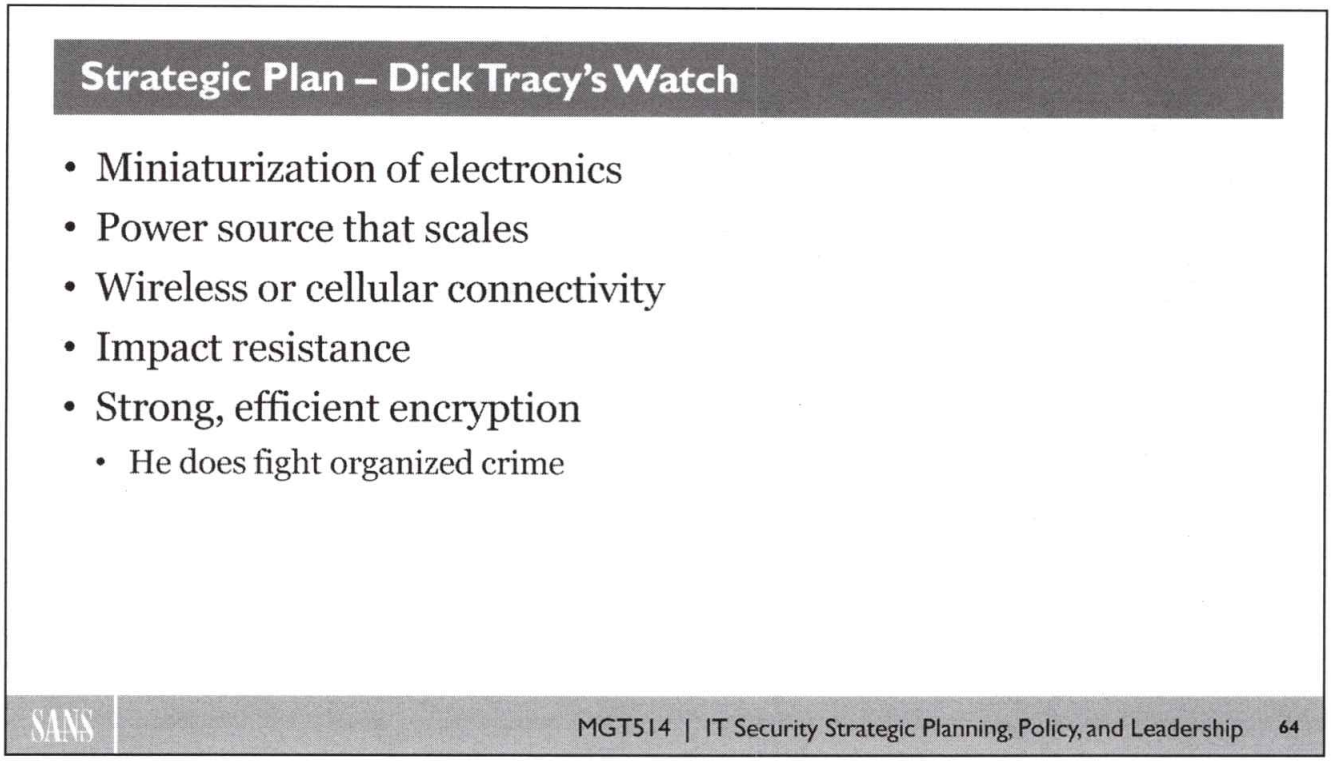


Dick Tracy is a fictional, comic book crime fighter who came into being in 1931. We do not actually know when the two-way TV wristwatch first appeared, but the point is, this is within the cone of plausibility, perhaps not for ten years, but given enough time.

References

http://en.wikipedia.org/wiki/Dick_Tracy

http://dailyspeculations.com/DickTracy.png



Say it is 1935 and we are a company that believes in the future and that there will be two-way voice and video communication devices. What are the big problems that need to be solved to make such a communications device a reality? If we were planning strategically, what would need to happen to make this plausible? Some of them are:

- Miniaturization of electronics
- Power source that scales
- Wireless or cellular connectivity
- Impact resistance
- Strong, but efficient encryption

Transistors

- 1971 Intel 4004: 2,300
- 1989 Intel 486: 1,200,000
- 2002 Intel Itanium 2: 220,000,000
- 2007 Intel Quad core: 820,000,000
- 2020 Intel ???: 4 Billion
  - Moore's law appears to have a limit
  - More transistors in the world than grains of sand?

Moore's law describes a long-term trend in the history of computing hardware. The number of transistors that can be placed inexpensively on an integrated circuit has doubled approximately every two years. This means the only things keeping the Dick Tracy wristwatch from being as powerful as a modern-day desktop computer will eventually be screen size and power source.

Reference

http://www.intel.com/content/www/us/en/history/historic-timeline.html

Jules Verne (1828 – 1905)

- French novelist who wrote:
  - *Journey to the Center of the Earth* (1864)
  - *From the Earth to the Moon* (1865)
  - *Twenty Thousand Leagues Under the Sea* (1870)
  - *Around the World in Eighty Days* (1873)
- He predicted many modern inventions
  - Electric submarines
  - Lunar modules
  - Videoconferencing
  - Taser
  - Skywriting: "Atmospheric advertisements"
  - Newscasts: "Instead of being printed the news will be spoken to subscribers"

Jules Verne is a French novelist who is most well-known for his adventure novels and influence on the science fiction genre.[1] His ideas were often a century ahead of his time. He predicted many modern inventions,[2] such as electric submarines, lunar modules, videoconferencing, the Taser, skywriting, and newscasts.

References

[1] http://en.wikipedia.org/wiki/Jules_Verne

[2] http://news.nationalgeographic.com/news/2011/02/pictures/110208-jules-verne-google-doodle-183rd-birthday-anniversary/

Nikola Tesla (1856 – 1943)

- Famous inventor who created:
  - Alternating current
  - Radio
  - Radar
  - X-rays
  - Hydroelectric power
  - Transistor
  - Remote control
  - Neon lighting
  - Electric motor
  - Wireless communications
- Good overview from *The Oatmeal*
  - "Why Nikola Tesla was the greatest geek that ever lived"
  - http://theoatmeal.com/comics/tesla

Nikola Tesla is a famous inventor who not only thought of amazing ideas, but he actually brought them to life. Among his most significant contributions are those inventions related to energy. He created alternating current, built the first hydroelectric power plant at Niagara Falls, and even came up with a system for wirelessly charging your home. He even created a tower near New York City that would have provided free wireless energy to the entire world. The project was scrapped when the investor realized there would be no way to regulate the energy and, therefore, charge for it.

Reference

http://theoatmeal.com/comics/tesla

Hedgehog Concept

- Based on an ancient Greek parable
  - "The fox knows many things, but the hedgehog knows one big thing."
- To be successful, focus on doing one thing extremely well
- Find your "Hedgehog Concept" by understanding what:
  - You are deeply passionate about
  - You can be the best in the world at
  - Drives your economic engine

The concept behind the Hedgehog Concept is based on a Greek poem about a fox and a hedgehog. A cunning and brilliant fox grasps the complexity of the woods around him. He sets his mind on eating a hedgehog and spends hours plotting the perfect attack. Meanwhile, the simple hedgehog goes about its business unaware. When the fox attacks, the hedgehog rolls himself into a spiny, impenetrable ball. The fox keeps re-strategizing, but the pattern repeats itself. "The fox knows many things, but the hedgehog knows one big thing." This understanding of what you can be the best at by focusing on doing one thing extremely well was described by philosopher Isaiah Berlin in his 1953 essay, "The Hedgehog and the Fox." Jim Collins further developed this idea in his 2001 book, *Good to Great: Why Some Companies Make the Leap...and Others Don't.*

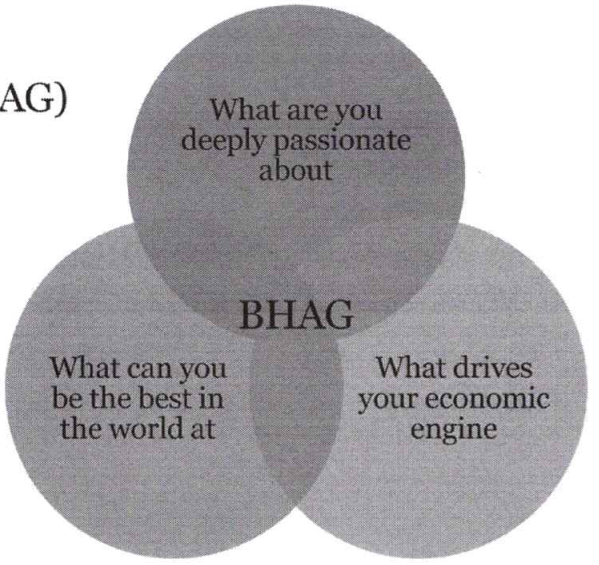
To find your Hedgehog Concept, you must understand three things:

- What you are deeply passionate about
- What you can be the best in the world at
- What drives your economic engine

Jim Collins refers to this as your "Big Hairy Audacious Goal (BHAG)."

BHAG

- Big Hairy Audacious Goal (BHAG)
  - Defines visionary goals
  - Common envisioned future



A deep understanding of the three intersecting circles is required to go from good to great. The most crucial point is that the Hedgehog Concept is not a goal to be the best, a strategy to be the best, an intention to be the best, and a plan to be the best. It is an understanding of what you can be the best at. The distinction is absolutely crucial.

A BHAG (pronounced bee-hag, short for "Big Hairy Audacious Goal") is a huge and daunting goal—like a big mountain to climb. It is clear and compelling, and people "get it" right away. A BHAG serves as a unifying focal point of effort, galvanizing people and creating team spirit as people strive toward a finish line. Like the 1960s NASA moon mission, a BHAG captures the imagination and grabs people in the gut.

Good BHAGs flow from understanding; bad BHAGs flow from bravado. Great BHAGs sit right smack in the middle of the three circles.

The good-to-great companies did not say, "Okay, folks, let's get passionate about what we do." Sensibly, they went the other way entirely: We should do those things that only we can get passionate about.

To go from good to great requires transcending the curse of competence. It requires the discipline to say, "Just because we are good at it—just because we're making money and generating growth—doesn't necessarily mean we can become the best at it." The good-to-great companies understand that doing what you are good at will only make you good—focusing solely on what you can potentially do better than any other organization is the only path to greatness.

A company does not need to be in a great industry to become a great company. All good-to-great companies build a fabulous economic engine, regardless of the industry. They are able to do this because they attain profound insights into their economics. The denominator can be quite subtle, sometimes even unobvious. The key is to use the question of the denominator to gain understanding and insight into your economic model.

An essential point: "Growth" is not a Hedgehog Concept. Rather, if you have the right Hedgehog Concept and make decisions relentlessly consistent with it, you will create such momentum that your main problem will not be how to grow, but how not to grow too fast.

Exercise 2.2 – Innovation

Estimated Time: 10 Minutes

- Goal of this exercise
  - Understand characteristics and different types of innovation
- Write down:
  - Three characteristics of innovation
    - Goal is to determine "What is innovation?"
  - Three companies you think are innovative
  - Three companies you think are not innovative

The goal of this exercise is to understand the characteristics of innovation and the different types of innovation. We'll start by simply writing down your answers to the questions below. Then, we'll discuss your responses and how they answer the question, "What is innovation?"

What are three characteristics of innovation?

1) _____

2) _____

3) _____

List three companies you think are innovative.

1) _____

2) _____

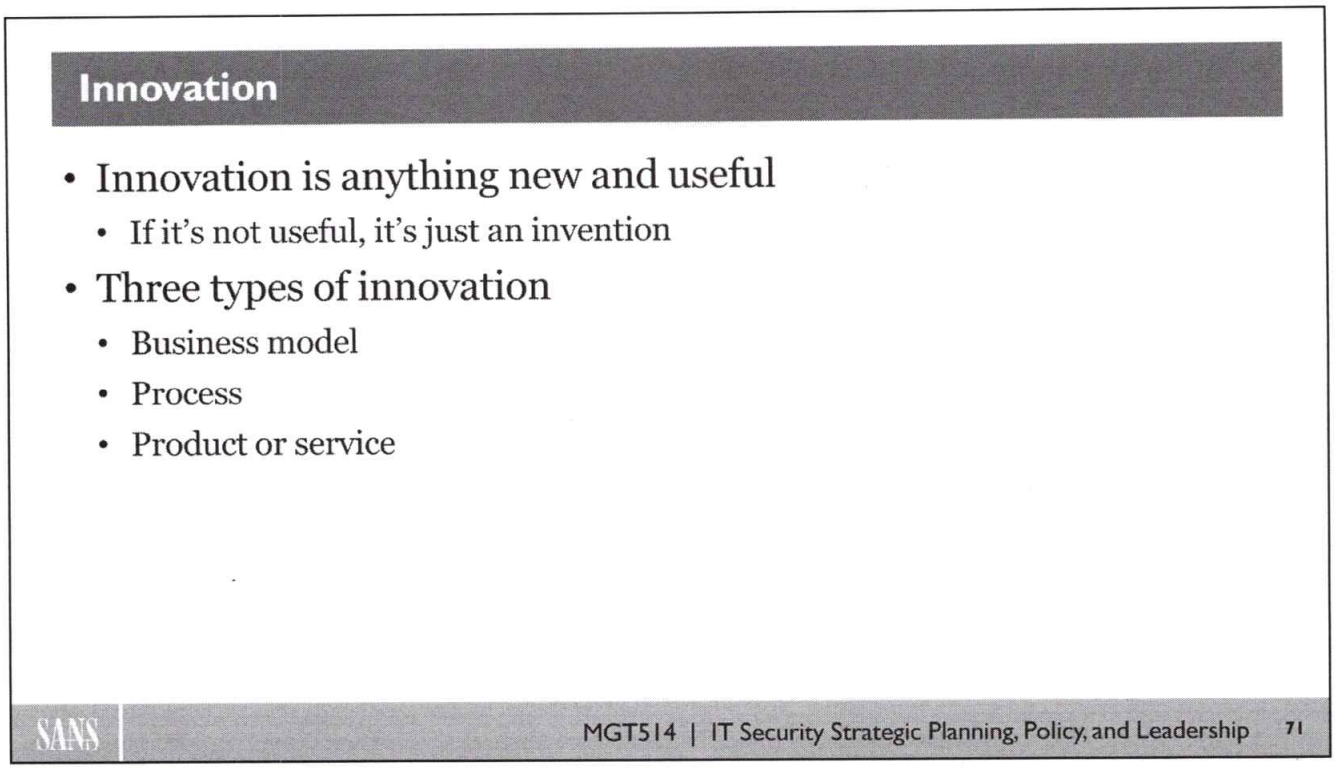
3) _____

List three companies you think are *not* innovative.

1) _____

2) _____

3) _____



When people think about innovation, the following characteristics might come to mind:

- Solves a problem
- Makes something easier
- Creates desire
- Is novel or new (e.g., technology)
- Is useful

These characteristics can be handy indicators, but how can you measure innovation? Revenue is an indicator that a company is producing items that meet customer needs but is not, in and of itself, a characteristic of innovation. Oftentimes, companies might measure the number of researchers or number of patents as an indicator of innovation. Are patents an innovation? Does a product have to be brought to market to be an innovation? Does it have to actually be useful?

If you are an engineer, you probably believe that products need to be useful. For example, what use is a blueprint for a bridge if you don't actually build the bridge itself? However, if you are a scientist, do you care if an idea is useful? A scientist would probably say, "It doesn't matter," because the act of discovery itself is what is important. That is what differentiates innovation from invention. Innovation is anything new and useful. If something is not useful, it's just an invention.

Many companies have produced useful things, but certain companies have a perception of being innovative or not. For example, Apple is often cited as an innovator for its products like the Mac, iPhone, and iPad. However, products are just one form of innovation. One of Apple's biggest innovations is the iTunes store, the unbundling of single songs from the larger album, and the creation of an online distribution platform to sell these songs. This was an important business model innovation. On the other end of the spectrum, Dell is seen by many as a boring, low-margin computer maker. However, Dell's innovation was not in the product space but was in its capability to create an approach for building extremely low-cost computers consistently and in extremely large quantities. Dell's was a process innovation.

Sustaining vs. Disruptive Innovation

- Sustaining innovation
  - Does not create a new market
    - Evolves an existing technology or process
- Disruptive innovation
  - Creates a new market
    - Eventually displacing an earlier technology or process
    - Typically starts with low-end disruption that serves least profitable customers with minimal functionality
  - Described in *The Innovator's Dilemma*
    - By Clayton Christensen

The Innovator's Dilemma[1] by Clayton Christensen is often cited as one of the most influential business books in history.[2] It describes how successful, incumbent companies often fail because they are focused on maximizing profits and meeting the needs of existing customers. By offering an ever-increasing number of features, performance, and higher quality products that will lead to greater profits, these companies neglect opportunities based on new technologies that don't serve the needs of current customers, don't fit with their existing business models, and provide lower margins. This leaves the door open to competitors who excel at different tasks and, as their products mature, take over the market. A prime example of this is with mobile phones and tablets, which have disrupted the traditional PC market. Mobile devices offer fewer features than PCs, but they provide other benefits like mobility that customers value in more situations. As these mobile devices continue to improve, the existing technology gets further displaced.

A sustaining innovation, on the other hand, is one that does not create a new market but simply evolves or improves upon an existing technology or process. In computing, this includes things like increased memory capacity, speed, and screen resolution or improving the process for assembling computers to reduce costs and inefficiencies.

References

[1] http://www.claytonchristensen.com/books/the-innovators-dilemma/

[2] http://www.wired.com/2014/12/understanding-the-innovators-dilemma/

Examples of Disruptive Innovation

- Cars (mass produced)
- Digital music
- Digital photography
- PCs
- Smartphones
- Telephone
- Wikipedia

There are many examples of disruptive innovations throughout business history. Cars replaced the horse and buggy, streetcars, and rail transportation. Digital music disrupted physical music sales and the business model of record labels. Digital photography displaced chemical photography. PCs disrupted typewriters and dedicated word processors. Smartphones then in turn disrupted the PC. The telephone disrupted the telegraph. Wikipedia disrupted print encyclopedias.

Jobs to Be Done Theory

- Idea that customers don't just buy products
  - They hire solutions to get various jobs done
  - The customer "simply has a job to be done and is seeking to 'hire' the best product or service to do it"
- The theory helps you:
  - Understand what your customers want
  - Gain new insights to innovate with the business

The "jobs to be done" theory is best illustrated by a famous story about milkshakes from Clayton Christensen.[1]

There was a fast food restaurant that wanted to increase milkshake sales. So, it hired some expensive consultants to do an analysis, ask customers what they wanted, segment the market by products and demographics, and come up with a recommendation. After analyzing all the data and changing the milkshakes per their research, what happened? Nothing. Sales did not improve.

The company then decided to hire a different expensive consultant. This time, though, it wound up hiring one of Clayton Christensen's fellow researchers. He spent a whole day sitting in one of these fast food restaurants carefully observing everyone who bought a milkshake, what time they bought it, and whether they drank it on site. He found that 40% of milkshakes were bought to go first thing in the morning by commuters.

He came back the next day and asked these customers what job they hired the milkshake to do. He found that most customers had a long, boring commute and wanted something to make the drive more interesting. They weren't hungry yet but would be by 10am and were in a hurry with only one free hand because they were driving. This needed something tidy and distracting. Trying to suck a thick liquid through a straw gave these commuters something to do. So, the fast food chain made milkshakes that were thicker to last through the commute and more interesting (with chunks of fruit). Milkshake sales increased drastically.

The idea is that customers don't just buy products. They hire solutions to get various jobs done. The theory helps us understand what customers actually want and value. It allows us to gain new insights on how we can innovate with the business.

Reference

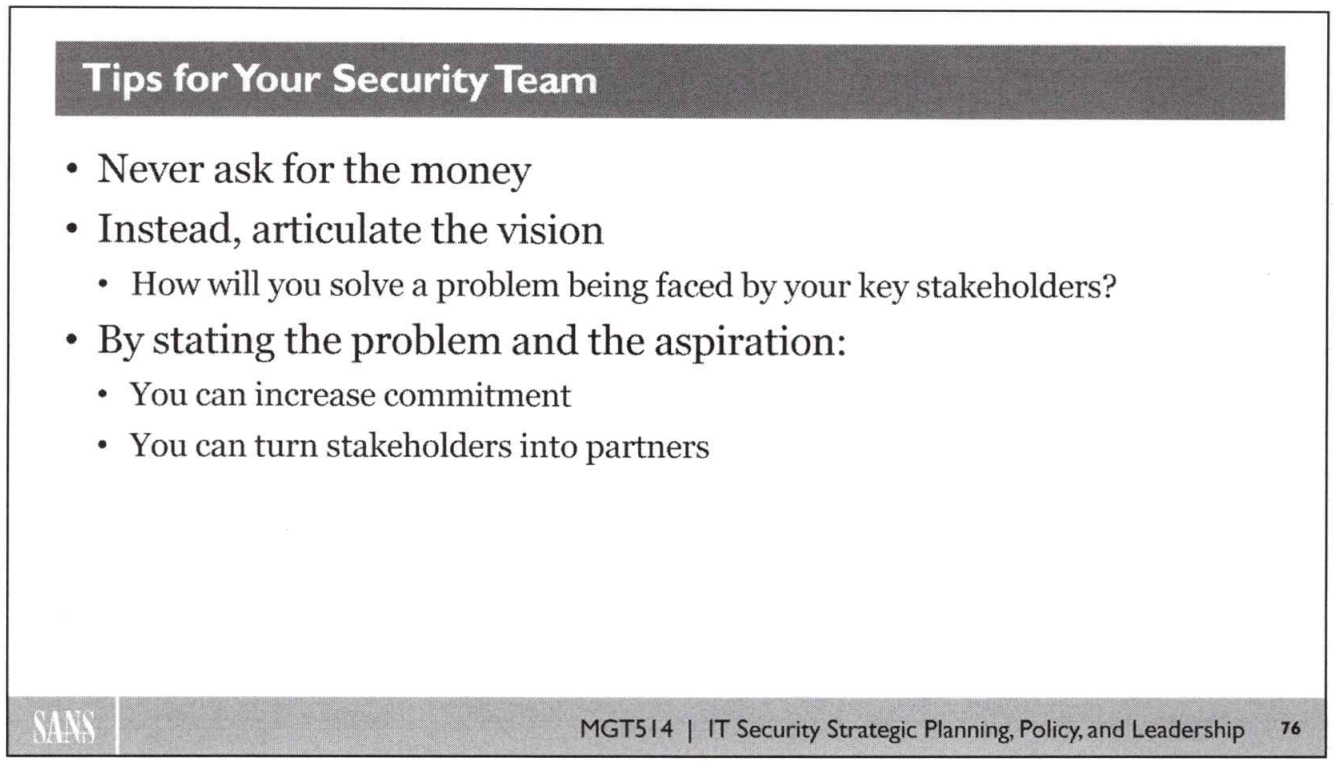
[1] http://hbswk.hbs.edu/item/6496.html

Innovation Key Questions

- How do we create value for our stakeholders?
  - That is the essence of strategy
- How do we innovate?
- Why does anyone need us?
  - What the problem is that needs to be solved
  - The aspiration that needs to be fulfilled

At the heart of disruptive innovation and jobs to be done theory is the question of creating value for our customers. What problems do stakeholders have that we can make better? The answer to this question is the essence of strategy.

By figuring out how to innovate with the business, we as the security team can increase our value. Oftentimes, the value that the security team provides is not clear. By identifying the problems that our key stakeholders need solved, we can help them fulfill the goals of the larger organization.



Simon Sinek is an author who is most well known for creating the concept of the "golden circle," which describes how great leaders inspire others by starting with "why" instead of the "how" or the "what." He states, "People don't buy what you do, they buy why you do it."[1] An example from his book, *Start with Why*,[2] helps illustrate this point:

"Samuel Pierpont Langley set out in the early 1900s to be the first man to pilot an airplane. Highly regarded, he was a senior officer at the Smithsonian Institution, a mathematics professor who had also worked at Harvard. His friends included some of the most powerful men in government and business, including Andrew Carnegie and Alexander Graham Bell. Langley was given a $50,000 grant from the War Department to fund his project, a tremendous amount of money for the time. He pulled together the best minds of the day, a veritable dream team of talent and know-how. Langley and his team used the finest materials, and the press followed him everywhere. People all over the country were riveted to the story, waiting to read that he had achieved his goal."[3]

Just a few hundred miles away, Wilbur and Orville Wright were also working on their own flying machine. They had no grants, no funding, no powerful connections, no advanced degrees, or even college educations. The odds were stacked against them, but on December 17, 1903, they successfully got a man to take flight for the first time in history. Why did the Wright Brothers succeed where Langley did not? They had a passion to fly that inspired all those around them. Their team didn't just want a job, they wanted to be part of the mission. Langley, on the other hand, quit shortly after hearing about the Wright Brothers' success.

When asking for funding, never ask for the money. Instead, articulate the vision. By stating the problem and your aspiration, you can increase commitment and turn stakeholders into partners. "People don't buy what you do, they buy why you do it."[3]

References

[1] https://www.youtube.com/watch?v=sioZd3AxmnE

[2] https://www.startwithwhy.com/Books.aspx

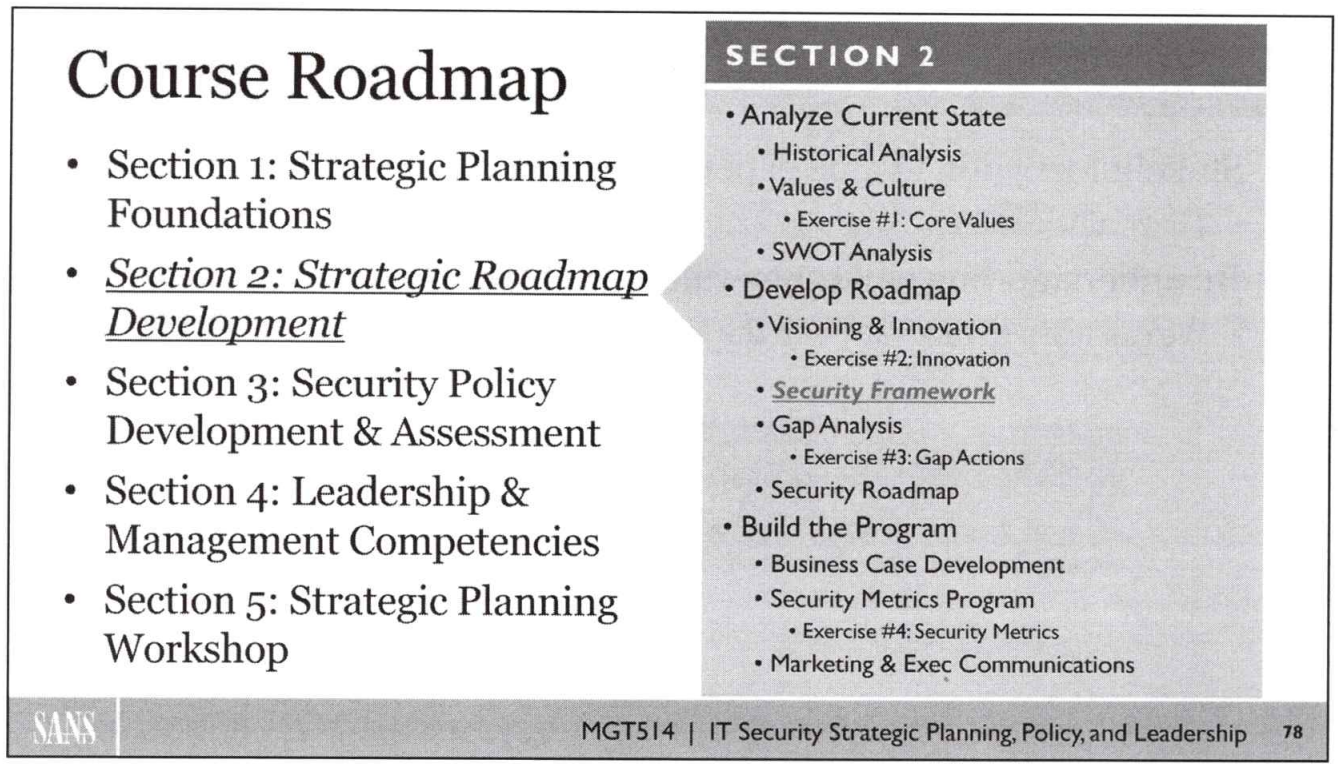
[3] https://www.startwithwhy.com/Portals/0/Downloads/StartWithWHYChapter.pdf

In Summary

- Stakeholders don't value expertise
  - They value results
- By understanding what they value:
  - We can learn to innovate with the business

> "The best way to predict the future is to invent it."
> - Alan Kay

When thinking about the future, about innovation, or about jobs to be done, the common theme is understanding "why" something needs to be done. By selling your vision and understanding what your key stakeholders value, you can create results that further business innovation. Your stakeholders aren't interested in how many vulnerabilities you patched, how many attacks were blocked, or how many scans you conducted. But, tying those important security activities to the results that they are driving toward can help you create results that transform stakeholders into partners.



This page intentionally left blank.

Security Framework

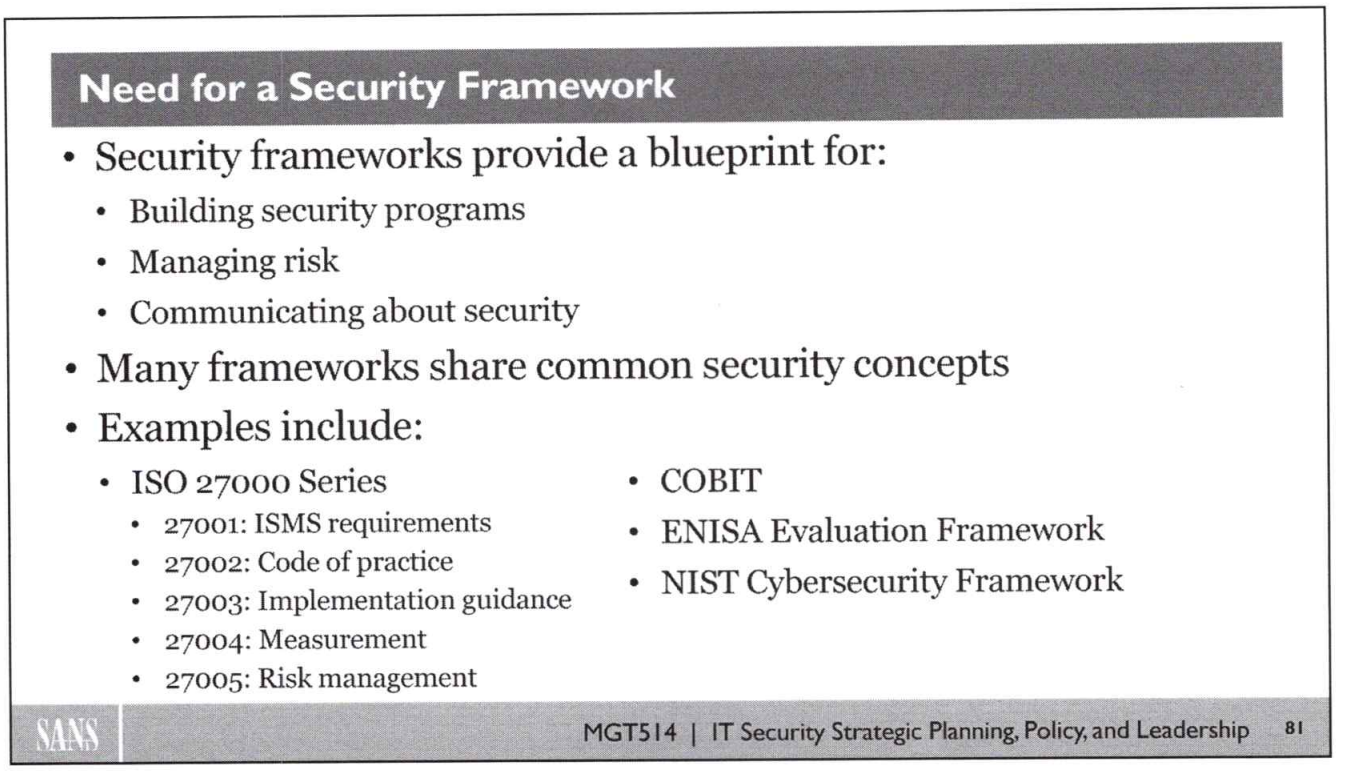
- Goals of this section
  - Introduce a framework that can be used to provide a high-level view of the security program
  - Learn how to convey maturity of the security program

In this section, you will be introduced to a framework that can be used to frame the work of the security team and overall program. With this framework in mind, you will learn how to convey the maturity of the security program in a way that is understandable to senior executives.

PharmaCo Case Scenario

- Cheryl Miller is Director of Security Strategy
- Her boss the CIO:
  - Agrees with her SWOT analysis
  - Is unclear how this translates into a security plan
  - Tells her not to come back to him until she has a strategic plan in place
- Cheryl is at first uncertain how to do this
  - Decides to utilize an industry-defined framework

When you last spoke to your friend Cheryl Miller, she had recently taken a new job as Director of Security Strategy at PharmaCo. She was in the midst of learning more about the organization's strengths, weaknesses, opportunities, and threats (SWOT). Now, one month later, you are having dinner again. In the meantime, she has met with a number of C-level executives and business unit leaders to learn more about the organization and how security can contribute. Based on her research, her boss, the CIO, believes that her SWOT analysis is accurate, but he is not certain how this translates into a security plan. He tells her not to come back to him until she has a strategic plan in place that they can discuss. Cheryl is at first uncertain how to do this, but she has decided to utilize an industry-defined framework to frame her strategic plan.



Security frameworks provide a blueprint for building security programs, managing risk, and communicating about security using a common vocabulary. There are many security-related frameworks, and it might sometimes be difficult to decide which one to use. Fortunately, many of these frameworks share common security concepts. Some common examples include:

ISO 27000

The ISO 27000 series[1] was developed by the International Standards Organization and provides a broad information security framework. It is applicable to any industry and can be used to map to multiple regulations with which your organization might need to comply (for example, PCI, HIPAA, SOX, and FFIEC). ISO 27001 defines the requirements for the program whereas ISO 27002 defines the code of practice. This is a very comprehensive framework and implementation can be long and involved. Achieving ISO 27000 certification is often important for cloud service providers looking to demonstrate a rigorous security program.[2]

COBIT

COBIT is a framework for managing and governing Enterprise Information Technology (IT) of which information security is an important component. COBIT started with a focus on reducing technical risks but, with COBIT 5, has evolved to include aligning IT with business and strategic goals. It is commonly used in relation to achieving SOX compliance.

ENISA Evaluation Framework

ENISA, the European Union Agency for Network and Information Security, has published "An Evaluation Framework for National Cyber Security Strategies,"[3] which includes 1) review the cybersecurity strategies of EU member states 2) identification of best practices conducted by these member states 3) development of an evaluation framework and 4) creation of key performance indicators (KPIs) to measure the security program.

NIST Cybersecurity Framework

NIST, the National Institute of Standards and Technology, has published the "Framework for Improving Critical Infrastructure Cybersecurity." The framework "created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[4]

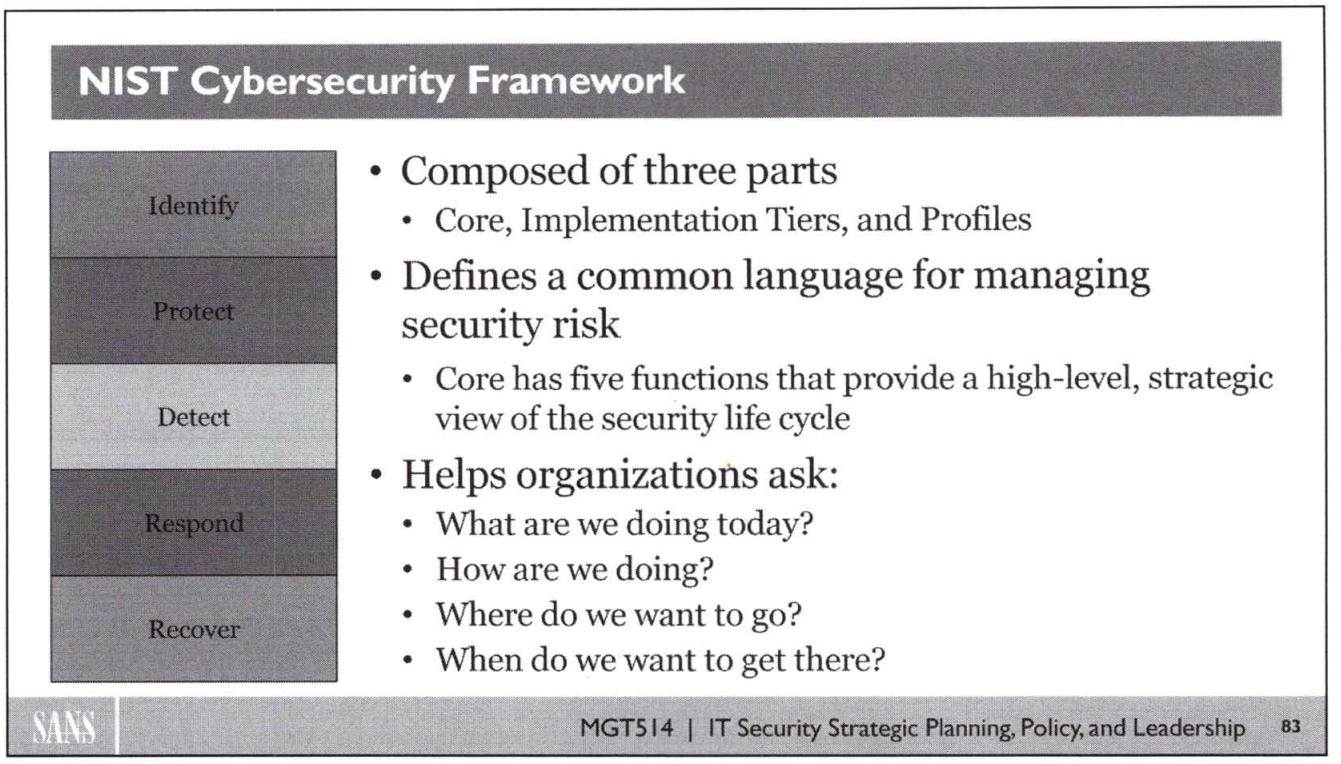
References

[1] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[2] http://www.isaca.org/cobit

[3] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1

[4] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf



In February 2013, President Barack Obama issued Executive Order 13636, which ordered that actions be taken to improve critical infrastructure cybersecurity.[1] One of the directives of the executive order included the creation of a cybersecurity framework. As a result, the National Institute of Standards and Technology (NIST) published the first version of the "Framework for Improving Critical Infrastructure Cybersecurity" in February 2014. It is commonly referred to as the "NIST Cybersecurity Framework" or simply the "Cybersecurity Framework."

The framework consists of five functions that provide a high-level, strategic view of the life cycle of managing security risk. These five functions comprise the "Framework Core" and they are:

Identify: Planning activities to understand business needs and threats so that initiatives can be prioritized based on risk

Protect: Activities that prevent or contain the impact of security incidents

Detect: Activities that identify security incidents

Respond: Incident response activities

Recover: Activities that restore normal operations and reduce impact of security incidents

By breaking down a security program into these five functions, the framework helps organizations:

1) Describe their current cybersecurity posture.
2) Describe their target state for cybersecurity.
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
4) Assess progress toward the target state.
5) Communicate among internal and external stakeholders about cybersecurity risk.

These benefits are taken from page 4 of the framework document.[2]

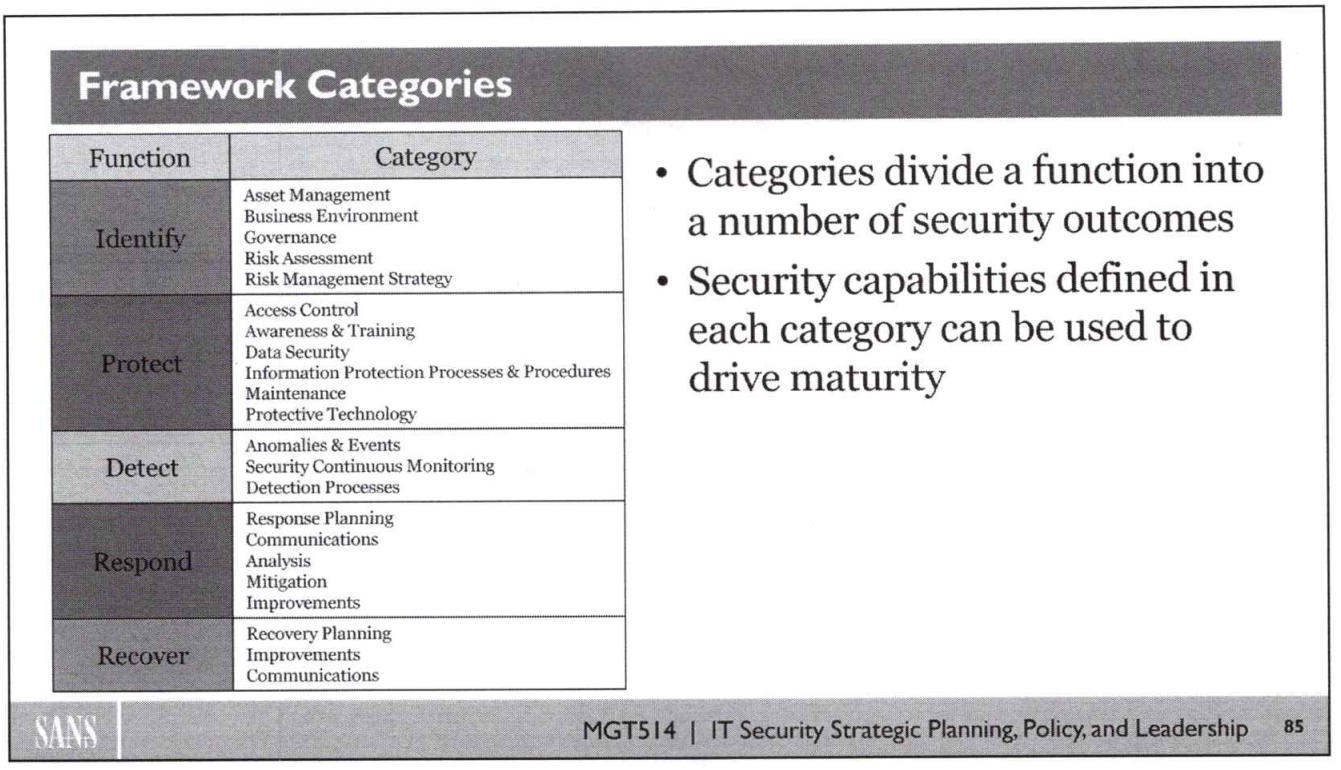
Because of its publication, many federal and state entities in the United States have started to adopt the framework.[3]

References

[1] http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[2] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[3] http://www.natlawreview.com/article/where-are-we-now-nist-cybersecurity-framework-one-year-later



Each high-level function is broken up into a number of categories that represent the security outcomes for that particular area. These categories can be used to drive maturity and improvements for the higher-level functions. As an example, the Identify function is composed of the following five categories:

Asset Management

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Business Environment

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Governance

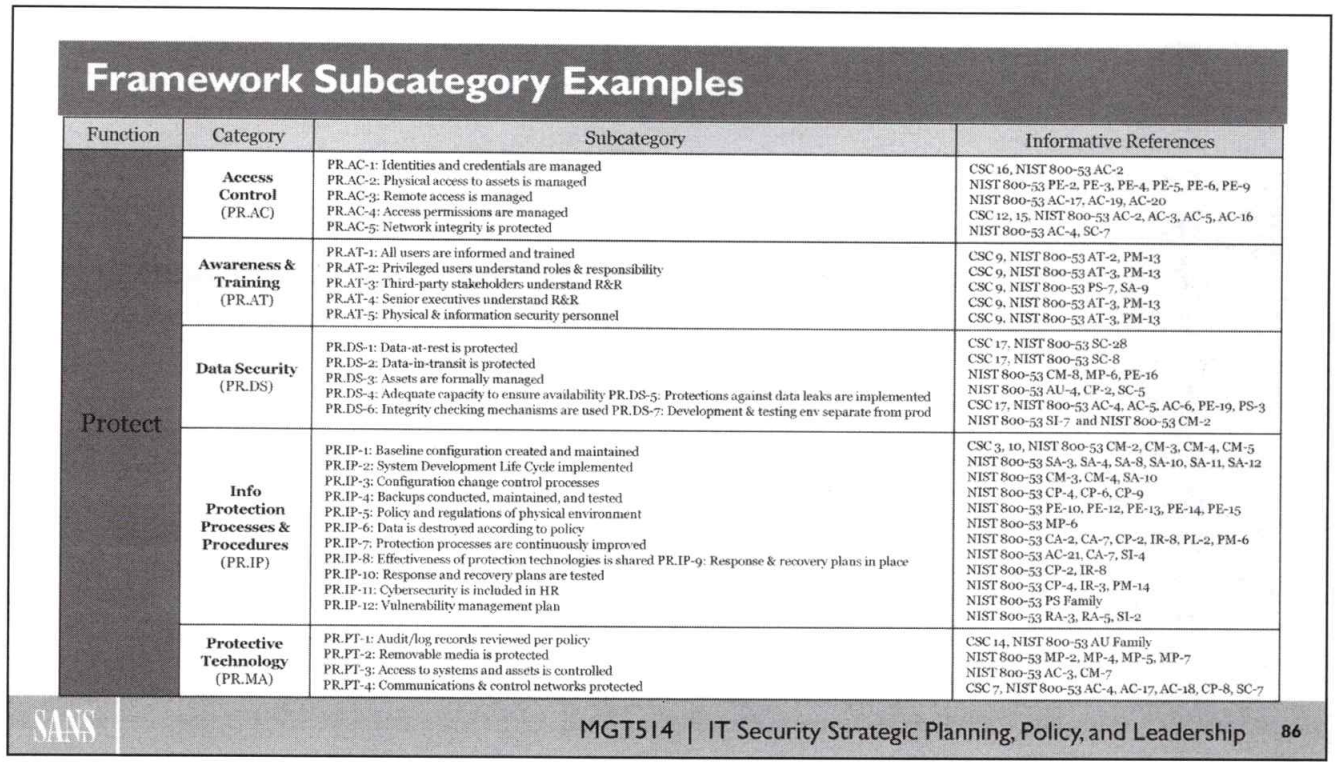
The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Management Strategy

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.



Framework Subcategory Examples

Function	Category	Subcategory	Informative References
Protect	**Access Control** (PR.AC)	PR.AC-1: Identities and credentials are managed PR.AC-2: Physical access to assets is managed PR.AC-3: Remote access is managed PR.AC-4: Access permissions are managed PR.AC-5: Network integrity is protected	CSC 16, NIST 800-53 AC-2 NIST 800-53 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 NIST 800-53 AC-17, AC-19, AC-20 CSC 12, 15, NIST 800-53 AC-2, AC-3, AC-5, AC-16 NIST 800-53 AC-4, SC-7
	Awareness & Training (PR.AT)	PR.AT-1: All users are informed and trained PR.AT-2: Privileged users understand roles & responsibility PR.AT-3: Third-party stakeholders understand R&R PR.AT-4: Senior executives understand R&R PR.AT-5: Physical & information security personnel	CSC 9, NIST 800-53 AT-2, PM-13 CSC 9, NIST 800-53 AT-3, PM-13 CSC 9, NIST 800-53 PS-7, SA-9 CSC 9, NIST 800-53 AT-3, PM-13 CSC 9, NIST 800-53 AT-3, PM-13
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected PR.DS-3: Assets are formally managed PR.DS-4: Adequate capacity to ensure availability PR.DS-5: Protections against data leaks are implemented PR.DS-6: Integrity checking mechanisms are used PR.DS-7: Development & testing env separate from prod	CSC 17, NIST 800-53 SC-28 CSC 17, NIST 800-53 SC-8 NIST 800-53 CM-8, MP-6, PE-16 NIST 800-53 AU-4, CP-2, SC-5 CSC 17, NIST 800-53 AC-4, AC-5, AC-6, PE-19, PS-3 NIST 800-53 SI-7 and NIST 800-53 CM-2
	Info Protection Processes & Procedures (PR.IP)	PR.IP-1: Baseline configuration created and maintained PR.IP-2: System Development Life Cycle implemented PR.IP-3: Configuration change control processes PR.IP-4: Backups conducted, maintained, and tested PR.IP-5: Policy and regulations of physical environment PR.IP-6: Data is destroyed according to policy PR.IP-7: Protection processes are continuously improved PR.IP-8: Effectiveness of protection technologies is shared PR.IP-9: Response & recovery plans in place PR.IP-10: Response and recovery plans are tested PR.IP-11: Cybersecurity is included in HR PR.IP-12: Vulnerability management plan	CSC 3, 10, NIST 800-53 CM-2, CM-3, CM-4, CM-5 NIST 800-53 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12 NIST 800-53 CM-3, CM-4, SA-10 NIST 800-53 CP-4, CP-6, CP-9 NIST 800-53 PE-10, PE-12, PE-13, PE-14, PE-15 NIST 800-53 MP-6 NIST 800-53 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 NIST 800-53 AC-21, CA-7, SI-4 NIST 800-53 CP-2, IR-8 NIST 800-53 CP-4, IR-3, PM-14 NIST 800-53 PS Family NIST 800-53 RA-3, RA-5, SI-2
	Protective Technology (PR.MA)	PR.PT-1: Audit/log records reviewed per policy PR.PT-2: Removable media is protected PR.PT-3: Access to systems and assets is controlled PR.PT-4: Communications & control networks protected	CSC 14, NIST 800-53 AU Family NIST 800-53 MP-2, MP-4, MP-5, MP-7 NIST 800-53 AC-3, CM-7 CSC 7, NIST 800-53 AC-4, AC-17, AC-18, CP-8, SC-7

The categories in the Protect function are:

Access Control (PR.AC)

Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Awareness and Training (PR.AT)

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security (PR.DS)

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

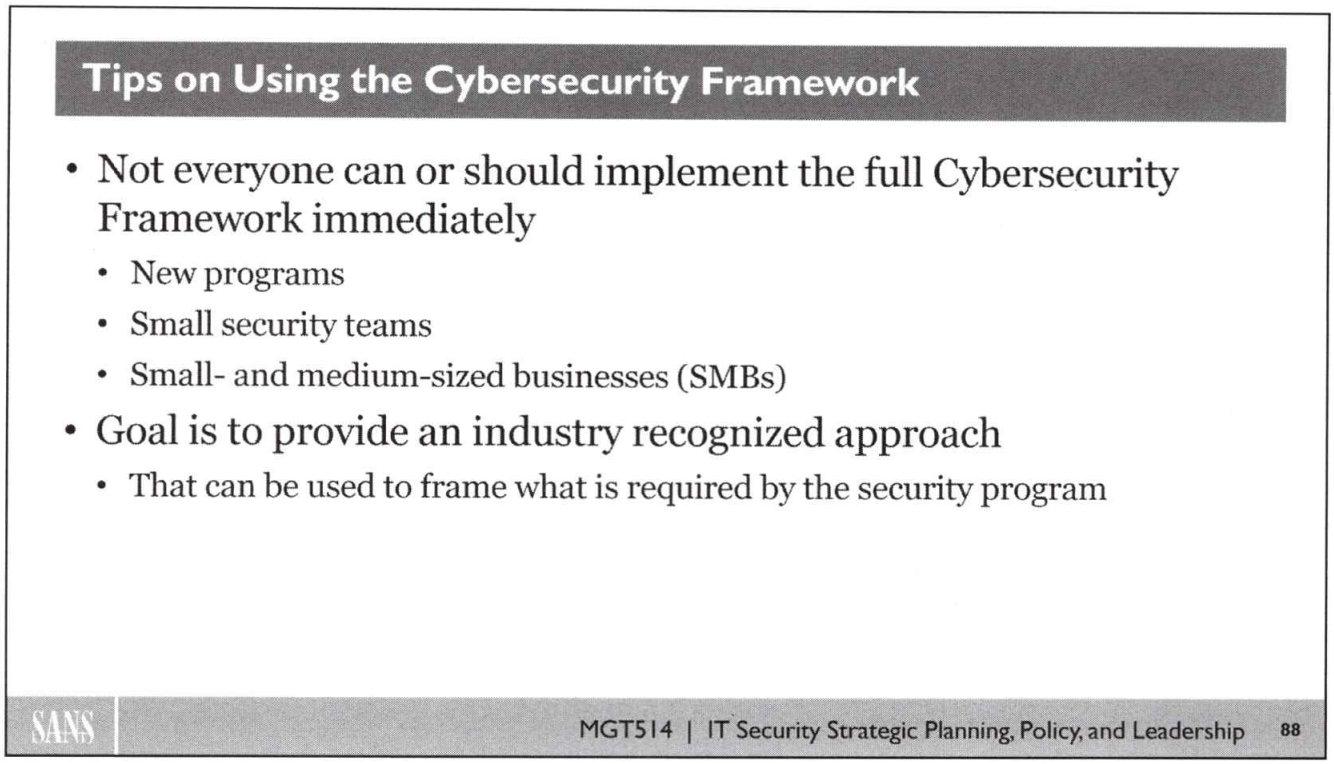
Maintenance (PR.MA): Note that this category has been left off the slide due to space limitations

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Protective Technology (PR.PT)

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Each category is composed of a number of subcategories that can be mapped to specific technical or management objectives. The Cybersecurity Framework includes Informative References that refer to standards, best practices, and guidelines like the Critical Security Controls (CSC), NIST 800-53, COBIT, and ISO 27001. This helps to map specific controls and objectives to the subcategory, category, and function.



The Cybersecurity Framework defines a comprehensive set of activities that can be conducted by your security program. Depending on where you are in your journey, you might not want to implement the full framework immediately. Oftentimes new programs can use the framework as a guiding light for what can be achieved in the future. Part of this plan has to incorporate the reality of available resources or lack thereof. Small security teams and small- to medium-sized businesses (SMBs) do not have the resources of multi-billion dollar enterprises. Large enterprises might have dozens or hundreds of people working on information security-related activities. In the United States, the Small Business Administration defines what constitutes an SMB based on industry, ownership structure, revenue, and number of employees. SMBs generally have up to 500 employees, but it can be as high as 1500 in some cases. In the European Union (EU), micro-enterprises have up to 10 employees, small enterprises have up to 50 employees, and medium-sized enterprises have up to 250 employees. It's clear that an SMB with only 50 employees will not be able to dedicate 20% of its staff to security activities. The goal is not to follow any framework blindly but to frame the work of the security team in a manner that makes sense for the current business risks and landscape.

Measuring Maturity

- Can't do everything at once
  - Need to define a progression of maturity
- Implementation Tiers
  - Defined in the Cybersecurity Framework
    - Tier 4: Adaptive
    - Tier 3: Repeatable
    - Tier 2: Risk Informed
    - Tier 1: Partial

"Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective."

- Need a way to measure maturity and determine where to invest

The Cybersecurity Framework defines four Implementation Tiers that represent an "increasing degree of rigor and sophistication in cybersecurity risk management practices." These Implementation Tiers are composed of three categories:

Tier	Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1 Partial	Practices are not formalized, ad-hoc, and reactive	Limited awareness of security risk at the organizational level	No processes to coordinate with external entities
Tier 2 Risk Informed	Practices are approved by management but not by organization-wide policy	Awareness of risk organizationally but organization-wide approach to risk has not been established	No formalized capabilities to interact and share information externally
Tier 3 Repeatable	Practices formally approved and expressed as policy	Organization-wide approach to manage risk is defined	Enables collaboration with partners and receives information in response to events
Tier 4 Adaptive	Practices based on lessons learned and predictive indicators from previous and current activities	Security risk management is part of the culture and evolves based on various inputs	Actively shares information with partners before events occur

Maturity Models

- Maturity models provide a standard way to:
  - Measure organizational capabilities
  - Identify areas of improvement
- Examples include:
  - Capability Maturity Model Integration (CMMI)
  - Enterprise Strategy Group (ESG) Maturity Model
  - Gartner ITScore
  - Cybersecurity Capability Maturity Model (C2M2)
  - Building Security In Maturity Model (BSIMM)
  - Open Software Assurance Maturity Model (OpenSAMM)
  - Capability Immaturity Model (CIMM)

Maturity models provide a standard way to measure organizational capabilities and identify areas of improvement. There are many security related maturity models. Some examples include:

Capability Maturity Model Integration (CMMI)

Originally developed to measure the maturity of software development practices, the core concepts have been extended to apply to a number of other domains. It is discussed in more detail on the upcoming slides.

ESG Maturity Model

The Enterprise Strategy Group (ESG) is an IT research, analysis, and strategy firm. It has created a basic security maturity model discussed on an upcoming slide.

Gartner ITScore

Gartner is an IT research and advisory firm that gathers industry data and publishes it under the ITScore umbrella. ITScore allows you to compare your IT and security activities in relation to other firms and other companies in your own industry.

Cybersecurity Capability Maturity Model (C2M2)

The Cybersecurity Capability Maturity Model (C2M2) was created by the U.S. Department of Energy (DOE) with work focused on the electricity and oil/gas subsectors. It has been updated so that it can be used by any organization and provides a self-evaluation methodology and toolkit.

Building Security In Maturity Model (BSIMM)

The BSIMM is designed to help you understand and improve software security programs and was created by analyzing data and activities of real-world software security initiatives. While focused on software security, it contains data and concepts like strategy and risk management that are applicable to any security program.

Open Software Assurance Maturity Model (OpenSAMM)

OpenSAMM is an open, vendor-neutral maturity model for improving software security from the Open Web Application Security Project (OWASP). It is used by a number of organizations to determine which software security-related activities to prioritize.

Capability Immaturity Model (CIMM)

Humorously, the Capability Immaturity Model was developed as a parody to the popular Capability Maturity Model (CMM). It defines a negative scale of maturity that arises in dysfunctional organizations. It was created to highlight the fact that management of specific projects is dysfunctional, because negative maturity can exist even in organizations with overall positive CMM levels. The immaturity levels include:

- Level 0: Negligent: Level 1 assumes eventual success, whereas Level 0 organizations generally fail to produce anything
- Level -1: Obstructive: Processes are implemented that tend to obstruct real work from being accomplished. For example, many government contracts require a certain level of CMM maturity. In some cases, this results in contractors performing work related to simply documenting and following CMM processes.
- Level -2: Contemptuous: Ineffective processes become institutionalized with measures of activity (e.g., test cases written, lines of code written, and hours worked) replacing measures of productivity (e.g., test success rates and % of functions completed).
- Level -3: Undermining: Rival teams downplay or sabotage efforts of other teams in a competition for scarce resources (e.g., people, funding, etc.).

References

[1] http://whatis.cmmiinstitute.com

[2] http://resources.idgenterprise.com/original/AST-0135469_ESG-Brief-HP-Maturity-Model-Oct-2014.pdf

[3] https://www.gartner.com/doc/2507916/itscore-information-security

[4] http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

[5] https://www.bsimm.com

[6] http://www.opensamm.org

[7] http://en.wikipedia.org/wiki/Capability_Immaturity_Model

Enterprise Strategy Group Security Maturity Model

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

Source: Enterprise Strategy Group, 2014.

This table is from the Enterprise Strategy Group (ESG)[1] and was taken from an article by Brian Krebs titled "What's Your Security Maturity Level?"[2] It lays out a progression for basic, progressing, and advanced organizations. An important component of this is the "philosophy," which indicates where an organization might be in relation to the need for managing security risk. Many organizations are finding that it is not sufficient to view security as a "necessary evil," but that it must be more integrated into the business. In the long term, perhaps security can even become part of the culture.

References

[1] http://resources.idgenterprise.com/original/AST-0135469_ESG-Brief-HP-Maturity-Model-Oct-2014.pdf

[2] http://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/

Capability Maturity Model Integration (CMMI)

- Process model that defines what should be done to improve performance
  - Originally created to improve software development practices
  - Now expanded to cover development, services, and acquisitions
- Defines five maturity levels
  - Widely recognized and understood by executives, business leaders, and technology managers

The CMMI originally started as the CMM by the Software Engineering Institute (SEI) at Carnegie Mellon University for improving the process of software development. The CMMI supersedes the CMM and was developed by representatives from commercial, defense, government, and academic institutions and is now operated and maintained by the CMMI Institute, [1] which is a part of Carnegie Mellon University.

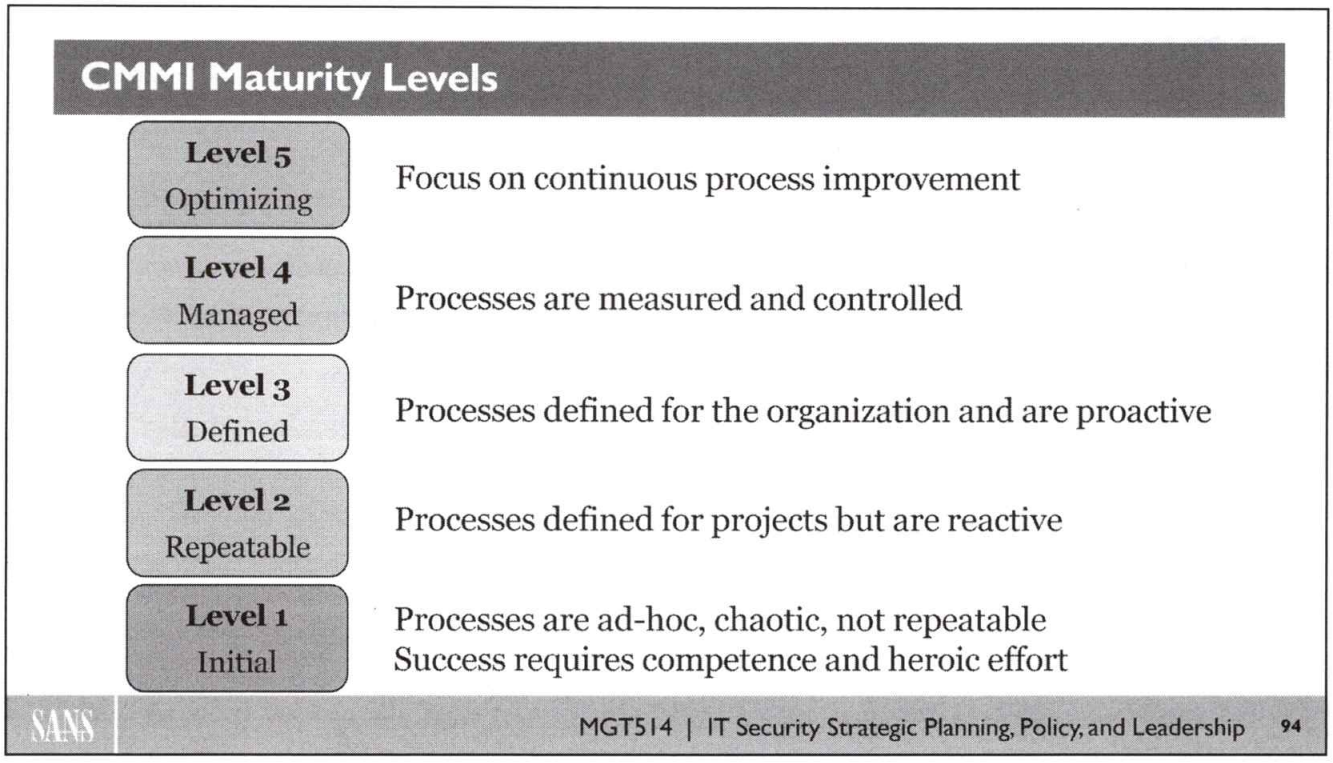
The CMMI currently addresses three areas of focus:

1) CMMI for Development (CMMI-DEV) for product and service development
2) CMMI for Services (CMMI-SVC) for service establishment and management
3) CMMI for Acquisition (CMMI-ACQ) for product service and acquisition

It is one of the most widely used and understood maturity models.

Reference

[1] http://whatis.cmmiinstitute.com



The five-point scale utilized in the CMMI is widely recognized and understood by executives, business leaders, and technology managers.

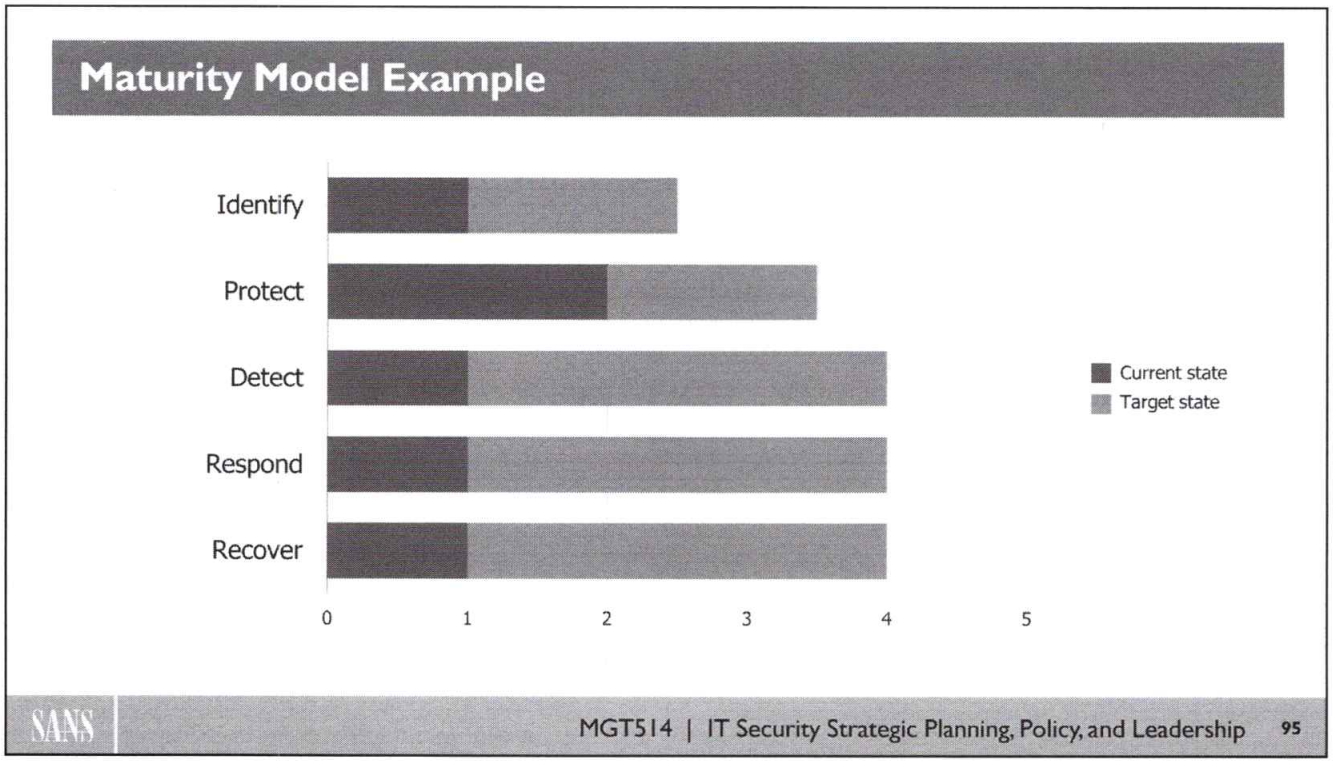
Level 1: Initial
Information security is weak and conducted in an ad-hoc manner. Security activities are typically not repeatable and focused on technical IT tasks. No formal security program exists.

Level 2: Repeatable
Processes are defined for specific projects but are reactive. Various stakeholders are beginning to communicate about security activities.

Level 3: Defined
Policies and rules are in place and some information security roles and responsibilities are established, but there is little accountability or enforcement. Information security efforts are still primarily IT-focused, and enterprise security awareness is still limited.

Level 4: Managed
Information security roles and responsibilities are clearly defined, and a formal information security committee with participation from business unit managers has been established. The enterprise is moving away from an IT-centric approach to information security, but business unit owners have not yet accepted explicit accountability for residual risk.

Level 5: Optimizing
Business unit managers now explicitly accept the residual risk associated with their use of information and technology and are accountable for security failures and policy violations. Continuous self-improvement practices are in place and are used to create a security-aware culture in the organization.



This is a useful way to visually represent the maturity of your security program. On the x-axis, we are using the five-point scale from the Capability Maturity Model. The y-axis has the five functional areas defined in the NIST Cybersecurity Framework. The current state and future state are clearly identified on the associated bars for each function. In this example, you can see that the Protect function has a higher maturity than the other areas. Perhaps this was by design or perhaps this is a result of an unintentional over investment in preventative security capabilities. By laying out security maturity in this manner, these types of trends can be identified and addressed by the leadership team.

Security Controls

- Strong security controls are the foundation of any program
  - This class is not intended to be a comprehensive review of control standards
- Commonly used control standards include:
  - Critical Security Controls (CSC)
  - Australian Signals Directorate (ASD) Top 35
  - NIST SP 800-53

The maturity of individual security capability areas (e.g., functions) is driven by the maturity of the people, process, and technology of associated security controls. Strong security controls are at the heart of any security program. There are a number of commonly used control standards including:

Critical Security Controls (CSC)

The Critical Security Controls are recommended actions that provide actionable ways to thwart the most pervasive attacks.

ASD Top 35

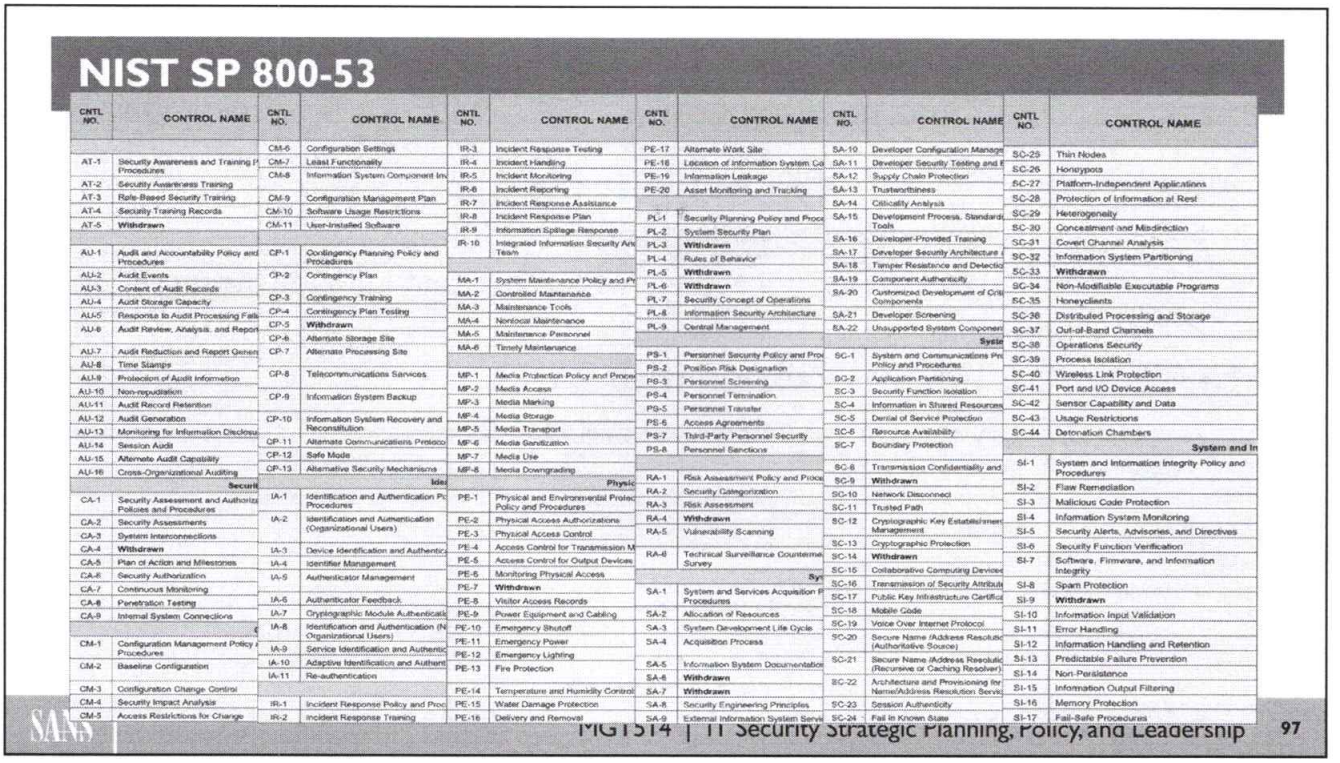
The Australian Signals Directorate (ASD) has developed "Strategies to Mitigate Targeted Cyber Intrusions" by analyzing cyber incidents, vulnerability assessments, and penetration tests conducted for various Australian government agencies. This list of strategies is ranked based on effectiveness, which has been calculated by including user resistance, upfront costs, and maintenance costs.

NIST SP 800-53

This is the standard required by U.S. government agencies to comply with the Federal Information Processing Standards (FIPS) 200 requirements. Although NIST SP 800-53 was created with government agencies in mind, it can also be applied to other industries and has been used as a model upon which other frameworks have been initiated.

References

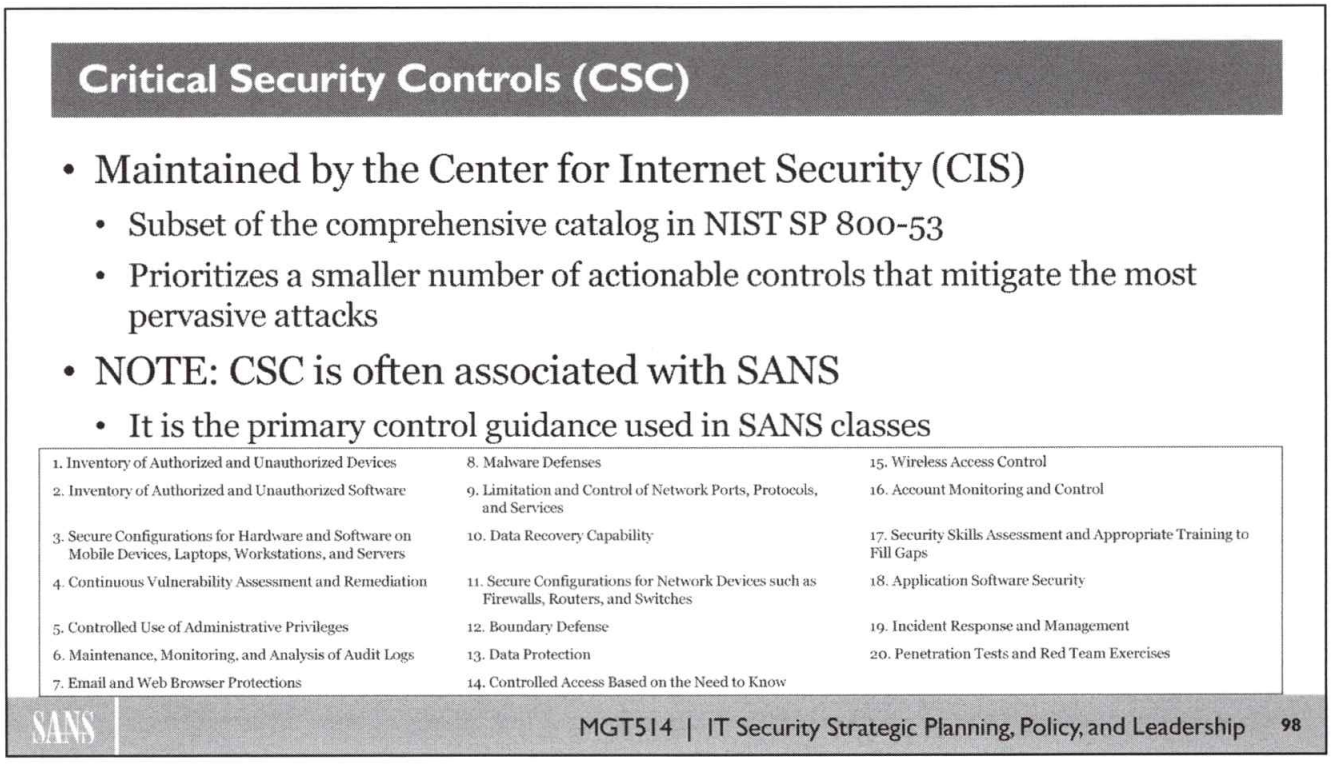
[1] https://www.cisecurity.org/critical-controls.cfm
[2] http://www.asd.gov.au/infosec/mitigationstrategies.htm
[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf



These are screenshots from the NIST Special Publication 800-53 revision 4 document[1] titled, "Security and Privacy Controls for Federal Information Systems and Organizations." NIST 800-53 is a comprehensive control catalog containing a large number of security controls that you can potentially use in your program.

Reference

[1] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf



The Critical Security Controls (CSC) are developed and maintained by the Center for Internet Security[1] and represent a subset of the comprehensive catalog in NIST SP 800-53. It prioritizes a smaller number of actionable controls that mitigate the most pervasive attacks. On the slide, you can see the Top 20 Critical Security Controls. Even though there are 20 high-level controls, there are actually over 180 sub-controls, which is still much less than what is defined in NIST 800-53.

The Critical Security Controls (CSC) are often associated with SANS, and it is the primary control guidance utilized in a number of SANS classes.

Reference

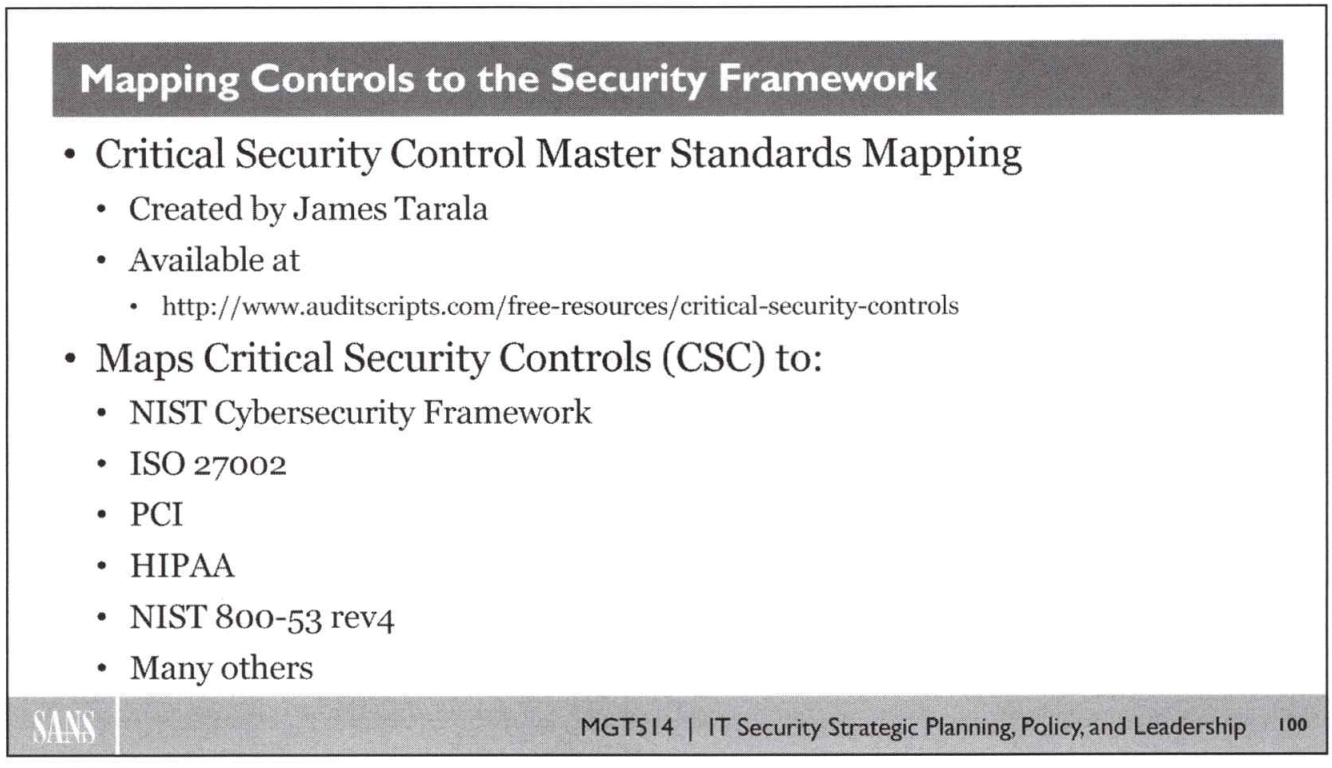
[1] https://www.cisecurity.org/critical-controls.cfm

Most Impactful Controls

- Focus on the controls that mitigate the most risk
  - Top four strategies (via ASD)
    - Controls that mitigate at least 85% of intrusion techniques seen by their SOC

Top Four
1. Application whitelisting
2. Patch applications
3. Patch the operating system
4. Minimize administrative privileges

The Australian Signals Directorate (ASD) has recognized the need to identify the controls that mitigate the most risk. The ASD, based on intrusion data seen by its Security Operations Center (SOC), has identified four controls that mitigate at least 85% of real-world intrusion techniques. Its data shows that focusing on 1) application whitelisting, 2) patching of applications, 3) patching of operating systems, and 4) limiting administrative privileges greatly reduces the available attack surface.



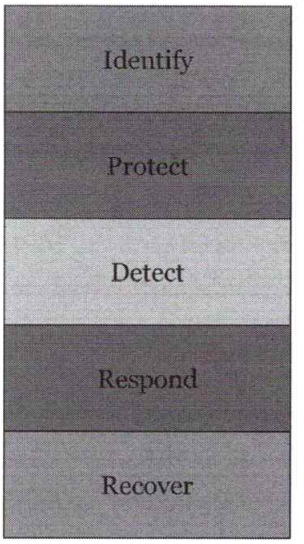
As mentioned, the primary control guidance utilized in SANS courses is the Critical Security Controls (CSC). However, different organizations might already use various security frameworks and control guidance. To help students rationalize the activities of their program with the CSC, SANS Instructor James Tarala has created the Critical Security Control Master Standards Mapping.[1] It maps the CSC to other commonly used security frameworks (for example, NIST Cybersecurity Framework, ISO 27000), compliance standards (for example, PCI, HIPAA), and control guidance (for example, NIST 800-53).

Reference

[1] http://www.auditscripts.com/free-resources/critical-security-controls/

In Summary

- Difficult to communicate need for security controls
  - Board, CEO, CFO, and business leaders don't understand security
  - Security often seen as a tax
- Utilizing a simple framework, we can highlight:
  - What security is doing
  - Areas of risk
  - Areas of over or under investment



With the growing number of data breaches and cyber intrusions, business leaders have an understanding of the importance of cyber security and the need to effectively manage security risks. However, these same business leaders have a difficult time understanding what it is that security needs to accomplish and how much should be invested. This is understandable. These business leaders are not and should not be expected to be security experts. They want to know the risk to the organization, what security is doing about it, and any areas that need additional investment. Using a commonly understood framework, like the NIST Cybersecurity Framework, can help frame the work of the security team in an easier-to-understand manner. By determining the current and target state maturity of these various capability areas, the security team can greatly improve the dialogue with senior business leaders.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - *Gap Analysis*
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

Gap Analysis

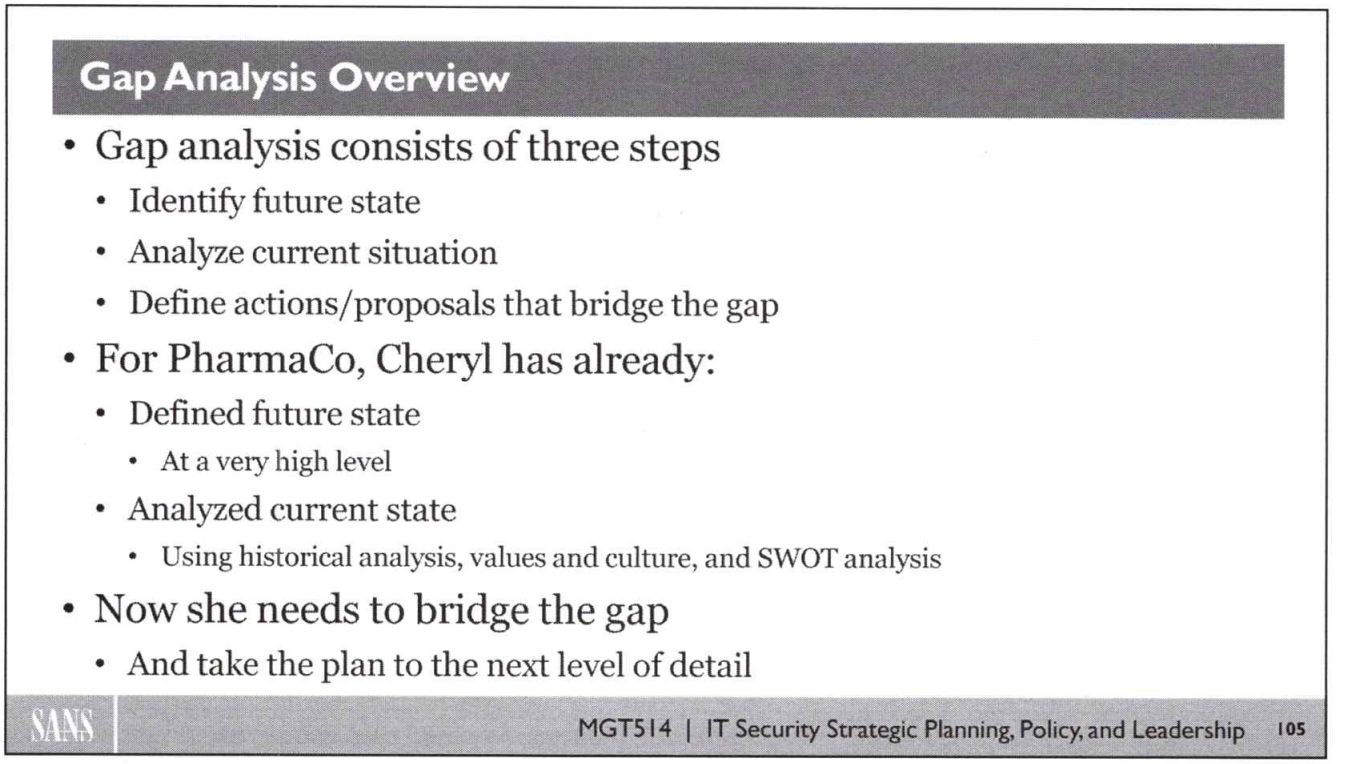
- Goals of this section
  - Understand Gap Analysis and how it can be used to identify candidate initiatives
  - Brainstorm initiatives to improve your security program

In this section, you will learn about Gap Analysis and how it can be used to identify candidate initiatives for your security program.

PharmaCo Case Scenario

- Cheryl Miller has been promoted to interim CISO
  - Her ability to connect with business leaders and socialize with key stakeholders have quickly allowed her to gain support across the company
- Was able to sell the vision
  - "Help people lead healthier lives by creating safe spaces for drug research and innovation"
- Now she has to put together a plan to improve the security team
  - Gap Analysis that will feed into a business case for the security program

Your good friend Cheryl Miller has just been promoted to interim CISO of PharmaCo. This is a great accomplishment that was the result of her hard work in connecting with senior business leaders in the organization. She took the time to understand that PharmaCo is driven to help people through drug research and innovation and was able to put together a high-level strategic plan to improve the security team that resonated with her boss the CIO. Now she needs to flush out the details of this high-level plan to identify specific actions and projects that she needs to initiate.



Gap Analysis consists of performing three steps:

1) Identifying the future state
2) Analyzing the current situation
3) Defining actions/proposals that bridge the gap between current and future state

In our example, Cheryl Miller has already defined the future state at a very high level. Through the visioning process and conversations with C-level and business leaders, she has identified a vision for security at PharmaCo: "Help people lead healthier lives by creating safe spaces for drug research and innovation." Her engagement with senior leaders in developing this mutually agreed-upon vision is key. It turns stakeholders into partners by obtaining their buy-in. Cheryl has also done the hard work of analyzing the current state of the organization using historical analysis, understanding the values and culture of the organization, and performing a SWOT analysis. This helps ensure that she understands current organizational obstacles, determines the norms for getting work done, and identifies areas of strength and weakness. Now, Cheryl just needs to bridge the gap and identify actions that will bridge the gap.

PharmaCo SWOT Analysis Refresher

	Helpful	Harmful
Internal	**Strengths** • Business mission to help people lead healthier lives • Culture of innovation and R&D • Ability to create breakthrough new drugs • Decentralized business units allow quick innovation • Strong geographic presence • Access to talent around the world	**Weaknesses** • No CISO or central security responsibility • Security is decentralized and understaffed • No central threat strategy • Technology is under utilized • Slow deployment of clinical trials • Aging workforce—key thought leaders near retirement
External	**Opportunities** • Hire a CISO • Operationalize around the kill chain • Organize personnel to improve security effectiveness (combining physical & info sec) • Leverage global presence to build 24x7 team • Increase staffing levels	**Threats** • Insider threat—geographically dispersed workforce and risk of data loss • Competitors—seeking intellectual property • Nation state—seeking to accelerate R&D • Regulatory—increased regulation results in delays getting new drugs to market

Before getting into the Gap Analysis, it is useful to review the SWOT analysis (from a previous section) that Cheryl conducted. A number of these strengths, weakness, opportunities, and threats will inform the current state analysis that leads to specific recommendations for improving the security program.

Gap Analysis Future & Current State

Function	Future State	Current Situation	Actions/Proposals
Identify	Centralized security governance to provide comprehensive risk management	Security is decentralized across business units	
Protect	Protect key systems and processes used for drug research, development, & trials	Security protections are not consistently applied	
Detect	Ability to quickly detect threats targeting intellectual property	Inability to detect malicious or negligent activity	
Respond	Ability to minimize data loss, block attacks, and determine root cause	Inability to mitigate attacks and limit the amount of data lost	
Recover	Capability to quickly return to normal operations and limit business impact of incidents	Recovery and business continuity is decentralized	

Based on the SWOT analysis, Cheryl has mapped some of the weaknesses to the five functions from the Cybersecurity Framework:

- **Identify**: Security is decentralized across business units.
- **Protect**: Security protections are not consistently applied.
- **Detect**: Inability to detect malicious or negligent activity.
- **Respond**: Inability to mitigate attacks and limit the amount of data lost.
- **Recover**: Recovery and business continuity is decentralized.

She has also identified the future state goal for each of these five functions:

- **Identify**: Centralized security governance to provide comprehensive risk management
- **Protect**: Protect key systems and processes used for drug research, development, and trials
- **Detect**: Ability to quickly detect threats targeting intellectual property
- **Respond**: Ability to minimize data loss, block attacks, and determine root cause
- **Recover**: Capability to quickly return to normal operations and limit business impact of security incidents

Exercise 2.3 – Gap Analysis Actions

Estimated Time: 20 Minutes

- Goal of this exercise
  - Develop proposed actions that can bridge from current state to future state
- Step-by-step exercise for PharmaCo
  - Review Future State & Current Situation
  - In the Actions/Proposals column:
    - Write down three proposed actions for each function on the previous slide

NOTE

Don't read the next section

It contains a debrief and potential exercise answers

The goal of this exercise is to develop proposed actions that will help PharmaCo go from its current state to the future for each of the five functions defined in the Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover).

For each of the functions on the previous slide, review the Future State and Current Situation columns. Then, in the Actions/Proposals column, write down three proposed actions that can help PharmaCo bridge the gap. These can be anything including technology initiatives, process improvement ideas, or organizational changes involving people.

Exercise Debrief

Note that this section contains a debrief and potential exercise answers

This page intentionally left blank.

Exercise 2.3 – Debrief

- Gap Analysis
  - Helps identify key actions to improve your program
  - Actions can be qualitative or quantitative
    - Use metrics where appropriate
- Technology is just one component
  - Obstacles and constraints are also people and process driven
  - Need to create appropriate countermeasures to ensure success of your initiatives

Gap Analysis helps you identify key actions to improve your program. These actions can be qualitative or quantitative. For example, using metrics like "reducing response time by 25%" or "increasing ability to detect advanced threats by 20%" can help your team identify specific measures that need to be taken to reach the goal.

Oftentimes, security teams focus on technology-based solutions. It's important to remember that technology is just one component of the overall solution. Based on your understanding of the organization (from your Values & Culture analysis) as well as the SWOT, you need to be aware of key obstacles and constraints that might exist in the organization. For example, a culture without a strong focus on process can make it difficult for the security team to implement new process-driven initiatives like DLP that require regular input from key business stakeholders. Additionally, certain influential people in the organization might not agree with certain security activities. As a leader and manager, you have to recognize these obstacles and develop the appropriate countermeasures to ensure the success of your initiatives.

Gap Analysis Sample Actions

Function	Future State	Current Situation	Actions/Proposals
Identify	Centralized security governance to provide comprehensive risk management	Security is decentralized across business units	Name a permanent CISO Develop central policy library Implement vuln management program
Protect	Protect key systems and processes used for drug research, development, & trials	Security protections are not consistently applied	Decrease patch deployment time Protect clinical trial systems Deploy systems in blocking mode
Detect	Ability to quickly detect threats targeting intellectual property	Inability to detect malicious or negligent activity	Deploy continuous monitoring & log management capability Advanced analytics and reporting Implement DLP to monitor IP loss
Respond	Ability to minimize data loss, block attacks, and determine root cause	Inability to mitigate attacks and limit the amount of data lost	Build and staff 24x7 SOC Develop advanced forensics team Create threat intelligence capability
Recover	Capability to quickly return to normal operations and limit business impact of incidents	Recovery and business continuity is decentralized	Develop business continuity plan Regularly test response plan Socialize & communicate with BUs

This slide identifies some potential actions that PharmaCo could take to improve its security program. For example, in the "Identify" row, the current state of security being decentralized across business units can make it more challenging to provide comprehensive governance and risk management. Naming a permanent CISO with overall enterprise accountability for security risk can help move the organization towards a more centralized governance structure. Developing a centralized policy library will also help. It's important to keep in mind, though, that just having a central policy library alone will not drive the organization. Establishing a policy steering committee with representation from key stakeholders helps institutionalize the work of the security team and helps ensure that key stakeholders are engaged in the process of governing the organization.

As another example, in the "Detect" row, the current state is an inability to detect malicious or negligent activity. This includes key intellectual property that might be lost or stolen. One potential solution is implementing a Data Loss Prevention (DLP) capability. However, in addition to the technology, it is important to remember identifying a business owner for this new initiative will be key. The business owner must weigh in on what constitutes intellectual property and what actions should be taken to mitigate risk.

There are a number of potential actions listed on this slide that can be taken by the security team. However, they can't all be done at the same time. The next step is to develop a roadmap for ordering these important initiatives.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - *Security Roadmap*
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

Security Roadmap

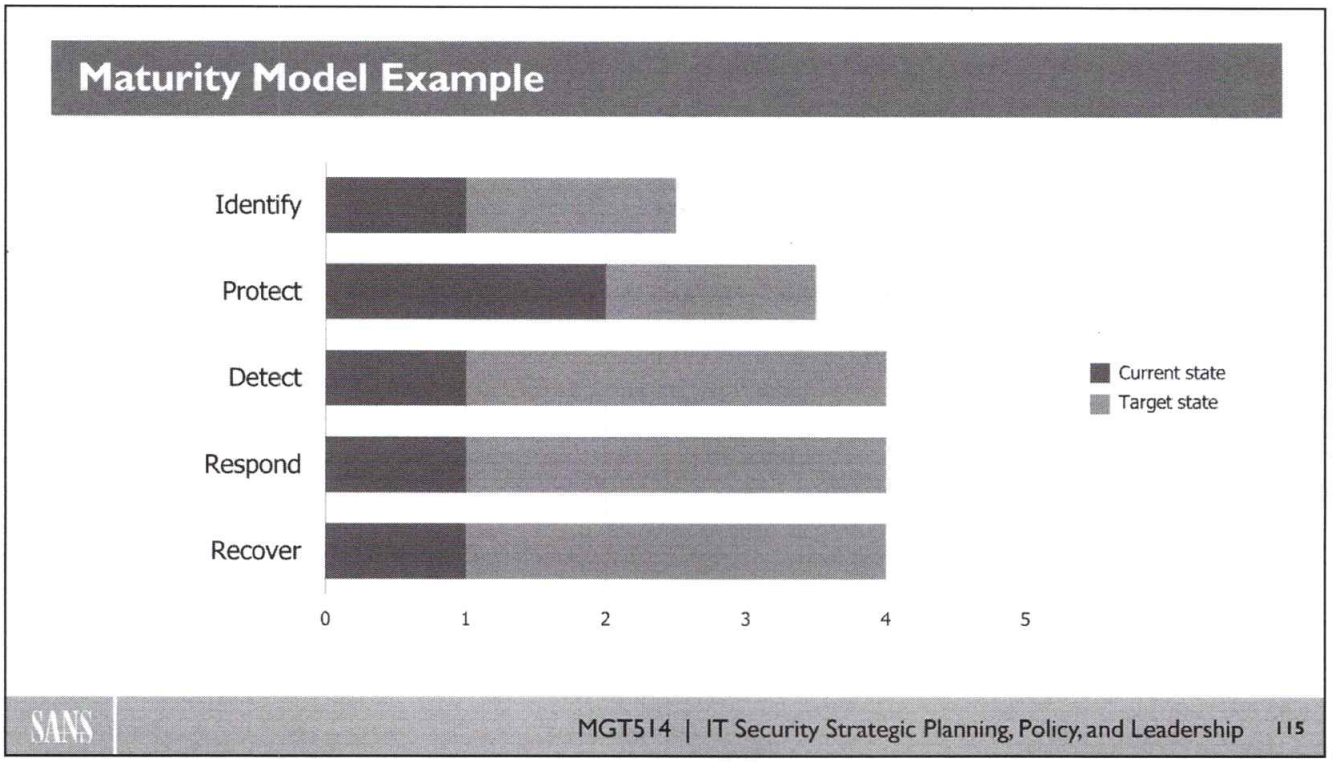
- Goals of this section
  - Learn the steps for developing a roadmap for your security program
  - Understand how previous steps in the strategic planning process assist in developing your roadmap

In this section, you will learn the steps for creating a roadmap for your security program and how previous steps in the strategic planning process inform that roadmap.

PharmaCo Case Scenario

- Cheryl Miller and her team:
  - Completed the gap analysis
  - Identified numerous initiatives to close gaps
  - Want to move forward on implementing solutions
- Don't have resources to do everything at once
  - Budget and staff need to be put in place
  - Can only mature security capabilities at the rate
    - At which the organization can accept them
    - That you can successfully deploy them

Cheryl Miller and her team have completed the gap analysis and identified numerous initiatives to close the gaps. They are eager to move forward on implementing solutions but don't have the resources to do everything at once. It takes time to put the budget and corresponding staff in place. Additionally, it takes time to implement new capabilities. Cheryl recognizes that it can take 3-5 years to build and mature a world-class security program and that she can roll out only new capabilities at the rate at which the larger organization can accept them. As a result, she is rightly focused on developing a roadmap that lays out the activities of the security program in the step-wise fashion.



This is the example maturity model from a previous section that shows the current state and target state for each of the five Cybersecurity Framework functions. Given the amount of work it takes to get from Level 1 to Level 4, it should be obvious that this cannot be accomplished overnight. Instead, this slide is a reminder that we have to make a gradual progression in improving the maturity of the security program.

Roadmap Development

Three-step process

1) Identify what is being done today
2) Map current capabilities to maturity levels
3) Prioritize new initiatives to increase maturity

Developing a roadmap consists of three steps:

1) **Identify what is being done today**

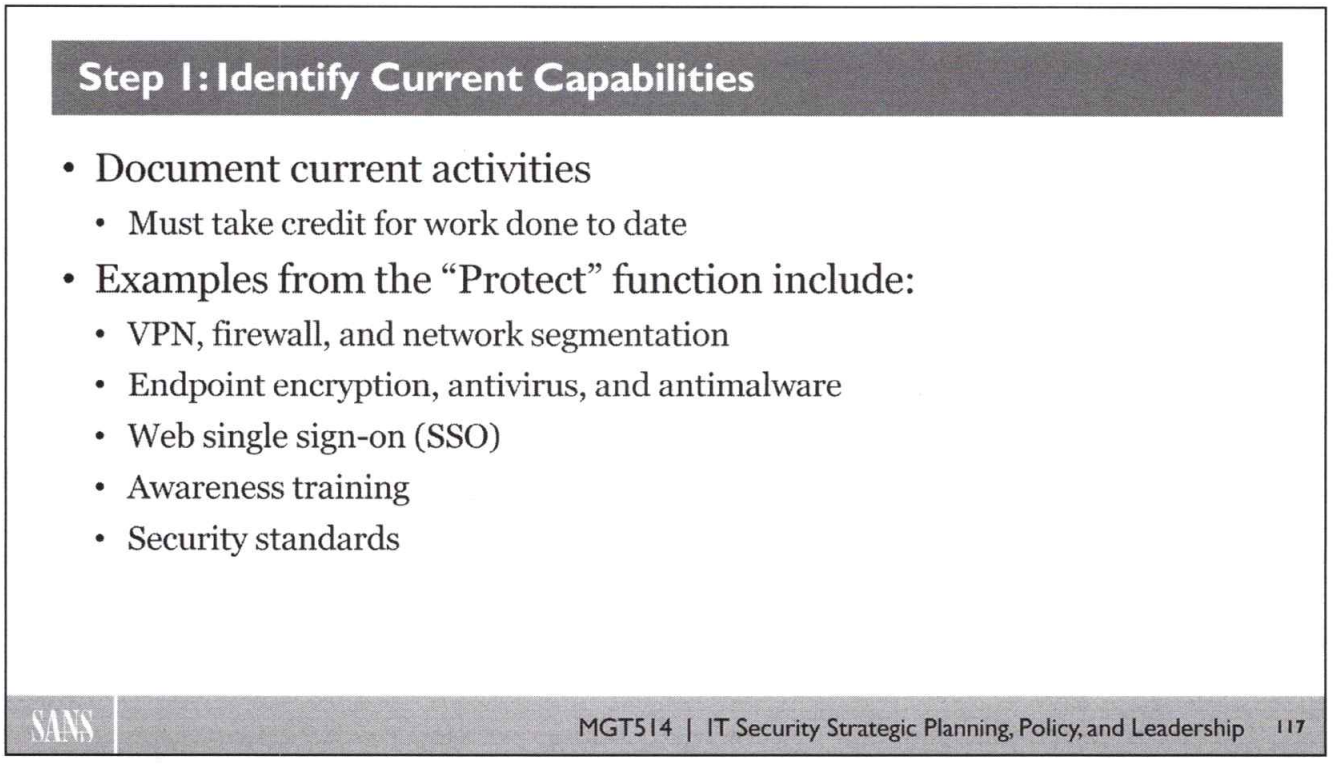
By cataloging the work of the security team, you not only begin to identify what else needs to be done but you also take credit for all the work that has been done to date. Don't underestimate the power of highlighting to leadership everything that the team has and is currently working on.

2) **Map current capabilities to maturity levels**

Ideally, the framework that you utilize will define capabilities that are required in each maturity level. However, many frameworks often do not get into enough detail to provide useful guidance in measuring current state maturity. This is in part due to the fact that every organization is, in fact, different. This is why various consulting firms offer maturity assessments because they can normalize information that they receive from various assessments across their customer base. Different organizations have different priorities and business drivers that affect where they are and where they might want to go in their security journey. As a result, the identification of specific capabilities in maturity level can sometimes be specific to the organization at hand.

3) **Prioritize new initiatives to increase maturity**

With the understanding that security initiatives can be organization-specific, the final step is to prioritize the work so that it can be done in an order that provides the most value for the organization.



Step 1 of roadmap development includes identifying current capabilities. What is it that the security team does today?

As an example, let's take the "Protect" function of the Cybersecurity Framework. This function includes many traditional security capabilities like network security (e.g., VPN, firewall, and network segmentation), endpoint protection (e.g., encryption, antivirus, and antimalware), authentication (e.g., SSO), as well as training and standards. Identifying the work done to date helps inform subsequent steps.

Step 2: Map to Maturity Levels

Function	Category	Level 1	Level 2	Level 3	Level 4	Level 5
Protect	Access Control	VPN Firewall Segmentation	Web SSO	Federated SSO		
	Awareness & Training	Basic awareness training	Phishing exercises			
	Data Security	Encryption data at rest and in-transit	Data segregation Asset destruction			
	Processes & Procedures	Security standards Change control	Integration with HR processes Incident response plan	Security development process		
	Protective Technology	Network and host security	Web application security program	Mobile application security		

Done today
Started doing
Start immediately
Plan to start

Step 2 of roadmap development includes mapping the initiatives identified in the previous step to specific maturity levels. For example, most people would agree that "basic" protections like VPN and firewall are Level 1 capabilities. On the slide, you can see that they are part of the "Access Control" category defined in the Cybersecurity Framework. More advanced capabilities would be implemented at higher maturity levels.

It's also useful to differentiate items that are done today, items that you have started doing, and items that you should start immediately or plan to start sometime in the future.

Step 3: Prioritize New Initiatives

- Determine which initiatives to prioritize to bridge the gap
  - Cost should not be the only factor
  - Incorporate business value and threat defense
  - Takes into account ability to execute and organizational support

Step 3 of roadmap developing includes prioritizing initiatives. What should be done first? A number of factors should be taken into account when prioritizing new initiatives including cost, value to the business, ability to defend against threats, and the ability to actually execute on the work and implement the solution.

Decision Matrix Analysis

- Tool to rank initiatives and inform decisions
  - While taking multiple factors into account
- Rank each factor from 0-5

Initiative	Cost	Ability to Execute	Stakeholder Support	Threat Defense	Total
Initiative #1					
Initiative #2					
Initiative #3					
Initiative #4					
Initiative #5					

Decision Matrix Analysis is a simple tool that can be used to rank initiatives and inform your decision making. It is the simplest form of Multiple Criteria Decision Analysis (MCDA) and provides a way for you to rank multiple factors in your decision making. In this example, we are ranking initiatives based on four key factors:

1) **Cost**

How much does this initiative cost? Will we get a better bang for the buck by investing in a different initiative? Again, this should be only one factor in your decision-making process.

2) **Ability to Execute**

If we decide to move forward with a specific initiative, do we have the skills and ability to execute? If we want to build an advanced analytics capability, do we even have basic analysis capabilities on hand to serve as a foundation? Or, do we need to hire an entirely new skill set?

3) **Stakeholder Support**

This item is meant to encompass overall business support and value. Do our key stakeholders value the initiative? What problem is it solving for them? Have we articulated the vision appropriately?

4) **Threat Defense**

How well does this capability protect us against existing and emerging threats? Does it allow us to detect threats more effectively? Is there overlap with other security capabilities?

Decision Matrix Analysis Example

- Simple tool to start ranking initiatives

Initiative	Cost	Ability to Execute	Stakeholder Support	Threat Defense	Total
Mobile & BYOD	3	5	5	4	17
DLP	2	3	4	5	14
Centralized Vulnerability Management	2	4	3	5	14
Risk-Based Authentication	3	3	4	3	13
Network Access Control	1	2	2	4	9

This slide lists five sample initiatives from the PharmaCo Gap Analysis in a previous section.

In the "Cost" column, a higher number indicates a more favorable score in that the initiative is not that expensive. For example, overhauling the network design to implement Network Access Control is an expensive proposition and received a low score of "1." In the other columns (Ability to Execute, Stakeholder Support, and Threat Defense), higher scores also indicate a better ability to deliver on those initiatives.

The "Total" column simply adds up the scores of the other columns. This simple analysis can be modified to weigh certain factors more heavily than others. For example, in an extremely cost conscious organization, you might weigh the "Cost" column more heavily, whereas in a very consensus-driven organization, you might weigh "Stakeholder Support" more heavily.

Protect Function Example Roadmap

Function	Category	Level 1	Level 2	Level 3	Level 4	Level 5
Protect	Access Control	VPN Firewall Segmentation	Web SSO	Federated SSO	Risk-based authentication	Network Access Control
	Awareness & Training	Basic awareness training	Phishing exercises	Role-based training	Executive education	Third-party training program
	Data Security	Encryption data at rest and in-transit	Data segregation Asset destruction	DLP (e-mail & host)	DLP (cloud data storage)	Self protecting data
	Processes & Procedures	Security standards Change control	Integration with HR processes Incident response plan	Security development process	Centralized vulnerability management	Continuous feedback with business processes
	Protective Technology	Network and host security	Web application security program	Mobile application security	BYOD security	Cloud security program

Done today
Started doing
Start immediately
Plan to start

Once the analysis is complete and you have prioritized your new initiatives, you can update your roadmap table to look something like the following. By placing different initiatives at varying maturity levels and marking them as "Done today," "Started doing," and "Start immediately," you convey to leadership that you have a plan (that follows a high-level framework) for improving the maturity of the security program. At this point, based on detailed project plans and staffing estimates, you can also assign target dates to the various initiatives and maturity levels.

In Summary

- Topics we have covered in the strategic planning process:
  - Leads up to the creation of your roadmap
- Understanding of the business and threats make it much easier to create your roadmap
  - Vision & Mission
  - Stakeholder Analysis
  - Threat Analysis
  - SWOT Analysis

In many respects, the roadmap is the end product of the strategic planning. All the activities that you previous conducted to understand the business (for example, Vision & Mission, and Stakeholder Analysis), understand the threats (for example, Threat Analysis), and analyze current state (for example, Values & Culture, and SWOT Analysis) have led you to this roadmap. Although it appears simple, all the deep thinking, analysis, and relationship building you performed throughout the process has made it much easier for you to create the roadmap.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- ***Build the Program***
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

How to Build the Program

1) Understand how to gain support and funding
   - Learn approaches for building a security business case
2) Map current capabilities to maturity levels
   - Build metrics and dashboards
3) Prioritize new initiatives to increase maturity
   - Develop effective marketing and executive communications

Building an effective security program is not just about developing a vision, developing a strategic plan, and executing on the technical aspects of that plan. As a leader and manager, you must also:

1) **Gain support and funding**

Without support and funding, your initiatives will not get off the ground. Understanding how to build a viable security business case is an important part of obtaining this support.

2) **Measure and report on security activities**

There's a saying, "What gets measured gets managed." Successful security leaders build metrics and dashboards that can be suitable for various levels of the organization.

3) **Promote your strategic efforts**

Our key stakeholders are extremely busy. Sometimes we have to remind them of the great work being done by the security team. This means that you have to develop effective marketing and executive communications.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - ***Business Case Development***
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

Business Case

- Goals of this section
  - Learn approaches for building a business case
    - How to justify your resource requests
  - Understand the components of a business case
    - Most companies have a formal business case template

In this section, you will learn approaches for building a security business case. Typically, IT security investments are a "cost of doing business" because they do not generate a return on investment. As a result, it's extremely critical that your resource requests have appropriate justification. By understanding the basic components of a business case and leveraging formal business case templates that you might have in your organization, you can gain improved support for your security initiatives.

Why Create a Business Case?

- Executive leadership is responsible for making sound decisions on the effective use of company resources
  - Business case helps estimate the costs and benefits of various initiatives
  - Helps management determine resource allocations
    - Level of effort and upcoming projects
    - Understand broader organizational constraints

Before gaining support for our security initiatives, we must understand that executive leadership is looking at security as just one risk and opportunity that needs to be addressed. By creating a comprehensive business case, we help management prioritize and determine appropriate resource allocations. For example, should executive leadership invest in new factory upgrades that could improve production or invest a portion of that money in improving information security? By providing a business case that clearly lays out the estimated costs and associated benefits, we put executive leadership in a position to make sound decisions that incorporate broader organizational constraints.

What Is a Business Case?

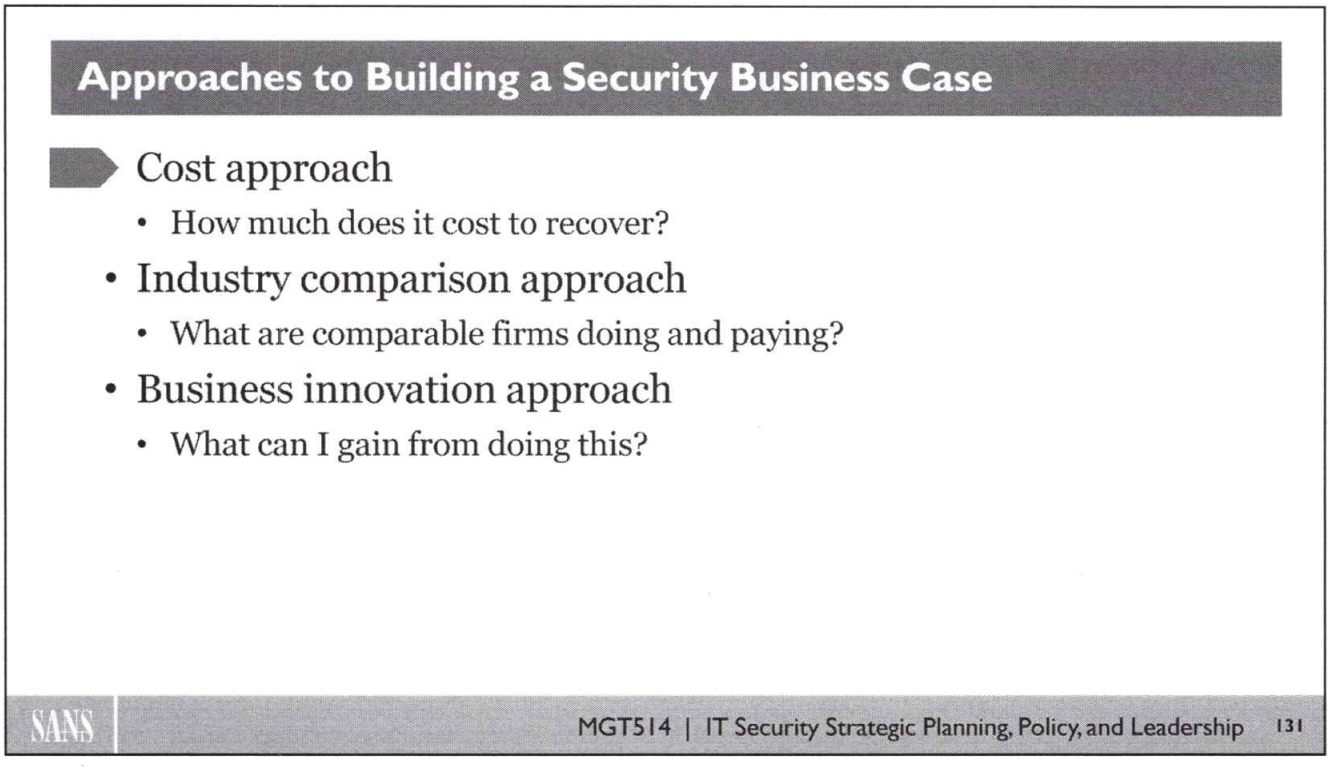
- Captures the reason for initiating the effort
  - Includes underlying assumptions and rationale
- Clearly estimates the cost and benefits
  - This usually means revenue
- Provides a detailed description and analysis of the initiative
  - Can be created in many forms including document, presentation, or spreadsheet

Simply put, a business case captures the reason for an initiative. It lays out a problem and the potential solution(s). Typically, this involves a new investment that could result in increased revenue. But, in the case of information security, the hard costs are usually associated with softer benefits. The more detailed that can be included in the analysis will go a long way in making executives more comfortable with your funding request. Your organization might have a standard template that includes documents, presentations, and spreadsheets for analysis.

Security Business Case Traps

- "If we don't do this, we'll get hacked"
- "It's the right thing to do"
- "This new technology will solve all our problems"
- "It doesn't cost that much"
- "Management doesn't get it"

Technical security professionals sometimes get frustrated with executive management for a perceived lack of interest in information security. To them, it seems obvious that a lack of security investment will result in getting hacked. Building out advanced security capabilities are obviously the "right thing to do." Sometimes solutions are technology focused: "This new technology will solve all our problems." These reasons, which presume that "Management doesn't get it," will not get you support or funding. Instead, the focus should be on building a comprehensive business case that incorporates a number of different factors for justifying the investment.



Before getting into the approaches for building a security business case, let's talk about the three approaches for appraising real estate. When you get an appraisal on your home, the report includes three approaches for calculating value:

1) **Cost approach:** How much would it cost to rebuild your home if it was destroyed?
2) **Sales comparison approach:** What are others paying for similar homes? This typically is calculated on a cost-per-square-foot basis.
3) **Income approach:** What is the revenue that I can make on this property?

The most appropriate appraisal method depends on the type of property and the type of buyer. For commercial real estate (e.g., office buildings), appraisers might prefer the income approach. For single family homes, the sales comparison approach is preferred. And for special use properties (e.g., marina), appraisers might prefer the cost approach. The key word here is *prefer* because the choice of a valuation method can depend upon the circumstances. For example, a single family home that is located in a neighborhood with primarily rental units might prefer a combination of the sales comparison and income approaches. All three approaches can inform the value of the property.

We can take a similar approach to building a security business case by focusing on the following:

1) **Cost approach:** If I get breached, how much will it cost to recover?
2) **Industry comparison approach:** What are comparable firms doing and paying?
3) **Business innovation approach:** What can I gain from investing in security?

Cost Approach

- Typically calculated using cost-per-record lost
- Ponemon Cost of Data Breach Study
  - $221 per record in 2016
  - $217 per record in 2015
  - $201 per record in 2014
  - $188 per record in 2013
- These numbers include direct and indirect costs
  - Engaging forensics experts, free credit monitoring
  - In-house investigations and communication
  - Extrapolated value of customer loss

Every year, the Ponemon Institute publishes its Cost of Data Breach Study, which analyzes security breaches around the world. Over time, the cost-per-record loss has been gradually increasing. In the United States, which has the highest per-record cost, the figure increased from $188 to $201 and $217 to $221 per record from 2013-2016. There is significant variation among the sampled countries that resulted in consolidated averages for all countries of $145, $154, and $158 per record from 2014-2016, respectively.

These numbers include direct costs such as engaging forensics experts, providing free credit monitoring to affected customers, as well as conducting in-house investigations and communications. Also included are indirect costs such as customer loss, diminished customer acquisition rates, reputational damage, and loss of goodwill.

Using these numbers (or the country-specific ones in the report[1]), a basic cost calculation can be done to estimate the cost to recover from a data breach.

Reference

[1] Ponemon Cost of Data Breach Study, http://www-03.ibm.com/security/data-breach/

Cost Approach Issues

- Not always accurate
  - Overestimates cost of large breaches
  - Underestimates cost of small breaches
- Verizon applied cost-per-record approach to cyber insurance claims data
  - Resulted in an estimated loss of only 58 cents per record

However, a simple, linear cost calculation would result in overestimating the cost of large breaches by a significant amount. This is perhaps one reason why Ponemon does not include data breaches of more than 100,000 records in its analysis. On the other end of the spectrum, a linear cost-per-record approach would also underestimate the cost of small breaches.

In its annual Data Breach Investigations Report[1], Verizon started to develop a modified approach. It analyzed data provided by NetDiligence about real losses paid on 191 cyber insurance claims. By conducting a log-scale analysis instead of a linear cost-per-record analysis, it estimated breach costs of only 58 cents per record! This low figure is problematic because indirect costs aren't included in the insurance claim data and the Ponemon data does not include breaches of more than 100,000 records.

Reference

[1] http://www.verizonenterprise.com/DBIR/

Ranges of Expected Loss

- Verizon developed a modified log-scale approach

RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

In addition to record count, Verizon attempted to identify other factors that could contribute to breach costs. After much analysis, it determined that there are other factors involved but, because there is insufficient data, it is unknown what those factors are. These factors could be having robust incident response plans, lawyers on retainer, increased executive support. They just don't know. At present, the number of records lost is still the best gauge of breach costs.

The table above has columns that show 95% confidence intervals for average and predicted loss based on record count. As you can see, smaller breaches have higher cost-per-record amounts than larger breaches. This lookup table can be used to provide estimates for average and predicted losses on the lower and upper ends of the spectrum.[1]

Reference

[1] http://www.verizonenterprise.com/DBIR/2015/

Approaches to Building a Security Business Case

- Cost approach
  - How much does it cost to recover?
- Industry comparison approach
  - What are comparable firms doing and paying?
- Business innovation approach
  - What can I gain from doing this?

This page intentionally left blank.

Industry Comparison Approach

- What is reasonable for security based on:
  - Industry
  - Size
  - Market position
  - Region
- Can be analyzed via:
  - Spending comparison
  - Maturity comparison

Executives and business leaders want to know what a "reasonable" level of security spending for the organization is. They want to make sure that limited resources are being spent appropriately and that the firm is not overinvesting or underinvesting in certain areas. Basically, business leaders are looking to you to help answer the question, "How much should I spend on security?" The answer is complex and depends on a number of factors.

Certain industries tend to spend more on cyber security. For example, the financial services industry tends to spend more on security. James Dimon, the CEO of JP Morgan Chase, stated that the company would double its spending on cybersecurity from $250 million annually over the next five years.[1] This was in response to a breach that affected 76 million households.[2] So, it's not only because JP Morgan Chase is a financial services company. It's also because of its size. It holds a large amount of sensitive customer information. As a global company, it is one of the worldwide leaders and brands in financial services. In short, it has a lot to lose by not investing in a world-class cyber security organization.

In contrast, a small credit union that serves a specific state or even a specific county does not have as much at stake. Even though the credit union is also in the financial services industry, its profile is vastly different from that of JP Morgan Chase. Moreover, differences also exist based on country. This is represented in the Ponemon breach costs with India having a much lower cost-per-record breach cost than the United States ($56 vs. $217).[3]

Spending is one way that maturity can be compared across firms. Comparing the maturity of security capabilities is another useful approach that we cover later in this section.

References

[1] http://www.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976

[2] http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372

[3] 2015 Ponemon Cost of Data Breach Study, http://www-03.ibm.com/security/data-breach/

Spending Comparison

- Percent of IT budget spent on security
  - Provides only a rough understanding of performance
  - Research from Gartner
    - 5.1% in 2013
    - 4.7% in 2012
    - 4.2% in 2011
- Can be a problematic metric
  - Depends on what is included in the percentage
  - Spending averages might not be a fit for every org
  - Do not make this the sole or primary focus of your business case

One way to compare your security spending to that of other organizations is by looking at the percent of the IT budget that is spent on security. According to a Gartner research paper entitled, "Don't Be the Next Target - IT Security Spending Priorities 2014"[1] companies, on average, spent 5.1% of the IT budget on security in 2013, 4.7% in 2012, and 4.2% in 2011. This measure provides a very rough understanding of organizational maturity and can indicate whether spending has been focused solely on meeting mandatory requirements (e.g., compliance), has expanded to necessary requirements (e.g., improving due diligence), or has progressed to elective spending (e.g., optimizing security capabilities). Although this metric can help highlight certain areas that might need further analysis, it is also very problematic. These spending averages might not be a fit for every organization because of differences in industry, size, region, culture, and business goals. Moreover, different organizations might include varying items in the overall "security" budget. For example, some organizations might include identity and access management, business continuity, and disaster recovery costs in these numbers, whereas others might not. The main takeaway is that this metric should not be the sole focus of your business case.

Reference

[1] https://www.gartner.com/doc/2703221/dont-target--it-security

Maturity Comparison

- What are other companies doing?
  - What is a reasonable level of maturity?
- Where can we get comparable data?
  - Information Sharing and Analysis Centers (ISAC)
    - FS-ISAC, REN-ISAC, etc.
  - Community projects
    - BSIMM, OpenSAMM, etc.
  - Research and consulting organizations
    - Gartner, Big Four, security service firms, etc.

Comparing maturity of security capabilities is a good way to get a sense of what other companies are doing and, by extension, what is a reasonable level of security for your organization. However, one problem exists. Where do you get the data to compare yourself with others?

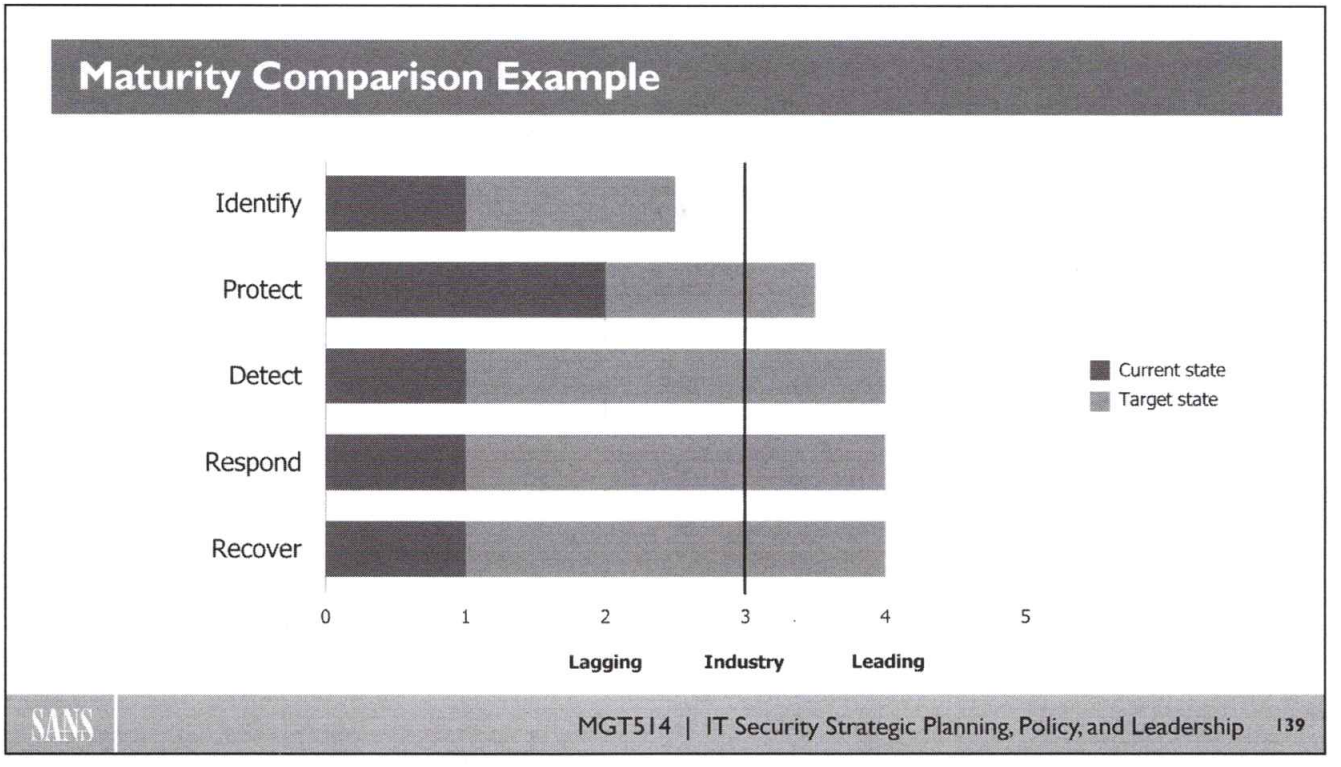
One good way to get information is by joining an Information Sharing and Analysis Center (ISAC). Various ISACs have been formed to represent different sectors of critical infrastructure such as Financial Services (FS-ISAC), Research and Education (REN-ISAC), and National Health (NH-ISAC). The mission of the ISACs is to "advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government."[1] ISACs provide a forum to develop relationships with industry peers, share information and best practices, and even conduct incident response exercises. The information gleaned from these interactions can help you gauge your relative level of maturity.

The data from various community projects can also be useful in evaluating your organization's maturity. The Building Security In Maturity Model (BSIMM)[2] is a collection of data about software security programs at various leading organizations. The Open Software Assurance Maturity Model[3] provides a similar framework for software security programs. Although these two models are focused only on a subset of information security, they contain broader components, like strategy and vulnerability management, that are central to an information security program.

It can be difficult to obtain current and comprehensive data regarding your industry peers. As a result, many organizations hire a third-party firm to conduct maturity assessments. This can provide some assurance that an appropriate level of benchmarking against actual data was conducted. Gartner, the Big Four (Deloitte, PwC, EY, and KPMG), and other professional services firms provide consulting services around industry benchmarking and analysis.

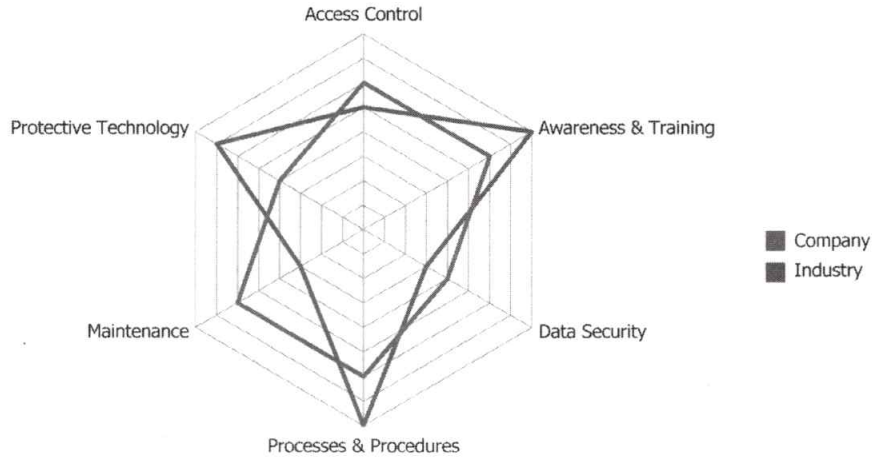
References

[1] http://www.isaccouncil.org
[2] https://www.bsimm.com
[3] http://www.opensamm.org



This is the example maturity model graph from earlier in the course. Each bar graph represents the current and target state maturity for each security capability area (Identify, Protect, Detect, Respond, and Recover). By agreeing upon an "industry standard" level of maturity, your company can begin to determine the appropriate level of investment required for each security capability. Over time, you can show incremental progress toward the target state by updating the maturity level for each specific capability.

BSIMM Maturity Comparison Example



This is an example radar chart (also known as a spider chart, or star chart) that represents your company's maturity level compared to your overall industry for various security capabilities in the Protect area of the NIST Cybersecurity Framework.

For example, the left-hand side of the radar chart shows that your firm is extremely strong in Protective Technology compared to the rest of the industry. This could indicate an over investment in this area or it could indicate a purposeful, strategic decision to grow this capability due to the nature of the organization's business. These radar charts are very helpful for showing differences in industry maturity levels for varying capabilities. In this specific case, it is important for Dennis to understand why certain areas might have an over or under investment.

Approaches to Building a Security Business Case

- Cost approach
  - How much does it cost to recover?
- Industry comparison approach
  - What are comparable firms doing and paying?
- Business innovation approach
  - What can I gain from doing this?

This page intentionally left blank.

Business Innovation Approach

- Plan security investments based on:
  - Business opportunities
    - Key enterprise initiatives
    - Process improvement opportunities
    - New product support
  - Business requirements
    - Compliance, regulatory
  - Business risk
    - Annualized Loss Expectancy (ALE = ARO x SLE)
    - Provide estimates based on business risk

A good way to gain support for security investments is by aligning the work of the security team to key business opportunities. For example, if your company is moving to support new enterprise initiatives like BYOD, mobile, could, or Big Data, you can gain support by helping business unit leaders deploy those technologies in a more secure manner. Providing security solutions before problems arise makes it easier not only for your key stakeholders but also for the security team by getting involved earlier in the system development process.

Process improvement opportunities are ways for security to provide value to the business. In large organizations, there are typically many systems all with different user ids and passwords. Even if users choose the same password for all systems, they might be required to sign on dozens of times per day. Reducing the number of times a user has to sign on increases productivity and decreases support costs by reducing the amount of password reset calls to the help desk. In this way, security can gain support for deploying a Single Sign On (SSO) solution that reduces time spent signing on to the multiple systems and allows users to focus on critical business tasks.

Security can also support business innovation by providing services to new products being rolled out by the company. These can be products utilized by customers such as new websites and mobile apps or even new systems that are important to the organization such as order processing or inventory systems.

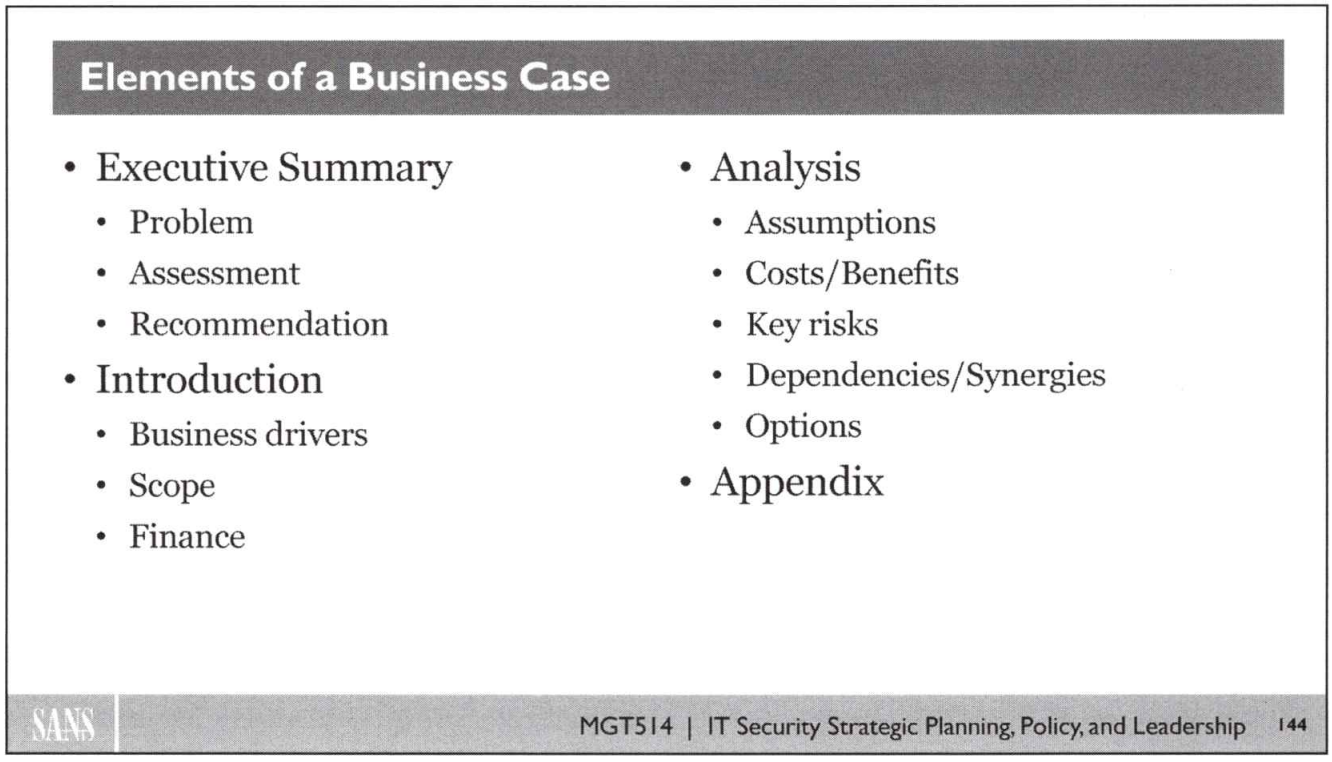
Compliance and regulatory requirements are an obvious area in which security can provide services to the company. For example, deploying PCI-compliant security infrastructure allows you to accept credit card payments. However, compliance often results in mandatory spending. It is the non-mandatory spending associated with overall business risk that is much harder to quantify. One approach for doing this is by using annualized loss expectancy (ALE), which is calculated by multiplying the annual rate of occurrence (ARO) of an event with the single loss expectancy (SLE):

ALE = ARO x SLE

First, you have to calculate single loss expectancy (SLE). This is based on exposure factor (EF) and the value of the asset. It's important to remember that exposure factor (EF) is a subjective, estimated percentage of loss to an asset if a specific threat is realized. It can be based on security vulnerabilities, threats, and the overall risk management framework used in your organization. For example, if you have an asset valued at $100,000 and an EF of 20%, then your SLE is $20,000.

Taking this SLE of $20,000, you can then multiply it by the annual rate of occurrence (ARO), which is an estimate of how likely it is that you will have a loss in one year. Again, the key word here is "estimate." By using a simple estimate of 10% likelihood in year 1, 20% in year 2, and so on, you can calculate that the ALE is $2,000 (10% x $20,000).

The key point here is that these are estimates. But, by using these estimates as a starting point, you can start to make the case that over five years the ALE is $10,000 (50% x $20,000). If the security control costs only $1,000, this could be a worthwhile investment. Point being, don't spend more protecting something than it's worth.



Different organizations might utilize different templates for creating business cases. However, the core elements of a business case will remain the same.

Executive Summary

This section is written for key decision makers and summarizes the problem at hand, your assessment of the situation, and the overall recommendation. The recommendation can be as simple as choosing to invest in a new security capability or, even better, it can ask key decision makers to choose from a set of options to solve the problem at hand. Providing at least three options involves decision makers in the process and turns them into active participants. The executive summary section, although it comes first in the business case, is usually created last after all the other analysis has been conducted. This ensures that you can more easily summarize the actual information in the overall case.

Introduction

This section provides background information about business drivers (e.g., new business initiatives, revenue, and cost drivers) and the threat landscape (e.g., recent breaches, internal security incidents, etc.). This is where you lay out the scope of your business case. For example, does it touch all public facilities, office buildings, employees, customers, etc. The scope will have a direct impact on the associated costs. This is where you can incorporate financial information related to the cost, industry comparison, and business innovation approaches we discussed previously.

Analysis

This is the meat of your business case and includes any assumptions that you have made in your model, the cost/benefit analysis, as well as key risks and dependencies/synergies. If your business case will be reviewed by a large number of key stakeholders, it is extremely important to include dependencies on other teams as well as

synergies that might help other teams. For example, if you are deploying a new patch management tool that has a side effect of reducing the number of hours that the IT operations team spends on managing systems, you would certainly want to highlight this fact to gain support from that key stakeholder. Finally, your analysis should include details about the various options that you considered or are proposing.

Appendix

What is included in this section depends largely on what key decision makers want to see and are interested in. Imagine that you have a CIO who is extremely focused on technology innovation and is a big picture thinker. She might not be as interested in the details of the ten-year financial forecast. However, if you have a CIO who is focused on improving current operations and reducing costs the ten-year financial forecast probably shouldn't be relegated solely to the Appendix.

Tips for Creating a Security Business Case

- As a manager and leader, you are expected to:
  - Understand the vision and mission of the company
  - Make security understandable to business leaders
- Don't just ask for the money
  - Sell the vision and how you will solve business problems
  - Use all the approaches to justify your request
    - Cost, Industry Comparison, and Business Innovation Approaches
- Let the case speak for itself
  - Allow decision makers to come to their own conclusion
  - Outline three options with various pros and cons
    - Let them pick one

Ultimately, a business case is about getting funding for your security initiatives. However, the framing associated with the request is extremely important. Instead of simply asking for the money, a better approach is to articulate the vision for the security program and the business problems that will be solved. By focusing on the problem and the eventual solution, you can increase commitment and turn stakeholders into partners.

By using the approaches discussed in this section to justify your request and letting the case speak for itself, you allow key decision makers to come to their own conclusions. Executives want to have a say in how to run the business and many are realizing that managing security risk is a key component of running the business. By outlining three options with various pros and cons, you can provide a say in how to manage business risk.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - *Security Metrics Program*
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.

Security Metrics Overview

- By the end of this section, you will understand:
  - Why metrics are important and the critical concern around security metrics
  - Various types of metrics including those beyond traditional technical metrics
    - Financial
    - Customer/stakeholder satisfaction
    - Business process
  - How to tailor your metrics program for specific audiences
    - Executive
    - Operational
    - Technical
  - How to use metrics to drive process improvement

Paving the road to success depends on you, and your leadership team being well informed and having the right information to make the right decisions.

As a security professional, it's your job to just that—understand the quality and progress of your "business of security," and communicate value and risks to your leadership in a manner that is easy to consume, and relevant enough to make well-informed decisions.

There is not a better, more effective way to understand and communicate all aspects of business than metrics. It's a common language that all leaders understand and has been used for decades.

Security is not exempt from demonstrating strategic value and operational effectiveness in organizations, but historically this has proven to be a significant challenge for many security organizations. In this security metrics section, we will cover topics related to metrics that will help you rise to the challenge of demonstrating value, and will help you communicate more effectively.

We will also demonstrate how you can leverage various types of metrics such as security, financial, customer satisfaction, and business processes to help you, your leadership, and your company become more holistically informed and make better decisions.

We will share security frameworks that you can leverage to build a metrics program and show you how you can translate business activities, security vision, and strategy into your metrics program.

We will show you how to tailor your metrics for specific audiences such as executives and stakeholders, and operations and technical; how to apply multi-dimensional views to effectively show the overall health and security posture of your organization; and how you can use metrics to identify improvement opportunities and drive process improvement.

We will also share visualization tips, communication channels to socialize your metrics program, and pitfalls to avoid when creating your metrics program.

Security Metrics – A Critical Concern

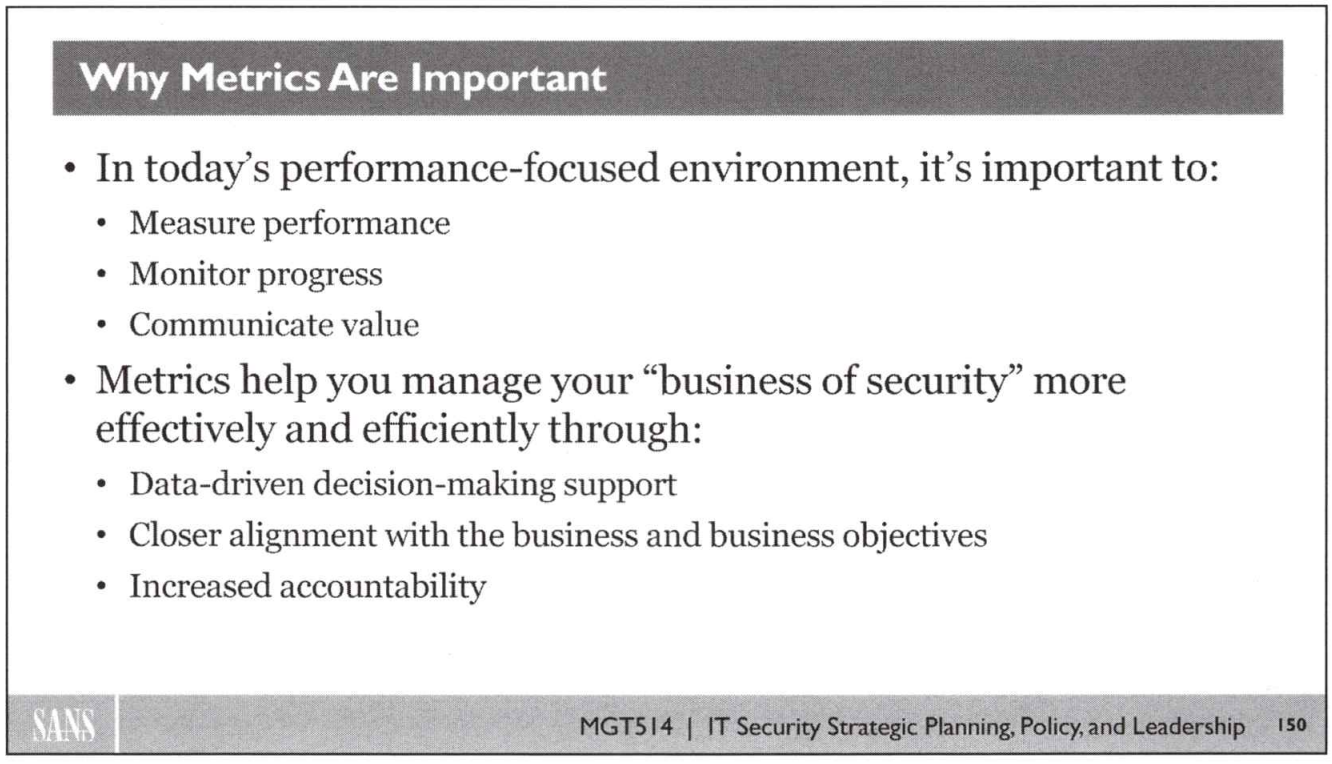
- Problem
  - Many executives are searching for security statistics that are important so they know when to pay attention
    - Metrics the security organizations track and present to management are not often aligned with business objectives
    - They often convey little information on a security program's effectiveness in reducing overall risk
    - They are often difficult to understand
- Solution
  - Provide essential metrics that transform and communicate complicated data into business language that can be easily understood

As pressure increases on security as a priority for many organizations, it's not unusual for executives and directors of boards to take an active interest in security. As reports of breaches hit the news almost daily, top executives want to be informed of the current and evolving threat landscape, as well as organizational risk, readiness, and response plan for incidents.

Security professionals are being brought before executives and asked to demonstrate the effectiveness of their security programs. It's not unusual for executives to be given volumes of data that is not relevant or aligned to the business objectives, convey little to no information on the effectiveness of security, are difficult to understand, and often lead to more questions than answers.

As stated previously, numbers are the common language of business that all leaders understand and rely on to make important business decisions. You must accept the fact that security metrics are no different than the metrics other business verticals would use to communicate value (such as Finance, Sales and Marketing, or even IT). It is your responsibility as a security professional to provide metrics that transform and communicate large quantities of complicated data into business-consumable language that can be easily understood, provide business value, and facilitate the decision-making process.

Executives and board members want to understand whether the decision they made to fund security has helped achieve a competitive advantage, and will keep them out of the news. They want information that will help them determine whether they are spending too little or too much on security, how their investments to date have improved the organizational risk posture, and/or where the accountability needs focus to influence culture and behavior change.



Why Metrics Are Important

Metrics are an essential tool for security professionals to understand all aspects of the "business of security" and encompassing components, such as understanding performance on specific technology capabilities and processes, progress towards pre-defined goals addressing security and risk posture, and how those security initiatives are paying off. Metrics can also help you build your business case to support organizational demand for security support on strategic initiatives that might require additional resources.

Metrics will help you further understand whether your security controls are producing the desired results, such as fewer malware infections as a result of your network segmentation and anti-malware programs. Time to containment and mitigation for incidents is within an established norm. Workstations and servers are patched well within an acceptable level of risk tolerance the organization has agreed upon.

If metrics are done right, security managers will better understand their business, which in turn will allow them to more effectively communicate and inform executives, stakeholders, and board members the complexities and risks of security, quantify security outcomes through the effectiveness of controls and processes, and demonstrate considerable value and alignment to the organization.

Metrics provide more than funding justification for more resources and shiny new technology. Properly designed metrics will facilitate objective data-driven decision making to critical areas such making adjustments to your strategy based on the diagnosis of a problem of more comprehensive understanding of an issue or root cause or the ever-changing threat landscape. Metrics can also drive performance and operational improvements such as improved SLAs, customer satisfaction, and improved tuning of technologies to improve security outcomes. Metrics will also aid in your overall organization approach to risk by determining which initiatives will be funded and in what order.

Security metrics can shine light on the organization's state of compliance against internal security guidelines and policies ultimately increasing accountability across business units. Comparing business unit result to an agreed upon risk tolerance level will increase motivation to improve results.

Metrics Resources

- Center for Internet Security (CIS)
  - CIS Controls for Effective Cyber Defense *Version 6.0*
  - A Measurement Companion to the CIS Critical Security Controls *Version 6.0*
  - CIS Consensus Security Metrics v1.1.0
  - CIS Quick Start Guide for CIS Consensus Security Metrics v1.0.0

There are several control frameworks that will provide guidelines you can use to identify metrics for monitoring your controls efficacy.

Some of these controls are regulated depending on your industry such as PCI, SOX, and HIPAA. There are also voluntary frameworks such as National Institute of Standards and Technology (NIST) Cyber Security Framework, ISO/IEC 27002:2013, COBIT 5, and Critical Security Controls.

Where regulated or contractually obligated, you will want to build your metrics program around the security controls that are prescribed, using the metrics to validate security controls. Your company might already have framework adopted (e.g., ISO, COBIT, etc.). To the extent feasible, you'll want to investigate how to leverage that framework in support of your security metrics program.

In addition, you will want to interview and consult with your stakeholders and executives in your organization to better understand what metrics are important to them and further understand what strategic objectives security can support.

A way to facilitate productive discussions with your stakeholders and executives is to have proposed metrics in hand prior to meeting with them. Below is a list of valuable metrics resources you can leverage to build your metrics arsenal.

Center for Internet Security (CIS): Mobilizes a broad community of stakeholders to contribute their knowledge, experience, and expertise to identify, validate, promote, and sustain the adoption of cybersecurity's best practices.

- **CIS Controls for Effective Cyber Defense Version 6.0**: A recommended set of actions that provide specific and actionable ways to stop today's most pervasive and dangerous cyber attacks

- **A Measurement Companion to the CIS Critical Security Controls Version 6.0**: This document provides guidance on how to measure the effectiveness and implementation of the CIS Controls

- **CIS Consensus Security Metrics v1.1.0:** A set of Consensus Security Metrics and data set definitions that can be used across organizations to collect and analyze data on security outcomes and process performance

- **CIS Quick Start Guide for CIS Consensus Security Metrics v1.0.0:** This document is a guide to help organizations get metrics programs started quickly and effectively, using the CIS Security Metrics Definitions

Keeping focus on producing information that is useful to your audience (regulators, stakeholders, executives, boards, etc.) is best practice, and will go a long way with gaining credibility for you and your security organization.

Metrics resources

- **Center for Internet Security (CIS):** https://www.cisecurity.org/critical-controls.cfm
  - **CIS Controls for Effective Cyber Defense Version 6.0**,
  - **A Measurement Companion to the CIS Critical Security Controls Version 6.0**:

- **CIS Consensus Security Metrics v1.1.0:** https://benchmarks.cisecurity.org/downloads/metrics/

- **CIS Quick Start Guide for CIS Consensus Security Metrics v1.0.0:** https://benchmarks.cisecurity.org/downloads/show-single/?file=metrics_guide.100

Control framework resources:

- **NIST Framework for Improving Critical Infrastructure Cybersecurity:** http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

- **ISO/IEC 27002:2013:** http://www.iso27001security.com/html/27002.html

- Control Objectives for Information and Related Technology (COBIT): https://cobitonline.isaca.org

Technical Measures – Critical Security Controls

Function	Example Measures	
Identify	CSC 1: # of unauthorized devices on the network CSC 1: Avg. time to detect new devices on network CSC 1: Avg. time to isolate/remove unauthorized devices CSC 1: # of devices blocked by network authorization CSC 1: % of systems not utilizing network authorization CSC 2: # of unauthorized software applications CSC 2: Avg. time to remove unauthorized apps CSC 2: % of systems not running app whitelisting CSC 2: # of software apps blocked by whitelisting CSC 2: Avg. time to detect new software installed CSC 2: Avg. time to remove unauthorized software CSC 20: Aggregate score of all penetration tests	CSC 4: % of systems that have not been scanned CSC 4: Avg. vulnerability score for systems CSC 4: Total vulnerability score for systems CSC 4: Avg. time to deploy OS software updates CSC 4: Avg. time to deploy app software updates CSC 18: % of custom applications that have not been scanned by an application security code scanner CSC 18: % of database systems that have not been scanned by a database specific vulnerability scanner CSC 18: Aggregate vulnerability rating for all application and database systems CSC 18: Avg. time for alerts to be generated and sent to system administrators that a vulnerability scan has or has not completed

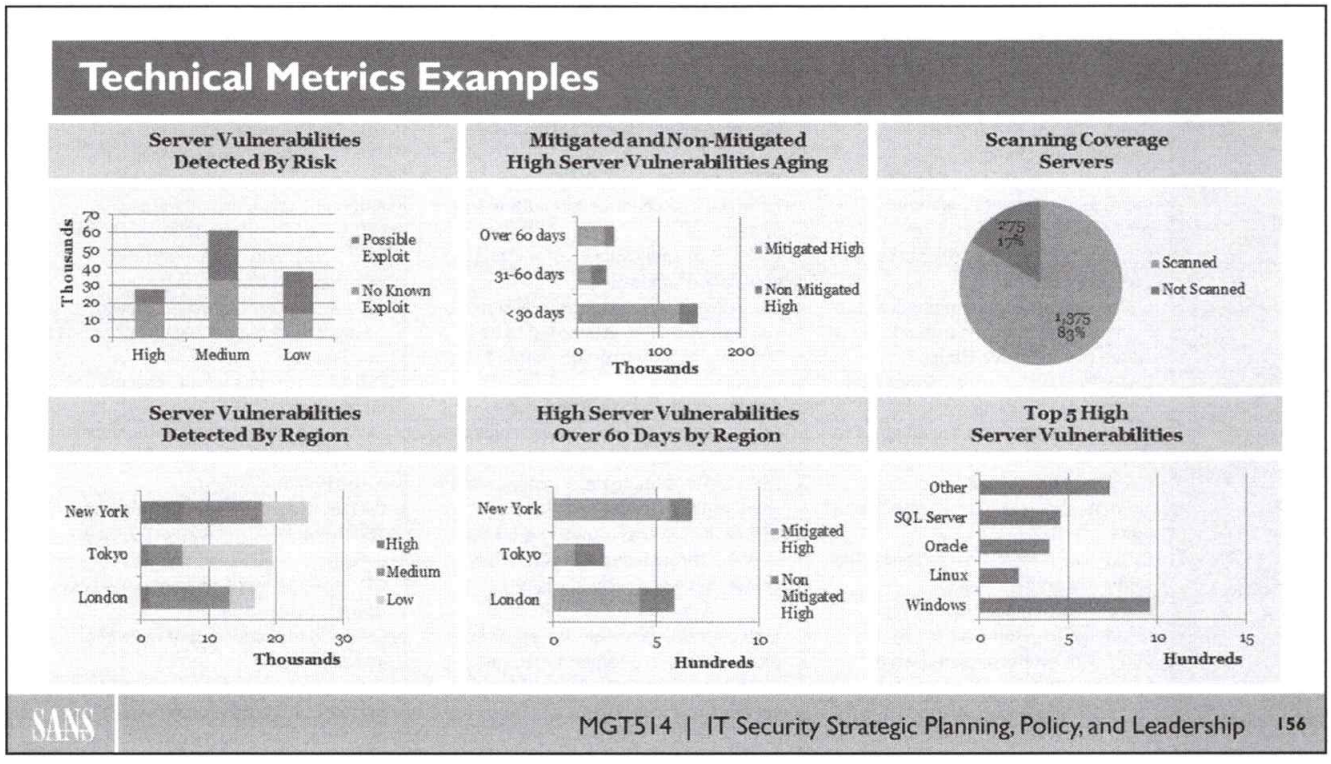
We talked extensively about various security frameworks in an earlier section of this course, and on the previous page we mentioned that CIS has published a measurement companion to its Critical Security Controls.

You will find on this page that we have completed a mapping between the three publications to illustrate how you can align your framework, controls, and proposed measurement in an effort to help you measure the effectiveness and implementation of your security program. We have provided the same mapping for the remainder of the NIST functions: Protect, Detect, Respond, and Recover on subsequent slides.

A mapping exercise such as this might be time intensive to build in the beginning, but the effort you invest in organizing your information with reputable and recognizable frameworks and controls will greatly benefit you and your team in the long run and you look to develop your reporting and communication efforts to share with your leadership team, executives, customers, and stakeholders.

Function	Example Measures		
Protect	CSC 3: % of systems not currently configured to approved configuration standards CSC 3: % of systems whose security configurations is not enforced by technical configuration management applications CSC 3: % of systems not up to date with the latest available OS security patches CSC 3: # of unauthorized configuration changes blocked by configuration management system CSC 5: # of unauthorized elevated application accounts currently configured CSC 5: # of unauthorized elevated OS accounts (local administrator/root) currently configured CSC 5: % of elevated account that do not require two-factor authentication	CSC 7: # of unsupported web browsers detected CSC 7: # of unsupported email clients detected CSC 7: % of devices not required to utilize network based URL filters CSC 7: Avg. % of users who inappropriately respond to sponsored email phishing tests CSC 8: % of systems deployed and not enabled with up to date anti-malware CSC 8: % of applications not utilizing application sandboxing CSC 9: % of systems not running host based firewall CSC 9: # of unauthorized services running on systems CSC 9: # of deviations from approved service baselines discovered	CSC 11: % of network devices not currently configured to approved configuration standards CSC 11: % of network devices not enforced by technical configuration management applications CSC 11: % of network devices not up to date with the latest available OS software security patches CSC 11: % of network devices that do not require two-factor authentication to administer the device CSC 12: % of remote access users not required to use two-factor authentication to remotely access the network CSC 12: % of remote systems not managed using the same security standards as internal network systems CSC 12: % of internal systems not on dedicated Virtual LANs (VLANs) that are segmented with access control lists CSC 14: % of systems not utilizing host based Data Loss Prevention (DLP) software CSC 17: % of workforce members that have not completed a core information security awareness program CSC 17: % of workforce member that have not passed general information security awareness assessments CSC 17: % of workforce members that have not passed job role specific information security awareness training

Function	Example Measures		
Detect	CSC 3: Avg. time to detect configuration changes CSC 5: # of detected attempts to upgrade an account to administrative privileges CSC 5: # of detected attempts to gain access to password files CSC 5: Avg. time for administrators to be notified about user accounts being added to super user groups CSC 6: % of systems that do not have logging per standards CSC 6: % of systems not configured to centralize logs CSC 6: # of discovered anomalies/events of interest in log files CSC 6: Avg. time for failure alert to be sent if system fails to log CSC 6: Avg. time for personnel to respond if a system fails to log CSC 7: # of events detected while examining logged URL requests	CSC 8: # of instances of malicious code detected by host based anti-malware systems CSC 8: # of instances of malicious code detected by network based anti-malware systems CSC 8: % of applications not utilizing application sandboxing CSC 8: Avg. time to identify malicious software installed, attempted to be installed, executed, or attempted to be executed CSC 9: Avg. time to identify new unauthorized listening network ports installed on network CSC 11: Avg. time to detect configuration changes to a network CSC 12: # of events discovered on the network through analysis of net flow configured on network devices CSC 12: Avg. time for unauthorized network packets are alerted on when passing through perimeter systems CSC 20: # of pen tests (internal & external staff)	CSC 13: # of unauthorized data exfiltration attempts detected by Data Loss Prevention (DLP) system CSC 13: # of plaintext instances of sensitive data detected through automatic scanning software CSC 13: # of attempts to access known file transfer and email exfiltration websites detected CSC 14: % of sensitive data sets not configured to require logging of access to the data set CSC 15: # of rogue wireless access points discovered CSC 15: # of wireless access points or clients discovered using an unauthorized wireless configuration CSC 15: Avg. time to generate alerts about unauthorized wireless devices detected CSC 16: # of invalid attempts to access user accounts detected CSC 16: # of accounts that have been locked out CSC 16: # of attempts to gain access to password files in the system have been detected
Respond	CSC 12: Avg. time to apply configuration changes to block unauthorized traffic passing through perimeter systems	CSC 19: % of employees that have not completed IR training CSC 19: # of incident handling exercises completed CSC 19: # of security incidents documented	
Recover	CSC 3: Avg. time to reverse unauthorized changes CSC 8: Avg. time to completely remove malicious code CSC 9: Avg. time to close or authorize newly detected system services CSC 10: % of systems where their OS or application binaries have not been backed up CSC 10: % of systems that have not had their data sets back up	CSC 10: % of backup have not recently been tested by personnel CSC 10: % of systems do not currently have a backup available to online operating system calls CSC 10: Avg. time to notify system personnel that a backup has failed CSC 11: Avg. time to reverse unauthorized changes on a network CSC 15: Avg. time to remove rogue access points from the network CSC 15: Avg. time for unauthorized wireless devices to be isolated/removed from the network	



This is an illustrative sample of technical metrics designed for discussion purposes only. There are hundreds, if not thousands, of technical metrics and data variations that can be generated to display security controls, understanding of threats, and vulnerabilities and evaluation processes.

These examples are focused around server vulnerabilities. Shown here are six ways to view the data related to server vulnerabilities. Each graph displays important data in an effort to further the assessment and understanding of vulnerabilities.

Technical Metrics Examples – What's Wrong?

- What's wrong with these metrics?
  - Message is diluted in operational details
    - They do not increase your understanding of security and risk
    - They are not ideal to increase security's visibility and generate awareness
  - They are not business consumable
    - Not aligned with the business or their objectives
    - They are not relevant for senior leaders, executives, or stakeholders
    - Will not boost your credibility
  - They do not measure progress and demonstrate value
    - Provides a snap shot in time only
    - Do not provide trending to determine progress, increased or decreased risk

There is an enormous amount of data that is waiting to be mined and displayed in various forms of graphs and/or charts with the hopeful outcome that you can present to your leadership, stakeholders, and company executives, and they immediately identify value in what you've provided, which in turn will lead to facilitated discussion that will ultimately ensure your metrics are leveraged to make data-driven decisions, or provide the perfect amount of information where they feel well-informed.

The metrics on the previous page are not those metrics described above. They are not the kind of metrics where executives can feel like they understand what is going on and they are well informed. They are not the kind of metrics that will enable an executive to respond quickly to make important decisions about security.

The message in these server vulnerability metrics is diluted because they focus on very technical operational details, which are spread over several metrics. They tell an incomplete story of security and risk, and require far too many assumptions to be made or erroneous conclusions to be filled in by the imagination of the recipient.

These server vulnerability metric examples are not business consumable. They do not satisfy a specific business requirement or address the question on every executive's mind, "So what?"

They are not aligned with the business or its objectives (unless your company's business objects happen to minimize vulnerabilities in the server environment). Your audience is not likely to understand the value of "Possible Exploit" versus "No Known Exploit," nor will they understand the real threat behind the Top 5 High Server Vulnerabilities list, or why an aging report is relevant to determining how long risk has been in your environment.

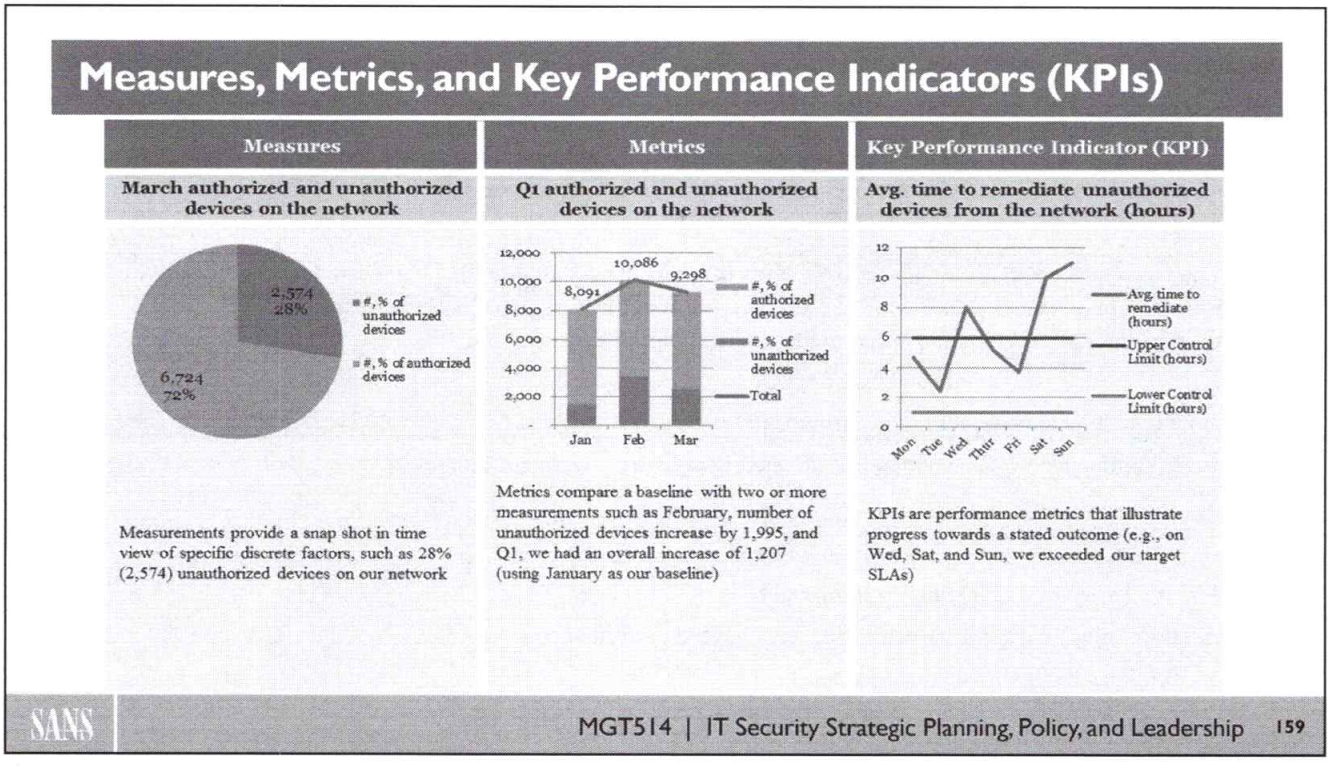
These metrics are not relevant for senior leaders, executives, or stakeholders. Presenting these detailed, technical metrics to this audience will leave them with more questions than answers. This approach will not boost your credibility.

These metrics do not measure progress or demonstrate value, they provide a snap shot in time, and they do not include trending data to determine progress or increased or decreased level of risk. The Aging metrics attempt to illustrate risk but doesn't tell us whether we are getting better or worse at mitigating server vulnerabilities. The scanning coverage is a nice, clean measurement, but there is no context to let the audience know whether this is an appropriate coverage level. Here is an example to illustrate context of value around scanning coverage metrics. Of the "Not Scanned" servers, how many of those servers contain regulated or sensitive data? If you have a high percentage of "Not Scanned" servers that are critical to business operations, then your risk is greater. You can ask the same questions with the Top % High Server Vulnerabilities metric. How many of these are on critical business applications?

The metrics you select should satisfy a specific business requirement and those metrics should be metrics that someone needs to know about. If there is not a compelling business need for the metrics, you should not share it with your stakeholders, executives, and/or board of directions. Again, you will likely cause more concern and questions to arise than you anticipated.

Effective metrics should

- Measure performance using baselines and trends
- Monitor progress towards stated goals
- Help the metric owner communicate value
- Facilitate the use of data for decision-making support
- Should be closely aligned with the business, and business objectives
- Provide line of sight to risks ultimately increasing accountability



There are similarities between measures and metrics in that both can be qualitative or quantitative. There is also a distinction that is often unclear. This distinction between measures and metrics is important to understand. The main difference is that metrics are measurements that use a baseline to establish normal operating levels and uses this baseline to compare when something is abnormal.

Another way to look at the distinction between measurement and metrics is that measurements provide a snap shot in time view of specific discrete factors. Measurements are objective raw data and generated by counting, such as "I have one widget." Using a security measurement example, you might count: 28% (2,574) unauthorized devices on our network.

Comparing a baseline that has been established with two or more measurements taken over time generates metrics. Metrics are generated from analysis, such as "I have 10 more widgets than I did yesterday, and I have 15 more widgets than when I started." Using a security metrics example, you might illustrate: In February, we had an increase of 1,995 unauthorized devices on the network, and in Q1, we had an overall increase of 1,207 (using January as our baseline).

KPIs are performance metrics that illustrate progress towards a stated outcome. KPIs are used across all industries, and are used to monitor how the organization is doing relative to goals. They are also used to monitor implementation and effectiveness of organizational strategies; they are also used to determine the gap between actuals and targets.

Companies will use KPIs, such as profit and loss statements, new membership growth, earnings per shareholder, etc. For security, KPIs should be customizable for the business unit(s) your security organization supports, and might include areas like avoiding data breach or meeting regulatory and compliance requirements.

For security, let's say that minimizing unauthorized devices on the network is a business imperative. You'll want to determine your thresholds or state your goals. For this example, we can use an upper and lower control limit to show the effectiveness threshold we want to operate in. Obviously, the closer we get to the lower threshold of removing unauthorized devices within 1 hour, the more effective we are in our security controls. When performance moves closer to, or exceeds the upper threshold of 6 hours, we have cause for alarm and we would need to look deeper at our performance and make necessary adjustments.

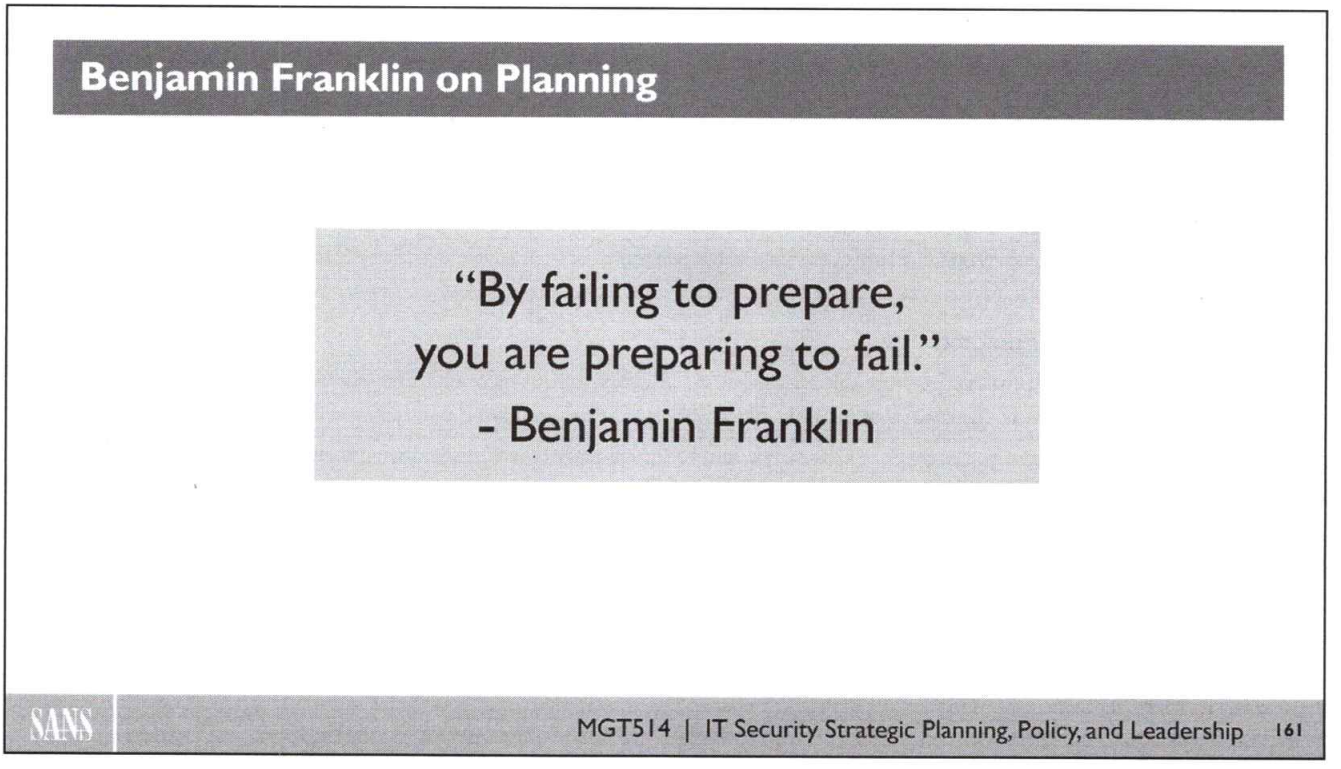
Developing relevant and actionable security KPIs is a critical step to providing value and building credibility for your security organization. The key to successful security KPIs is to map closely to business KPIs. In other words, develop KPIs that are important to the business, not just security.

Good KPIs will include the following attributes:

- Monitors the implementation and effectiveness of organizations' strategies
- Determines effectiveness and operational efficiency
  - Effectiveness is "Doing the right thing."
  - Efficiency is "Doing the thing right."
- Determines the gap between actual and targeted performance
- Provides focus for what matters most
- Is not limited to work being performed; it illustrates accomplishment
- Provides business-consumable context in a common language that facilitates communication

Reference

http://balancedscorecard.org/Resources/Performance-Measures-KPIs



Benjamin Franklin[1] was a leading author, politician, scientist, and investor. He was also a renowned polymath, a person whose expertise spans a significant number of different subject areas. This term is often used to describe great thinkers of the Renaissance and the Enlightenment who excelled at several fields in science and the arts.

Franklin was a leading author, printer, political theorist, politician, freemason, postmaster, scientist, inventor, civic activist, statesman, and diplomat. One of Franklin's most notable discoveries was through his electrical experiments, which led to his invention of the lighting rod.

In a 1772 letter to Joseph Priestley,[2] an 18th-century English theologian, dissenting clergyman, and natural political theorist, Franklin describes the earliest known description of a planning technique using the Pro & Con list. He writes "... my way is to divide half a sheet of paper by a line into two columns, writing over the one Pro, and over the other Con. Then during three or four days' consideration, I put down under the different heads short hints of the different motives that at different times occur to me for or against the measure. When I have thus got them all together in one view, I endeavor to estimate their respective weights; and where I find two, one on each side, that seem equal, I strike them both out, If I find a reason pro equal to some two reasons con, I strike out the three. If I judge some two reasons con equal to some three reasons pro, I strike out the five; and thus proceeding I find at length where the balance lies; and if after a day or two of further consideration nothing new that is of importance occurs on either side, I come to a determination accordingly."

References

[1] https://en.wikipedia.org/wiki/Benjamin_Franklin

[2] https://en.wikipedia.org/wiki/Joseph_Priestleyphilosopher, chemist, educator, and Liberal

Planning Is Fundamental

- Creating a plan will ensure success of your metrics program
  - State your program goals
  - Define the metrics that will help you reach your goals
    - Addressing the "so what" your organization cares about
  - Determine your method
    - Identify metric owners: Accountable for the people, process, and/or technology associated with each metric
    - Define metric classification: For example, data spill prevention: count of unencrypted outbound email
    - Describe business purpose: For example, visibility to email activity where sensitive information is leaving company
    - Determine data source: For example, data loss prevention system
    - Decide publication frequency: For example, weekly, monthly, quarterly, etc.
    - Build operational definitions: Define acronyms, processes, teams, etc., that will be useful to your audience
    - Establish review process: For example, leadership, legal, communications etc.
    - Metrics hierarchy classification: For example, Balanced Scorecards, Operational Dashboards, or Technical charts & graphs

Creating a measurement plan will aid in the success of your metrics program. Planning is fundamental and will aid in the assurance of your metrics plan success. It will also align expectations between your teams, your leadership, customers and stakeholders, executives, and ultimately benefit the board of directors.

State your program goals

You first need to understand and define the goals of your metrics program. Without these stated and defined goals, you might end up somewhere you didn't intent your program to be. It's important to also remember that the goals of the program should extend beyond traditional security and include more than what "you" want to see. Your program should include what your customers, stakeholders, and executives "need" to know. If you want to make progress with the business, take your security hat off and put your consumer hat on.

The goals of your metrics program could be any combination or all of the examples listed below. These examples are not exhaustive, and you might find you have your own unique drivers for your metrics program.

The goal of the metrics program is to:

- More effectively align to what our customers and stakeholders value, drive transparency, and communicate more effectively
- Optimally manage my business of security
- Identify improvement opportunities to minimize risk and optimize costs
- Drive compliance and behavior change
- Improve specific security capabilities (e.g., password protection, vulnerability management, etc.)

Define the metrics that will help you reach your goals

Include various types of metrics that address the "so what" for your organization. The metrics you select should be aligned to your goals and tell you what you are going to measure to achieve those stated goals. On the following page, we've outlined in further detail some metrics considerations.

Determine your method

A measurement plan is your roadmap that defines the who, what, why, when, and where of your metrics program. A measurement plan is critical to the success of your metrics program because it will drive accountability, and ensure a repeatable process and more reliable output results. The components of a measurement plan are listed below:

- **Identify metric owners**: Metric owners are the individuals accountable for the people, process and/or technology associated with a specific metric. You will have many metrics owners within your metrics plan. Metrics owners are accountable to create a measurement plan for their respective area of responsibility.

- **Define metric classification:** You should create a high-level classification schema. This will give you greater flexibility on your reporting capabilities down the road, such as reporting all metrics that are related to data spill prevention or vulnerability management. You might want to include subdomain as well, such as unencrypted outbound emails, which will give you even more flexibility in your reporting down the line.

- **Describe business purpose**: This component of your measurement plan is critical. If you cannot describe the purpose of each of your metrics in business-consumable terms, you will not be able to communicate with people outside of your security organization. For example, let's look at the count of unencrypted outbound emails. A business purpose definition might be to provide visibility to email activity where sensitive information is leaving the company.

- **Determine data source**: As stated previously, there are hundreds, if not thousands of technical measures and data variations that can be generated to display security controls. Designating the specific source of raw data that will be used to generate each of the metrics within your program is important for continuity of your metrics program. Using the same example as above—unencrypted outbound emails, your data source might be your data loss prevention system. We will talk more specifically about the data sources on the next page.

- **Decide publication frequency:** For each metrics, you'll want to indicate on your measurement plan what the publication frequency is (e.g., weekly, monthly, quarterly, etc.). This will set expectations for all consumers.

- **Build operational definitions**: This section is another critical component of your metrics program and your measurement plan. Security in general is very technical, complex, and difficult to understand for non-security professional, let alone, one team's definition of process, procedure, or technology usage might vary slightly or significantly from another team. It's important that you define operational and technical terms, acronyms, and anything else that might be useful to your audience and help them to better understand the story you are trying to tell with your metrics. As an example, Severity 1 might mean something entirely different from team to team. It's important to define what Severity 1 means related to that specific metric.

- **Establish review process**: It's important to determine what the review process will be in order to ensure success of your program. For instance, you wouldn't want metrics going to your customers or stakeholders without your leadership review, or if by chance the metrics you are producing are intended for consumers outside of your organization, you would likely need your leadership review and possibly legal and/or your communications team.

- **Metrics hierarchy classification:** We are going to talk more about metrics hierarchy in the coming slides but for the purposes of understanding this measurement plan requirement, you will need to know that each metrics should be classified based on your reporting output (for example, Executive Balanced Scorecards, Operational Dashboard, or Technical Charts & Graphs).

Metric Selection Is Important

- Metrics should answer the "so what" for your organization
  - They need to be transformed into more meaningful data through analysis
    - Many data sources you can use (e.g., antivirus, antimalware systems, SPAM filters, etc.)
  - Financial metrics should be considered in two ways
    - How much does it cost to operate security (e.g., % of security budget compared to IT)
    - How security incidents impact your company financially (e.g., direct loss of intellectual property or cost of downtime)
  - Customer/stakeholder satisfaction and business process should measure what's important to the org
    - Value: For example, reliability, responsiveness, and assurance of service
    - Invisible value: For example, activities and controls that are our corporate responsibility but have little to no impact on what the customer perceives as value

Your metrics program should be inclusive of various types of metrics such as security, financial, customer satisfaction, and business process. Including these categories of metrics will provide your leadership, stakeholders, and executives a strategic and holistic view of your efforts.

Security Metrics

As stated previously, there are hundreds, if not thousands, of technical security metrics that you can generate based on the data that can be gathered from your environment. The following is a list of some of the potential sources you can collect raw data from in support of your security metrics. As a reminder, these data sources are a good starting point. However, the data from these tools often have to be transformed into more meaningful information through analysis in order to provide intelligence that enables key decisions to be made.

- Antivirus, antimalware, systems
- Spam filters
- Firewalls
- Vendors or managed security services
- Web logs
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Patch logs
- Vulnerability scans
- Penetration tests
- Databases
- Network access control
- Data loss prevention systems

- Access logs
- Server logs
- VPN
- Configuration hardening
- Secure web gateways
- Web application firewalls
- Mobile data protection
- Governance, risk, and compliance management
- Storage encryption
- SIEM

Financial Metrics

For financial metrics, you might want to consider looking at this from two angles. First, how much does it cost to operate security? Some examples of this might be "Security budget as a % of overall IT." You might want to further group by business unit, or specific to application development or some other important category, or categories your company will find useful. You might also want to show a % of change in security budget from previous fiscal year, % of security budget dedicated to contractors, outsourcing, and/or training. You will also want to provide information on operational budget (OPEX), which lays out ongoing spending on routine daily operations. You will also want to include capital expenditures or (CAPEX), which refers to a one-time investment on hardware, software, and in some instances project-related resources.

Secondly, you'll want to show how security incidents or the lack thereof either positively or negatively impacts your company financially such as cost of incidents. This could include:

Direct loss might include the value of intellectual property, customer lists, trade secrets, or assets that are destroyed.

- Cost of business system downtime would include cost of refunds for failed transactions, or cost of lost business directly attributed to the incident.
- Cost of containment includes efforts and cost for existing security resources and assets, and potentially consulting services.
- Cost of recovery could include the cost of incident investigation and analysis, efforts required to repair and/or replace systems, consulting services for repairs and/or investigations, and additional costs not covered by an insurance policy.
- Cost of restitution could include penalties and other funds paid out due to breach of contracts or SLAs resulting from the incident, and cost of services provided to your customers as a direct result of the incident such as ID theft insurance and/or credit monitoring. This could also include public relations costs, and cost of disclosures and notifications and legal costs, fines, and settlements.[1]

Customer/Stakeholder Satisfaction and Business Processes

Customer and stakeholder satisfaction is another way a security organization can evaluate its goals and measure progress. In order to develop metrics for this, a security organization must understand who its customers and stakeholders are, and what's important to them. We covered stakeholder management in Section 1: Strategic Planning Foundations.

It's important to note that customer satisfaction might be the results of the metrics you capture and report on in your business processes. The efficiency in your business process often influences and/or has direct correlation to your customer's satisfaction.

The first thing you must do to determine what customer/stakeholder satisfaction metrics you can produce is understand what types of services or business processes your security organization provides to your customers and stakeholders. More importantly, you need to know what your customers and stakeholders "value" verses the "invisible value" we "think" is important to organizations because of our roles, responsibilities, and due diligence we must perform as a security organization.

- **Value:** A customer or stakeholder might value reliability, which is your team's dependable and accurate performance against what was promised. A customer might also value responsiveness, which is your team's willingness to provide prompt service for client needs. A customer and stakeholder might also value assurance that your team has knowledge and competence in the services performed.

- **Invisible Value:** As security professionals, we perform many tasks to secure an environment and meet regulatory and contractual compliance. Many of these tasks go unseen or unnoticed and are in essence invisible to our customer and stakeholder. If we as security professionals measure what we "think" is important to our customers and stakeholders—the invisible value—we will miss the mark every time.
  - An example of this would be end point protection. We might have several layers of controls for our end point protection. The majority of our customers do not care about all of these layers of control. It's invisible to them. What will be of concern is if all these layers are causing performance latency issues that impact their ability to perform their job.
  - For another example, if you are performing a security assessment for a new application that will be deployed to the environment, a customer generally won't care about all the specific tasks that you performed through the assessment. What will be of value to them is that you completed the assessment on time and on budget, and you helped them get through any remediation of findings with ease so they can meet their deadlines.

To summarize, you must select metrics that are important to your customers and stakeholders, and remember, they may come from various groups within your organization such as Finance, Sales & Marketing, Legal, and Compliance to list a few. Your metrics need to be customized for what's important for each respective group. Below are a few examples for consideration:

- Percentage of security projects delivered on-time and on-budget
- Customer facing (such as e-commerce sites) incidents and time to remediate
- Productivity incidents and time to remediate
- SLAs on various security capabilities (for example, delivery of evidence to Legal and/or HR on investigations?

Reference

[1] https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf

Metrics Programs Should Be Prioritized

- Metrics programs should provide useful and actionable information on performance and progress against goals such as:
  - Program priorities (including the business)
  - Compliance and/or behavior change
  - Corrective actions and process improvement
- Like any other program, metrics have to be:
  - Properly designed: Visually appealing and easy to understand
  - Economical to collect: Automatic to the extent possible
  - High leverage: Don't collect metrics just because you can
  - Encompass a feedback mechanism in two ways
    - Technical and operational (e.g., tuning and/or corrective actions)
    - Feedback from your consumer (e.g., clarification or additional information requested)

As stated previously, as a security professional, it's your job to understand the quality and progress of your "business of security" as well as communicate value and risks to your leadership in a manner that is easy to consume and relevant enough to make well-informed decisions.

There is not a better, more effective way to understand and communicate all aspects of business than metrics. It's a common language that all leaders understand and has been used for decades. Considering these factors, your metrics program should be a priority.

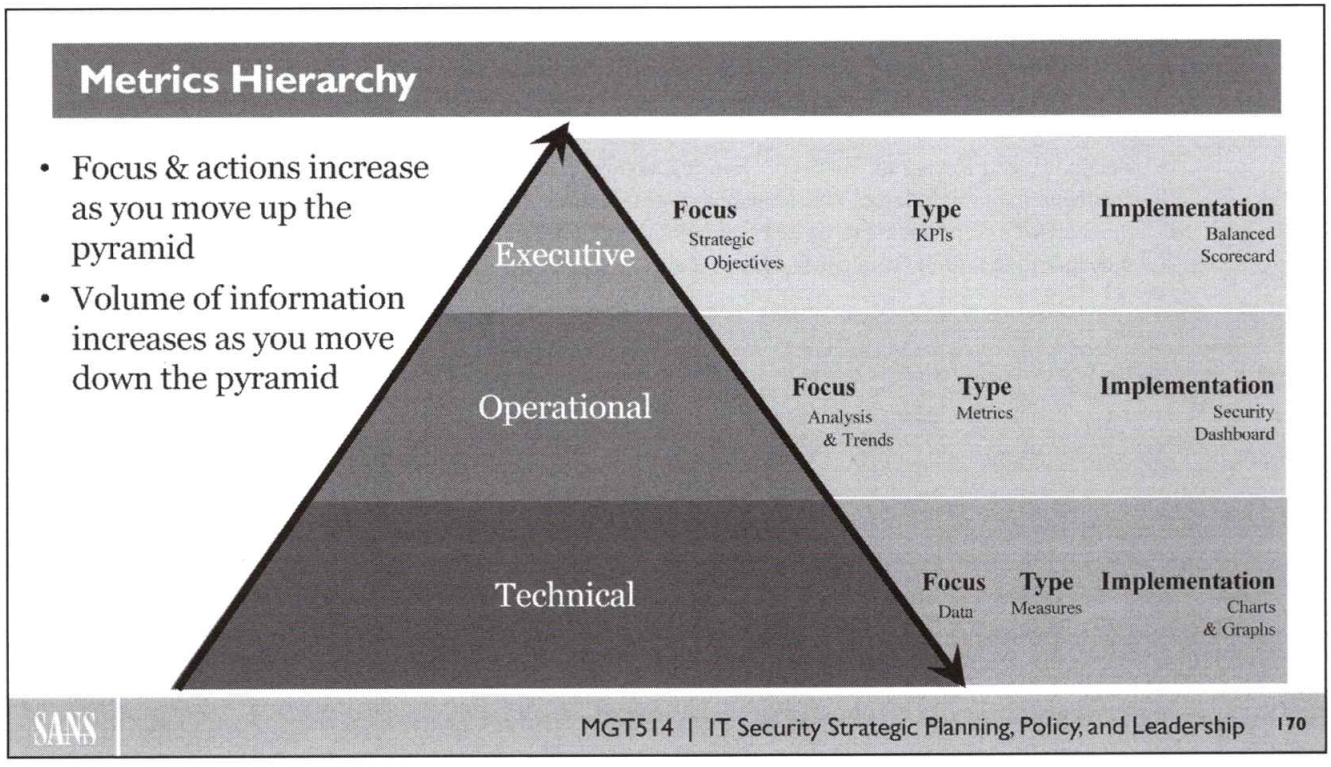
Your metrics program doesn't need to be all-inclusive out of the gate. Your program can mature over time. However, even in program infancy, your metrics have to be:

- **Properly designed:** Metrics need to be properly designed in a manner that is visually appealing and easy to understand. If you are the only one that can understand the data or read the story the data is telling, then this information is useless to anyone besides you and as Albert Einstein said, "If you can't explain it simply, you don't understand it well enough."

- **Economical to collect**: As you develop your program, this should be a prime consideration. With all the metrics options, your program could easily get bogged down in heavy administrative costs to produce. You'll want to automate as many metrics as possible, create a repeatable process to eliminate variation, and re-work.

- **High leverage**: Don't collect metrics just because you can. As we mentioned previously, there are numerous metrics that can be collected for a security organization. You want your resources focused on collecting, analyzing, and producing the most valuable metrics to you, your leadership, and the organization as a whole.

- **Encompass a feedback mechanism:** There are two angles to consider as feedback mechanisms:
  - First from a technical and operational perspective, when the results are produced and analyzed, are there any process and technology considerations that need to change as a result of the results (e.g., policy tuning on network firewalls, corrective actions on processes, etc.)?
  - Secondly, you'll want to work with your leadership, customers, and stakeholders to include any feedback they might have. This feedback might come in the form of questions they have because your metrics were not clear, or items you didn't consider. It might also come in the form of wanting a deeper dive into the root cause of the results.



The metrics hierarchy is an illustrative arrangement or classification diagram designed to help you identify the functional relationships among technical, operational, and executive design elements related to your metrics program. The key thing to remember is focus, actions, and simplicity increases as you move up the pyramid, and volume of information also increases as you move down the pyramid.

Technical

At the base of the pyramid is Technical. The focus here is on data that typically provides a snap shot in time view of specific discrete factors. The example used previously to describe a measurement was 29% (2,574) unauthorized devices on the network. This is the area where you might also include project level details to include on time and on budget. You might want to evaluate resource allocation or customer satisfaction by team. This is the area you will have detailed data, and lots of it. The implementation or output in this area is typically charts and graphs

Operational

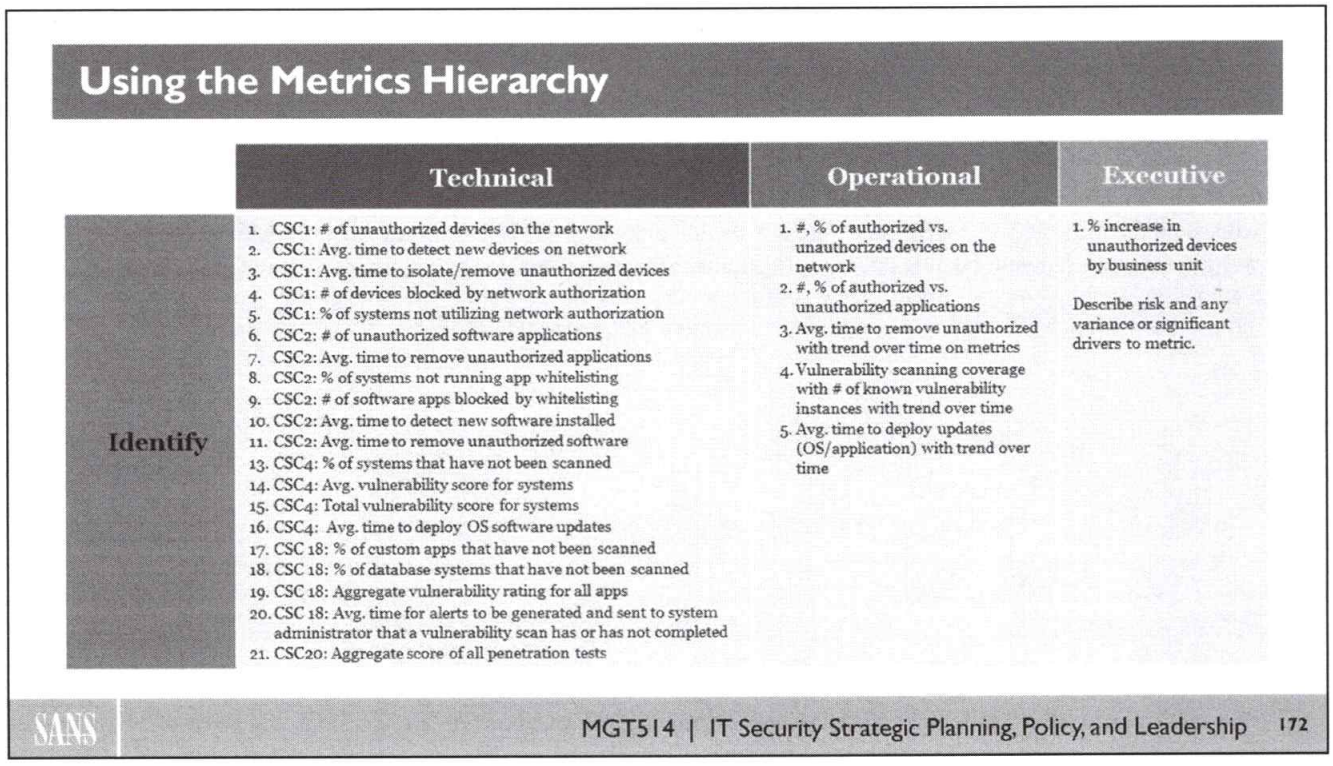
Moving up the pyramid to Operational, your focus and action increases as described in the first paragraph. In this section, the focus is more on analysis and trends, where you will typically use metrics to describe the results. As a reminder, metrics compare a baseline with two or more measurements such as, February, number of unauthorized devices increase by 1,995, and Q1, we had an overall increase of 1,207 (using January as our baseline) as we described in the previous section. The implementation or output in this area is typically a dashboard and for a security organization, this would be a Security Dashboard. We will share attributes of a dashboard coming up later in the section.

Executive

At the top of the pyramid is Executive. Again, your focus and action increase even more. The specific focus in this section is around strategic objectives with results of progress illustrated through Key Performance Indicators (KPIs). KPIs are performance metrics that illustrate progress towards a stated outcome (e.g., on Wed, Sat, and

Sun, we exceeded our target SLAs). Implementation for this section is generally displayed through a tool like the Balanced Scorecard. We will share attributes of a Balanced Scorecard later in this section.

The key takeaway from this slide is to remember as you are designing your metrics program, you wouldn't likely share "all" technical measures with executives for a couple of reasons. You wouldn't want to inundate them with data, just because you can, and you want your story to come through loud and clear. You can do this with selecting the high value KPIs that align to strategic objectives of the organization. At the same time, you wouldn't want to run your business of security on only KPIs. You need to have more information. You need analysis and trending on your security controls and processes to be well informed as a security leader, and you have to have enough information to make decision and/or take corrective actions.



This table further illustrates how focus and actions increase as you move toward the Executive section, and how volume and information increases as you move toward the Technical section.

In this example, we've elected to use the NIST function "Identify" to illustrate what we've been discussing about the various level of the metrics hierarchy. We've listed some measurements, metrics and KPIs to share with you as examples that are likely to appear in each of the respective section on the pyramid.

Again, you wouldn't want to take twenty-one measures to your CEO to describe your security controls. Besides the fact that there is too much information, and the information is not sufficient for them to make important decisions, it doesn't answer the "so what?" At the same time, you wouldn't expect your security operations team to manage its business of security with one metric such as that found in the Executive section.

Security Dashboards

- Security Dashboards should:
  - Focus on analysis and trends that impact the overall health of your security organization, which includes:
    - Financial
    - Customer and stakeholder satisfaction
    - Business processes
    - Security metrics
  - Be designed with a security leader in mind
    - High level, multi-dimensional summary showing:
      - Analysis and trends
      - Highlighting anomalies and variations
      - Illustrating progress to goals

A successful security leader wants to know all aspects of running the business of security. This includes more than just security metrics.

Dashboards are an ideal format to provide the results of your analysis and trends related to operations to security leadership. Carefully selected metrics will provide a good indication of the overall health of the security organization.

The key to remember when designing your dashboard is that you need to have an inclusive set of metric categories such as:

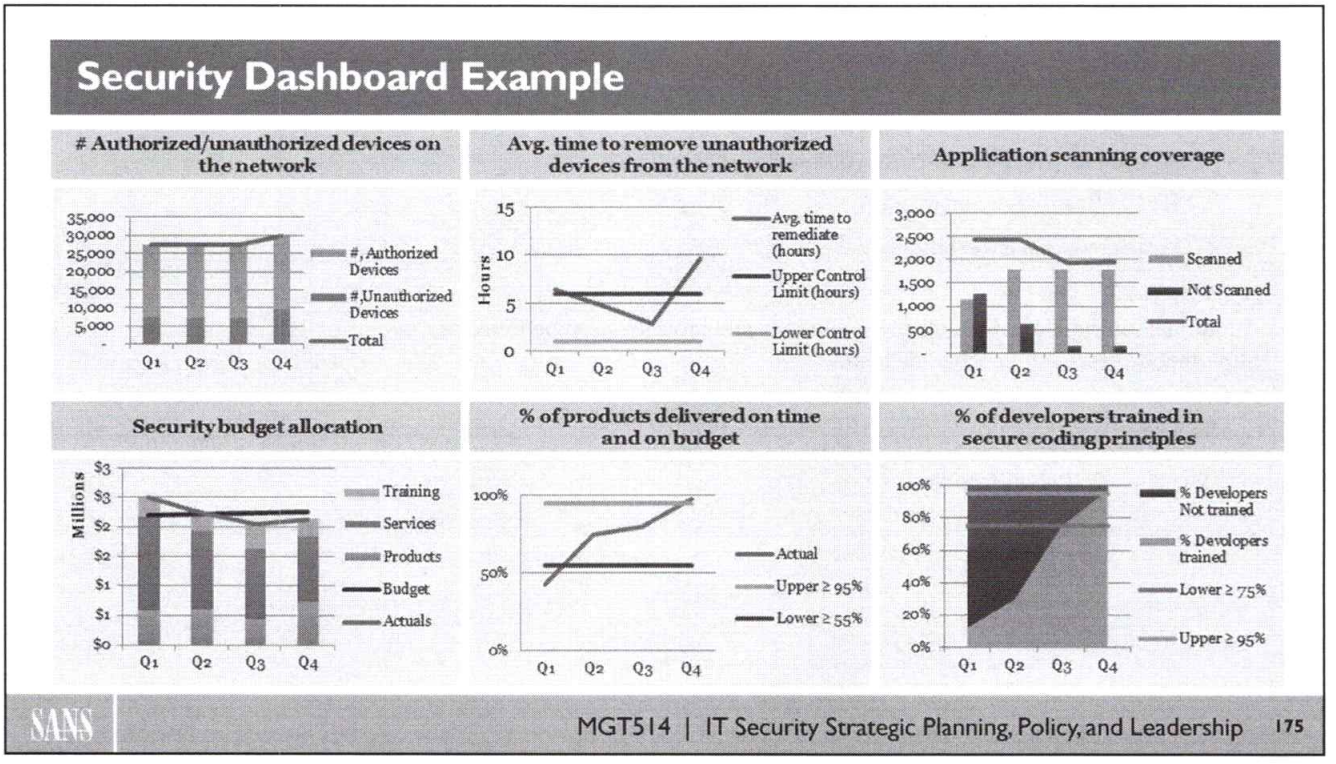
- **Financial:** Metrics that indicate the financial health of your security organization. This might include metrics such as:
  - Security budget allocation, trending and year-over-year comparison. You might also include categories such as OPEX and CAPEX
  - % of security budget compared to overall IT
  - Run rate on high priority initiatives

- **Customer and stakeholder satisfaction**: Metrics that measure what's important to your customers and stakeholders. This might also include regulatory agencies or contractual obligations. This might include metrics such as:
  - % of security projects delivered on time and on budget with outliers explained
  - Incident and down time on customer facing applications such as e-commerce with trend analysis and variation and outliers explained
  - Productivity incidents and time to remediate, with a trend analysis and variation and outliers explained

- **Business processes**: Metrics that communicate how effective and efficient business processes are, and how you are improving over time. This might include metrics such as:
  - Avg. time to deploy updates (O/S and application) against SLA, with trend over time analysis, and variation and outliers explained
  - Avg. time to detect, respond, and remediate an incident against SLA, with trend analysis
  - Avg. time to remove unauthorized devices from the network against SLA, with trend over time

- **Security metrics:** Metrics that indicate how effective and efficient your security controls are, and should illustrate how your security controls are improving. This might include metrics such as:
  - Number of encrypted/unencrypted outbound email containing sensitive information, include false positive, true positive analysis, and trend over time
  - Number of authorized/unauthorized devices on the network including false positive, true positive analysis, and trend over time
  - Number of dangerous websites blocked, with classification analysis and trend over time

Your security dashboard should be designed with the security leader in mind. You need to provide a high-level, multi-dimensional summary of activity across the security organization. Your metrics should clearly show your analysis and trends highlighting any anomalies and variations. You should also be prepared when presenting your dashboard to security leaders, to speak in detail to these anomalies and variations if asked. Lastly, your security dashboard should illustrate your progress to the goal.



This is an illustrative sample of metrics that would be appropriate to display in a security dashboard, the Operational section of the pyramid. As a reminder, your focus is more on analysis and trends when you are describing your results, and metrics compare a baseline with two or more measurements.

An important thing to remember when you are preparing your security dashboard is that you should be prepared to provide additional details on the trend and any anomalies and/or variances. We will describe two of the metrics illustrated on this page for discussion.

- Number of **authorized/unauthorized devices on the network**: Q1, Q2, and Q3 remain steady. In Q4, the number of unauthorized devices increased by 34% (2,458) over Q3 results. Further investigation will lead you to determine this increase is the result of a BYOD pilot program your IT department implemented.

- **Avg. time to remove unauthorized devices from the network**: Will tell the story that in Q1, your response time exceeded your upper control limit. This means you have work to do in improving your response time. In Q2 and Q3, you make tremendous improvements towards your goal (lower control limit), but in Q4 your response time rockets past the upper control limit, which indicates this process is in trouble. Do you think this has any correlation to the first metric we discussed and the root cause could be the BYOD pilot? You need to be prepared to explain this to your leadership.

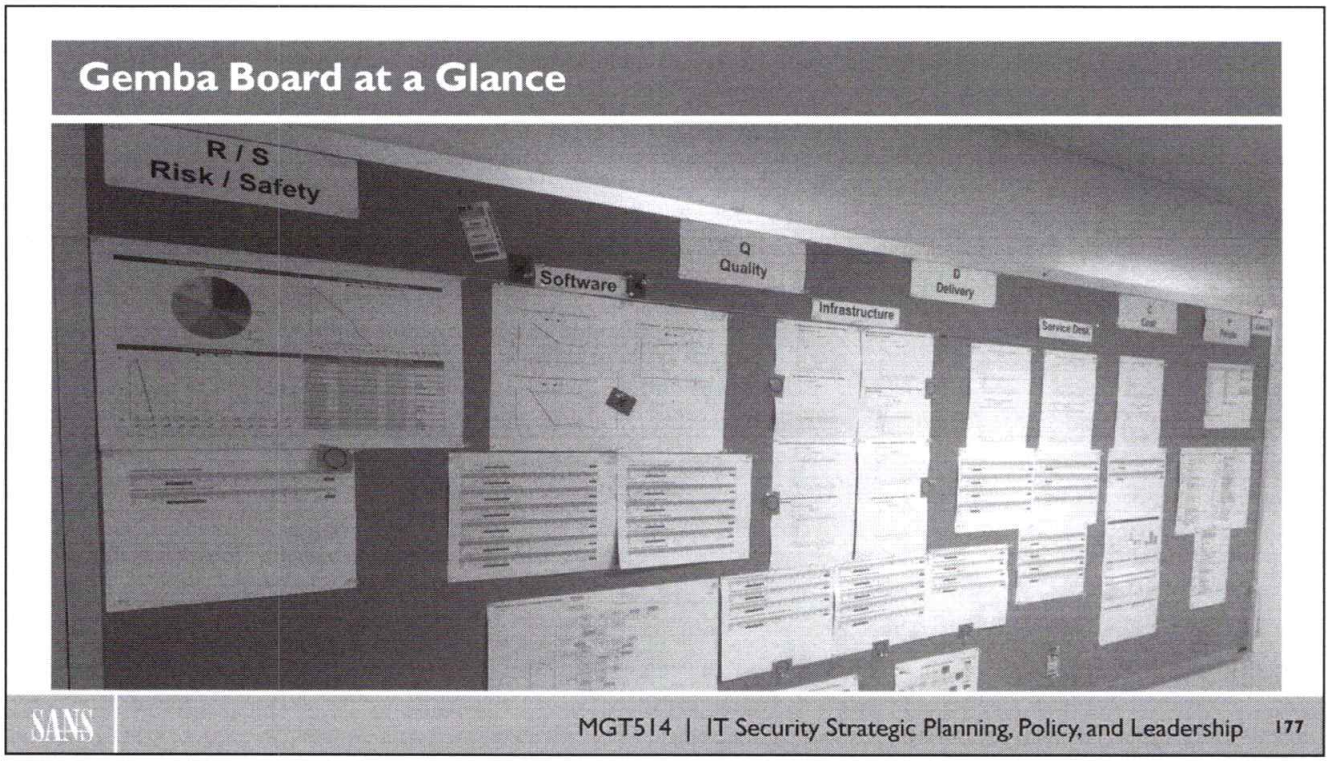
Below is a reference list of Business Intelligence (BI) solutions that can help you automate the output for your dashboard. They are not in any particular order of preference.

- Microsoft BI using SharePoint and SQL Server Reporting (SSRS)
- Pentaho: http://www.pentaho.com
- SiSense: http://www.pentaho.com

- Tableau: http://www.tableau.com
- Domo for BI: https://www.domo.com/roles/bi
- QlikView: http://www.qlik.com
- Beyond Intelligence: http://beyondintelligence.org
- Birst: https://www.birst.com
- Board: http://www.board.com/

Additional information about other BI solutions and processes can be found at http://thebusinessintelligenceguide.com.

The top 50-rated BI tools from Docurated can be found at http://www.docurated.com/all-things-productivity/50-best-business-intelligence-tools.



A Gemba board can be an effective place to start for your security reporting efforts.

Jack Nichelson, who was recognized by SANS as one of the "People Who Made a Difference in Security in 2013," provided the Gemba board image above. Paraphrasing, he describes Gemba as the Japanese expression, identifying the location where value is created. Jack's Gemba board is located on a prominent wall near his office that includes security components for five distinct areas of the security department:

- **Security**: Data capturing the risk assessments, attacks, incidents, and other important threat or business metrics
- **Quality**: Performance metrics such as the SLAs delivered by the security team and customer feedback data
- **Delivery**: Metrics about the roadmaps, milestones, and completion schedule for security initiatives
- **Cost**: Information about the budget, costs, and life cycle of security projects being used at the company
- **People**: Training schedule, on-call contact information, and other relevant security team staffing and organizational data

The public nature of the board generates discussions during scheduled stand-up meetings as well as with executives that walk by and stop when something catches their attention. Building a Gemba board can effectively get the security conversation started. What you show and how you display your data will keep the discussion going.

Gemba is often used in lean manufacturing[1] and the "Gemba Walk" is the process of visually identifying areas of improvement by viewing the front lines of a manufacturing floor, workers, and technologies.

Often, Gemba is used to reduce the effects of the seven wastes.[2] These include:

- Defects
- Overproduction
- Stagnate inventory
- Over-processing
- Inefficient employee motion
- Transportation and handling waste
- Waiting or idleness

These same principles can be applied to information security.

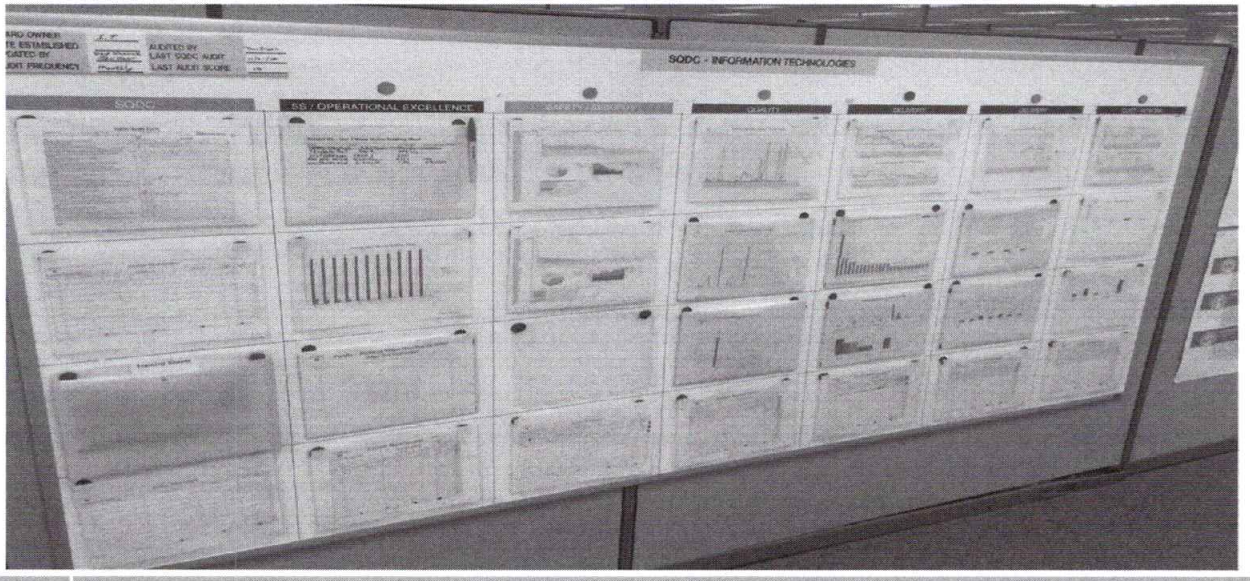
"The most dangerous kind of waste is the waste we do not recognize."—Shigeo Shingo

References

[1] http://www.lean.org/WhatsLean/

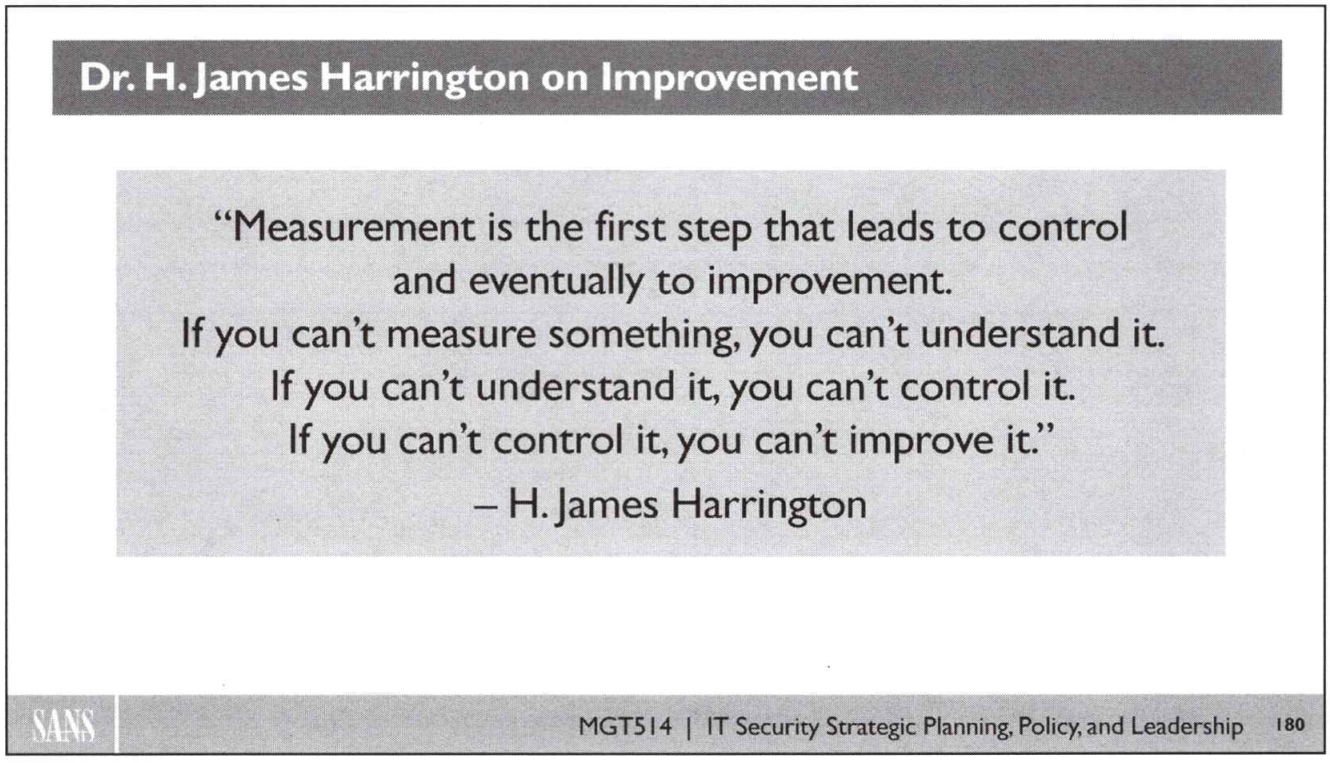
[2] http://www.systems2win.com/LK/lean/7wastes.htm

Gemba Board at a Glace (2)



In information security, the Gemba board can be a highly effective tool to gather IT and security teams together to review the most relevant metrics or areas where improvement is needed. Socializing and discussing the areas needed for improvement in a regularly occurring discussion can greatly improve the visibility and provides greater accountability for those involved. Gemba boards are also very useful when executives attend the stand-up discussions, and they can be highly effective change agents in organizations that are struggling to get traction with security initiatives.

The Gemba board above was provided by Ed Pollack and is a recent example of an approach that has worked to change culture.



IBM quality expert Dr. H. James Harrington is credited with developing the cost of poor quality (COPQ) concept.

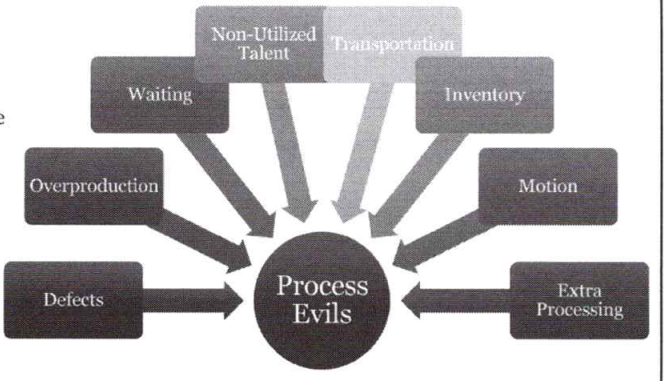
Dr. Harrington defined COPQ in his 1987 book *Poor Quality Costs*. COPQ is a refinement of the concept of quality costs, or the total costs of related problems associated with creating a quality product or service. IBM undertook an effort in the 1960s to study its internal quality process, and Harrington helped identify process improvement steps and quality measures that made IBM a technology leader.

Dr. Harrington also went on to write other books such as the *Business Process Improvement Workbook: Documentation, Analysis, Design, and Management of Business Process Improvement* and *Statistical Analysis Simplified: The Easy-to-Understand Guide to SPC and Data Analysis.* He also wrote or co-authored dozens of other books including Six Sigma and process improvement handbooks and *The Complete Benchmarking Implementation Guide: Total Benchmarking Management.*

These concepts apply to information security efforts as well. It is critical for security practitioners to provide accurate benchmarking, statistical measurement, and Key Performance Indicators (KPIs) to executives so they can understand current threats, the controls already implemented to mitigate those threats, and the gaps that exist in security controls or policies that are needed to manage the residual risk.

Metrics Should Drive Process Improvements

- Metrics will help you identify "DOWNTIME"
  - **D**efects: Products or services out of specification and require correction
  - **O**verproduction: Producing too much of a product
  - **W**aiting: For previous step in the process to complete
  - **N**on-Utilized Talent: Employees not effectively engaged or utilized
  - **T**ransportation: Items or information that is not required to perform the process from one location to another
  - **I**nventory: Inventory or information sitting idle (not being processed)
  - **M**otion: People, information, or equipment making unnecessary motion
  - **E**xtra Processing: Performing any activity that is not necessary to produce a functioning product or service.



On this slide, we have described eight Process Evils. Process Evils equate to process waste. Waste can cause processes to be ineffective, inefficient, or cumbersome, costly, and there is a high likelihood that your customers, stakeholders, and even your employees are negatively impacted.

Removing waste from your processes will increase your effectiveness and operational efficiency, ultimately increasing your customer, stakeholder, and even your employee's satisfaction.

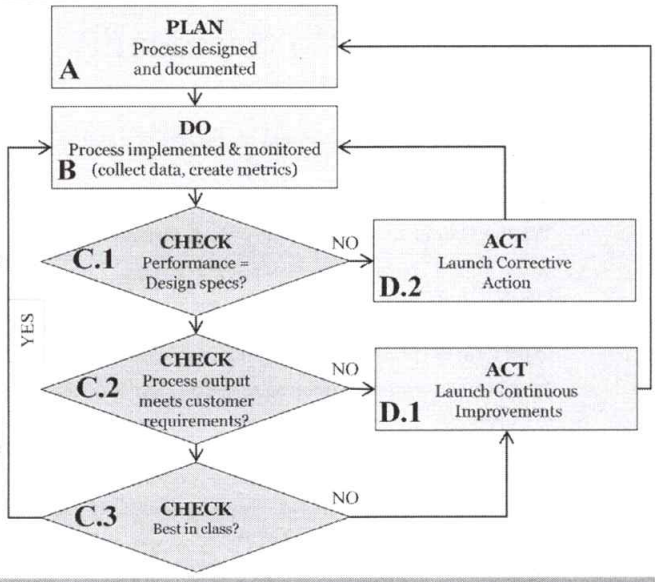
You can evaluate your processes using metrics to determine whether you have any "DOWNTIME."[1] In the next few slides, we discuss this further, and we look at a simple diagram that will take you through process review in an effort to determine effectiveness and operational efficiency. As a reminder, effectiveness is "doing the right thing" and efficiency is "doing the thing right."

Reference

[1] https://goleansixsigma.com/8-wastes/

Process Improvements: Plan, Do, Check, Act (PDCA)

- Process owners need to know where they are at all times
  - They need to be leading the efforts to continually move down through this flow
  - You need to wear two hats: technical expert and consumer
  - Ensuring rapid and appropriate response will ensure a great success for you
- A simple formula to validate your effectiveness and efficiency
  - **A** = What we do (process designed & documented)
  - **B** = How we do it (process implemented & monitored)
  - **Cs** = Results we achieve (C.1, C.2, and C.3)
  - ***IF*: C is inadequate, change A and/or B by launching a D**



Plan, Do, Check, Act (PDCA)[1] is an iterative four-step management method used in business for the control and continuous improvement of processes and products. Dr. W. Edwards Deming (who is considered by many to be the father of modern quality control) made PDCA popular.[2]

Process owners need to know where they are at all times. Don't be fooled by the term "process owners" because security professionals are process owners. For example, someone will own the process for data loss prevention, someone else might own the process for vulnerability management, and there might be an incident management process. Security has many more processes than described here, but the point is that security has process, and should have process owner(s) who are accountable for ensuring operational effectiveness and efficiency. Using the PDCA tool will help you as a security professional/process owner do that.

PLAN (A): Process designed and documented. In this step, you are establishing the service objectives and processes necessary to deliver expected results (target or goals). The services are the outputs that you deliver to your customers and/or stakeholders. "Services" could literally mean a service you provide with or an actual product such as a widget or related to security it might be an antimalware solution. It could also mean internal services such as a work output required by others in your organization. A security example of services would be assessments, advisory, remediation, etc.

DO (B): Process implemented and monitored (collect data, create metrics, etc.). This includes the total array of methods, processes, activities, and controls that people in the specified process follow in their efforts to deliver the required outputs described in "PLAN." It's important to monitor your process, and collect data for analysis for evaluation that will occur in the "CHECK" step below.

CHECK (C.1, C2, C3): Study the data collected in the "DO" step, and compare against the expected target or goals from the "PLAN" step. The key in this step is to look for deviation from the plan, and look for

appropriateness and completeness. Metrics can make this much easier to see trends. The results here are vital to the success of your organization. If any of the Cs is fully satisfactory, the B is working for the delivery of A and your baseline will continue or if improvements were made, the improvements will be your new baseline. If any of the Cs are unsatisfactory, then B is not working for the delivery of A and you must ACT and do something about it.

- **CHECK (C.1) Performance – Design specs?** This step or control is to ensure that the process performs the way it was designed. The design should also include some dimension of volume or capacity for the process. Few processes have infinite capacity and adding more workers or machines will not necessarily work as volume increases beyond a certain threshold.

- **CHECK (C.2) Process output meets customer requirements?** This step is the market response to the value of the services delivered (as they are delivered). This measure indicates the extent to which the specifications of the service offering are aligned to the real requirements of the customers and/or stakeholders. In other words, how well your services are aligned with their needs and values. Here is a very strong hint for you. The client's needs are always changing, and you need to be in lock step partnership with them to ensure you keep up with the demands and expectations.

- **CHECK (C.3) Best in class?** This step provides the opportunity for your organization to be proactive in leading the direction for the type of service offered. Competitive information is valuable within this context but not necessary. An assumed virtual competitor can serve as the philosophical threat that will take market share from you by delivering greater value than you do. The virtual competitor is working to move through the same logic flow (above) more quickly than you are. If it sets the pace, you will be a market follower and not likely to attract or maintain the best customers and/or stakeholders.

ACT (D1, D.2): Based on the results in the CHECK step, you will either Launch a Corrective Action **(D.2)**, and then go back through the process cycle to see whether the new results are satisfactory, or you will Launch a Continuous Improvement **(D.1)** where you will go back to the beginning of the PLAN phase.

A fundamental principle of this method is once a hypothesis is confirmed (or negated); executing the cycle again will extend the knowledge further. Repeating the PDCA cycle can bring us closer to the goal, usually improved operations and output.

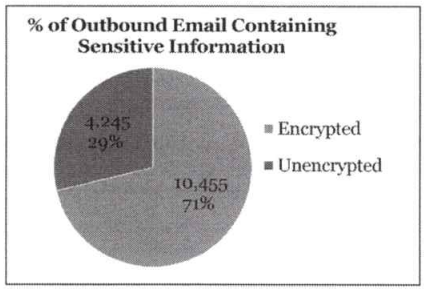
For this model to be successful, security practitioners within your organization need wear two hats: 1) a technical expertise hat sufficient to understand and communicate the service deliverables and processes and 2) a business manager hat always knowing where they are in the flow model described above and ensuring the rapid and appropriate responses to the monitoring (diamond) results indicated.

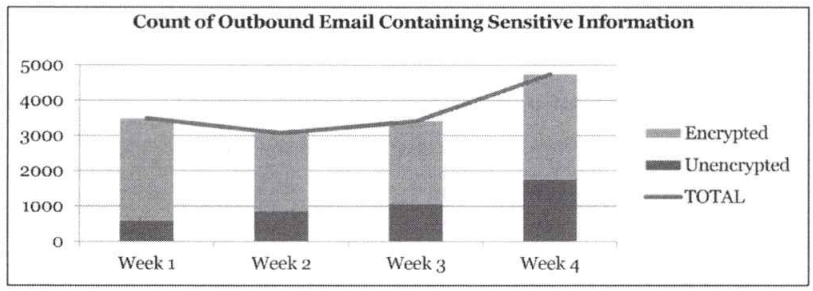
References

[1] https://en.wikipedia.org/wiki/PDCA

[2] https://en.wikipedia.org/wiki/W._Edwards_Deming

Example of Using PDCA and Metrics to Identify Opportunities





- Is 29% Unencrypted acceptable?
- Is 29% an anomaly and if yes, what is the root cause? OR
- Is the trend something I should be concerned with?

Conclusion:

- It's determined that 29% is NOT an acceptable % of outbound email containing sensitive information
- The trend is increasing week over week
- I need to implement improvements to minimize risk to the organization
- **Where do I start?**

For the purposes of this example, we are going to assume that you have already completed your PLAN step by designing and documenting your controls process around outbound emails containing sensitive information. In addition, you already completed your DO step by implementing and monitoring your controls. You have collected the data and created metrics. Now, let's see whether our process is satisfactory.

First, we take a look at **% of Outbound Email Containing Sensitive Information**. In this measure, 29% (4,245) outbound emails are unencrypted.

The first question is C.1: Is our process performing as designed? The answer is yes—our encryption controls are working as designed.

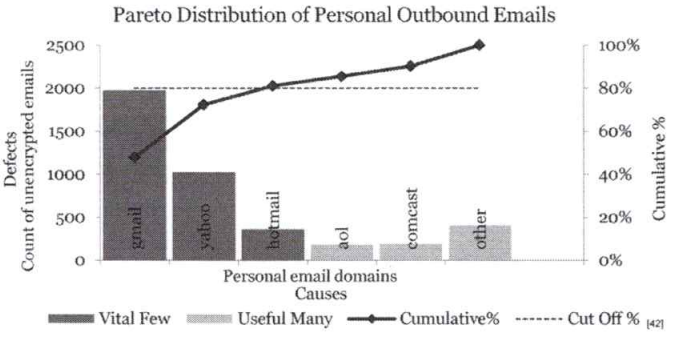
The second question is C.2: Is our process output meeting our customer requirements? It's not likely that 29% of the volume of emails containing sensitive information unencrypted would be acceptable to your organization. But before you go to your leadership, you might want to perform some additional analysis to better understand what's going on with this process.

If you look at the Count of Outbound Email Containing Sensitive Information graph, you'll see that the trend for unencrypted outbound email is increasing week over week, and therefore, the point in time measure of 29% is not an anomaly. As a security professional accountable for this process, you need to immediately ACT and Launch a Continuous Improvement (D.1) to get the output up to par with our customers' and stakeholders' expectations. But where do you start?

Example of Using PDCA and Metrics to Identify Opportunities

Data deep dive unencrypted outbound emails

- Let's look at the email recipients
  - The first 3 causes cover 81.11% of the total Defects
- If you address the vital few, you will address 81.11%% of the problem
- You could approach this in a number of ways depending on the risk appetite of your organization
  - Block the domains
  - Force encrypt domains
  - Security Awareness Training



Cumulative Percentage Cutoff: 80%

#	Causes	Defects	Cumulative%
1	gmail	1975	47.65%
2	yahoo	1024	72.35%
3	hotmail	363	81.11%
4	aol	182	85.50%
5	comcast	195	90.21%
6	other	406	100.00%

A good place to start to understand what is driving 29% of outbound emails containing sensitive information to be unencrypted is to do a deep dive of the data using a Pareto chart (Pareto distribution diagram), which is a vertical bar graph where values are plotted in decreasing order of relative frequency left to right.

Pareto charts can be used to quickly and easily identify what business issues need priority attention, by using hard data instead of guessing; in other words, a Pareto chart will help you identify the vital few areas you should focus on to get the biggest gains for your effort.

In the example, Pareto Distribution of Personal Outbound Email, you can see that the first three personal email domains (gmail, yahoo, and hotmail) account for 81.11% of the problem. If you focus your approach on managing these domains, you would solve over 80% of your problem.

There are a number of ways you can approach this problem depending on the risk appetite of your organization and the needs of the business. Following are a few examples for consideration. It's important to know that your options are not limited to only one solution.

If your company has a low tolerance for risk, or you believe there might not be a legitimate business use case for these domains, you might consider blocking the domains outright. If your company has a medium tolerance for risk, and there could potentially be a legitimate business use case for these domains, you might want to consider forced encryption. Lastly, if your company has a high tolerance for risk and you are uncertain of the use cases, you might want to approach this through security awareness training.

Harold S. Geneen on Performance

"It is an immutable law in business that words are words, explanations are explanations, promises are promises but only performance is reality."

- Harold S. Geneen

Harold Sydney Geneen[1] was an American businessman most famous for serving as president and CEO of ITT Corporation. He grew the company from a medium-sized business with $800 million sales into a multinational conglomerate with $17 billion sales ranking ITT as America's 11th biggest firm. ITT extended its interest from manufacturing of telegraph equipment into insurance, hotels, real estate management, and other areas.

ITT grew primarily through a series of approximately 350 acquisitions and mergers in 80 countries. Some of the largest of these were Hartford Fire Insurance Company in 1970 and Sheraton Hotel.

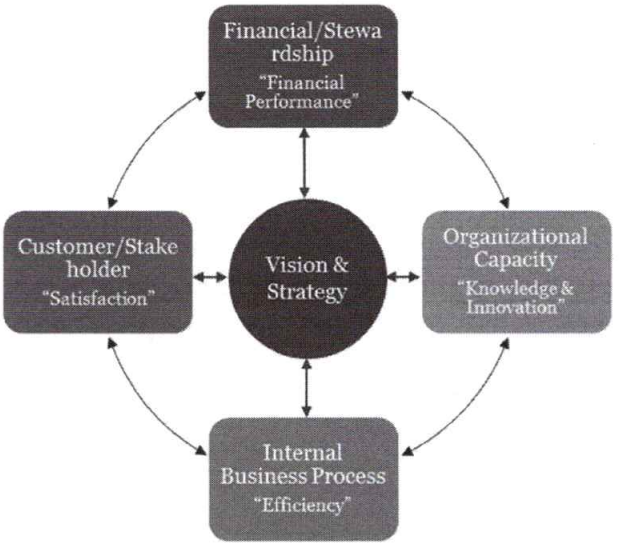
In 1977, Geneen retired as CEO and president and was chairman of the board until 1970. He stayed on the board four more years.

Reference

[1] http://www.economist.com/node/108412

Balanced Scorecard

- Strategic planning and management
  - Executive metrics
  - Focus on strategic objectives
  - Using KPIs
- Used across all industries
  - Including security
  - Align business activities to vision and strategy
  - Improve communications
    - Internal
    - External
  - Monitor performance against strategic goals



As a reminder, at the top of the pyramid is the Executive layer where the focus is on strategic objectives with results of progress illustrated through KPIs (performance metrics that illustrate progress towards a stated outcome). Implementation for this top of the metrics hierarchy pyramid can be displayed through a Balanced Scorecard.

As you design a Balanced Scorecard, don't inundate executives with data. Select high-value information that will tell your story in the most compelling manner. This information should always be aligned with the strategic objectives of your organization.

Balanced Scorecards are used across all industries, including security. If designed well, they can improve communications internally and externally. A Balanced Scorecard generally views an organization from four perspectives to tell a holistic story: 1) financial, 2) capability, 3) process, and 4) customers and stakeholders.

Focusing on all four areas helps keep the vision and strategy aligned.

Financial Stewardship – "Financial Performance"

From a financial perspective, the Balanced Scorecard will measure the financial capabilities of a company, or in the case that we are describing here, for your security organization. It will describe the capability to spend, and/or gain money through profit streams, and very importantly, how you are sustaining your business with existing funds. As we discussed previously, you'll want to look at the Financial Performance on the Balanced Scorecard from two angles, first: How much does it cost to operate Security? This is directly related to your security budget. Secondly, you'll want to include the cost of incidents to your company overall. This would include direct loss, downtime, cost of containment, recovery, and restitution. For metric examples, please refer to the "Metric Selection Is Important" slide.

Organizational Capacity – "Knowledge & Innovation"

In this section of the Balanced Scorecard, you want to include indicators that illustrate your security organization is improving from a capability and capacity standpoint, such as improving tools and technology, and how you are improving knowledge and skillsets, such as strategic security awareness training for the organization or how you are developing and retaining top talent. You might want to "customize" this category for security by naming it "Security Capability" to make it more meaningful for your team.

Internal Business Process – "Efficiency"

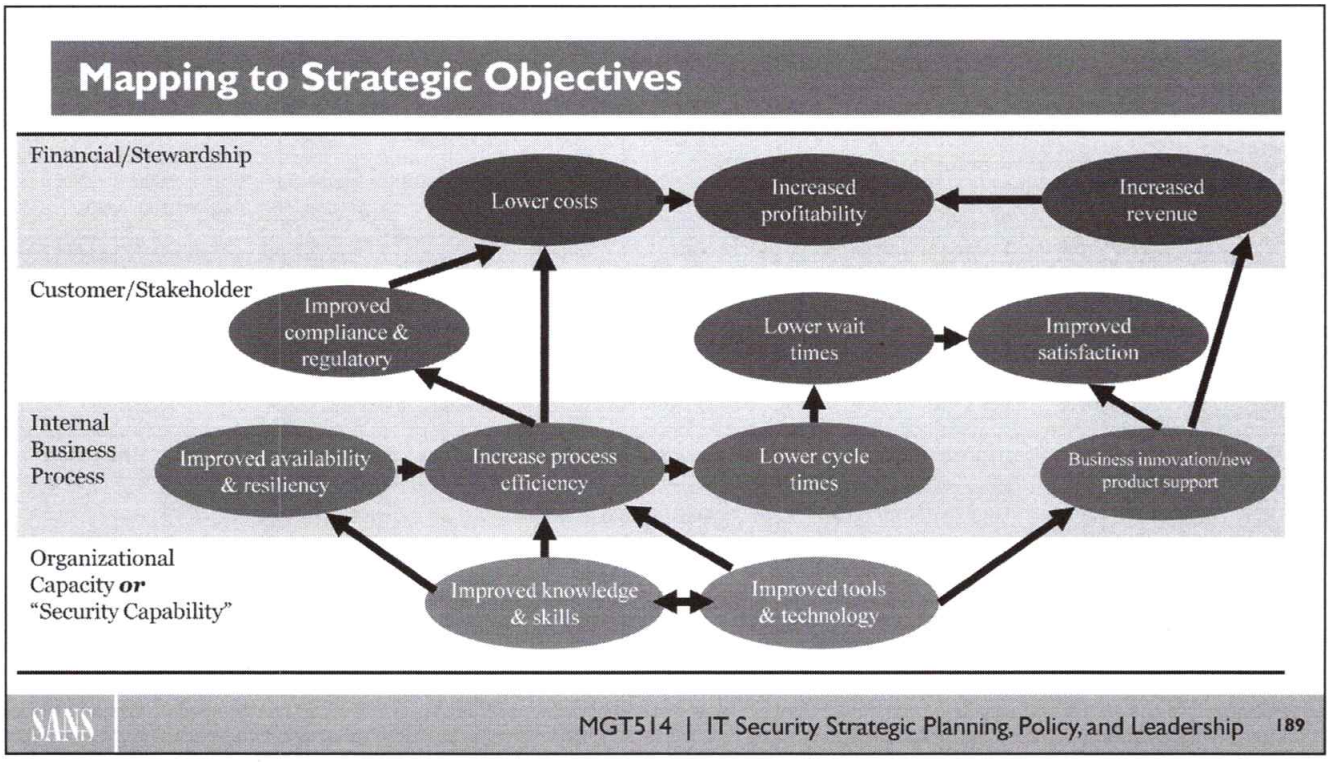
In this section, the KPIs communicate how effective and efficient your business processes are, and how you are improving over time. As a reminder, the results in business processes often influence how satisfied our customers are, and it's equally, if not more important, to select KPIs for this section that our customers will value.

Customer/Stakeholder – "Satisfaction"

Select KPIs for this section that are important to your customers and stakeholders. You must understand what types of services or business processes your security organization provides and what they value. For instance, Finance and IT might value the % of security projects delivered on time and on budget, whereas Sales and Marketing might value customer-facing incident time to remediate from their customer-facing e-commerce sites, and Legal and HR might value meeting SLAs to produce electronic evidence files involved in investigations.

Reference

http://balancedscorecard.org/Resources/About-the-Balanced-Scorecard

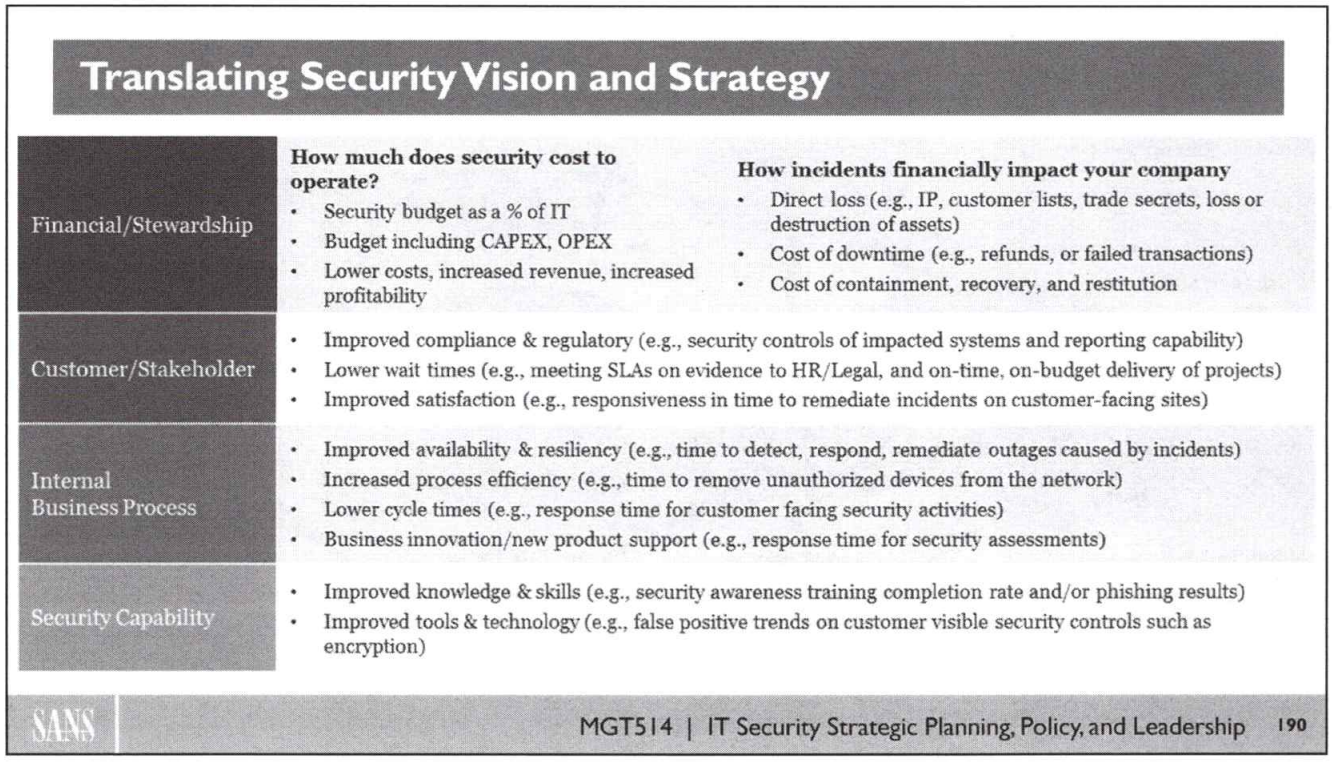


On day one, we introduced "Mapping to Strategic Objectives." As a reminder, we as security professionals often focus on the bottom row of this diagram; improving our security capabilities by increasing our knowledge and skills or improving our tools and technology. It's critical that we expand our line of sight and align our activities and efforts to the overall strategic objectives for the organization as a whole, which includes Internal Business Process, Customer/Stakeholder, and Financial/Stewardship.

Mapping your organization's strategic objectives to the Balanced Scorecard quadrants will help you tell the story of how value is created by your security organization. A diagram such as this will highlight the cause and effect of your security initiatives and activities that will make sense to the business as a whole. As an example, if you were to have a strategic initiative to support business innovation/new product support that would in turn improve customer/stakeholder satisfaction and likely increased revenue. This is something the business understands and appreciates.

Reference

http://balancedscorecard.org/Resources/About-the-Balanced-Scorecard



Now that you've mapped your organization's strategic objectives and you have a better understanding of what is important for your organization, you will need to translate this information to your Security Vision & Strategy in order to ensure the output of your Balanced Scorecard has meaningful information that you can share with executives. As a reminder, you don't want to inundate executives with data just because you can.

Balanced Scorecard Example

Financial/Stewardship

Q4 % Product Development Budget Allocated to Security

Target 5% ✔
Trend →

5%

- Increased support for legal as they piloted their case management system

Q4 & YTD Security Budget Allocation

	Q1	Q2	Q3	Q4	YTD
Products	$575,000	$597,000	$425,000	$732,000	
Services	$1,590,000	$1,320,000	$1,190,000	$1,090,000	
Training	$326,000	$315,000	$427,000	$301,000	
Actuals	$2,491,000	$2,232,000	$2,042,000	$2,123,000	
Budget	$2,190,000	$2,211,900	$2,234,019	$2,256,359	
$ Variance	-$301,000	-$20,100	$192,019	$133,359	

Customer/Stakeholder

Q4 % of Products Delivered On Time and On Budget

Target 95% ✔
Trend ↑

95%

- 18% increase over Q3 in on-time and on budget delivery. Security staffed temporary PMO team to meet goal

Customer Satisfaction

Target 90% ✗
Trend ↑

85%

- 8% increase over Q3 in customer satisfaction rating of 4 or higher out of 5 possible

Internal Business Process

Q4 % of Developers Training in Secure Coding Principles

Target 95% ✔
Trend ↑

97%

- 100% of flagship application developers completed training reducing overall risk to organization

Q4 % of Developers Attaining Certification

Target 95% ✗
Trend ↑

42%

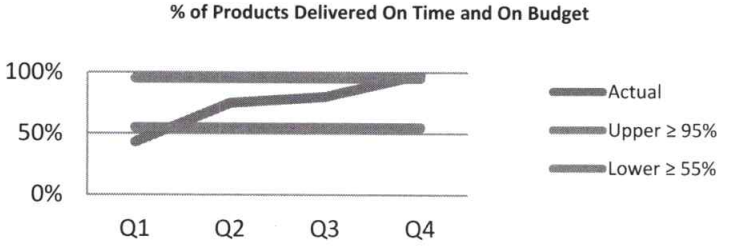
- Mitigation plan: Follow-up with developers after training is complete for certification

Earlier in this section, we talked about the shift we are seeing in Security where more and more security professionals are being brought before executives and asked to demonstrate the effectiveness of their security program. Executives and board members want to quickly understand whether the decisions they made to fund security has helped achieve a competitive advance or will help keep them out of the news.

It's important to remember that executives are tasked with making many decisions in a day across multiple lines of business. The more relevant, useful informative information you provide to them, the more confidence they have in you and your security capabilities, and the easier it is for them to come to an informed conclusion and make decisions.

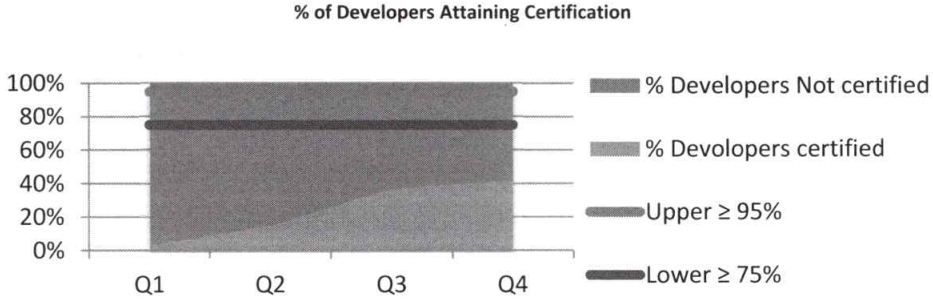
It's critical that you find the right KPIs that are of value. It's equally as important to provide a multi-dimensional view so they have a complete understanding of targets and trends, and very high-level summary of trend drivers. You will see we elect to display a much different view for our executives than the charts and graph we use on a security dashboard.

As an example, look at the middle top tile—Q4% of products delivered on time and on budget. We have met our target of 95%. Our trend indicates a positive increase, so we describe the driver behind this for example, 18% increase over Q3, because we staffed a temporary PMO team to meet goals.



Another example is in the middle bottom tile—Customer satisfaction. Our trend over time is increasing showing an 8% increase over Q3 results. We have not met our target of ≥ 90%, but we are within the control limits we established.

One last example is in the right bottom tile—Q4% of Developers Attaining Certification. We have a target of ≥ 95% and our trend is increasing over Q3 results, but we are still well below our lower control threshold of ≥ 75%. You will want to let executives know what you are doing to turn this KPI around to reflect positive results as in this example—you will do immediate follow-up with developers right after training to encourage certification completion.



Balanced Scorecard Example

Security Capability	Status	Trend	Highlights

Identify: Manage risk to systems, assets, data, and capabilities	Yellow	↑	• 32% increase in unauthorized devices
			  • 29% IT
			  • 3 % HR
			• 27% increase in unauthorized software
			• Attributed to Q4 BYOD pilot

Protect: Ensure delivery of critical infrastructure services	Green	→	• 12% of users failed sponsored email phishing tests • 15% of employees have not passed security awareness assessments
Detect: Identify occurrence of a cybersecurity event	Green	↓	• 27% decrease in elevated access accounts • 275 total elevated access accounts
Respond: Take action regarding a detected cybersecurity event	Green	→	• 5% of database systems with sensitive information have not been scanned by vulnerability scanners
Recover: Maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity event	Red	↑	• 34% of systems not enabled with up-to-date anti-malware • Attributed to Q4 BYOD pilot

KPI selection for this section of the Balanced Scorecard is very important. They should align to what's important to the organization. We've established that there are many metrics you could use to describe your security controls but for this section, you really want to select metrics that will be meaningful to executives and what they need to know versus what you want to tell them.

What executives need to know is how is security improving the risk posture of the organization, how is security supporting strategic imperatives, what business units should they be concerned with, and how you are going to keep your executive team out of the news. You'll want to do this through displaying improved knowledge and skills, and improved tools and techniques.

For this Balanced Scorecard example of security capabilities, we've elected to use the NIST functions as technology categories and selected KPIs that align to strategic imperatives.

We have also listed two security initiatives that align to our company's overall strategic imperative to make our environment more secure through developer training and certification.

As a reminder, you want to be very selective with what you choose to display on your Balanced Scorecard in this section. You have to provide just the right amount of information to answer the "so what" and allow them to make important decisions in a very short amount of time.

Metrics Visualization Considerations

- When you build your metrics program:
  - Discuss visualization strategy with your Marketing team
    - They are experts in message management
    - Will help you follow branding and style guides for your organization
  - Avoid busy-looking charts and graphs that appear cramped or confusing
    - Test your message on subject matter experts
      - To ensure the message you're trying to convey is the message that will be received
        - Balanced scorecards—Test on someone who is non-technical
        - Security dashboards, charts, and graphs—Test with your security peers
  - Remember there is an element of art and design in this work
    - Use colors in a familiar way (e.g., green = good, and red = bad)

You've gone to great lengths to build your metrics program from gathering raw data and turning this into valuable information for you and your teams, leadership, customers and stakeholders, and the executives of your organization. It's vital that your reports whether they are charts and graphs, a security dashboard, or a Balanced Scorecard are relevant and most importantly persuasive. But that's not enough. The data must be portrayed in a manner that is visually appealing, logical, and tells the story you are intending.

You can avoid confusion regarding the meaning of your information if you are mindful of your audience. Take your security hat off and put your business hat on, and view it through the lens of your audience.

In addition to this, you'll want to discuss your visualization strategy with the Marketing team or an employee that has experience in design. Your marketing department has experts in product design, and can help you manage your message effectively and help you follow branding and style guides for your organization.

Avoid busy-looking charts and graphs that appear cramped or confusing. You might want to test your message on subject matter experts to ensure the message you're trying to convey is the message. You might also want to test on someone that is non-technical to ensure your information is business consumable. For the security dashboard and associated charts and graphs, you might want to test on your peers to ensure alignment with your message

There is an element of art and design in this work. You will want to use colors in familiar ways (e.g., green = good, and red = bad). When using colors, you also need to factor in the chance that your report might be printed out in black and white or a member of your audience might be color-blind. It's always good practice when using colors to accompany the color with its designated work.

Metrics Communication Guidelines

- Technical/Charts and graphs
  - Focus on data and measurements
  - Daily, weekly, monthly review as appropriate
  - Staff meetings and/or direct report meetings (1:1's), cross-functional team meetings.
- Operational/Security Dashboards
  - Focus on analysis and trends
  - Monthly review with security leadership and metrics owners
  - Real-time alerts when process and/or technology deviates outside control limits
- Executive/Balanced Scorecards
  - Focus on strategic objectives (high level and business consumable)
  - Monthly review with executives and key stakeholders
  - Monthly or quarterly review with Board of Directors

Security is not exempt from demonstrating value, and your metrics program is an ideal way to communicate and socialize your efforts whether it's across your teams, to your peers, for your leadership and executives, and to your customers and stakeholders.

We've provided a basic set of guidelines on this slide for each of the sections we've covered: Technical, Operational, and Executive. It's understood that you might have additional communication requirements and you might need to customize your communications methods and cadence to meet the needs of your organization.

Metrics – Pitfalls to Avoid

- Get leadership support
  - Show how your efforts can better demonstrate Security's commitment and value
- Too much information, too soon
  - Be selective
  - Collect feedback and incorporate it
- Wrong information
  - Select information appropriate for your audience (e.g., leadership, executives versus operations)
- Inaccurate, misleading, and/or incomplete information
  - Check and re-check your information for errors
  - Define confusing terms and all acronyms

Get leadership support: You need to gain support before you begin to develop your metrics program. The best way to do this is by showing them how your efforts can better demonstrate Security's commitment to supporting organizational strategic imperatives and better indicate the overall health of the security organization.

Too much information, too soon

We have established that there is an abundance of data related to security that can be translated into valuable information, but just because it's there, doesn't mean you need to use it all out of the gate. Be selective on what you choose to display, solicit feedback to ensure value, and build on your program and collect only data that is used. There is nothing more frustrating to teams that do perform an activity and generate an output that goes into a black box and nobody sees it.

Wrong information

This has been a historic problem not only in Security and across all industries. People want to display what's important to them in an effort to describe how busy they are, and how much value they bring to the organization. What is important to a security operations analyst might not be what a CEO needs to know. This is not meant to diminish what's important to security operations analysts—they are very valuable and that's why they were hired to do the job, but the information analysts need to do their jobs more effectively and more efficiently might not be the same information a CEO needs to know to make a decision to fund security initiates. Make sure you select the right things to share, and they are addressing the questions people are asking.

Inaccurate, misleading, and/or incomplete information

A good practice is to always validate and re-validate your information. There is nothing that will take your credibility away faster than if you have reporting errors or misleading information. Make sure you clarify the intent of your information with others to ensure the same message received is the same message you intended to deliver. It's always a good idea to define any terms and acronyms that might be confusing to your audience.

Exercise 2.4 – Security Metrics

Estimated Time: 15 Minutes

- Goal of this exercise
  - Identify security metrics that support overall business goals and strategic objectives
- Develop metrics for PharmaCo
  - Review the strategic objectives and initiatives on the next slide
  - For each initiative, write down at least one metric that can be used to support the business

NOTE

Don't read the next section

It contains a debrief and potential exercise answers

Your good friend Cheryl Miller was originally hired as director of security strategy but quickly rose to the rank of interim CISO of PharmaCo as a result of her hard work and efforts to understand the company and the needs of her business partners. She did this by accomplishing the following:

- Gained an understanding of the values and cultures of the organization and the current state through SWOT, PEST, and historical analysis
- Defined the future state at a very high level through her visioning process and conversations with C-level and business leaders
- Created a vision for Security to "Help people lead healthier lives by creating safe spaces for drug research and innovation."
- Selected an industry-recognized framework to develop and deliver a strategic plan
- Performed a Gap Analysis to develop proposed actions that will help PharmaCo go from its current state to future state
- Created a roadmap of planned activities

Now that Cheryl has a roadmap in place, she must ensure that the team defines appropriate metrics to track progress and deliver business value.

Metrics Planning Worksheet

Strategic Objective	Security Initiatives	Metric
Get drugs to market faster	• Secure mobile apps for clinical trials	
	• Provide security assessments for research systems	
	• Ensure availability of key research systems	
Provide safe spaces for drug research	• Decrease patch deployment time on research systems	
	• Implement DLP to monitor for IP loss	
	• Create 24x7 SOC to quickly respond & recover	

PharmaCo has two important strategic objectives:

1) Get drugs to market faster.
2) Provide safe spaces for drug research.

Every department in the company must support these two objectives because they help drive increased growth and revenue.

In the "Initiative" column, Cheryl has identified some key actions and proposals from her team's Gap Analysis and mapped them to these strategic objectives. In the "Metric" column, write down at least one metric that can be used to track progress toward supporting the business.

For your reference, the PharmaCo Gap Analysis is included on this page:

Gap Analysis Sample Actions Refresher

Function	Future State	Current Situation	Actions/Proposals
Identify	Centralized security governance to provide comprehensive risk management	Security is decentralized across business units	Name a permanent CISO Develop central policy library Implement vulnerability management program
Protect	Protect key systems and processes used for drug research, development, and trials	Security protections are not consistently applied	Decrease patch deployment time Protect clinical trial systems Deploy systems in blocking mode
Detect	Ability to quickly detect threats targeting intellectual property	Inability to detect malicious or negligent activity	Deploy continuous monitoring & log management capability Advanced analytics and reporting Implement DLP to monitor IP loss
Respond	Ability to minimize data loss, block attacks, and determine root cause	Inability to mitigate attacks and limit the amount of data lost	Build and staff 24x7 SOC Develop advanced forensics team Create threat intelligence sharing capability
Recover	Capability to quickly return to normal operations and limit business impact of security incidents	Recovery and business continuity is decentralized	Develop business continuity plan Ensure that response plan is regularly tested Socialize and communicate with BU leaders

Exercise Debrief

Note that this section contains a debrief and potential exercise answers

This page intentionally left blank.

Exercise 2.4 – Security Metrics Debrief

Strategic Objective	Initiative	Example Metric	Example Goal
Get drugs to market faster	• Secure mobile apps for clinical trials	• % of mobile devices using MDM • % of mobile apps built with standard controls	• 100% coverage • 100% coverage
	• Provide security assessments for research systems	• % of systems deployed on time • % of assessments completed w/in SLA	• 95% deployed on time • 95% completed w/in SLA
	• Ensure availability of key research systems	• % of researchers served • % availability of research systems	• 100% researchers served • 99.999% availability
Provide safe spaces for drug research	• Decrease patch deployment time on research systems	• % of systems patched on time	• 90% patched on time
	• Implement DLP to monitor for IP loss	• Amount of revenue lost due to stolen IP	• $100,000k
	• Create 24x7 SOC to quickly respond & recover	• % of incidents with same root cause	• 0%

A key component of creating meaningful metrics is to ensure that they meet overall business goals. On this this slide, we see two of PharmaCo's strategic objectives: 1) Get drugs to market faster and 2) Provide safe spaces for drug research. These goals indicate that PharmaCo is extremely focused on growing revenue by creating breakthrough new drugs. Its scientists and researchers are key to this effort and, as a result, the ability to serve researchers and enable them to do their work effectively and quickly is of extreme business importance.

Getting drugs to market faster requires new mobile apps that support clinical trials as well as access and availability of key research systems. Because these are important business initiatives, it's important that security align with them by providing appropriate protections. This includes mobile device management (MDM) software to ensure that mobile devices are encrypted and mobile application development controls like access control (% of mobile devices using MDM and % of mobile apps built with standard controls). However, it's not enough to simply enable these controls. Security needs to provide these tools and assessments as quickly as possible to align with PharmaCo's needs to get to market quickly (e.g., % of systems deployed on time and % assessments completed within SLA). Ultimately, this means happier researchers (% of researchers served).

In addition to enabling key systems, security must also protect the organization's key assets (% of systems patched on time), safeguard intellectual property created by researchers (e.g., revenue lost due to stolen IP), and continuously improve security capabilities (% of incidents with same root cause).

With these metrics in place, Cheryl can now determine the target state. These are represented in the "Example Goal" column. This takes into account the current state and, by implication, the delta of improvement. This is extremely important to define and might be unique for your own organization because the threshold that you define as the goal represents your Key Performance Indicators (KPIs) by which you will identify leading or lagging indicators to see whether there is a problem to which management must respond.

Metrics in Summary

- Make sure your metrics program is:
  - A priority for your organization
    - Designed to depict the overall health of your security organization
    - Leveraged to identify improvement opportunities
    - Included in team goals
  - Simple to collect data (preferably automated)
    - Actionable
    - Measured frequently
  - Related to the business
    - Appropriate amount of information for your audience
    - Easy to interpret
    - Evangelized to educate, communicate, and build credibility

When we introduced this metrics section, we stated that paving the road to success depends on you and your leadership team being well informed and having the right information to make the right decision and as a security professional, it's your job to do that—understand the quality and progress of your "business of security."

Ensuring your metrics program is a priority for your organization will ensure a greater level of success. Your metrics program should be designed to depict the overall health of your security organization as well as identify improvement opportunities to make your security processes more effective and efficient. One way to ensure your metrics program is a priority is to include this in everyone's goals and make everyone accountable in some manner.

Your metrics program should be simple to collect. Automation is a consideration for addressing this concern. Your metrics program should be actionable and measured frequently depending on the respective needs and demands of your organization.

Most importantly, your metrics program should be integrated with the business and include only information that is relevant to your audience. Your output should be easy to interpret and should certainly be evangelized at every opportunity to educate customers, stakeholders, leadership, executives, and board of directors. Your metrics program is a mechanism for you to build credibility for your security efforts.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - *Marketing & Exec Communications*

This page intentionally left blank.

Marketing and Executive Communications

- Goals of this section
  - Learn to promote your strategic efforts
  - Understand why marketing is important to security
  - Learn how to develop effective marketing
  - Learn how to effectively communicate with executives

The goals of this "Marketing and Executive Communication" section are for you to learn to promote your strategic efforts and understand why marketing is important to security. A marketing framework is also provided that will take you through the steps of how to develop an effective marketing plan and, most importantly, how to effectively communicate with executives.

What Is Marketing?

- Internal and/or external activities for a security organization that:
  - Builds your brand
  - Promotes your value
    - Products and services
    - Capabilities
    - Skillset
    - Relationships
      - Stakeholders
      - Customers
      - Employees

Simply stated, marketing for a security organization is all of the activities you can do internally and/or externally, to build or enhance your brand and promote the value of your security organization. You might want to market things such as the products and services your team provides, your capabilities and team skillsets and lastly, you might even want to promote your relationships such as your partnership with key stakeholders or customers, or the top talent of your employees, and the industry expertise they have.

Internally, you might want to market to your own security team (or to other teams within your company) and company executives, or your stakeholders. You may want to market externally to your customers or possibly even outside industry experts.

Your marketing is limited only by the activities you decide to take on in your marketing efforts, and the number of people and/or groups you determine should hear your marketing messages, which we will discuss later on in this section.

Why We Need Marketing

- Security is no longer just an IT issue
- Marketing ensures that you:
  - Stand out from other organizations in your company
    - Gain support on your overall strategic plan
    - Increase funding
    - Improve employee satisfaction and retain top talent
  - Maintain or gain an advantage over your competitors to:
    - Attract and retain top talent
    - Strengthen brand/image
    - Build partnership in the community

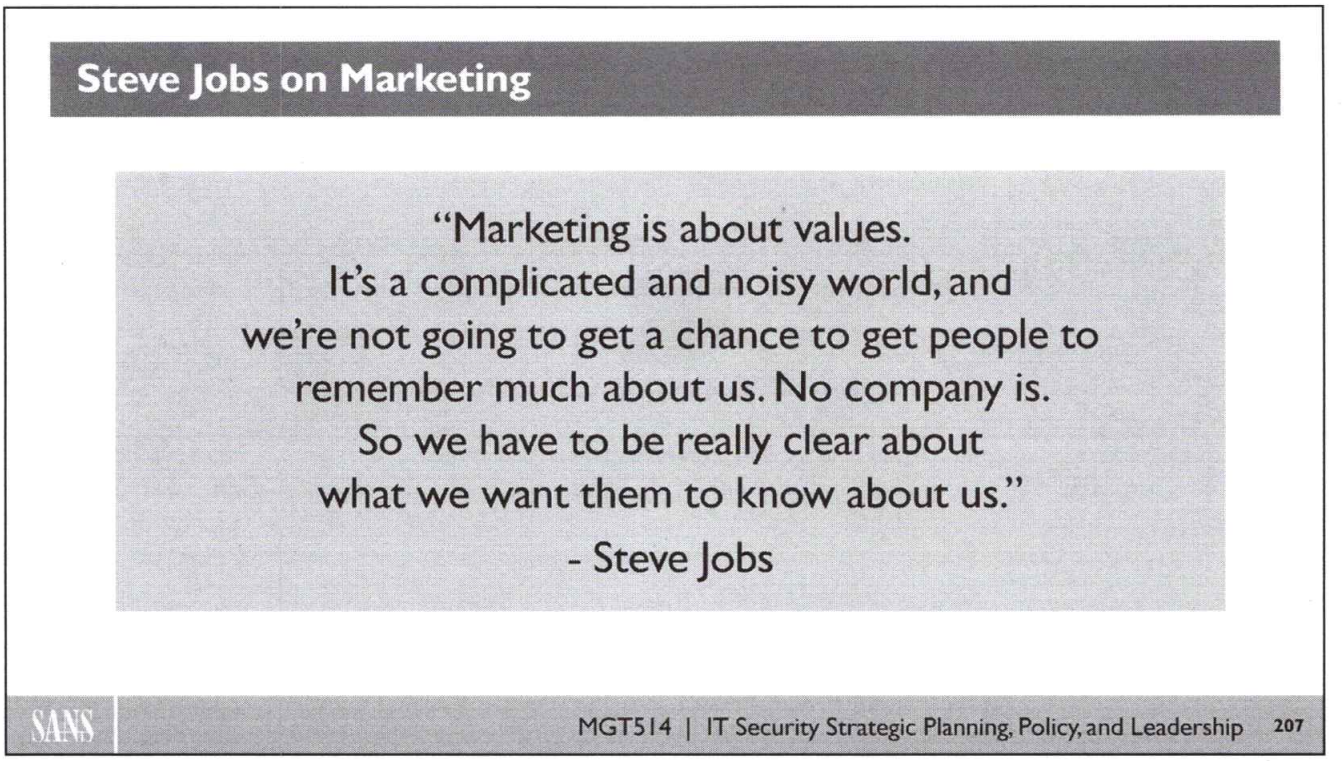
Security is no longer just an IT issue. The topic of security has reached the Board of Directors and most Boards have heard the message loud and clear that security is important. This doesn't, however, give you an automatic pass on marketing, and a blank check. Security budgets still need to be balanced with other investments, and as a security leader, you will want to develop a competitive advantage and stand out from other organizations in your company.

In addition to standing out from other organizations in your company, you can gain vital support on your overall strategic plan and/or any initiatives you are taking on. You can use marketing to increase funding for your team and/or initiatives. You can even market to your team to improve employee satisfaction and retain top talent.

Outside of your company, you can use marketing to maintain or gain an advantage over your competitors to attract top talent to your team, and strengthen your company and your specific security organization's brand and image. You can use marketing to build partnerships in the community.

For the bottom line as a security organization, people need to hear and understand your value as stated in the previous slide. Through these efforts, you begin to build or enhance your brand and gain a competitive advantage through your marketing efforts.

Marketing is imperative to the successful adoption of your strategy and/or security initiatives, as well as retaining top talent, and all the other benefits we discussed thus far, and will continue to expand on as we progress through this section.



Steve Jobs is quoted as saying, "Marketing is about values. It's a complicated and noisy world, and we're not going to get a chance to get people to remember much about us. No company is. So we have to be really clear about what we want them to know about us."

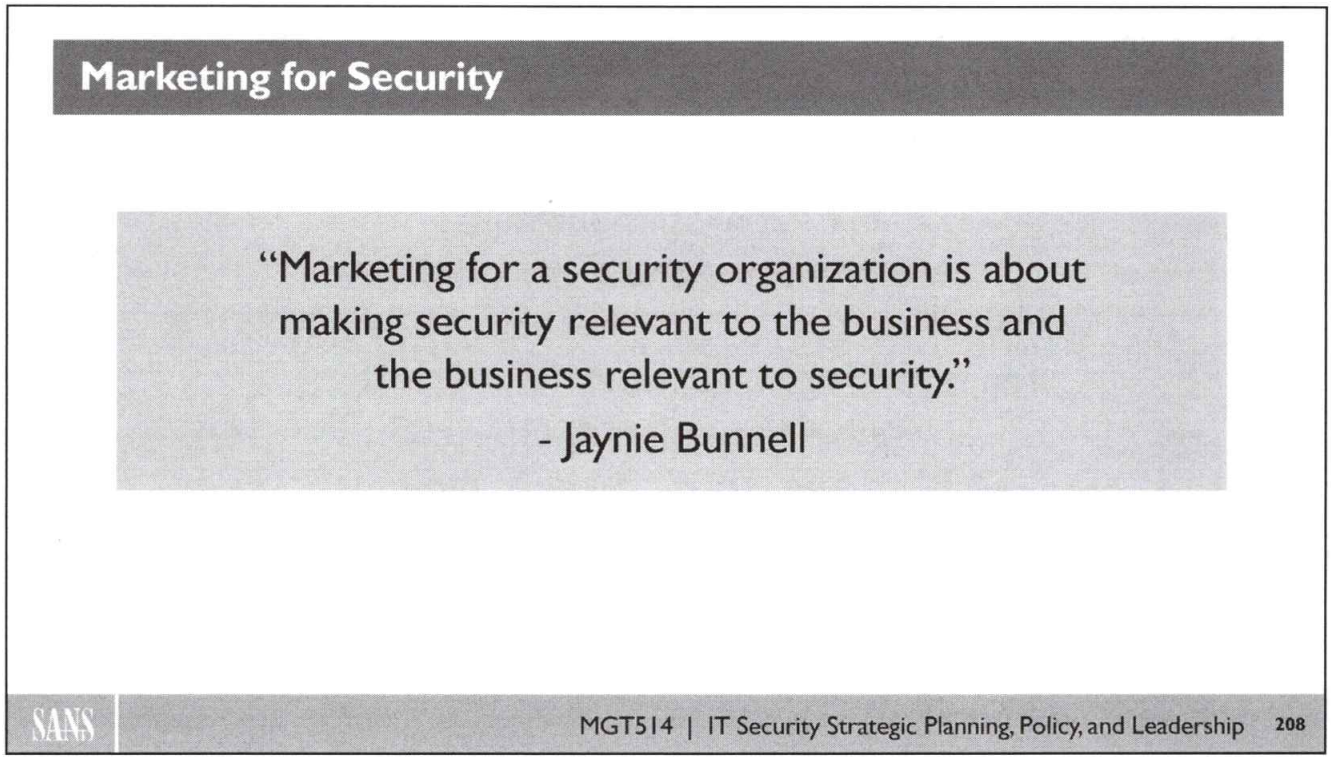
Jobs is the undisputed king of wow marketing. He was also considered one of the most charismatic business leaders in the world. He took every opportunity to market to others and he made it look effortless, and he did this through simplicity but the truth is, he worked very hard to make it look simple.

Jobs says that marketing is not about touting features and speeds and megabytes or comparing yourself to the other guys, it's about identifying your own story, your own core, and being very, very clear about what you are all about, and what you stand for…and then being able to communicate that clearly, simply and consistently. Jobs believes that brand should always come back to its core values.

As Apple's CEO, Steve Jobs will be remembered for many things—not just a purveyor of innovative, landscape-changing products. He'll also be remembered as one the most powerful and charismatic orators and marketers of our time.

For additional highlights on Jobs' values and identifying your core, top speeches and marking lessons Steve Jobs taught us, please see the following URLs:

- http://www.presentationzen.com/presentationzen/2011/10/steve-jobs-on-values-and-identifying-your-core.html
- http://www.pcworld.com/article/238905/top_three_steve_jobs_speeches.html
- http://postcron.com/en/blog/10-amazing-marketing-lessons-steve-jobs-taught-us/



"Marketing for a security organization is about making security relevant to the business relevant to security." Security is complex by nature, and not easily understood by people who are not security professionals. Not only that, security has primarily been a back office function for years and just recently, security leaders have been given the opportunity to sit at the table with business executives and the Board of Directors.

If you can't effectively articulate security relevance to the business, you are seen as just another IT cost, and this is not an ideal perception that will by any means win you support and buy in for your strategy and/or initiatives. Remember, your security team is competing for funding and support with other organizations, and these organizations are likely to provide distinct value that is generally understood throughout the business, such as your sales and marketing teams who are generating revenue, your accounts receivable teams who are collecting money, research and development teams who are developing products to take to market, etc.

The key to determining how to make security relevant to the business is to think beyond the technology and consider how your team enables the business. We've talked about this concept in nearly all the content we've covered so far. Find stories of interactions and events where the security team has helped the business get its business done. Some examples include:

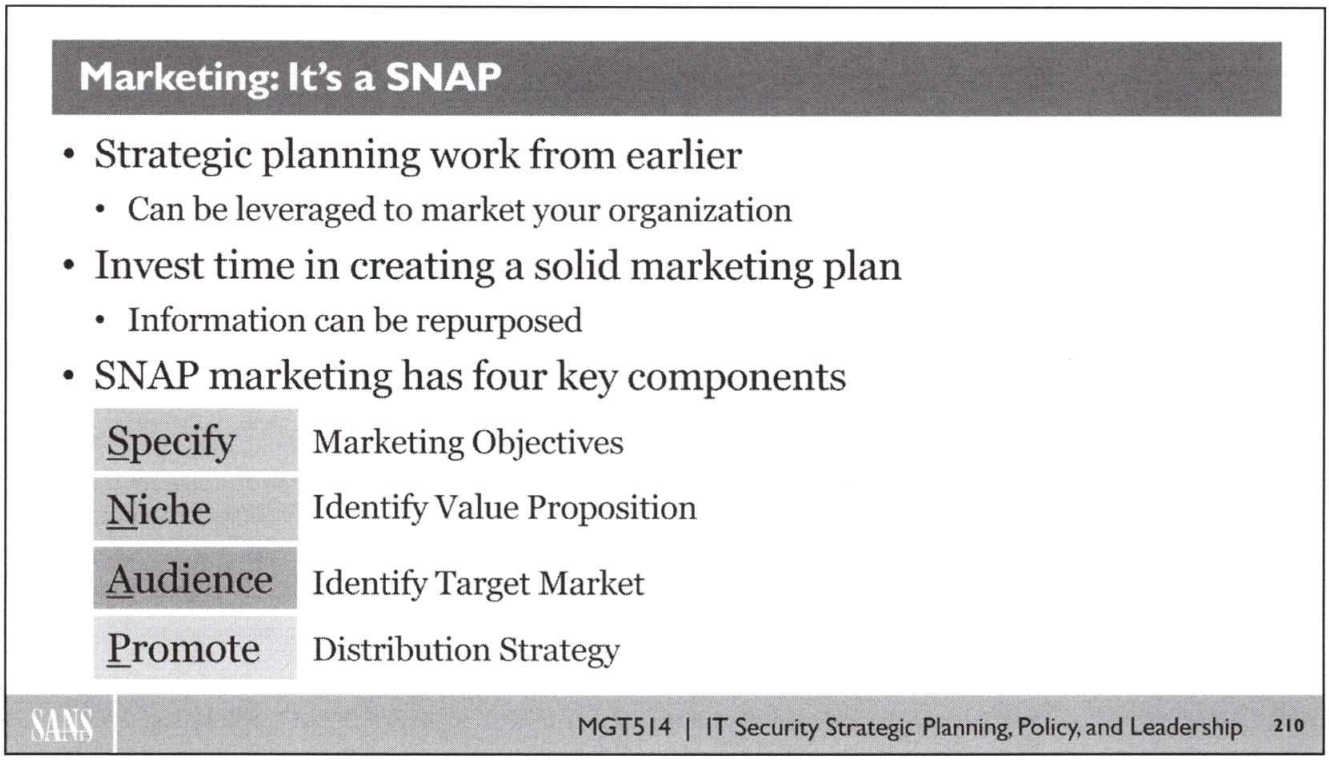
- Application security team creating secure code development training for the Web Development team, enabling it to develop more secure code for your company's on-line transactions to protect customer and cardholder data
- Incident response team is on call for executives to address any security-related concerns such as phishing e-mails by providing immediate support as questions arise

In addition to the stories of interactions, use the content you've generated throughout the strategic planning process. Think back to the PEST and Porter's Five Forces examples that we worked through. In PEST, we

determined that security could develop relationships with airline intelligence agencies and monitor potential terrorist activities, as well as provide due diligence before airline consolidation by providing M&A security technology reviews and monitoring for potential data loss. Lastly, we said that security could provide forensics and eDiscovery services as support for legal cases. These examples illustrate how security can enable the business, and goes well beyond describing security controls, further enabling you to have a deeper, more meaningful dialogue with your business partners and executives.

Making security relevant to the business is not enough! You must also make the business relevant to security. If security doesn't understand the importance of the business, it might in fact hinder instead of enable. Think back to the stakeholder management story of Robert Taylor and his missed opportunity. As you recall, Bob took the lead on a network blocking security initiative and he didn't engage all of his stakeholders. Bob thought his project was a straightforward security technology deployment, and he didn't take the time to understand the business impact of his efforts. He blocked the network as designed, but as a result, Bob also blocked the sales team and research and development team from access to vital information they needed to do their job. Remember, these two teams generate revenue and develop new products for the company. Bob also caused additional work for the Help Desk because he did not consider business relevance in his technology deployment.

This is not an easy concept, and it takes a lot of consideration and practice, but as security leaders interact with executives, and security teams interact with business partners more and more, you will find it necessary to master this skill for your continued success.



The approach outlined in SNAP marketing is fairly straight forward and simple to develop and execute. The SNAP marketing method has four key components that drive your marketing plan through successful execution:

Specify: Marketing objectives: You'll need to determine your marketing goals. As an example, you'll need to decide whether you want to strengthen the stakeholder relationship and gain support, establish brand awareness, retain and/or recruit top talent, increase your revenue, increase funding, etc. Once you determine the goals you want to target in your marketing plan, you'll need to describe some specifics around the goal.

Niche: Identify Value Proposition: Having a strong value proposition is of critical importance, because it distinguishes your organization from others in your company to your stakeholders and business partners, against competitors, to your employees and future employees, and to your customers.

Audience: Identify Target Market: These are the people and organizations that are key to your continued success such as executives, business units, employees, and customers.

Promote: Distribution Strategy: You need to determine the most effective method by which you promote your marketing—in other words, how your messages will reach your audience. This is your distribution strategy and it includes critical components needed to execute a successful marketing effort.

It's necessary to invest appropriate time in creating a solid marketing plan using the SNAP components. The good news, however, is the SNAP method is designed to leverage the output from your strategic planning work you've already completed in this course, such as Threat Analysis, Historical Analysis, Gap Analysis, Security Roadmap, Metrics & Dashboards, SWOT Analysis, Vision and Mission, PEST Analysis, Porter's Five Forces, Values and Cultures, Stakeholder Management Strategy, and project planning.

You will find that once you've created and refined the messages from this framework, you will have a ready portfolio of information available to you for multiple uses, such as meetings with executives, teams, stakeholders, vendors, or the output of this effort can be used for vendors, customers, or potential employees.

References

http://www.forbes.com/sites/davelavinsky/2013/09/30/marketing-plan-template-exactly-what-to-include/

http://und.edu/academics/extended-learning/summer/_files/docs/mktg-plan-sample.pdf

www.sba.gov/blogs/5-tips-writing-basic-and-un-daunting-marketing-plan

www.wikihow.com/Create-a-Marketing-Plan

http://smallbusiness.chron.com/essential-elements-marketing-plan-60625.html

https://marketing.ucr.edu/importance.html

http://www.investopedia.com/terms/m/marketing.asp

https://www.everclearmarketing.com/blog/19-blog/everclear-insights/91-top-5-cybersecurity-marketing-challenges-and-how-to-overcome-them#.VU5y4Os2JUQ

Specify: Marketing Objectives

- Determine marketing goals
  - Increase funding and/or revenue
  - Build stakeholder relationship and gain support
  - Establish brand awareness
  - Retain and/or recruit top talent
- Specify your objectives as brief descriptions that are business consumable
  - Example goals from Cheryl Miller interim PharmaCo CISO

- Attackers don't sleep so we can't either
  - Fund 24x7 Security Operations Center
- Share intelligence to respond and block attacks
  - Establish Cyber Threat Intelligence function

Every marketing plan needs objectives, and a way of measuring success (metrics) to ensure your marketing efforts are not wasted. You'll need to determine your marketing goals. As an example, you'll need to decide whether you want to strengthen stakeholder relationship, and gain support, establish brand awareness, retain and/or recruit top talent, increase your revenue, increase funding, etc. Once you determine the goals you want to achieve, you'll need to describe some specifics around the goal.

Stating that you want to increase stakeholder engagement and buy in for additional funding isn't specific enough. Think about what actions you want your target audience to take after they are made aware of your campaign or promotional activity. In the example above, Cheryl Miller, interim PharmaCo CISO, is acutely aware that attackers don't sleep, and in order for the security team to defend the company, a 24x7 Security Operations Center must be funded and a Cyber Threat Intelligence function must also be established. Cheryl is very specific about her marketing objectives and has translated them into business consumable language that non-security professionals can understand.

Cheryl used outputs from the strategic planning process, such as Threat Analysis, Historical Analysis, Gap Analysis, Security Roadmap, Metrics & Dashboard, and SWOT Analysis to determine where she should focus her marketing objectives.

In the Threat Analysis section, she gained an understanding of how attackers work by applying the Intrusion Kill Chain, and that threat intelligence can create a feedback look that can be used to disrupt attackers. She also learned that defenders must move detection and analysis up the kill chain, and implement defenses across the entire kill chain, and lastly the intrusion kill chain provides a structure to analyze intrusions, extract indicators, and drive defensive courses of action.

In the Historical Analysis section, she learned that her company is facing increased risk due to the evolving threat landscape such as organized crime, advanced persistent threats, and increasing business requirements such as Cloud computing, Big Data, and the Internet of Things, which all result in operational risks.

In the Gap Analysis section, it was identified that the current state of defense was limited, due the inability to mitigate attacks and limit the amount of data loss.

The Security Roadmap section identified numerous initiatives, such as Establishing a 24x7 Security Operations Center and Cyber Threat Intelligence capabilities. It was at this point that she realized there wasn't enough resources to do everything at once—budget needed to be secured, and staff needed to be put in place.

Through the SWOT Analysis (Specifically the Weaknesses, Opportunities, and Threat quadrants), we learned that PharmaCo has access to talent around the world. It also confirmed that security is decentralized and understaffed. The opportunities also confirmed the need to operationalize around the kill chain, and leverage the global presence to build 24x7 team, and increase staffing levels. Most importantly this section confirmed there are threats that are cause for alarm. These include insider threats due to a geographically dispersed workforce, competitors seeking intellectual property, and lastly nation states seeking to accelerate research and development, which could all potentially result in data loss.

Niche: Identify Value Proposition

- How is your organization, department, or team different?
  - From other organizations in your company
  - For stakeholders and business partners
  - Against competitors
  - To your employees and future employees
  - For your customers
- Specify your value proposition as a brief paragraph
  - Example from Cheryl Miller, interim PharmaCo CISO

"Help people lead healthier lives by creating safe spaces for drug research and innovation."

Having a strong value proposition is of critical importance because it distinguishes your organization from others in your company, to your stakeholders and business partners, against competitors, to your employees and future employees, and for your customers. The hallmark of several great companies is their niche or value proposition. For example, FedEx's Unique Selling Proposition (USP) of "When it absolutely, positively has to be there overnight" is well known and resonates strongly with customers who desire reliability and quick delivery.

Cheryl used the information she had completed to date such as her Vision &Mission, PEST Analysis, Porter's Five Forces, Values & Cultures, and SWOT Analysis to identify her value proposition or niche, which is "Help people lead healthier lives by creating safe spaces for drug research and innovation."

Through the Vision & Mission work that was done, the security organization realized that through security and innovation, trust and safety could be promoted.

Through the PEST (specifically, the Economic, Social, and Technological quadrants), it was determined that protecting intellectual property and brand is very important.

Through Porter's Five Forces, it was determined that competitive rivalry was high and protecting drug research and innovation is one way security could enable the business.

Through the Values & Cultures, it was determined that the security team culture must align with the values of stakeholders, and the culture of the overall organization.

And through the SWOT Analysis, (specifically in the Strengths quadrant), it was determined that the business mission to help people lead healthier lives and the culture was one of innovation and research and development.

Audience: Identify Target Market

- Build a picture of your target market
  - Identify the people and organizations that are key to your continued success
    - Executives
    - Business units
    - Employees
    - Customers
  - Positioning
    - Determine how to best influence your audience
  - Consider what actions you want your audience to take
    - Approve additional funding
    - Buy in and support your effort
    - Remain committed to the security organization mission

You need to identify your target market—in other words, your audience for your marketing efforts. These are the people and organizations that are key to your continued success such as executives, business units, employees, and customers. You'll need to build a precise picture of who your audience is. If you are not precise, you run the risk of a scatter-gun approach that will dilute your message and possibly limit your success. The more specific you can be, the easier it will be to craft the right message for the right person, and develop the right distribution plan.

You'll need to determine positioning of your marketing efforts. You can achieve this only through understanding how to best influence your audience. A common mistake is to latch onto an idea without first understanding your prospective audience, and what they want to hear and more importantly, what motives them. If you try selling something that people don't want or don't understand why they need it, they won't buy into it and by that way, that also includes request for additional funding from your company's top executives. "Because security is important" is not an ideal motivator and will not likely get you where you need to go.

You need to consider what actions you want your audience to take such as approving additional funding, gaining buy in, and supporting your efforts, or remaining committed to the security mission.

The information that you previously developed through your Stakeholder Management Strategy and your Visioning and Innovation will help you identify your target market, position you for a success outcome, and clarify what actions you want your audience to take. As an example, through your stakeholder management strategy, you learned your stakeholders will have different views on your project. You also learned that office politics and/or personal interests will likely be key factors in distilling true stakeholder motivations. You also know that the approach for each group and/or individual will need to be tailored to support the varying motivations of each of your stakeholders. For example, you wouldn't want to take cost, risk information that you would typically provide to the CFO to the head of HR who is interested in the impacts on employee policies.

From your Visioning and Innovation, you also learned tips for your security team. Never ask for the money; instead articulate the vision and describe how you will solve a problem being faced by your key stakeholders. By stating the problem and aspiration, you can increase commitment and turn stakeholders into partners.

Three Things That Make Executives Unique

1) Executives are extremely busy
   - Want solutions not more problems
   - Looking to you for answers
2) They are required to make rapid decisions with limited information
   - Want assurance you have comprehensiveness of thought
   - Everything we have done in the past two days, leads to this
3) They have a complex enterprise to run
   - Security is only one component of the overall organization
   - Help them tie all the pieces together with security
   - Communicate in business consumable language

Executives are important to you because they impact or provide oversight and are accountable for nearly every aspect of the work that you do. They generally make decisions on initiatives and/or strategic direction, they are likely the individuals that stand between you and appropriate funding that is needed for your security organization, and more often than not they have a lot of questions that likely require rapid response from you. It's important to understand what makes executives unique and the importance of positioning yourself appropriately when you interact with them so you can do so effectively.

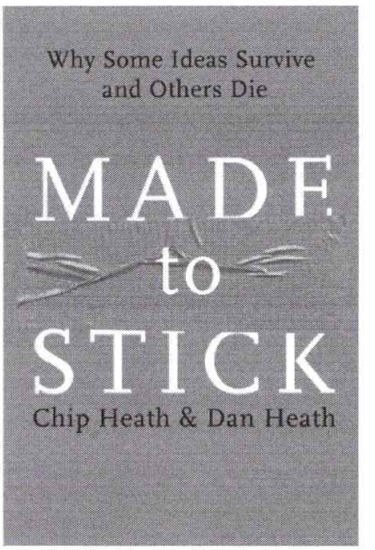
The first thing you need to understand is, executives are extremely busy. You might be thinking to yourself right now, "Well I'm busy too." But the fact of the matter is, as stated above, executives are the individuals that hold the keys to get you what you need to do your job. You have an accountability to them to appropriately interact with them, and provide them information that they need in a manner in which they can consume it and can make decisions on behalf of the company. Executives want solutions, not more problems, and they are looking to you for the answers not more questions.

Secondly, executives are required to make rapid decisions with limited information, and they want assurance that you have comprehensiveness of thought. The good news is everything we have done in the past two days leads up to this and will provide you all the factors you will likely need to establish yourself in this area.

Lastly, executives have a complex enterprise to run, and security is only one component of the overall organization. Oftentimes, we get so focused in our own organization, and what we are expected to deliver, we forget this. It's up to you as a security leader to help them tie all the pieces together with security in mind. They are not the security experts—you are, and you need to understand what business factors your executives are concerned with, and tie it back to security in a business consumable language that is easy for them to understand.

Made to Stick

- **S**imple
  - Find the core of any idea
- **U**nexpected
  - Grab attention with surprise
- **C**oncrete
  - Make sure they can be grasped & remembered
- **C**redible
  - Make an idea believable
- **E**motional
  - Help people see the importance
- **S**tories
  - Use narrative



Many technical security professionals suffer from what is known as the "Curse of Knowledge." In short, it occurs when someone is better informed than another person and finds it extremely difficult to think and communicate about topics with people who are less knowledgeable about a subject.

With this in mind, how can you connect with your target audience and create a message that will be memorable? Two brothers, Chip and Dan Heath, have written an excellent book entitled, *Made to Stick: Why Some Ideas Survive and Others Die*. They outline five important characteristics that help make an idea sticky. These can be used to market your work with the security team:

Simple: Oftentimes, security professionals default to detailed technical communications and do not focus on the "so what" for the business. By ignoring the impact and resulting risk to the organization, we can inadvertently "bury the lead."

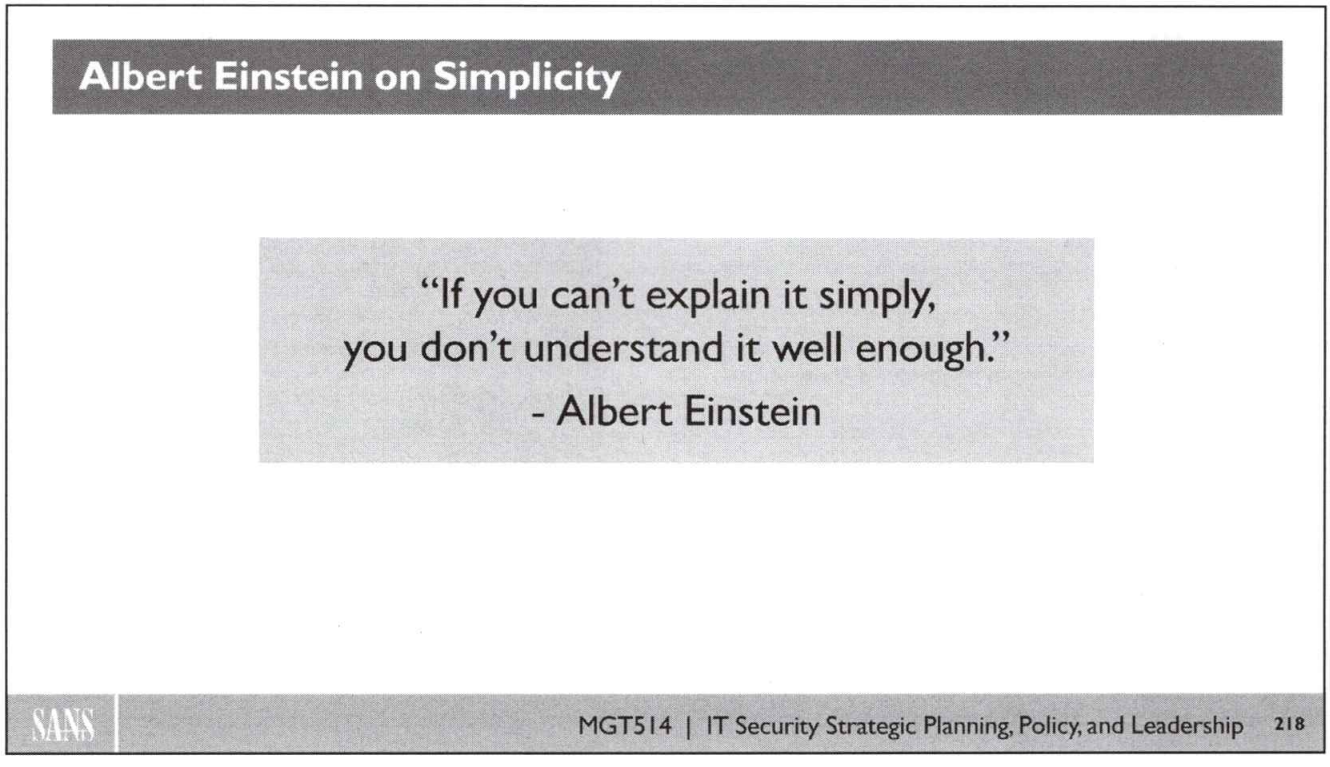
Unexpected: Memorable ideas are ones that are unexpected. People don't expect security to be a business enabler. If you can lead with that story, it will be more likely to resonate with your stakeholders.

Concrete: Don't focus on technical feeds and speeds, which can be abstract for many people. Instead focus on how security supports specific business initiatives.

Credible: Develop the credibility of your security team not only by being security experts, obtaining certifications, and speaking at well-known industry events, but also by seeking endorsements from key business partners.

Emotional: Maya Angelou has a well-known saying, "People will forget what you said, people will forget what you did, but people will never forget how you made them feel." By focusing on the emotional aspect of a situation, you can help people see the importance of your work.

Stories: Stories are one of the most effective teaching tools. They are containers for wisdom and knowledge, and really help drive home the point of a particular idea.



Albert Einstein said, "If you can't it explain it simply, you don't understand it well enough."

Simplicity is the quality of condition of being easy to understand. Counter to simplicity is our basic human nature to over complicate everything we touch, especially when we are trying to convey information or ideas verbally, or in writing such as e-mails, presentations, and/or meetings. We use words people don't understand such as techno-speak, regulatory jargon, abbreviations, and far too many acronyms. We often document the complexity instead of revealing the simplicity. If people have to decode your complex language, they can't hear or understand what you are intending to say, and it begs the question if you really understand it well enough yourself.

Your message is important and learning to simplify will benefit you in so many ways. We will share some tips, techniques, and examples on the following pages to help you further understand the importance as well as provide guidance on how to simplify your message for marketing.

Example 1: Bad Exec Communication (Heartbleed)

Heartbleed is a bug in the **Open SSL** cryptography library, the widely used **TLS** protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable Open SSL instance for TLS is a server or client. It results from improper **input validation** in the implementation of the TLS **heartbeat extension**. This **vuln** is classified as a **buffer over-read**.

Source: http://en.wikipedia.org/wiki/Heartbleed

Your boss, the CISO, is on vacation with no access to email or a cell signal, and he has delegated responsibility for the security organization to you the Director of Security Operations. On day one of your delegate duties, you receive an email from the CEO of your company who read about Heartbleed in the *The New York Times* Twitter feed. He is immediately alarmed your company might be impacted. In his email, he simply asks, "Are we affected by Heartbleed?"

You're excited about the opportunity to finally interact directly with the CEO, and as luck would have it, you've already received threat intelligence from your team, and they are actively assessing the situation and impact to your company. You provide your CEO with the following information: "Heartbleed is a bug in the Open SSL cryptography library, the widely used TLS protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable Open SSL instance for TLS is a server or client. It results from improper input validation in the implementation of the TLS heartbeat extension. This vuln is classified as a buffer over-read."

You anxiously await a reply from the information that you provided to the CEO and moments later, he responds with a copy to the CIO and your boss the CISO and asks, "Are we impacted?" At this point, you know you did not provide your CEO with the information that he needed the first time, and this made you look bad in the eyes of the CIO and your boss the CISO. You take a step back and think to yourself. This was a very short, concise message, and it gives all the technical details about Heartbleed and you're a bit perplexed as to why he doesn't get it.

What do you think was wrong with this message to the CEO?

You are correct that this is a very short, concise technical summary of Heartbleed, but your CEO is not a technologist. Your message was not written in business consumable language so he could understand what this bug is all about and in all reality, he shouldn't have to understand it. That's why he has a security team. You

didn't provide the direct answer to his question about how the organization is impacted. The message is geared more towards showcasing your technical acumen. There are clearly no solutions provided in your communication, and your message opens up more questions for the CEO than you've provided answers. Lastly and most importantly, there is no indication of comprehensiveness of thought. Your message is clearly a reaction to respond expeditiously without thinking through what he really wants and needs to know. You provided what you wanted to tell him.

Reference

Source: http://en.wikipedia.org/wiki/Heartbleed

Example 1: Better Exec Communication (Heartbleed)

A security vulnerability called "Heartbleed" was disclosed Monday night, which could impact our **websites**. Our investigation to date indicates that we have **not been comprised** and our **data is not at risk**.

This bug allows private data such as **usernames**, **passwords**, and **credit card numbers** to be stolen from the memory of a website's server.

Our security team immediately began scanning our environment for potential impact. As we continue scanning, if it is determined any of our systems are vulnerable to this bug, our security team is positioned to immediately remediate with the available patch that was released to address this issue. We will provide updates as they become available.

Although the previous summary of Heartbleed included some technical jargon, this version is more focused on the impact to the company and what the security team has done and is doing about it.

When you are crafting your communications, it's important to consider how you want to be perceived by the receiver. In a more technical company, it might be wholly appropriate to position yourself and the security team as technical subject matter experts. In that type of environment, you might want to focus on technical analysis and technical solutions. However, if your leadership team is not very technically savvy, it might see this type of communication as too detailed and perceive you to be merely a "problem finder." In those cases, you will be better served by positioning the security team as a business leader and solution provider. The example communication on this slide highlights that Heartbleed impacts "websites" (hopefully something everyone in the company can understand) and that it could result in the theft of sensitive data like usernames, passwords, and credit card numbers (making the impact very concrete). The writing goes on to highlight how this currently impacts the company. Doing this shows that you have done your due diligence and provides the "so what" that executives are most concerned about. In fact, you might decide to lead with this in the very first paragraph to immediately highlight the impact to your company.

Example 2: Bad Exec Communication (DMARC)

DMARC is an email validation system designed to detect **email spoofing** by providing a mechanism to allow receiving **mail exchangers** to check that incoming mail from a domain is authorized by that domain's administrators and that the email (including attachments) has not been modified during transport.

It expands on two existing mechanisms, the well-known Sender Policy Framework (**SPF**) and DomainKeys Identified Mail (**DKIM**), coordinating their results on the alignment of the domain in the **From: header** field, which is often visible to end users. It allows specification of policies (the procedures for handling incoming mail based on the combined results) and provides for reporting of actions performed under those policies.

Source: https://en.wikipedia.org/wiki/DMARC

Imagine that you are preparing for annual budget meetings. There are a number of security initiatives for which you would like to obtain funding including DMARC to help prevent email spoofing. As part of the business case, you need to provide a justification and decide to supply the project managers with the text above. Although the statement above is technically correct, there is very little in this description that will resonate with non-IT personnel. Terms like "mail exchangers," "SPF," and "DKIM" only add to the confusion. If others have done a better job articulating the business value of their projects, then you might not be very likely to get funding for your important security initiatives.

Example 2: Better Exec Communication (DMARC)

The solution prevents scammers from sending **fraudulent email** to our customers. These fraudulent emails result in **stolen usernames, passwords**, and **fraudulent transactions**. The solution reduces the number of stolen accounts by 20%, **account fraud** by 10%, and the total amount of fraudulent transactions by **$1 million** per year.

This summary of DMARC is much more powerful because it articulates the business value to your organization. Specific terms like "fraudulent email" and "stolen usernames" are much more understandable to non-technical people. Additionally, this version actually quantifies to the impact to the business in terms of reducing the number of stolen accounts, minimizing account fraud, and saving the company $1 million per year. The more you can articulate the value provided by your security projects, the more likely you will be able to succeed and stand out in a competitive market (i.e., the market for limited attention).

Example 3: Bad Exec Communication (DDoS)

DDoS is an attack where multiple **compromised systems**, which are often infected with a **Trojan**, are used to target a single system causing a Distributed Denial of Service (DDoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems **maliciously used** and controlled by the hacker in the distributed attack. The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via **botnets**.

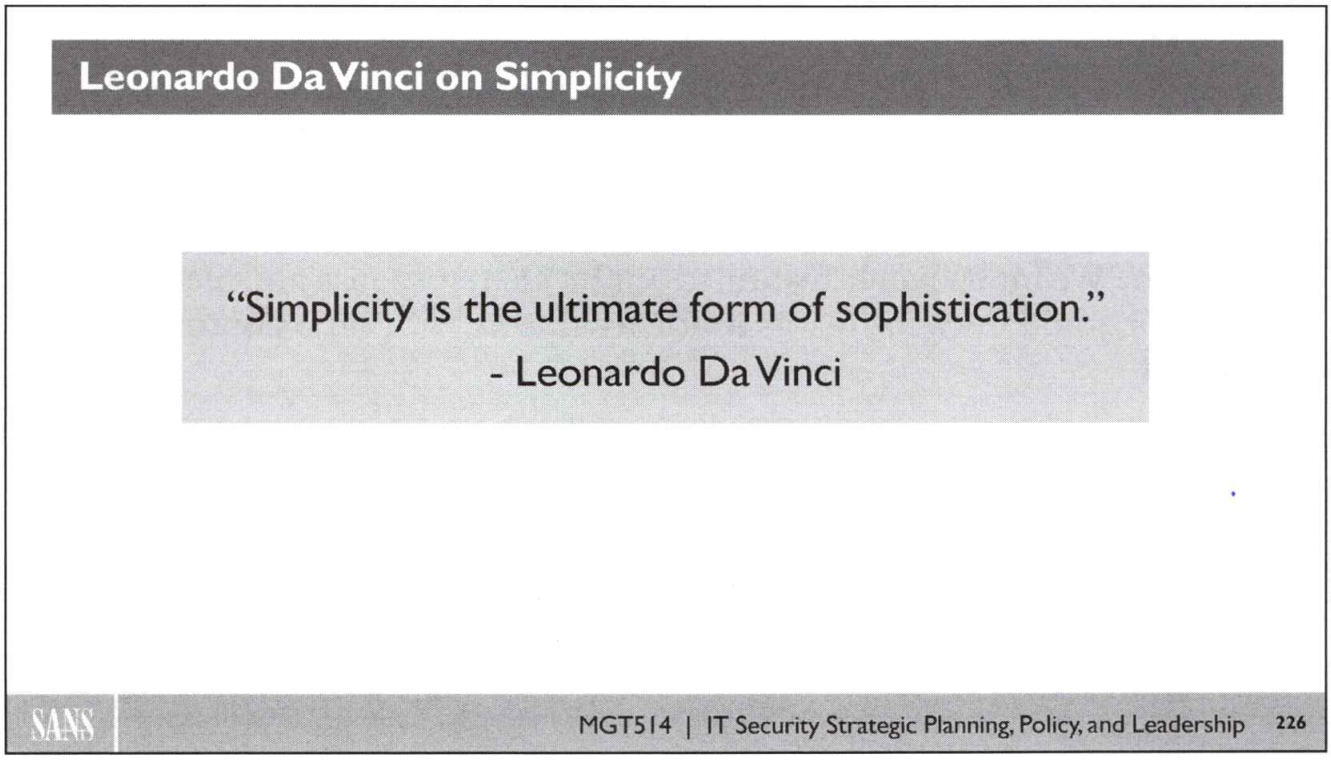
Source: http://www.webopedia.com/TERM/D/DDoS_attack.html

Earlier this morning, your company was hit with a distributed denial of service (DDoS) attack. To close out the incident response process, your manager has asked you to draft a summary of what happened. This is the first time you've had to draft such a communication and are not sure how to respond. You decide to start the writeup with some background information about the attack to ensure that everyone understands what a DDoS actually is. And that is where you make your first communications mistake. The writeup above focuses too much on what DDoS is and does not describe at all the impact to the organization. If non-security leadership is not familiar with dealing with denial of service attacks, then it will likely be confused by terms such as "Trojan," "maliciously used," and "botnets."

Example 3: Better Exec Communication (DDoS)

On Friday night, our **primary web site** was **unavailable** for **two minutes** because it was **flooded** with traffic from the Internet by cyber attackers. We immediately instituted our incident response and recovery procedures and the website was **made available** with **zero customer impact**.

This version is much better because it focuses on the impact to the business. The company's primary website was "unavailable for two minutes" because it was "flooded with traffic." It was quickly made available with "zero customer impact." Senior leaders want to know the "so what" of your security work. They are looking to you for simple answers that describe why something is important and relevant to the complex business that the organization is running.



Leonardo Da Vinci said, "Simplicity is the ultimate form of sophistication."

Ideas are the currency of the 21st century and some people are exceptionally good at presenting their ideas. For these people, this particular skill elevates their stature and increases their influence. There is nothing more inspiring than a bold idea, delivered by a great speaker or easy-to-understand words.

Ideas effectively packaged and delivered can change the world. John F. Kennedy gave a speech at Rice University of September 12, 1962, where he outlined his vision to explore the moon.[1] He captured the collective imaginations of millions of Americans and thousands of top scientists to put their time and energy into this effort. It was one of the most important speeches in American history and it took only 17 minutes and 40 seconds.

There is evidence all around us that illustrates simplicity is the way to go. Ikea provides instructions that are only pictures, no words. Twitter limits its tweets to 140 characters, so they can be easily consumed. There are wildly popular TED talks that cover complex topics like the history of the world, all 13 million years of it, in only 18 minutes. All of these examples are made possible by one concept. Keeping it simple!

Reference

[1] http://er.jsc.nasa.gov/seh/ricetalk.htm

Promote: Distribution Strategy

- Includes critical components needed to execute successful marketing
- Distribution strategy should include the following
  - Inbound content marketing
    - Blogs
    - White papers
    - Online talks and videos
    - Internal website
  - Outbound marketing
    - Advertisements
    - Promotional videos

Now that you know who you want to reach, and what actions you want them to take, you need to determine the most effective method by which you promote your marketing—in other words, determine how your message will reach your audience. This is your distribution strategy, and it includes critical components needed to execute a successful marketing effort.

Primary information and/or tools that you can leverage from past work to create your distribution strategy can be found in your project plan or security roadmaps along with other critical pieces of information you've collected as a result of the strategic planning process. The information about the who, what, when, where, and how should be available to you at this point, and the distribution strategy is formalizing the method by which you will deliver the messages for marketing.

Inbound content marketing is promoting your efforts through blogs, white papers, videos, and internal websites. The idea is to draw key stakeholders in by providing content that is relevant and useful to them. For example, you might do regular security briefings focused on the threats to a particular line of business. By producing interesting or relevant content, you develop more engaged customers.

Outbound marketing on the other hand relies on traditional approaches to buy a customer's attention such as TV, print, or radio advertisements, flyers, brochures, spam, and promotional videos. These types of activities are associated with traditional brand advertising, which can also be useful for your security team to build awareness of your activities across the larger organization.

Market and Communicate to Employees

- Market to your current employees for retention
  - Brownbags
  - Challenge coins
  - Newsletters
  - Specialized security training
  - Highlight innovation and thought leadership
- Market to future employees to attract top talent
  - Recruit at major conferences
  - Speaking engagements from your star performers

Oftentimes, leaders forget that it's important to market and communicate to current employees for retention, and to future employees to attract top talent. As you are aware, the security industry is in high demand and the effort you put into marketing to current and future employees will result in far greater benefits than dealing with vacancy factors. Remember that high-performing team members often know or network with top talent and might become a great partner in your recruiting efforts.

Below are some ideas to market to your current employees:

You can hold brown bag sessions on a variety of topics, such as showcasing great work that various individuals and/or teams are doing. This also provides transparency across your organization. You can also invite key stakeholders to these events, which will also provide insight to all the great work your team is doing. You can bring in non-security related topics that might be of interest to provide insight to your security team such as someone from your sales and marketing team to talk about how they use technology to generate revenue, or have one of your key stakeholders provide information on what his or her organization does. This has the potential to build trust and collaboration, and provide much needed visibility to both groups. You can even have vendors come and present innovative technology.

Publicly acknowledging the work of your team in brown bag sessions is a great way to increase commitment and morale. Providing special recognition or awards are another great approach. Challenge coins are a great way to do this and serve as a highly visible token of appreciation and achievement.

Newsletters are a great way to communicate a variety of topics to your employees. You can communicate what's top of mind from your leadership team, new security trends, highlight accomplishments, or recognize outstanding performance.

Specialized security training is one area you can invest in, and market to your security team. This shows your commitment to developing your team and providing them with the necessary tools and skills to perform their job and stay agile in the industry and illustrate clear paths for promotion.

Innovation and thought leadership will advance your organization's mission and, therefore, you want to market by highlighting those individuals and/or groups that are displaying these attributes. Not only will it reinforce your appreciation to those individuals that you are highlighting, but it will also encourage others to move in that direction by highlighting desired behaviors.

Marketing to future employees to attract top talent is very important for you to build and maintain high-performing teams. You can hold recruiting events at major industry conferences and distribute marketing collateral. Consider holding a specific recruiting event at the location with hiring managers and recruiters on-site to talk with potential candidates. Face time with potential candidates goes along way.

You might want to encourage your star performers to seek out speaking engagements on topics of interest for the industry or specialized subject matter expertise. For this, it's particularly important that you manage your message. Ensure that your speakers are fully trained for public speaking, and the content and messages in their presentation fully represent your organization and are enticing and engaging to the audience.

Market and Communicate to Customers

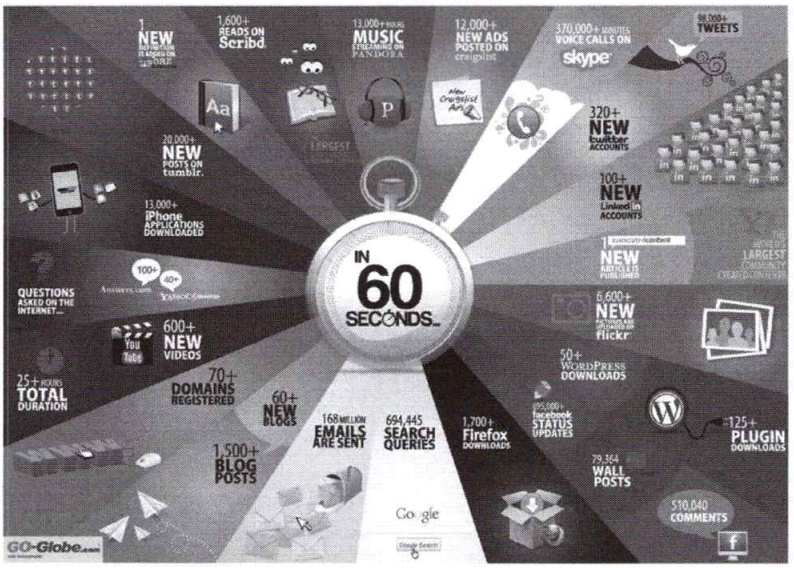
- Customer recognition
  - Challenge coins, awards for advocates
- Invite your customers to key conferences
  - That are relevant to the work they do
  - Are innovative and insightful
- Security awareness and training
  - Ask a hacker/security expert series
  - Security booths at corporate events
  - Personalizing security
    - How to keep your kids safe online

Just as employees should be engaged and recognized, your customers should also be formally recognized when they do something notable related to security. This can be for something as simple as fixing all the defects from a recent penetration test to partnering with you to roll out a new enterprise security initiative. When this does occur, make sure to publicly recognize these customers. These success stories and associated awards help highlight the work you are doing and build advocates for future security efforts.

As security professionals, we have a wealth of security events that we can attend. Think about inviting some of your customers to these key conferences to present with you about the work that they do and how security plays a part. Oftentimes, security conferences do not have much information about the business reasons for undertaking a particular initiative. As the business continues to innovate, think about how you can share these insights with the rest of the security community to highlight the work that your stakeholders are doing.

Finally, make sure to constantly work on building awareness for your security activities. There are a number of approaches to accomplish this including conducting regular information sessions about current threats (e.g., "Ask a Hacker Anything"), having booths at company events, and publishing information that can be used at home (e.g., how to keep your kids safe online).

Infographic Example I



Infographics are powerful marketing tools. Many people are visual learners and infographics provide a mechanism to transmit complex information to audiences in a manner that can be quickly consumed in a digestible manner.

According to NeoMam Studios,[1] whose business is to produce exceptional visual content that inspires people to take action, the average person is exposed to 174 newspapers full of information everyday and 99% of that information is filtered out through the brain almost immediately, leaving only 1% of the information actually getting to the brain. It also claims that 90% of information transmitted to the brain is visual and half of the brain is dedicated to visual function. It also tells us that 65% of the population are visual learners and images are processed simultaneously at the rate of 60,000x times faster in the brain than text. Text is processed sequentially, and most people retain only about 20% of what they read.

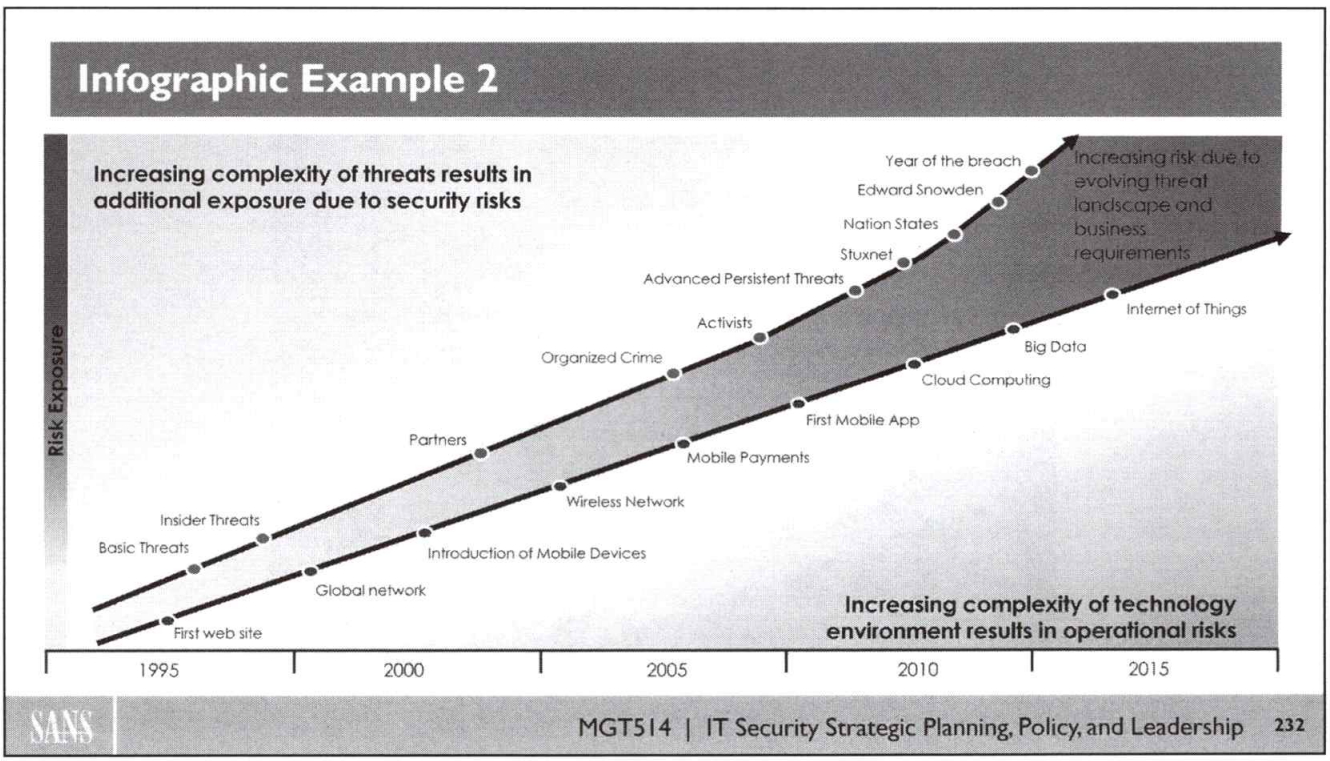
Infographics are an effective way to market information about your security organization. More and more infographics on security topics are showing up in search engines, and based on the above information, it's clear as to why this is happening. Security is a complex topic and not easily communicated to non-security professionals. Take the infographic shown on this page. It illustrates the things that happen on the web in 60 seconds.[2] In a very quick easy-to-understand, pleasing view, it gives the audience an idea of how big the web is.

How could you take a concept such as this and provide your audience with an indication of all the activities your security team conducts? As an example, I would imagine that your network blocking and/or malicious website blocking numbers are pretty impressive. What about the number of spam e-mails you block on a daily basis. Think about what meaningful information would be important to your organization. How could you leverage a visual message such as this for your security efforts?

References

[1] http://neomam.com/blog/infographics-make-great-marketing-tools/

[2] http://www.go-gulf.com/blog/60-seconds/



Here is another example of an infographic that illustrates the increasing complexity of threats, technology environments, and the associated risk. In one slide, you can convey a tremendous amount of information in a visual story that will be simple, unexpected, concrete, credible, and emotional.

SNAP Marketing Tools to Leverage

- Leverage strategic planning work for marketing

Category	Description	Planning Tools	
Specify	Marketing Objectives	Threat Analysis Historical Analysis Gap Analysis	Security Roadmap Metrics Program SWOT analysis
Niche	Identify Value Proposition	Vision & Mission PEST Analysis Porter's Five Forces	Values & Cultures SWOT Analysis
Audience	Identify Target Market	Stakeholder Management	Visioning & Innovation
Promote	Distribution Strategy	Project Plan	Security Roadmap

As stated previously, you can leverage the strategic planning work from earlier in this course to create your marketing plan. Your output for each of these SNAP categories are certainly not limited to the planning tools described in the table. These are simply a good place to begin to collect data points for your marketing efforts.

In the Specify category, where you determine your marketing objectives, you can use output from the Threat Analysis, Historical Analysis, Gap Analysis, Security Roadmap, Metrics & Dashboards, and SWOT Analysis (specifically, Weaknesses and Opportunities & Threats).

In the Niche category, you identify your value proposition. You can utilize output from the Vision & Mission, PEST Analysis (specifically, the Economic, Social, and Technological quadrants), Porter's Five Forces, Values & Cultures, and SWOT Analysis (specifically, strengths).

In the Audience category, where you identify your target market, you can leverage output from the Stakeholders Management and Visioning & Innovation sections.

Finally, for the Promote category, you need to develop your distribution strategy. For that, you can leverage your project plan as well as your Security Roadmap.

In Summary

- Marketing efforts can help increase:
  - Revenue and/or funding
  - Brand recognition
  - Product and/or capability visibility
  - Customer and stakeholder support
  - Aid in employee retention and recruiting efforts
- It's important to evaluate your results and make modifications to your marketing plan as necessary

Marketing your security organization internally and/or externally can help increase revenue and/or funding, brand recognition, product and/or capability visibility, customer and stakeholder support, and aid in employee retention and recruiting efforts.

Invest the time into building your marketing plan and perfecting effective messaging techniques is of vital importance and will benefit you tremendously as security is a complex field and not easily understood by non-security professionals. Security is no longer just an IT issue, and these topics have reached the most senior executives in your company because security breaches are in the media, it seems almost daily. Now is a great time to market your organization and get the best value for your efforts.

Course Roadmap

- Section 1: Strategic Planning Foundations
- *Section 2: Strategic Roadmap Development*
- Section 3: Security Policy Development & Assessment
- Section 4: Leadership & Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Analyze Current State
  - Historical Analysis
  - Values & Culture
    - Exercise #1: Core Values
  - SWOT Analysis
- Develop Roadmap
  - Visioning & Innovation
    - Exercise #2: Innovation
  - Security Framework
  - Gap Analysis
    - Exercise #3: Gap Actions
  - Security Roadmap
- Build the Program
  - Business Case Development
  - Security Metrics Program
    - Exercise #4: Security Metrics
  - Marketing & Exec Communications

This page intentionally left blank.