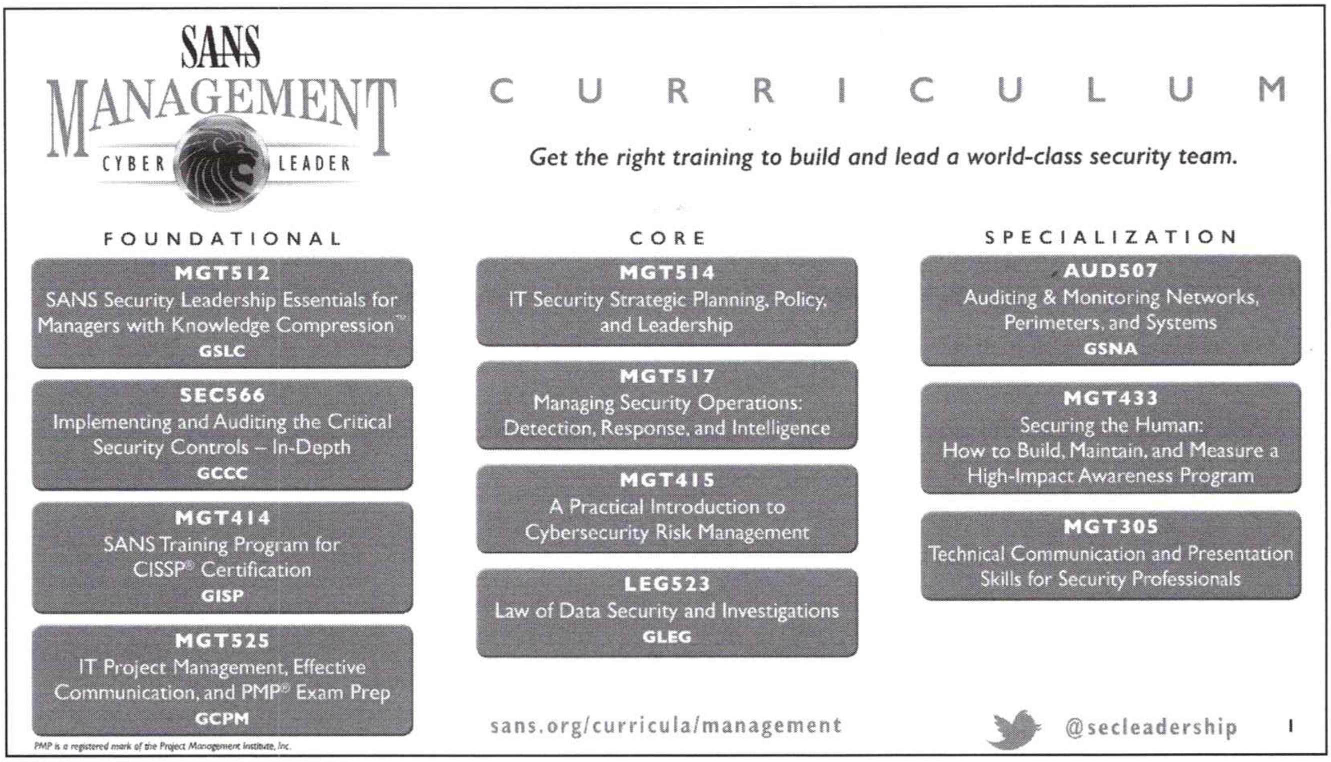
514.1

Strategic Planning Foundations

SANS

MGT514_1_B01_01



The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world.

SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system—the Internet Storm Center.

SANS offers a number of courses that prepare cyber leaders and managers for building and leading world-class security teams. As security becomes more relevant to the business we need to develop business, leadership, and technical skills to effectively interact with business leaders as well as lead and inspire our technical teams. The following courses give you the necessary skills to navigate in the new world of security:

MGT512: Security Leadership Essentials for Managers

Get up to speed on information security issues and terminology. You don't just learn security, you learn how to manage security.

MGT514: IT Security Strategic Planning, Policy, & Leadership

Learn to build and execute strategic plans, develop and assess policy, and utilize management tools to lead, inspire, and motivate your teams.

MGT517: Managing Security Operations: Detection, Response, and Intelligence

Learn to manage and prepare your security operations and incident response teams.

SEC566: Implementing and Auditing the Critical Security Controls In-Depth

Learn about the Critical Security Controls that can serve as the foundation for your security program.

LEG523: Law of Data Security and Investigations

Understand key lessons on the law of data security and investigations that all managers, leaders, & executives should know.

MGT525: IT Project Management, Effective Communication, and PMP Prep

Learn how to effectively drive and manage projects and key initiatives.

MGT415: A Practical Introduction to Cyber Security Risk Management

Understand how to assess and manage cyber security risk.

MGT305: Communication Skills for Security Professionals

Develop foundational skills to become a more effective communicator and leader.

MGT433: Securing the Human: How to Build, Maintain, and Measure an Awareness Program

Learn to build a security awareness program the right way.

MGT414: SANS Training Program for CISSP Certification

Gain the knowledge to pass the CISSP exam.

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems

Learn how to audit and monitor your key controls.

MGT514.1 | IT Security Strategic Planning, Policy, and Leadership

SANS

Strategic Planning Foundations

Welcome to SANS MGT514: IT Security Strategic Planning, Policy, and Leadership!

A Note about URLs

Sometimes this courseware cites URLs, which were valid at the time they were originally sited. URLs change all the time. This courseware does not necessarily update all URLs. Out-of-date URLs have several values. They show that a statement is based on scholarship. They can give hints about how to find source material, even if it is no longer at the original URL. They can also be used to find material at the Wayback Machine maintained by the Internet Archive.

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 1

- *Background*
  - About This Course
  - Need for Strategic Planning
    - Exercise #1: Case Scenario
- Understand the Business
  - Vision & Mission
    - Exercise #2: Mission Statement
  - Stakeholder Management
  - PEST Analysis
    - Exercise #3: PEST
  - Business Strategy
- Understand the Threats
  - Threat Actors
    - Attack Case Studies
  - Asset Analysis
    - Exercise #4: Attacker Motivation
  - Threat Analysis
    - Exercise #5: Intrusion Kill Chain

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 4

This page intentionally left blank.

Background

- Focus on cyber security is at an all-time high
  - Increasing number of breaches
  - Visibility at the Board and CEO levels
- Information security teams have
  - More budget and more opportunity
  - Increased responsibility and scrutiny
- Security is not just an IT concern
  - It's a vital part of the growth of your business
  - Security business leaders must learn how to navigate in this new world

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 5

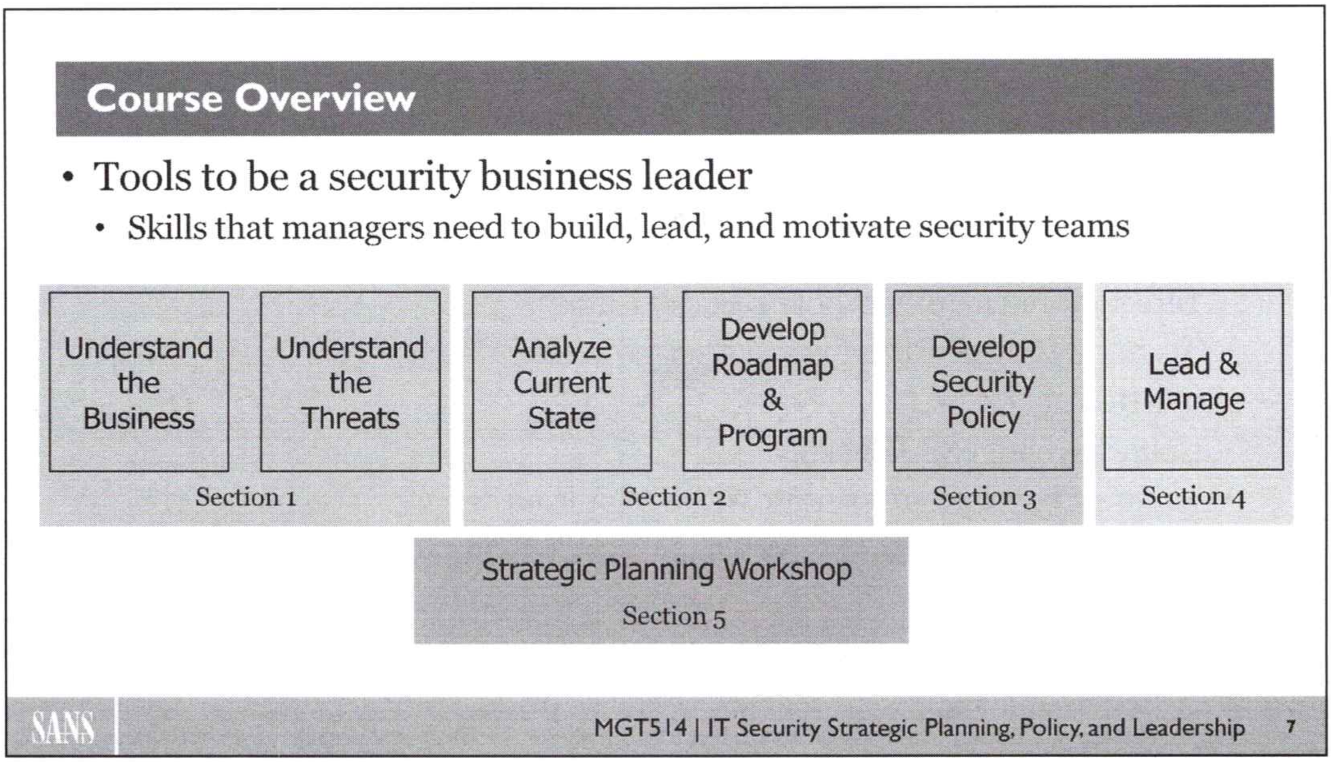
As security professionals, we have seen the landscape change. Information security is now more vital, crucial, relevant, and important to the growth of your organization than ever before. As a result, information security teams have more budget, more opportunity, and more visibility to the Board and executives. With increased opportunity comes increased responsibility and scrutiny. Security business leaders must learn how to navigate in this new world.

About This Course

- This course teaches you how to
  - Build and execute strategic plans
    - That resonate with other IT and business leaders
  - Develop and assess security policy
    - To help steer your organization
  - Utilize management tools and frameworks
    - To better lead, inspire, and motivate your teams
- The goal is to teach you
  - What to do to become a security business leader
    - Not only an information security specialist

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 6

This course covers the skills and tools that managers and leaders need to effectively build, lead, and motivate security teams. As a first step, security leaders must get buy-in for their security initiatives. This means that you need to know how to build strategic plans that not only make technical sense, but you also need plans that resonate with other IT and business leaders. Moreover, you have to effectively steer the organization toward these strategic goals. Effective development of security policies and effective assessment of security policies are key skills that security managers and leaders need to possess. Finally, effective security leaders know what motivates and drives their teams and how to inspire and motivate people to achieve a larger goal.



The goal of this course is to give you the knowledge to go beyond technical information security work and become a security business leader who can not only build effective security plans and programs, but can also make information security relevant and understandable to key stakeholders across your organizations. To develop these skills, the course covers the following topics:

Section 1

Use tools to understand the business and, given this understanding of key business drivers, understand the threats so that we can better protect the organization.

Section 2

With an understanding of the business and the threat landscape, we can analyze the current state of our security program and develop a roadmap to accomplish our goals. Once we have a strategic plan in place, we can use tools to build and maintain our security program.

Section 3

Security policy is one of the key tools we can use to influence and guide the organization.

Section 4

Leadership competencies are developed to lead, motivate, and inspire our team as we work to implement the strategic plan.

Section 5

Case studies and group discussions teach you to apply the tools from class to real-world scenarios.

Who Should Take This Course?

- Intended audience:
  - Senior security and IT leaders (for example, CISO and CIO)
  - Directors and managers of IT security teams
  - Team leads responsible for security operations
- Anyone interested in
  - Going beyond technical skills
  - Learning how to communicate with senior leaders
  - Talking about security in ways business leadership can understand

This course is for anyone interested in going beyond technical skills and learning how to communicate with senior leaders who may not have much experience in information security or even Information Technology (IT). Anyone in a leadership position, including senior staff, team leads, managers, directors, and senior leaders (such as the CISO and CIO) will benefit from taking this course. The point of the course is to make you more effective as a security professional and leader in managing your team, your business, and your relationships with other leaders across the organization.

How the Course Works

- Expectations
  - Managers and leaders are expected to voice opinions
  - This class will give you opportunities to practice
- Success of the class depends on you
  - Highly interactive
    - Group exercises, group discussions, case studies, and case scenarios
  - How exercises work
    - We will often break into teams of 3-5 to discuss the exercises at hand
    - They require you come up with solutions as a team
    - Team members will share thoughts in a class debrief

People in leadership positions are expected to voice their opinions. If leaders do not speak up, what is the perception? The perception is they don't have the appropriate knowledge, savvy, or confidence to be in a senior leadership position!

Because this is a management class, we will model that expectation by providing you the opportunity to practice in class. As a result, the success of this class depends largely on you. A number of group exercises, group discussions, case scenarios, and case studies require you to break into teams to discuss the exercises at hand. Based on the group discussion, team members will report to the rest of the class. Please be prepared for this opportunity.

Need for Strategic Planning

SANS

MGT514 | IT Security Strategic Planning, Policy, and Leadership 10

This page intentionally left blank.

Background and Need for Strategic Planning

- Security and business goals must be aligned
  - Security is just one type of risk that needs to be addressed
  - Security budgets need to be balanced with other business investments
  - Strategic planning is needed to ensure that all business goals are considered

Strategic planning enables us to align security with business goals. Successful security planning requires an understanding of not only security threats and capabilities, but also a deep understanding of the business environment and organizational goals. An organization faces many risks in the course of doing business, and security is just one of the risks that needs to be addressed. By balancing security needs with those of other business investments, security can be seen as a business partner and not just a cost of doing business.

Technology and the Threat Landscape

- Dependence on technology
  - Transformative effect
  - Global connectivity
  - Opens the doors equally to benefits and harm
- Security breaches are on the rise
- Cyber challenges are emerging as fast as we can combat them

Business leaders understand that technology and the dependence on technology has had a transformative effect on our society. We have entered an era of global connectivity that opens the doors equally to benefits and harm. Almost weekly, there are new reports in the media of data breaches that range from Personally Identifiable Information (PII) to sensitive government documents to credit card data. Security breaches are on the rise and new cyber security challenges are emerging as fast as experts can combat them.

DRIVE the Vision

- Directional
  - Does it help you decide what activities to pursue?
- Relevant
  - Takes into account the organization's history, current state, culture, and values, thereby making it visible. Is it authentic and true to the organization?
- Inspirational
  - Inspires people to commit to a shared goal. Captures the hearts and minds. Do you find it personally inspiring?
- Vivid
  - Clear and concrete. Describes the future in a way that is easy to imagine. Would it be greeted with enthusiasm by most people in the organization?
- Extremely Bold
  - Audacious. Does it feel potentially unattainable?

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 33

Good vision statements have the following five characteristics:

- **Directional:** It is obvious where the organization is going—so obvious, in fact, that a vision statement that is directional can even help people decide which activities to pursue on a daily basis.

- **Relevant**: Takes into account the organization's history, current state, culture, and values, thereby ensuring that the direction is not only visible but also authentic and true the organization.

- **Inspirational:** Inspires people to commit to a shared goal. Captures the hearts and minds. Individuals find the vision personally inspiring.

- **Vivid**: Clear with enough detail to make it concrete. Describes the future in a way that is easy to imagine.

- **Extremely bold:** Seems almost impossible to achieve and audacious.

Space Vision

"I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the Earth."

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

On May 25, 1961, U.S. President John F. Kennedy announced before a special joint session of Congress the ambitious goal of sending an American to the moon and back by the end of the decade. This vision had all five elements of successful vision statements:

Directional: It was extremely clear what needed to be accomplished and by when.

Relevant: During the Cold War, the United States was in a race for technological dominance with the Soviet Union. At the time, the Soviet Union had already had successful space missions, and the the perception was that the United States was falling behind.

Inspirational: Shortly after this announcement, JFK was touring NASA headquarters for the first time. He introduced himself to a janitor who was sweeping the floor and asked him what he did at NASA. The janitor replied, "I'm helping put a man on the moon." The simple announcement helped inspire many people in the country.

Vivid: It was very easy to imagine. Not just sending a man to the moon but "returning him safely to the Earth."

Extremely Bold: This type of space travel had never been accomplished and, at the time, was considered an audacious goal.

Eight years later, on July 20, 1969, the mission was accomplished.

Susan G. Komen Vision

"To end breast cancer forever."

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 35

In 1980, Nancy G. Brinker promised her dying sister, Susan G. Komen, that she would do everything in her power to end breast cancer forever. Now the Komen Foundation is the most widely known, largest, and best-funded breast cancer organization in the United States.

This simple vision statement guides everything that the organization does:

Directional: The organization is focused solely on breast cancer.

Relevant: Hundreds of thousands of women get breast cancer every year, and the Komen Foundation has helped make this issue much more visible through its activities.

Inspirational: The simple vision has helped the organization grow to more than 100,000 volunteers worldwide, spending of $1.5 billion for breast cancer research, education, advocacy, and health services.

Vivid: This vision is easy to imagine.

Extremely Bold: It seems impossible to end breast cancer forever, but that is what makes this vision extremely bold.

Whose Vision Is This?

"To make people happy."

Disney's vision of making people happy is supported by its mission to "Create happiness by providing the finest in entertainment for people of all ages, everywhere." This has guided the company's goal of providing family-friendly entertainment in the form of amusement parks, movies, television shows, and toys.

Technology Vision

"A computer on every desk and in every home."

In 1980, Bill Gates's vision was "A computer on every desk and in every home." At the time, the concept of a computer in every home was almost inconceivable. Incumbents like IBM scoffed at the idea.

What Microsoft didn't articulate publicly was its actual vision: "A computer on every desk and in every home *running Microsoft software*." Microsoft ruthlessly achieved this vision with Office, Internet Explorer, and of course, Windows. One could argue that once Microsoft achieved its vision from the 1980s, that's when the company started to falter. What is its rallying cry now?

But, this vision guided Microsoft for decades because it was:

Directional: Microsoft created compelling software and partnerships to help make this vision a reality.

Relevant: It wasn't obvious to many in the early 1980s, but decreasing technology costs coupled with the convenience of having the power of a computer on your desk made this vision especially relevant for the times.

Inspirational: Everyone could buy in to this shared goal.

Vivid: It was very simple and easy to imagine.

Extremely Bold: Given that only large corporations or the extremely rich could afford a computer, this vision was definitely a bold proclamation at the time.

Vision_cabulary

- Aspires
- Preeminent
- Strives to achieve
- Sustains growth
- Best
- Center of excellence
- Inspires
- Top performing
- Fulfilling
- Innovative
- Excellent

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 38

If you spend an hour surfing the web looking at various vision statements, you will see certain words appear again and again. The majority of the time, these organizations have gone through a process to determine what "they want to be when they grow up." If your vision statement does not have any of the words on the slide, or words similar to these, you might want to look it over again and see if it truly expresses vision.

Purpose of a Mission Statement

- Mission statement
  - Describes what we are and what we do today
- Why is the mission important for strategic planning?
  - As we set goals, priorities, and intermediate steps, the mission statement reminds us of our purpose and helps keep us on track
- Let's look at some corporate mission statements for various industries
  - Discuss how they might impact security

A mission statement describes what we are and what the organization does today. As we set goals, priorities, and intermediate steps, the mission statement reminds us of our purpose and that helps keep us on track. When we look at a new task, we can determine whether or not expending resources on it will help us achieve our goals. If not, we should elect to defer or delete that task.

According to Karen Scharf, "A well-defined mission statement will keep you from spreading yourself too thin. As entrepreneurs, we're constantly coming up with new ideas and inspiration. However, not all of our ideas are the perfect fit for our business. But once your mission statement is created, you'll have a barometer to measure each new idea by. You'll know that every new project you take on is one that is propelling your business forward."[1]

Individuals also an use mission statements to help guide their efforts toward setting and achieving personal goals.

Reference

[1] http://ezinearticles.com/?Small-Business-Marketing---Making-Use-of-a-Mission-Statement&id=4401845

Is This a Good Mission Statement?

- State of North Carolina

The Enterprise Security and Risk Management Office (ESRMO) provides leadership in the development, delivery and maintenance of an information security and risk management program that safeguards the state's information assets and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss.

The ESRMO supports a comprehensive statewide program that encompasses information security implementation, monitoring, threat and vulnerability management, cyber incident management, and enterprise business continuity management.

The ESRMO works with executive branch agencies to help them comply with legal and regulatory requirements, the statewide technical architecture, policies, industry best practices, and other requirements.

Working with state agencies, federal and local governments, citizens and private sector businesses, ESRMO helps to manage risk to support secure and sustainable information technology services to meet the needs of our citizens.

This mission statement is from the security department at the State of North Carolina.[1] It says that the department is responsible for security and risk management and describes what the department does to support the state and executive branch while working with state agencies, federal and local governments, citizens, and the private sector. However, this extremely verbose mission statement does not map back to the larger organizational mission of which security is a part.

The most successful security team mission statements will be informed by the mission of the larger organization and show a direct link to how it helps meet corporate goals. To see how the mission of the larger organization can impact the security team, let's review some real-world corporate mission statements.

Reference

[1] http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management

Retail Industry Mission (1)

"To provide outstanding service, every day, one customer at a time."

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 41

This mission statement is for Nordstrom, which is an upscale clothing retailer in the United States headquartered in Seattle, Washington. Nordstrom, from its founding, was focused primarily on providing outstanding customer service. According to John W. Nordstrom, the founder of the company, this is best exemplified by the famous "tire story."[1] Mr. Nordstrom was at a store in Fairbanks, Alaska, meeting with the sales and management team when they saw a gentleman rolling a tire into the store so that he could return it. Obviously, an upscale clothing retailer does not sell car tires, but Mr. Nordstrom advised the manager to let the sales clerk handle the situation to see what he would do. It turns out that there was a tire shop at that location before Nordstrom opened. The gentleman was obviously confused, but the sales clerk happily volunteered to take the tire back without a receipt and gave him $25. To this day, that tire is nailed to a wall at the back of the store as a reminder about providing outstanding customer service and empowering employees to make their own decisions and "do the right thing."

In this type of environment, what can security do to be more successful? It is likely that, in an organization so focused on customer service, this would permeate the internal culture also. This means that security, instead of being the group that simply says "no," would have to find ways to partner with internal stakeholders and provide solutions that empower employees to make more secure decisions.

[1] http://www.scoremoresales.com/nordstrom-tire-story

Retail Industry Mission (2)

"To save people money so they can live better."

This mission statement is for Walmart, which operates a chain of discount retail stores and warehouses around the world. In the retail industry, where profit margins are already very thin, Walmart is extremely focused on maintaining low cost.

In this type of environment, what can security do to be more successful? Security activities would ideally be tied to cost-saving measures with strong justification for any security spend.

Healthcare Industry Mission

"To provide high quality, affordable healthcare services and to improve the health of our members and the communities we serve."

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 43

Kaiser Permanente is the largest not-for-profit health plan and integrated healthcare provider in the United States. Its mission is to provide "high quality, affordable healthcare services" to not only its members but also the communities it serves. As an integrated healthcare provider, Kaiser Permanente provides both insurance *and* healthcare services. As a result, it has a large focus on improving health and not simply providing treatment.

In this type of environment, what can security do to be more successful? In addition to the obvious need to secure protected health information (PHI), security can succeed by enabling and protecting new methods of care delivery including remote care, telehealth, medical devices, and health information exchanges.

Higher Education Mission

"We strive to create knowledge, to open the minds of students to that knowledge, and to enable students to take best advantage of their educational opportunities.

We seek to identify and to remove restraints on students' full participation, so that individuals may explore their capabilities and interests and may develop their full intellectual and human potential."

Harvard College is the undergraduate school at Harvard University. Its mission is to "remove restraints on students' full participation, so that individuals may explore their capabilities and interests and may develop their full intellectual and human potential."[1] Like many educational institutions, Harvard wants to remove barriers to learning. Doing so can be a challenge for security, which typically wants to introduce additional controls.

In this type of environment, what can security do to be more successful? Instead of saying "no," security will have to find ways to minimize risk while still providing an open environment for faculty, students, and staff to share information and further their academic goals.

Reference

[1] http://compact.org/resource-posts/the-mission-of-harvard-college/

Defense Industry Mission

"To ensure the nation's sovereignty, territorial integrity, and domestic security in order to continue national development."

This could be the mission of any country in the world. In this case, it is the mission statement of the People's Liberation Army (PLA) of China.[1]

Reference

[1] http://www.rand.org/content/dam/rand/pubs/testimonies/2009/RAND_CT332.pdf

Mission_cabulary

- Branding
- Consistency
- Core
- Detail
- Dominant player
- Enterprising
- Innovation
- Inspire
- Profit
- Quality
- Research
- Service
- Social responsibility
- Opportunity

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 46

These are examples of some words you will commonly see in a mission statement.

Example of Long but Clear Mission Goals

- NSA's Information Assurance Directorate (IAD)
  - "IAD is responsible for NSA's defensive mission and is widely acknowledged for leading innovative security solutions"

    IAD delivers mission enhancing cyber security technologies, products, and services that enable customers and clients to secure their networks; trusted engineering solutions that provide customers with flexible, timely and risk sensitive security solutions; as well as, traditional IA engineering and fielded solutions support.

    Information Assurance Operations which include remote and deployed operational groups, with 24X7 integrated support as needed that protect critical national security networks.

    Fusion, Analysis, and Mitigations teams that analyze and characterize large volumes of IA data, using an automated and persistent approach to identify vulnerabilities, and develop solutions to mitigate them.

    Training and security awareness support.

    The Key Management Infrastructure that provisions end cryptographic units.

The Information Assurance Directorate (IAD) within the National Security Agency (NSA) of the United States is responsible for protecting and defending national security information and systems. Its website makes it clear that the IAD provides five things:[1]

1. Security products, services, and engineering
2. Security operations to protect critical national security networks
3. Vulnerability management including analysis and mitigation
4. Training and security awareness
5. The key management infrastructure

If only the security goals at most enterprises were so straightforward. Unlike the IAD, most security departments have to struggle with creating a mission that resonates with the rest of the organization and the business.

Reference

[1] https://www.nsa.gov/ia/ia_at_nsa/

Departmental Mission Statements

- Must be aligned with the mission of the larger org
  - Useful for keeping the security team focused
- If a departmental mission statement exists:
  - Review and update it if necessary
  - Organizations change over time and your goal of ten years ago may not be the same today
- If you need to update or create one from scratch:
  - Focus on the purpose of the organization
  - Be realistic—does it represent what you are now?
  - Keep it short and focused—can you tweet it?

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 48

If you have an existing mission statement for your department, then review and update it as necessary. It is simply reality; organizations change over time and your purpose of ten years ago may not be the same purpose today. Apple used to be primarily focused on selling endpoint computers and some servers. Then, a tremendous part of the company's income was the iPod, then later the iPhone, and then iPad. The strategic planning process should generate a number of questions or issues to help evaluate the mission statement. For example, one of the questions should be: "Is our mission statement focused on satisfying customer needs rather than being focused on the product?"

If your security department does not have a mission statement, then you will need to develop one. The key is to tell the world the purpose and the focus of your organization. Keep in mind the vision statement is what you aspire to become; the mission statement is what you are. Work hard to reduce this statement to the minimum number of words. People are unlikely to read anything that runs on. Additionally, it is easier for your employees to remember a short, pithy mission statement. Be sure to try out your mission statement on several people and ask them to state what it means in their own words. Sometimes we write things that look correct to us, but other people interpret the words differently than we would think.

Creating a Mission Statement for the Security Department

- A good mission statement guides our decisions
- Consider what IT or security can do to:
  - Protect the company (prevent failure)
  - Enable the business (ensure success)
- If you're stuck, you can use this as a starter:
  - "To advance *company's* mission by securing, defending, and monitoring our *most important assets.*"
- Or follow the four-step process for creating a mission statement
  - From nonprofithub.org

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 49

A good mission statement helps guide the decisions that the security department needs to make. How can the security team better protect the company and enable the business? By crafting a simple, meaningful mission statement that resonates with key stakeholders in the company, you will be that much closer to making security relevant and understandable to non-IT and non-security leaders.

It can be very difficult to create a mission statement. If you're stuck, you can use the following as a starting point:

"To advance the *<insert company's mission>* by securing, defending, and monitoring *<insert company's most important assets>*"

Alternatively, you can follow the "Step-by-step Exercise for Creating a Mission Statement" developed by nonprofithub.org to create a mission statement for your security team.[1] That is what we will do in the rest of this section.

Reference

[1] http://nonprofithub.org/wp-content/themes/nonprofithub/img/landing-pages/mission/nonprofithub-missionstatement.pdf

Step 1: Tell a Story

"By enabling teleconsult, we helped Dr. Dell perform a remote consultation that allowed her to rapidly diagnose the appropriate treatment to a stroke. This quick treatment saved the patient from potential disability and even death."

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 50

In Step 1, tell a story about a time that the security team did something meaningful. It doesn't have to be something that changed the world, saved a life, or prevented a dramatic attack. It can be something as simple as a time when another team really appreciated the output or service that the security team provided. If you are stuck trying to think about a good story, ask yourself, "What *does* it look like when we're doing our best work?" This question can prompt some good ideas. If you still can't think of a good story, then just make one up. Ask yourself, "What *would* it look like when we're doing our best work?"

The story on this slide is about the security team at a hospital. In event of a stroke, it is extremely important to obtain a timely diagnosis from a neurologist to determine appropriate treatment. By enabling teleconsult, the team helped Dr. Dell perform a remote consultation that allowed her to rapidly diagnose the appropriate treatment to a stroke. This quick treatment saved the patient from potential disability and even death.

In this example, the security team did its best work by helping physicians deliver great care.

Step 2: Highlight Key Words

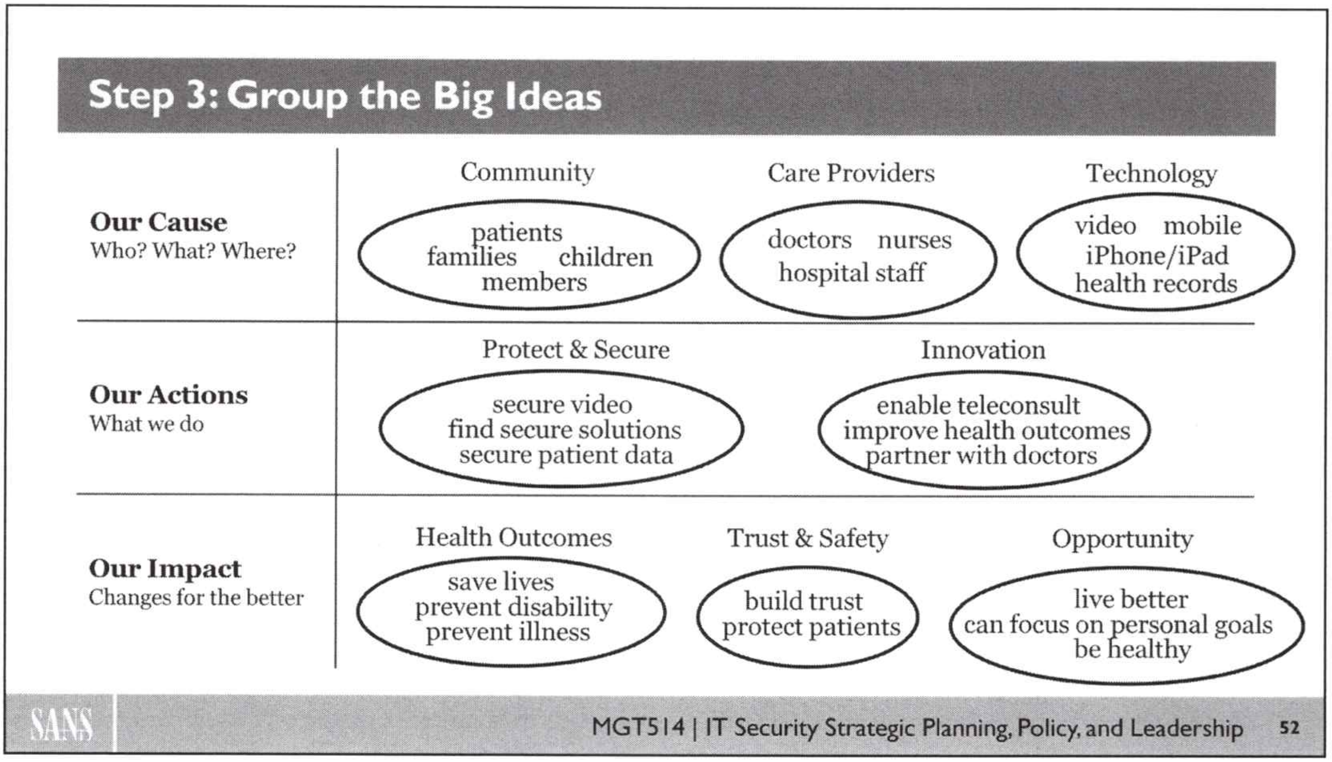
"By enabling teleconsult, we helped Dr. Dell perform a remote consultation that allowed her to rapidly diagnose the appropriate treatment to a stroke. This quick treatment saved the patient from potential disability and even death."

Circle the people or places
Put a square around any mention of making a difference
Underline when something changes for the better

In Step 2, simply highlight the key words in your story:

- Circle any time you mention a specific person or place.
- Draw a square around items that describe your team making a difference or taking action.
- Underline anything in the story when something changes for the better.

This step helps you identify the important parts of your story so that you can share them with your team.



In Step 3, group the big ideas. Start by writing down all the highlighted words and phrases from Step 2. Patterns and similarities will develop naturally. Group them together like we've done on this slide.

In some cases, your story might lead you to write down other ideas that preceded the story itself. For example, how did you know that teleconsult was a potential solution? You may have partnered with some doctors and discovered that they were looking for solutions to improve the outcomes of stroke victims. As a result, "partner with doctors" and "improve health outcomes" are listed under "Innovation" on the slide.

As another example, you may know that securing the video communication and corresponding health information has to be done before deploying the solution. This is why these items are listed under "Protect & Secure" on the slide.

The section titled "Our Impact" is arguably the most important one. Succinctly categorizing the overall change for the better is what truly matters to your stakeholders. This is why "save lives," "prevent disability," and "prevent illness" are listed under "Health Outcomes."

Grouping and naming the common ideas in your story helps identify themes that you can use to craft your actual mission statement.

Step 4: Craft the Mission

"We help patients stay healthy by enabling and securing innovative healthcare systems."

"Helping build healthy communities by giving care providers secure tools to improve health outcomes."

"Through security and innovation, we promote trust and safety with members and care providers."

In Step 4, you actually create the mission statement itself. Creating a mission statement can be a difficult process. However, by telling a story, identifying key words, and grouping the big ideas, you can draft a mission statement that will resonate with your key business partners.

Here, we have taken the previously circled, squared, and underlined words and crafted three sample mission statements.

Exercise 1.2 – Creating a Mission Statement (1)

Estimated Time: 30 Minutes

- Goal of this exercise:
  - Draft a mission statement for your security department by going through the four-step process
- Step 1: Tell a story
  - A time when security did something meaningful
  - What *does* it looks like when we're doing our best work?
  - What *would* it look like when we're doing our best work?
- Step 2: Highlight key words
  - Circle the people or places
  - Put a square around any mention of making a difference
  - Underline when something changes for the better

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 54

The goal of this exercise is to create a mission statement for your security department by going through the four-step process we just discussed.

Step 1

Tell a story about a time your security team did something meaningful. It can be about anything. Any situation that you are proud of when the team did its best work. If you can't think of a story, then make one up. What *would* it look like when the security team is doing its best work?

Step 2

After you've written down the story, then highlight the key words. Circle the important people or places. Put a square around any mention of making a difference. Finally, underline the items when something changes for the better.

Creating a Mission Statement (2)

- Step 3: Group the items in each category
  - Find the Big Ideas
  - Write them on the next page
- Step 4: Draft the mission statement
  - Incorporate the Big Ideas
  - Don't worry about word choice
  - Keep it short and simple
  - If no one disagrees with it, then it's too generic

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 55

Step 3

Then, group the Big Ideas. The next page has an empty worksheet that you can use.

Step 4

Finally, try to write a draft of the mission statement for your security team by incorporating the big ideas you have just identified. Don't worry about making the words perfect. Try to keep the statement short and simple by conveying the main point. If no one else disagrees with the draft mission statement, then it may be too generic. In that case, you may want to incorporate more big ideas.

Security Department Big Ideas

Our Cause Who? What? Where?	
Our Actions What we do	
Our Impact Changes for the better	

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 56

Use this page as a worksheet for your ideas.

In Summary

- As a manager and leader:
  - You are expected to understand what the organization does and is trying to achieve
  - Understand the mission and vision are key
- Crafting a team mission statement
  - Maps back to the mission of the larger org
  - Shows that you understand organizational goals
  - Helps your team focus on work that is important to the organization

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 57

As a manager and leader, you are expected to understand what the organization does today and what it is trying to achieve in the future. This is why understanding the mission and vision of the organization are so important. This understanding helps you set appropriate direction for your team and identify security initiatives that will be valuable to key stakeholders; it also helps your team focus on work that is important to the organization.

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 1

- Background
  - About This Course
  - Need for Strategic Planning
    - Exercise #1: Case Scenario
- Understand the Business
  - Vision & Mission
    - Exercise #2: Mission Statement
  - *Stakeholder Management*
  - PEST Analysis
    - Exercise #3: PEST
  - Business Strategy
- Understand the Threats
  - Threat Actors
    - Attack case studies
  - Asset Analysis
    - Exercise #4: Attacker Motivation
  - Threat Analysis
    - Exercise #5: Intrusion Kill Chain

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 58

This page intentionally left blank.

Stakeholder Management Strategy

- By the end of this section, you will understand
  - The importance of stakeholders
    - Common stakeholders
  - Stakeholder management
    - How to identify stakeholders
    - How to map their interests and influence
    - How to develop and drive your relationship plan
  - Common communication methods
    - Managing resistance to your project

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 59

In this section, we cover the importance of stakeholders and stakeholder management. It may not be apparent initially, but even a simple technology deployment as part of your strategy could impact not only your security organization but also the overall enterprise. As a result, all stakeholders and associated impact need to be identified and managed through a Stakeholder Management Strategy.

As an example: As part of your data encryption strategy, you'd like to force encrypt all outbound e-mail messages containing sensitive data. The technology deployment is straightforward and can be done in a couple of weeks. At first glance, it is just that—"a technology deployment"—but the organizational impact that may not be factored into this effort could indeed have a high impact on your team. You will need to consider all areas, such as Legal or Compliance for review of the messaging that end users will receive to ensure your company is held harmless of any legal and/or regulatory risks. You may also want to consider your sales team if applicable, to help you determine if the user interface to unencrypt the message is acceptable for customers. You may also need to consider your help desk or call center teams to make certain they have up-to-date information on your go-live date. You will also need to provide these teams with appropriate user guides so they can help end users who call in and need help unencrypting the messages they receive.

For the success of any effort you undertake, it's important to understand the process of how to identify all of your stakeholders and reach beyond the people and groups that are typically involved in security initiatives—those that may have an indirect impact or where the impact is currently unknown. These types of stakeholders may be a bit more difficult to identify, but they need to be factored into your Stakeholder Management Strategy.

It's equally as important to understand how to map your stakeholders' interest and influence and to drive your relationship plan so that you can get the support you need to successfully manage the deployment of your strategy and/or initiatives.

Why We Need a Stakeholder Management Strategy (1)

- Understanding the business is not just about understanding the goals of the company
  - It's also about understanding key stakeholders, their motivations, interests, and power
- As you become more successful in your career, the initiatives you run will affect more people
  - It's likely your work will impact people who have power and influence over your projects
  - These people can support or block you

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 60

Stakeholder management has always been important, but arguably it is more important now than ever before. This is due in large part to our increasing dependency on technology and interconnectivity that's at the core of nearly all personal and business usage. It's equally as important to know that understanding the business is not just about understanding the goals of the company; it's also about understanding key stakeholders, their motivations, interests, and power.

The level of stakeholder engagement in any project will be a direct result of the the Stakeholder Management Strategy. Excellent stakeholder management results in good stakeholder engagement and entails the recognition, acknowledgment, and management of stakeholder needs, concerns, wants, authority, common relationships, and interfaces, and the realization that any changes in business processes increase the impact to the organization and could potentially cause reputational risks that come from poor stakeholder relations. In this context, good stakeholder relations are a prerequisite for good risk management.

As you become more successful in your career, the initiatives you run will affect more people who have power and influence over your projects. These same people can support or block you. It's important you realize that relationship building takes time. Many of the hallmarks of a good relationship—trust, mutual respect, understanding—are intangibles that develop and evolve over time, based on individual and collective experiences and interactions.

Why We Need a Stakeholder Management Strategy (2)

- Proactive management and engagement of key stakeholders
  - During the creation and implementation of your efforts is a critical success factor
- Involving stakeholders early helps positively shape the project, which can help with
  - Higher quality
  - Additional resources
  - Capability to avoid roadblocks

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 61

Proactive management and engagement of key stakeholders during the creation and throughout implementation of your efforts are crucial. Often, stakeholders are engaged right before go-live, and at this point, you have little to no time to consider what needs to be done to gain support and/or reduce opposition to your efforts.

In Paul Nutt's *Why Decisions Fail*, he conducted an analysis of 400 strategic decisions and found that half of these decisions failed—that is, they were not implemented, only partially implemented, or otherwise produced poor results—in large part because decision makers failed to attend to interest and information held by key stakeholders.

A Stakeholders Management Strategy provides a mechanism to socialize vital information with your stakeholders and those people and/or groups that influence them. It will also give you the opportunity to address important areas such as what type of information your stakeholders need to make better decision and how you can best address questions and mitigate concerns that will ultimately help in avoiding roadblocks.

Involving stakeholders early enables you to positively shape your project with higher-quality results and possibly gain additional resources in support of your effort.

Why We Need a Stakeholder Management Strategy (3)

- Stakeholder Management Strategy will help you:
  - Identify key people you have to win over
  - Understand and prioritize interest and influence of key stakeholders
  - Develop and drive your relationship plan

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 62

Some stakeholders are more obvious than others, and some stakeholders are more challenging to win over. Your Stakeholder Management Strategy will help you identify key people you have to win over in support of your efforts from either a financial standpoint or resource allocation, assist you in influencing other stakeholders, or simply provide support and buy-in for your efforts.

Considering specific interests your stakeholders may have with your initiatives will help you prioritize. You will also need to consider the benefits your stakeholders might anticipate, plus activities that might cause a sense of loss or power by your stakeholders, and those activities that could create potential conflict. You will need to consider changes that your initiative might require from your stakeholders, such as business processes. The way they operate today will not be the same as the way they operate after your initiative is launched, and that may be problematic in the eyes of your stakeholders.

Stakeholders play an important role in making your initiative successful, and managing supportive stakeholders and potential negative responses, whether real or perceived, early on will help you develop and drive your relationship plan.

What Are Stakeholders and Why Are They Important to Me?

- A stakeholder may be a person or a group
  - Who will affect or be affected by your work
  - Who may be internal, external, or both
  - Who can be divergent and vocal with differing expectations about outcome needs
- Stakeholders have a vested interest in your work
  - Unaddressed concerns from stakeholder may undermine your efforts
  - Buy-in is necessary for your success

The term *stakeholder* has become well-known terminology in management theory and practice over the last decade. There are many variants to the definition, but they can all be summarized as the following: Stakeholders are people or groups with a vested interest in the success of your strategy and who will affect or be affected by your team's work. In other words, anyone impacted by the project or its outcome is a stakeholder. These people or groups may be internal or external to your organization or both, and their support, cooperation, and buy-in are necessary for you to succeed.

Stakeholder groups can be divergent and vocal with differing expectations about outcomes and the need for change. Unaddressed stakeholder concerns can undermine your efforts and result in lack of strategy and goal buy-in.

Here is a story about a missed stakeholder opportunity:

Robert Taylor, a senior security professional who had been at his company for over five years was given the opportunity to take the lead on a network blocking security initiative that had the potential for organization-wide visibility. Robert, or Bob as he prefers to be called, knew that this would be a great promotional opportunity in his career. After all, he was the subject matter expert in this domain and was a seasoned network security professional of over 20 years. He knew this technology inside out. Bob quickly and eagerly assembled a project team with the typical folks that he'd previously worked with on numerous other security initiatives. Everyone was on board to make this happen.

The plan progressed flawlessly. The project was on time and on budget, all the equipment arrived as scheduled, and network blocking was implemented four days ahead of schedule. Bob knew this would make his boss and the leaders of the organization happy. Bob was at home enjoying his success when he got an urgent call from his boss less than 24 hours after go-live. Bob's boss relayed to him that he had received several calls and e-mails from key people and groups within the organization, and they were complaining they didn't have access to Internet sites they needed to access to get their job done. Bob's boss also received a call from the help desk director stating that her team had received over a hundred calls concerning end users' inability to access Internet sites, and she was concerned there may be a network connectivity problem.

Bob missed the opportunity to engage all of his stakeholders. For Bob, this was a straightforward technology deployment and he didn't think about the impact to users and how they use the Internet to do their job. There could be a number of impacts in a scenario such as this. The sales team or a research and development team may need access to various sites throughout the world to access vital information for their jobs.

The help desk is the first line of defense to field end-user support questions, and Bob's effort was not on the team's radar, nor were they involved. In addition, he didn't engage Communications, a prominent stakeholder to help him get out the message regarding impact to the organization beforehand. This would have given him the opportunity to know the challenges before go-live and work through any obstacles

It is important you and your team know who your stakeholders are and fully understand their needs and expectations. Stakeholders should be proactively included in your efforts to develop your overall strategy, as the process of overcoming stakeholder resistance after initial implementation is complex and time consuming. It often involves trust and credibility issues that may or may not be overcome at that point.

Stakeholder Management Key Components

- Stakeholder management is composed of three phases:
  - Phase 1: Identify stakeholders
  - Phase 2: Understand stakeholders
  - Phase 3: Manage relationships

Stakeholder Management is composed of three key phases:

- **Phase 1:** Identify stakeholders.
- **Phase 2:** Understand stakeholders.
- **Phase 3:** Manage relationships.

We will talk about each of these phases in more detail on the subsequent slides.

Identify Stakeholders

Phase 1

- Can be a complicated process
- A single initiative can impact many people throughout your organization
- It is important to identify those who can impact or will be impacted by your strategy

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 66

Identifying stakeholders can be a complicated process. As we alluded to previously, a single security strategy or initiative, large or small, can produce numerous impacts not only to your security organization but also the overall enterprise. Because this is an important component of your strategy, you'll want to get this right by identifying all appropriate stakeholders.

To identify your stakeholders, you could hold a meeting with your team of managers and staff to brainstorm who your key stakeholders might be You realize that with the limited resources you have, you can't possibly do everything for everyone. Your team has taken your beliefs and this assignment to heart. They have submitted numerous names and groups, and in no time at all, you have a large list with some potential problems because your team generally interacts only with the security teams and those teams outside of security that directly work with them on technology deployments. You know this will limit your influence in the organization and possibly the success of your effort. You know it's important to identify those who can impact or will be impacted by your strategy in any way.

Example: Stakeholders

Phase I

- Security department stakeholders

Your boss	Lines of business	Customers	Prospective customers
Senior Executives/Board	IT	Finance	Suppliers
Colleagues	Help Desk	HR	Vendors
Your team	Operations	Legal	Shareholders
Your family	Procurement	Compliance	Government
Your peers	Communications	Facilities	Regulators

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 67

Listed here are some examples of security department stakeholders. Some of them are obvious and would likely appear on the results of your team's stakeholder brainstorming activity. Less-than-obvious stakeholder examples might be:

- **Procurement**: Procurement will be responsible for negotiating pricing terms and conditions for hardware, software, and services for all of your efforts. They may also provide vendor management to ensure your vendors are performing as stated in the contract and deliver exactly what you need.

- **Finances**: The Finance team is responsible for monitoring budget and will typically require business justification or a business case before you can receive funding for your projects. Finance can be a strong ally in helping you get your business case approved through the proper channels, such as business partners and executives. Without Finance, you will likely not receive funding.

- **Facilities**: You may engage Facilities for asset tracking or the convergence of IT and physical security systems. You may also need their assistance in building out specialized rooms for security usage, such as labs, security operations centers, and/or team rooms.

- **Compliance**: Complying with government and industry regulations is a major concern for security departments because many organizations in the public and regulated industries such as utilities, finance, and healthcare are required to demonstrate adequate security policies are in place and prove compliance such as PCI, HIPAA, and so on. Compliance can help you interpret regulations, and often this team will lead and/or participate in audits to ensure your organization meets compliance requirements.

- **Legal counsel**: Because regulatory compliance is part of greater information management and governance control, many organizations have started seeking the advise of legal counsel to help them make the right business decisions.

You may need to engage Human Resources (HR) for identity and access-management-related efforts because often most databases obtain information from the employment or HR systems. After an employee is activated, he or she has access, but access is terminated when the employee is deactivated. HR will also be instrumental in interpreting employment law and employee enforcement against security policies.

We talked about engaging the Help Desk or Call Center as part of your data encryption strategy and the roll-out of forced encryption on all outbound e-mail containing sensitive data. Most security efforts that affect or could potentially affect users will need to partner with the Help Desk because this team is generally the first line of defense to support for end users.

It's always a good idea to get Communications involved to help you craft messages about your security initiatives. This team can partner with you and help you sell the value of your initiatives to your stakeholders. They are also likely to understand how to effectively distribute your messaging so that you get the highest degree of penetration throughout the organization.

SIPOC Stakeholder Identification Tool

Phase I

- SIPOC stands for
  - (S) Suppliers
  - (I) Inputs
  - (P) Process
  - (O) Outputs
  - (C) Customers
- SIPOC provides a template
  - For defining and mapping a process and allows for identification of end-to-end process touch points
  - Will ensure greater success in identifying all stakeholders that could be impacted or have a vested interest in your efforts

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 69

The acronym SIPOC (Suppliers, Inputs, Processes, Outputs, and Customers) is pronounced "sigh-pock." A SIPOC is a high-caliber method of showing how current processes actually work. It breaks down exactly what needs to be done and how it needs to be done. Teams use it to identify all relevant elements of a project before work begins, and it helps to visualize a complex project in a simple table format. This model is particularly useful in helping you identify stakeholders that may not have been previously visible and/or considered.

The SIPOC model can be traced to the teaching of W. Edwards Deming and his lectures to post-war Japanese business leaders in 1950. He introduced Japan and ultimately the world to the idea of systems thinking. In Deming's lectures, he used simple line flow diagrams to illustrate his ideas regarding the need for taking a systems perspective. It was that diagram that later influenced Peter R. Scholtes (a Deming protégé) to create what has become known as the SIPOC model, and is now widely known and used throughout the business process community. Scholtes fully describes this in his book *The Leader's Handbook: Making Things Happen, Getting Things Done,* a guide to inspiring your people and managing the daily workflow.

For your security team, using the SIPOC template for defining and mapping a process allows for identification of end-to-end process touch points. This method will ensure greater success in identifying all stakeholders that would be affected by a proposed change and will often help you identify those that would not have been typically considered.

SIPOC Matrix

Phase I

- Enables you to comprehensively identify and document all stakeholders for your initiative
  - By considering Inputs, Processes, and Outputs
  - Which are provided by Suppliers to Customers

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 70

A SIPOC may also be used as a collaboration tool with your stakeholders to arrive at a consensus on the process and requirements before progressing further in your strategy. It can enhance communication cross-functionally, and it helps your organization and the company as a whole better understand what you are implementing.

Suppliers (S) are those people and/or groups who provide inputs; *they are regarded as Stakeholders*. Please note: These are not "suppliers," as in vendors, but those who provide input into your process. They may be internal and/or external to your organization.

Inputs (I) are the key requirements needed for the process to work. The inputs should represent information and/or materials the suppliers provide to you.

The Process (P) is a defined series of activities. Keep this high level and simple. Ideally, this should contain between five and eight steps.

The Outputs (O) are tangible results of the process steps. The outputs can be used as discussion points with customers to validate and ensure your delivery is in alignment with your customers' expectations.

Customers (C) receive or use the outputs. Your customers are recipients or users of the outputs produced at every step in the process. *They are regarded as stakeholders* and may be internal and/or external to your organization.

There are some potential challenges to keep in mind: Processes may not be adequately or completely documented, and/or you may have several processes that need to be factored into your overall strategy.

If this is a challenge you are facing, remember to keep this activity high level and include between five and eight steps of the process. Documenting this process will be a team activity and should involve brainstorming to find and/or determine the hard to see details. Doing research on best practices and using these as your guidelines, in addition to brainstorming, will be tremendously helpful. Remember, this method is used to comprehensively identify and document all stakeholders for your initiatives.

SIPOC Case Scenario Office365

Phase 1

- The CIO of your company is under pressure to reduce costs of the e-mail infrastructure
  - Including e-mail, calendar, document storage, messaging
- She has asked your boss, the CISO, to help get the migration to Office365 completed
  - As a result, you now have to help get the project deployed in addition to doing a security and risk review
- You quickly realize that it's not a technical limitation but one of perception and comfort with the cloud
  - What do you do?

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 72

The CIO, Sherry Davis, has been at your company for a little over four months now. In that short amount of time, she has gained significant influence over most of the organization, including several senior executives. You heard Ms. Davis speak at the last town hall, and you thought to yourself, "This woman has raw intelligence and plenty of charisma; it's not a wonder she's made such an impact on the organization in such a short period of time." She certainly seems to be the kind of leader that not only thinks differently but also acts differently. This thinking was further confirmed when she called a meeting with your boss Barry McKnight, the CISO, to explain she was under pressure to reduce costs of the e-mail infrastructure. Ms. Davis wanted to do a wholesale migration to Office365 including e-mail, calendaring, document storage, and messaging in the next four months. She reaffirmed her confidence in Barry's ability to make this happen as she explained how she had successfully done this in her previous company. She concluded the meeting with enlisting Barry's help to get the migration completed.

After the meeting, Barry calls you into his office, and the two of you discuss the CIO-sponsored migration effort. Certainly, the two of you realize that over the past decade, cloud services have become one of the most defining buzzword technologies in IT, and you both feel as though it's a a risky move. More importantly, you are both aware the cloud is a new concept for your organization, and migration to Office365 would be the first cloud installation of any magnitude. The two of you quickly realize it's not a technical limitation with this Office365 migration, but one of organizational perception and comfort with the cloud. You both recognize you will have to manage and overcome a level of anxiety related to mistrust and fear of the unknown with the cloud.

Office365 Next Steps

Phase 1

- Need to identify all stakeholders
  - To ensure that you have the support and backing of key influencers
- This can be accomplished by following the step-by-step process to complete the SIPOC matrix
  - Helps map all the key players in your organization

Barry was involved in a previous security initiative gone bad. It was the implementation of a case management system for eDiscovery and Forensics that was shut down by Legal one week before go-live. He and his team missed the opportunity to engage Legal and others as key influencers that would provide the support and backing he needed to successfully implement this much-needed technology.

The Legal team had their own ideas about how cases should be managed in the organization, what system should be used, and who should manage the process. In addition, Finance didn't want to fund any unnecessary expenditures. Barry didn't want to make the same mistakes this time. He knew he had to do something different for this Office365 migration and deliver as the CIO had requested.

Barry recalled a recent Leadership training class he attended, where the importance of developing a Stakeholder Management Strategy was reinforced. He knew this would be the key to a successful migration he'd been tasked with delivering.

Step 1: Identify Key Process Steps

Phase 1

- List high-level process steps
  - Which are required to deploy Office365

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
		Define requirements		
		Design		
		Procure		
		Build & Deploy		
		Manage the solution		

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 74

We will walk you through the steps to complete a SIPOC over the next few slides.

The first step in completing your SIPOC is to list high-level process steps that are required to deploy your product. As a reminder, the Process (P) is a defined series of activities. Keep this description high level and simple. Ideally, it should contain between five and eight steps. In the case scenario of Office365, we have provided the following as an example:

- **Define requirements:** To successfully deploy a Software as a Service (SaaS) offering, you must have clearly defined business requirements, objectives, and timelines. You need to address the questions of how the application should be designed to run, how it will be accessed, where the users of the application are located when accessing, and whether the SaaS offering will meet your company's scalability needs.

- **Design:** You will need to design the solution with a clear understanding of the application and the service offering. The next step for the team is to ensure the design integrates with the organization's existing infrastructure. For traditional projects, this can include creating physical and logical solution designs for infrastructure components, including things like network components and connectivity; security; hardware such as system hardware; storage and backup; monitoring tools; and system management tools.

- **Procure:** After the solution has been designed, you will need to procure the solution components that meet scalability and business requirements, in addition to services to meet uptime commitments.

- **Build & Deploy:** Normally, network equipment is racked, configured, and tested in this phase. For a SaaS-based deployment of Office365, this will include configurations to the central Active Directory (AD) infrastructure, for example.

- **Manage the solution:** When your infrastructure is in place and all components are working together, ongoing success will result from diligent management. Maintenance tasks should be produced for every device in the infrastructure, and system logs should be reviewed for error and warning messages. Response scenarios are created and updated as needed.

As you can see, each process is complex by nature, but for the purposes of the SIPOC, you want to keep it high level and simple.

Step 2: Identify the Outputs

Phase I

- For each Process step, identify the Outputs

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
		Define requirements	Use cases Project plans	
		Design	Technical architecture Technical reqs	
		Procure	Executed contracts	
		Build & Deploy	Migration plan Running system	
		Manage the solution	Maintenance plan	

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 76

As a reminder, the Outputs (O) are tangible results of the process steps. The outputs can be used as discussion points with customers to validate and ensure your delivery is in alignment with your customers' expectations.

The output to the process step "Define requirements" is generally use cases and project plans. A use case is a list of steps that describe the interactions between a role/actor and a system and how it will work to achieve a goal—more specifically, your stakeholders' goals. Use cases are an important requirement technique widely used in modern software engineering since their formal introduction by Ivar Jacobson in 1992 through his book *Object-Oriented Software Engineering: A Use Case Driven Approach*. You can read more about it by visiting his website at http://www.ivarjacobson.com/default.aspx. A project plan is used to document project scope, schedules, and tasks. Among other things, a project plan can be used to facilitate communication with your stakeholders. Project Management Institute (PMI) is a globally recognized organization that has a wealth of information on project management expertise, resources, and so on. You can read more about this organization at www.pmi.org.

The output to the process step "Design" is the technical architecture that defines and specifies the interfaces, parameters, and protocols used by product architecture and system architecture layers. The output also includes the technical requirements, which are a set of statements that identify a system's functions, characteristics, and/or constraints. These outputs are generated from physical and logical solution designs to accommodate scalable architecture for hosting the SaaS platform and are based on the applications.

The output to the process step "Procure" is executed contract(s) signed by all parties that includes various components stipulating what products and/or services you require to meet your commitments. The terms and conditions within the contract will specify scalability and business requirements for uptime commitments and include various terms and conditions for hardware, software, and service specifications, and legal terms and conditions to protect your company.

The output to the process step "Build & Deploy" is the Migration plan, which maps existing capabilities to a new infrastructure; it is also the process by which you will assess the current state and architected state of your infrastructure. It will address how it will happen for tasks such as moving information and/or functionality and consolidating information and/or functionality. Your company's technology and information life cycles need to be factored into this plan. The other output for this process step is a "Running system." Obviously, many additional steps need to occur between the Migration plan and deploying a running system such as QA and User Acceptance testing.

The output to the process step "Manage the solution" is a documented Maintenance plan that includes maintenance schedules, system logs that can be reviewed and completed, and response scenarios that can be tested and updated as necessary.

Step 3: Identify the Customers

Phase I

- Identify the Customers that will receive the Outputs

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
		Define requirements	Use cases Project plans	Business owner Technical teams Project managers Finance, Comms
		Design	Technical architecture Technical reqs	Engineering team Security team Operations team
		Procure	Executed contracts	Business owner Legal and Vendor
		Build & Deploy	Migration plan Running system	Business owner Technical teams Vendor, Leadership Help Desk
		Manage the solution	Maintenance plan	Business owner Leadership

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 78

As a reminder, Customers (C) receive or use the outputs. Your customers are recipients or users of the outputs produced at every step in the process. They are *regarded as stakeholders* and may be internal and/or external to your organization.

The customers that will receive the outputs of the use cases and project plans will be the business owners, who will need to sign off on the use cases to ensure requirements are met; technical teams that will be building, deploying, and running your SaaS; project managers; and Finance. Please note: Finance may be interested in only some aspects of both of these outputs and generally for purposes of helping to build your business case. You will also want to engage the Communications team at this point to begin building your communication plan to adequately socialize with your stakeholders as your effort progresses.

The customers that will receive the outputs of the technical architecture and technical requirements are the Engineering team, which is accountable for the build function; the Security team; and Operations team, which is responsible for the overall deployment effort.

The customers that will receive the outputs of the executed contract will be the business owners, who will keep records and manage the contract; the Legal team, which generally will maintain original contracts on file; and the vendors with whom the contract is signed, who will need a copy of the fully executed agreement.

The customers that will receive the outputs of the migration plan and a running system will be the business owners, who will be receiving the benefit of the SaaS, and technical teams and vendors, because they are responsible for migration. Leadership will need to be advised of your migration plan and when the system is fully deployed, and you will want to communicate success stories. You will also want to get the Help Desk team involved and provide them with any artifacts and/or training they will need to support end users.

The customers that will receive the maintenance plan output will be business owners and leaders such as the CEO, CFO, CIO, and CISO. Performance metrics to track progress against the maintenance plan will also be included.

Step 4: Identify the Inputs

Phase I

- Identify the required Inputs for each Process step

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
	Requirements	Define requirements	Use cases Project plans	Business owner Technical teams Project managers Finance, Comms
	Approved use cases Approved project plans	Design	Technical architecture Technical reqs	Engineering team Security team Operations team
	SLAs, Budget, HW & SW reqs	Procure	Executed contracts	Business owner Legal and Vendor
	Technical reqs System configuration	Build & Deploy	Migration plan Running system	Business owner Technical teams Vendor, Leadership Help Desk
	SLAs Business uptime reqs	Manage the solution	Maintenance plan	Business owner Leadership

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 79

As a reminder, Inputs (I) are the key requirements needed for the process to work. The inputs should represent information and/or materials the suppliers provide to you.

For the process step "Define Requirements," the supplier must provide you with requirements as inputs. Requirements are a statement or a list of statements that a product or service must do or a quality it must have. You may have multiple types of requirements, including but not limited to business, security, legal, and/or regulatory.

For the process step "Design," the supplier must provide you with the approved use cases and approved project plans as inputs. These items as inputs will ensure everyone is on the same page and expectations are in alignment.

For the process step "Procure," the supplier must provide you with desired Service Level Agreements (SLAs), budget information, and hardware and software requirements. The contract must include numerous terms and conditions to be in compliance with your organization and groups, such as security that may have the right to audit and test security controls in a vendor environment, and legal terms and conditions such as the right to terminate agreement with or without cause, and remediation terms if a vendor is found in default of agreement and procurement, which may include payment and receiving terms.

For the process step "Build & Deploy," the supplier must provide you with technical requirements and system configuration parameters.

For the process step "Manage the solution," the supplier must provide you with the desired SLAs and business uptime requirements so you can build these expectations into the maintenance plan.

Step 5: Identify the Suppliers

Phase I

- Identify the Suppliers of the Inputs

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
Business owner, Legal, Security, Regulators	Requirements	Define requirements	Business case Use cases Project plans	Business owner Technical teams Project managers Finance, Comms
Business Operations team	Approved use cases Approved project plans	Design	Technical architecture Technical reqs	Engineering team Security team Operations team
Business owner, Legal, Security, Vendors	SLAs, Budget, HW & SW reqs	Procure	Executed contracts	Business owner Legal and Vendor
Vendors, Architects, Engineers	Technical reqs System configuration	Build & Deploy	Migration plan Running system	Business owner Technical teams Vendor, Leadership Help Desk
Technical teams, Vendors	SLAs Business uptime reqs	Manage the solution	Maintenance plan	Business owner Leadership

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 80

As a reminder, Suppliers (S) are those people and/or groups who provide inputs; *they are regarded as Stakeholders*. Please note: These are not "suppliers" as in vendors, but those who provide input into your process, and they may be internal and/or external to your organization.

Suppliers to the process step "Define requirements" are generally the business owner and Legal, Security, and Regulators, who will provide their requirements. Regulators will often be a big influence in what can and cannot be done and/or what controls need to be considered, especially in heavily regulated environments such as Finance, Health Care, Transportation, Power, and so on.

Suppliers to the process step "Design" are generally the business and Operations team, who will provide approved use cases and approved project plans. Teams often go wrong and projects fail when considering the business for input. The product and/or services have to meet business expectations, so it's imperative they are factored into this process step. This step is necessary to ensure that all parties approved, and by doing this, you will ensure that what is delivered is what was agreed to.

Suppliers to the process step "Procure" are generally the business owner, Legal and Security departments, vendors, and the technical teams, who will provide SLAs, budget, hardware, and software requirements.

Suppliers to the process step "Build & Deploy" are generally vendors, architects, and engineers, who deliver technical requirements and system configuration inputs to the process.

Suppliers to the process step "Manage Solutions" are generally the technical teams and vendors, who will provide the SLAs and business requirement uptimes as input to this process.

Stakeholder Identification Complete

Phase I

- These stakeholders will need to be managed throughout your project

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
Business owner, Legal, Security, Regulators	Requirements	Define requirements	Business case Use cases Project plans	Business owner Technical teams Project managers Finance, Comms
Business Operations team	Approved use cases Approved project plans	Design	Technical architecture Technical reqs	Engineering team Security team Operations team
Business owner, Legal, Security, Vendors	SLA's, Budget HW & SW reqs	Procure	Executed contracts	Business owner Legal and Vendor
Vendors, Architects, Engineers	Solution Designs, equipment configuration	Build & Deploy	Migration plan Running system	Business owner Technical teams Vendor, Leadership Help Desk
Technical teams, Vendors	SLAs Business uptime reqs	Manage the solution	Maintenance plan	Business owner Leadership

Now that we have the SIPOC completed for the CIO-sponsored Office365 migration effort, you can see that key stakeholders have been identified in the (S) Suppliers and the (C) Customers columns.

Many of these stakeholders reach well beyond those people and/or groups that would typically be considered for a standard technology deployment. By using the SIPOC template for identification of end-to-end process touch points, you and your boss, Barry McKnight, the CISO, have greater visibility into the overall impact your efforts will have on the organization. By having greater visibility, you will be better positioned to proactively address your stakeholders' motivations and concerns, which we will discuss in more detail in the upcoming slides.

Understand Stakeholder Motivations

Phase 2

- Stakeholders are both organizations and people
  - Identify the specific individuals within each group
  - They may have different views of your project
  - So you need to tailor your approach
- Follow a three-step process to manage stakeholders:
  - Understand motivations
  - Map power and interest
  - Prioritize relationships

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 82

Now that you have identified your stakeholders, and you know that stakeholders are both organizations and people, you need to understand their motivations. A mistake that teams often make is ignoring the motivations of their stakeholders or making assumptions about what we believe their motives are. It is more than likely your stakeholders will have a different view of your project than you do.

Let's think for a moment about the stakeholders identified in the Office365 migration effort. How would motives vary between business owners, Legal, Security, Regulators, the Operations team, vendors, technical teams, architects, engineers, project managers, help desk, communication team, and leadership?

It is highly likely that your stakeholders will have different views of your project. In addition, office politics and/or personal interests will likely be key factors in distilling true stakeholder motivation; therefore, the approach for each group and/or individual will need to be tailored to support the varying motivations of each of your stakeholders because they can and will affect your efforts. Many of them will have the power to veto your project, as in the example of case management system effort that CISO Barry McKnight was trying to implement when Legal and Finance vetoed his initiative. Some of your stakeholders will voice their opinions, and as you well know, some people have very strong voices in an organization, so your project may be delayed and/or derailed.

resulting in a breach of 4.6 million usernames and phone numbers. As part of the settlement, Snapchat agreed to implement a comprehensive privacy program that will be monitored by an independent privacy professional for the next 20 years.[3]

References

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

[2] http://www.zdnet.com/article/hacker-leaks-vmware-esx-kernel-source-code-online/

[3] https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

Political – Google (Alphabet) Example

Political	Economic
• Anti-trust action in response to being viewed as a monopoly • Increased privacy and data regulation in response to excessive use of personal data; increased government data requests • Target of nation states due to wealth of info about customers • Inability to operate in lucrative markets • Entering heavily regulated fields like telecom and automobiles • Incumbents engage in legal action or espionage	
Social	**Technological**

Google's dominance in web search and mobile operating systems has created a belief, particularly in Europe, that it has monopoly powers, which has led to some antirust actions. The company's market success has resulted in the collection of vast amounts of data about customers that could also result in increased privacy and data regulations. Interestingly, because of this vast amount of information, Google often receives requests from various governments to turn over data such as e-mail communications that could aid in national security-related investigations. Others, instead of asking for this information through established channels, attempt to steal it directly from Google or its users. For example, Google was hacked in an attempt to steal information about Chinese dissidents. These types of activities, along with other factors, have resulted in Google withdrawing from the lucrative Chinese market. As Google (now Alphabet) seeks to broaden its product and revenue base, it is entering new markets like telecommunications and the auto industry that are heavily regulated. These markets expose the company to increased business risk, such as legal action from entrenched competitors and even espionage in attempts to determine Google's product plans.

Economic

- Examines the economic issues
  - That play a role in the company's success
- Common factors include
  - Consumer confidence
    - Consumer confidence index
    - Inflation rates
    - Unemployment rate
  - Interest and exchange rates
    - Credit rating and availability
  - Policies
    - Taxation and economic policies
    - Government spending
  - Economic stability
    - Economic growth
    - Business cycles
    - Disposable income
    - Commodity shortages
    - Potential for disruption of supply
    - Profit and growth trends
    - Investment levels
    - Market competition

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 102

Economic factors looks at the overall health of the economy and how these factors influence companies, organizations, and their decisions. These forces include items like inflation, interest and exchange rates, the unemployment rate, economic policies, and economic stability. Economic factors have a high influence on business regardless of the industry.

Inflation impacts businesses by increasing expenses such as rent or lease, utilities, and cost of materials used in production. A typical response to increased expenses is increased prices on products and services by the business to maintain profits. In addition to inflation, consumer confidence impacts business. Confident consumers have a tendency to spend more money than low-confidence consumers.

Many businesses rely on loans from banks or other financial institutions for financing, and interest rates impact business expense for companies with debt. High interest rates will also reduce consumer spending because people are less willing to take out loans on vehicles and homes, for example. Exchange rates also play an important role for companies that import or export goods because depreciated exchange rates will make export less expensive, and vice versa, appreciated exchange rates will be more expensive. Credit ratings affect debt obligation and security, preferred stock, and insurance companies.

The economy tends to follow a business cycle of economic booms followed by periods of stagnation or decline. During boom periods, jobs tend to be plentiful because companies need workers to keep up with demand. When unemployment is low, consumer spending tends to be high because most people have income to spend, which helps drive growth. When unemployment is high, consumer spending tends to be low because unemployed people don't have excess income to spend.

Governments spends trillions of dollars per year through direct spending, which will help businesses such as construction companies, which may be contracted to build schools or libraries; engineering companies, which are contracted to build bridges and roads; and defense companies, which specialize in military systems and any fluctuation in spending by the government would have an impact in these areas. When tax rates increase for businesses, many companies respond by increasing prices on goods and services. Economic policies also affect wages. For example, an increase to minimum wage would benefit workers by providing them more money, but it may be challenging for businesses to absorb the increased labor costs.

There are advantages to having a stable economy, such as increased productivity, improved efficiencies, and low unemployment. Common signs of instability in the economy would be recession, rising inflation, and volatile currency exchange rates, and we know this causes a decline in consumer confidence, stunted economic growth, and reduced international investments.

Economic – Examples

- Business cycles
  - Annual tax filing deadline
  - Risk: tax return fraud
- Economic downturn
  - Recession leading to layoffs
  - Risk: disgruntled employees and corresponding malicious activity
- Stock market manipulation
  - Associated Press (AP) Twitter account hacked
  - Risk: economic panic and insider trading

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 104

The following are examples of organizations being affected by economic factors.

Every year, employees receive tax documents (for example, W-2 forms) that they use to file income tax returns. Attackers have started sending targeted spear phishing attacks to HR and payroll administrators while posing as company executives to harvest large numbers of W-2 forms. They may have simple messages such as "I want you to send me the list of W-2 copies of employee wage and tax statements for 2015; I need them in PDF file type. You can send it as an attachment. Kindly prepare the lists and email them to me asap."[1] By collecting this information, attackers then file fraudulent tax returns with the Internal Revenue Service (IRS) and state governments requesting tax refunds that are then sent to attacker-controlled mailing addresses or accounts.

In poor economic times, customer confidence can be low. For organizations facing a downturn, layoffs might be necessary. The risk of unemployment is a major stress for many people and can lead to abnormal behavior. In these times, it's important to be cognizant of disgruntled employees conducting malicious activity to harm the organization.

In 2013, the Twitter account of the Associated Press (AP) was hacked and sent the following message to its, at the time, two million followers: "Breaking: Two Explosions in the White House and Barack Obama is injured." In just three minutes, this false tweet had caused the stock market to crash by $136 billion. Although this panic lasted only three minutes, the damage that could be done by a 140-character message was alarming.

References

[1] https://www.irs.gov/uac/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s

[2] https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

Economic – Google (Alphabet) Example

Political	Economic
• Anti-trust action in response to being viewed as a monopoly • Increased privacy and data regulation in response to excessive use of personal data; increased government data requests • Target of nation states due to wealth of info about customers • Inability to operate in lucrative markets • Entering heavily regulated fields like telecom and automobiles • Incumbents engage in legal action or espionage	• Higher taxes in response to large amount of cash overseas • Large cash balances means the company is vulnerable to inflation; drop in currency results in drop in company value • Vulnerable to exchange rate fluctuations • Majority of revenue from ads and existing web properties • Regular acquisitions into new business ventures • Divesting of unfavorable assets
Social	**Technological**

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 105

Google has a large amount of cash overseas to avoid paying U.S. taxes. Bringing this money back home would result in large tax bills. As a result, many such companies are lobbying for "tax holidays" to avoid large tax bills. These large cash balances also leave Google vulnerable to inflation. A devaluation of certain currencies can result in a drop in company value. Varying exchange rates are also a concern. For example, a weaker Chinese yuan means that products that do not have prices updated frequently are effectively cheaper to buy.

At its core, Google is still an advertising business. It makes money by identifying a user's intent and interest in particular goods or services and placing well-timed ads as this user is searching for said products. One reason Google reorganized to become Alphabet was to try to separate its core search/advertising business from the numerous new business ventures it is pursuing. These include self-driving cars, biotechnology, and telecommunications. At the same time, Google has divested itself of unfavorable assets, including most of Motorola.

Social

- Demographic and cultural aspects of the company's market
  - Examine consumer needs to determine what motivates them to purchase
- Main issues include
  - Customer demographics
    - Age, gender, race, family size, etc.
    - Population shifts
    - Occupations and earning capacity
    - Diversity
  - Cultural limitations
    - Cultures and religions
  - Lifestyle attitudes
    - Lifestyle changes
    - Living standards
    - Work week
  - Education
    - Education trends and standards
    - Skilled workforce availability
    - Career trends

Social factors look at cultural aspects of the market and how they affect the demand for a company's products and/or services; they also examine consumer needs and determine what incents them to make purchases. Common forces addressed in this section include customer demographics, cultural limitations, lifestyle attitude, and education.

Many companies identify their key customers through various demographic traits such as age, gender, race, family size, and so on, and based on this, build their advertisements and promotions. For example, younger people are more likely to buy high-tech products than an older age group, and certain buying groups have more buying power than other groups. For example, the baby boomers are the single largest population segment. Business needs to be agile and responsive to population shifts and lifestyle changes.

Cultural limitations are important for a company to understand. For instance, when doing business with an affiliate from another country, you must consider the cultural differences such as language, body language, dress, religion, and traditions. You wouldn't want to schedule meetings during religious observations. Political influences past and present can affect the way a person or company does business. Some cultures have a strong sense of nationalism and government pride and may have a preference to doing business with like-minded companies.

Lifestyle attitudes include, for example, lifestyle changes, living standards and work week, quality and availability of employment, class disparity, quality and affordability of housing, hours of work required to purchase necessities, and access to healthcare. This category is often used to compare between states and countries, such as the lifestyle of the United States versus England or Utah versus New York.

When labor supply increases, there is more pressure on wage rate. If the demand for labor does not keep up with the supply of labor, wage rate will be depressed. This is harmful for employees in industries where higher education and training are not required. Industries with higher education and training requirements generally pay higher wages.

Social – Examples

- David Carroll
  - Canadian musician whose guitar was broken on a United Airlines flight
  - Risk: negative public perception, brand damage, lack of trust
- Global expansion
  - Hiring in other countries
  - Risk: onboarding malicious individuals
- Executive peer pressure
  - Latest mobile device support
  - Risk: unprepared for technology changes, unhappy users

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 107

The following are examples of organizations being affected by social factors.

Canadian musician David Carroll took a United Airlines flight and discovered that his $3,500 guitar was severely damaged in transit. After nine months of talking with indifferent United employees trying to seek reimbursement, he grew frustrated and created a video called "United Breaks Guitars," which became an Internet hit. United quickly reached out to apologize and now has teams monitoring social media to quickly respond to customer complaints. David Carroll is now in great demand as a speaker on effective customer service.[1]

When a company grows globally, it must carefully consider its hiring practices. Do the same security controls, policies, and procedures afford the same protection in this new environment? Are there different assurances required to verify identity and conduct appropriate background checks? What is the threat level in the country overall? Onboarding a malicious individual that can harm the organization or damage its reputation can have severe consequences when social factors are not appropriately considered.

Another social factor is peer pressure, especially executive peer pressure. In the time that the Blackberry was still the predominant mobile device used at various enterprises, many organizations struggled with the increasing use of iPhones that did not have equivalent security controls. Often, executives were clamoring for these new devices. This pressure left many organizations scrambling to support this new technology while trying to maintain the same level of control provided by other platforms.

Reference

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

Social – Google (Alphabet) Example

Political	Economic
• Anti-trust action in response to being viewed as a monopoly • Increased privacy and data regulation in response to excessive use of personal data; increased government data requests • Target of nation states due to wealth of info about customers • Inability to operate in lucrative markets • Entering heavily regulated fields like telecom and automobiles • Incumbents engage in legal action or espionage	• Higher taxes in response to large amount of cash overseas • Large cash balances means the company is vulnerable to inflation; drop in currency results in drop in company value • Vulnerable to exchange rate fluctuations • Majority of revenue from ads and existing web properties • Regular acquisitions into new business ventures • Divesting of unfavorable assets
Social	**Technological**
• Change in computing preferences; less laptop and desktop use • Increased use of social media as an alternative to search • Distrust of Google (e.g., "Don't be evil") • Concerns about energy use and global warming; data centers that consume large amounts of electricity	

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 108

When Google was first created, the web browser was the primary mechanism for accessing the Internet. This was done through traditional laptop and desktop computers. Now, though, mobile devices have changed the way people communicate and share information. For many, social media is the gateway to the web, and Amazon is the gateway for online shopping. These changing usage patterns are a threat to Google's traditional approach.

Google's motto is "Don't be evil." But, as the company has grown, this motto has become an ironic slogan of the market power that Google holds. As a result, there is a certain distrust of Google. Therefore, some people use alternative search engines, like DuckDuckGo, that emphasize protecting users' privacy. Apple has also made privacy and security features a core part of its products because its business model does not require access to personal information to improve search results.

Finally, many large technology companies with large data centers and huge energy footprints can be scrutinized for excessive energy use in relation to overall global warming trends.

Technological

- How technology can
  - Impact the introduction of a product or service into a market
- The factors addressed in this section are
  - Technological advancement
    - Rate new discoveries
    - Manufacturing advances
    - New industries
    - Automated processes
  - Lifecycle of technology
    - Rate of technology change
    - Rate of obsolescence
    - Waste removal/recycling
  - Technology innovation
    - Internet, cloud, mobile, IoT

SANS

Technological factors include how technology can either positively or negatively impact a business and the products and/or services they provide. Common forces addressed in this section include technology advancements, lifecycle of technologies, and technology innovation.

The impact technology advancements have over daily life is increasing and expanding. As technology continues to evolve, businesses will also need to evolve to keep a competitive edge.

Technology lowers the cost of production and provides new products; it increases both productivity and efficiencies for businesses. The entire supply chain ecosystem encompassing equipment, manufacturing, distributors, and retailers is undergoing business transformation in response to changing customer expectations, time-to-market demands, and intense global competition that is being dictated by the Internet and mobile economies. Manufacturers must accelerate production cycles, and distributors must shorten delivery times, and much of this is accomplished by automated processes in industry.

Lifecycles of technologies in companies generally always have some impact that should be considered. For example, new technology is expected to be integrated with legacy systems. The environmental factor related to waste removal and recycling will also have an impact on companies because there may be regulations and/or company policies that you will need to adhere to. With technology, you always need to consider sensitive data being wiped from things like servers, hard drives, and even printers to ensure your company's sensitive information remains secure.

The Internet has allowed companies to find new ways of lowering operational costs on production of goods and services. Some companies may elect to outsource and/or take some of their functions offshore in the hope of driving innovation or lower labor cost. Some of the typical services that are taken off-shore or outsourced are customer support, development, programming, manufacturing, data entry, research and development, creative services, and engineering.

Technological – Examples

- Connected medical devices
  - Vice President Cheney disabled wireless capabilities in pacemaker
  - Risk: death
- Industrial Control Systems (ICS)
  - Ukrainian power grid attack
  - Risk: power outage, decreased confidence in government
- Food and agriculture
  - Attacks on smart farming technology
  - Risk: crop and pricing manipulation, data theft or destruction

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 110

The following are examples of people or organizations being affected by technological factors.

Dick Cheney, former vice president of the United States, had the wireless capabilities in his pacemaker disabled due to concern that it could be hacked in an assassination attempt. His doctor stated, "It seemed to me to be a bad idea for the vice president to have a device that maybe somebody on a rope line or in the next hotel room or downstairs might be able to get into."[1]

In December 2015, Ukrainian power distribution centers were hacked, leaving 225,000 Ukrainian residents without power.[2] The attack was carefully planned. Once the attack began, backup power supplies were disabled, and operator workstations were wiped using the KillDisk malware, making it harder to respond to the attack. Attackers also overwrote the firmware on substation serial-to-Ethernet convertors, making them inoperable and unable to be controlled remotely. This meant that to get power back up, operations had to control breakers manually, reducing response time. Attackers even went so far as to conduct a telephone denial-of-service attack, flooding the call center with thousands of bogus phone calls and preventing legitimate callers from reaching the power companies. The telephone denial-of-service attack, in particular, could be evidence that a key motivation in the attack was to weaken the public's trust in power companies and the Ukrainian government.

Precision agriculture, or smart farming, includes the use of sensors to monitor crop growth to provide insight on how to farm more efficiently. These sensors provide data used to track and anticipate crop availability and pricing. With access to such data, attackers could exploit agriculture resources and market trends, causing farmers to take less optimal actions, such as planting the wrong crops or harvesting at less optimal times. Additionally, hacktivists could destroy or alter data about the use of pesticides or genetically modified organisms (GMOs) in protest.[3]

References

[1] https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/

[2] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[3] https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf

Technological – Google (Alphabet) Example

Political
- Anti-trust action in response to being viewed as a monopoly
- Increased privacy and data regulation in response to excessive use of personal data; increased government data requests
- Target of nation states due to wealth of info about customers
- Inability to operate in lucrative markets
- Entering heavily regulated fields like telecom and automobiles
- Incumbents engage in legal action or espionage

Economic
- Higher taxes in response to large amount of cash overseas
- Large cash balances means the company is vulnerable to inflation; drop in currency results in drop in company value
- Vulnerable to exchange rate fluctuations
- Majority of revenue from ads and existing web properties
- Regular acquisitions into new business ventures
- Divesting of unfavorable assets

Social
- Change in computing preferences; less laptop and desktop use
- Increased use of social media as an alternative to search
- Distrust of Google (e.g., "Don't be evil")
- Concerns about energy use and global warming; data centers that consume large amounts of electricity

Technological
- Alternatives to search that limit access and visibility to data
  - Mobile: apps are self-contained allowing users to bypass search; other mobile platforms provide alternatives to search
  - Social media: new "front door" to the Internet
  - Messaging: Facebook Messenger, WhatsApp, WeChat as new platforms for commerce
  - Voice: Apple Siri, Google Now, Microsoft Cortana
- New technology ventures under the Alphabet umbrella

Google's mission is to "Organize the world's information and make it universally accessible and useful." As a result, it wants access to as much data as possible. When the Internet was primarily accessed via the web, Google was able to collect data largely unfettered. Now, though, Google faces a risk that alternatives to search will limit access and visibility to the data it requires. Mobile apps are self-contained and allow users to bypass search entirely. For example, users can shop in individual apps and search restaurants in Yelp. Additionally, competing mobile platforms provide their own alternatives to search, such as Apple's Siri on iOS devices; it does not require users to search via Google (although Google is still the default search engine for other features in iOS). Additionally, many people throughout the world use social media sites like Facebook as the "front door" to the Internet. Their Facebook feed helps keep them up-to-date, not only on what their friends are doing, but also on current events, local news, shopping, and more. This is one reason that Google has invested so heavily in its Google Now product: to help ensure that competing voice products do not squeeze Google out of the market for alternatives to search. Aside from search and its obvious competitors, Alphabet is also heavily investing in other cutting-edge technology ventures.

Exercise 1.3 – PEST and Security

Estimated Time: 20 Minutes

- Goal of this exercise
  - Identify items that security can provide to help the business respond to each of the PEST macro factors
- For each PEST quadrant:
  - Write down 2-3 things that security can do to address the issues on the previous slide
- Use the blank worksheet on the next slide
  - Note that some of the PEST items will not have an obvious information security response
  - Part of the thinking process is to understand larger organizational concerns and where security can assist

NOTE

Don't read the next section

It contains a debrief and potential exercise answers

The goal of this exercise is to identify items that security can provide to help the business respond to each of the PEST macro factors. It's important to note, however, that some of the PEST items will not have an obvious information security response. The exercise is intended to help you understand larger organizational concerns and the specific areas where security can potentially provide assistance.

PEST and Security Worksheet

Political	Economic
Social	**Technological**

Use this page as a worksheet for your ideas.

Political

Economic

Social

Technological

Exercise Debrief

Note that this section contains a debrief and potential exercise answers

This page intentionally left blank.

Exercise 1.3 – PEST and Security Debrief

Political	Economic
• Product security features to protect user data • User data transparency report for government requests • Recommended actions in response to regulatory and compliance requirements • Security intelligence and monitoring to identify espionage and insider threat	• Review of funds transfer processes • Protect online properties that are primary source of revenue (e.g., secure SDLC, pentesting, bug bounty program) • M&A security review for due diligence before purchase • Planning for divestitures and downsizing
Social	**Technological**
• Security initiatives to counter public distrust (e.g., Project Zero as counter-surveillance initiative) • Hosting security conferences and community events • Social media monitoring to identify issues, information disclosure, etc.	• Build in-house security technology vs. buying off-the-shelf solutions to limit supply chain risk • Provide secure standards for vendors • Improve security features in mobile, messaging, and voice products • Strict access control between various Alphabet ventures

The goal of the PEST analysis is to understand the macro forces that affect your business, articulate the cyber risk associated with some of these forces, and determine, when relevant, how security can support business goals.

As you think about the factors that affect Google (Alphabet) and extend this thought process to your own organization, it's important to keep in mind that security will not be able to provide responses for every threat that is identified in your PEST analysis. Stated another way, this debrief slide does not contain responses to every PEST factor that was identified earlier. Nor should it. Implementing information security controls and protections is just one response an organization can choose to implement to mitigate risk. That being said, this slide provides some potential things Google (Alphabet) can do to mitigate the risk associated with some of the PEST factors that were previously discussed.

Political

As Google receives increasing requests for information about users, it, like many other companies, has started publishing data transparency reports[1] that provide information such as the number of requests and the countries making such requests. This transparency helps Google in the court of public perception as it complies with various international laws. For groups that don't seek data in lawful ways (for example, attempting to hack users or Google itself), a number of product security features have been introduced. These include multistep authentication, summaries of account activity to identify suspicious logins, the capability to terminate all logged-in sessions, and end-to-end encryption. Such features make it harder for attackers to compromise end users directly. For more advanced attacks, Google can also share threat intelligence with other firms to identify malicious activity and conduct additional monitoring to identify espionage and insider threats seeking to steal intellectual property and sensitive data. Finally, increased privacy and data regulations mean that Google will have to provide customers assurance (for example, SOC 2, ISO 27000 certification) and meet compliance regulations (such as PCI, SOX).

Economic

Google still makes the majority of its revenue from online properties such as Search and Gmail. As a result, it is extremely important that these products remain secure and trustworthy. This means integrating security throughout the product development process with investments in items like secure SDLC practices, penetration testing, and bug bounty programs. With these large amounts of revenue, it would also be wise to review the funds transfer processes to mitigate business e-mail compromise, also known as CEO e-mail fraud, to prevent unauthorized transfers from being initiated via fraudulent emails. Identifying higher risk individuals and groups like the Treasury Department in the organization is also useful from a risk assessment and management perspective. As Alphabet continues to grow, providing security due diligence before any merger or acquisition activity could also help the firm negotiate risk discounts into the purchase price. On the flip side, divestitures need to be carefully considered to manage access, deprovisioning, and the threat of disgruntled employees.

Social

In the wake of previous hacking attempts such as Operation Aurora,[2] the Edward Snowden revelations, and widespread security vulnerabilities like Heartbleed, Google initiated a program called Project Zero, which is the name of the team of Google employees charged with finding previously unknown vulnerabilities (that is, zero-day exploits) in *any* software used by the company. This project is related to Google's counter-surveillance initiatives and can also be viewed as helping to counter some of the public distrust and skepticism in Google. Aside from such programs, Google can continue to build trust in the larger security community by hosting conferences and other community events. From a monitoring perspective, Google could also track issues in social media and other hacking forums to identify trends.

Technological

As other technologies such as mobile and social media grow, they have the potential to displace search and limit Google's access to data. As Google invests in new technology areas, it can improve and build new security features in mobile, messaging, and voice products so that they remain on par with technology from competitors. In addition to products for customers, Google also utilizes a large number of products in-house. Similar to other companies, risk is introduced in the supply chain and off-the-shelf products it may purchase. As part of a vendor risk management program, the company could provide security standards for vendors. It may also decide, given its wealth of internal engineering talent, to build versus buy security tools and capabilities to limit supply chain risk. As Alphabet grows and extends into new business areas, maintaining strict access control between different ventures may also become an important business requirement.

References

[1] https://www.google.com/transparencyreport/

[2] https://en.wikipedia.org/wiki/Operation_Aurora

In Summary

- PEST analysis
  - Is used to understand
    - What is driving business decisions
    - How market forces can affect business long term
  - Will help you have more meaningful dialogue with business leaders
    - Articulate cyber risk associated with macro forces
    - How security can support business goals

It is important to understand business goals to avoid disconnects between security and business leaders. In this section, we discussed the importance of understanding the market forces that affect your business, as these are the factors that are driving the strategic decisions.

Security leaders must create broad strategies that reach beyond the security organization and traditional security controls. When you have the full picture of what is driving business decisions for your organization, you can better understand how security can support business goals and, in turn, build a more cohesive, comprehensive strategy with the business in mind. Articulating the cyber risk associated with forces affecting the business and defining potential responses to these risks will enable you to have more meaningful and successful dialog with your 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 1

- Background
  - About This Course
  - Need for Strategic Planning
    - Exercise #1: Case Scenario
- Understand the Business
  - Vision & Mission
    - Exercise #2: Mission Statement
  - Stakeholder Management
  - PEST Analysis
    - Exercise #3: PEST
  - *Business Strategy*
- Understand the Threats
  - Threat Actors
    - Attack case studies
  - Asset Analysis
    - Exercise #4: Attacker Motivation
  - Threat Analysis
    - Exercise #5: Intrusion Kill Chain

This page intentionally left blank.

What Is a Business Model?

- Business model
  - Description of what your organization does
  - How you make money
  - How you deliver value at a reasonable cost
- Example business models
  - Direct sales
  - Franchise
  - Freemium
  - Subscription

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 120

A business model describes how your company or organization operates. It is the plan for how you will generate revenue and actually make a profit from that revenue. This is, of course, done by delivering something of value to your customers. When someone asks, "What is your business model?" he or she is really asking a combination of questions that encompass the following:

- Who are your customers?
- What problem do they have?
- How are you solving that problem?
- How will you find and retain customers?
- How do you generate revenue?
- What is your cost structure?
- What is your profit margin?

There are many ways that a business can potentially generate revenue and make a profit. One of the most straightforward ways is to simply make a product and sell it directly to customers. This approach requires you to control some sort of distribution channel. If direct sales is difficult, you could instead sell your product wholesale to distributors or retailers. Another approach may be to franchise your business model to others, similar to what many fast-food chains have done. You can also license your product for sale by others. The freemium approach can include advertising, like many social networks, or be based on paid upgrades, which is an approach taken by many mobile games. Many Software as a Server (SaaS) companies utilize a subscription approach that helps ensure a continuous source of revenue over time.

Whatever the business model may be, the point is that, as a security leader and manager, you must have some understanding of how your company actually generates revenue and makes a profit.

Bundling Versus Unbundling

"There are only two ways to make money in business: one is to bundle, the other is to unbundle"
- Jim Barksdale

- Examples
  - Music album -> MP3 -> Streaming services
  - Network TV -> Cable TV -> Netflix/Apps
  - Newspapers -> Blogs -> Google/Facebook

Jim Barksdale was the CEO of Netscape Communications, the creator of the first widely popular web browser, when he found himself at the end of a very long road show as the company was taking Netscape public. Just as he was about to leave the meeting, he was asked, "How do you know that Microsoft isn't just going to bundle a web browser into their product?" To end the conversation, he replied, "Gentlemen, there's only two ways I know of to make money: bundling and unbundling" and immediately left the room.[1]

This now-famous quote not only served as a nice ending to the meeting but has also proven to be very true.

In the music industry, songs were bundled together into albums, records, and CDs. Then, along came the MP3 format, and songs were subsequently unbundled and distributed via file sharing services like Napster and BitTorrent. This unbundling was then legitimized by Apple's iTunes music store. Now, we see songs being bundled together again in the form of streaming services like Pandora and Spotify.

In the television industry, shows were bundled together by the TV and cable companies. You could only get certain shows and channels if you subscribed to cable TV and purchased select packages. Now, we see shows being unbundled by new streaming players like Netflix and even stand-alone apps like HBO, which was previously available only as part of a cable TV package.

In terms of news articles, they were bundled together and aggregated by newspaper companies. Large national publications like the *New York Times* served as the curators of content while regional newspapers served the same role on a local scale. Because of this bundling of information, newspapers had tremendous power and reaped the corresponding financial benefits from advertisers. With the rise of the Internet, effectively reducing the cost of distribution to zero, anyone with good ideas could now become a publisher. Blogs and easy access to online articles unbundled the news. This unbundling, however, created a discovery problem. How could someone searching for interesting news find it online in a vast sea of information. So, now we see news articles getting bundled by Google, which provides an easy way to search for meaningful content, and Facebook, which is often the "front door of the Internet" for many people based on their personal interests and the interests of their connections. This rebundling of online content has, of course, driven large amounts of revenue for these new aggregators.

Reference

[1] https://hbr.org/2014/06/how-to-succeed-in-business-by-bundling-and-unbundling/

Unbundling Example

Source: SupplyDemanded.com

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 123

Craigslist, founded in the early days of the Internet, is an online advertisement website with sections for jobs, housing, personal ads, items for sale, and more. It is one the most successful classified advertisement websites, and its user interface remains largely unchanged from its inception. It is a good example of bundling multiple types of ads into one website.

Over time many start-ups and entrepreneurs have tried, to varying degrees of success, to unbundle various portions of the craigslist.org website into stand-alone web or mobile applications. Venture capitalist Andrew Parker first created a graphic to illustrate how different companies have attempted to carve out niches from Craigslist.[1] Since then, David Haber has created the updated graphic shown on this slide.[2]

This graphic nicely illustrates how various portions of Craigslist have been unbundled by various other services:

- Uber and Lyft for rideshares and transportation
- AirBnB for sublets and temporary rentals
- Zillow and Trulia for apartment rentals (not shown on this slide)
- GitHub and StackExchange for software-related work
- Coursera and edX for educational lessons
- Ashley Madison and others for online dating
- Quora for online discussion forums
- Gazelle for used cell phones
- StubHub for tickets

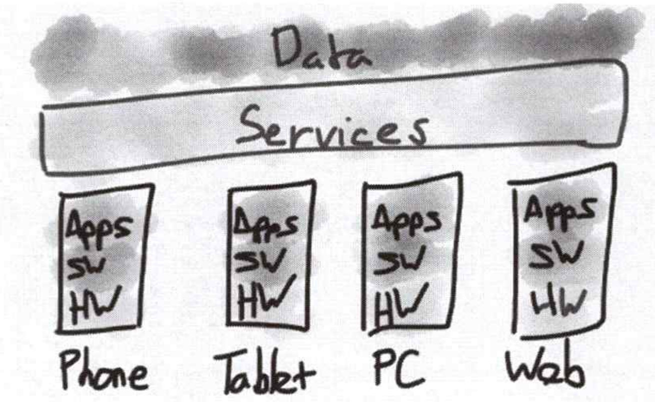
References

[1] http://thegongshow.tumblr.com/post/345941486/the-spawn-of-craigslist-like-most-vcs-that-focus

[2] http://techcrunch.com/2012/12/01/the-future-of-online-marketplaces/

Vertical Versus Horizontal Business Models

- Vertical business model
  - Consolidate multiple steps in the value chain
  - Example: manufacturing, distribution, retail in one org
- Horizontal business model
  - Focus on one area in the value chain



Source: stratechery.com

It is also useful to consider whether your company employs a vertical or a horizontal business model. Vertical business models consolidate multiple steps in the value chain into one organization. For example, a shoe company may decide to integrate vertically by owning design, manufacturing, distribution channels, and retail stores to control all aspects of the business. On the other hand, a company with a horizontal business model may decide simply to focus on one layer of the value chain. For a shoe company, this may mean controlling just the design or retail distribution of shoes.

In the technology industry, Apple is a good example of a company with a vertical business model. Apple not only designs the overall device but also manufactures its own custom ARM chips, creates the operating system, and develops apps that run on the device. On the other hand, companies like Google, Facebook, and Dropbox have a horizontal business model. They provide services to customers that they want to make as broadly available across as many device types as possible. Apple wants its proprietary services, like iCloud, to run only on Apple devices (that is, vertical). Dropbox, however, wants its apps and services on as many devices as possible to ensure ubiquitous access to data (that is, horizontal).[1]

Ben Thompson of Stratechery nicely summarizes this concept: "Vertical players typically monetize through hardware, only serve a subset of users, and any services they provide are exclusive to their devices. Horizontal players, on the other hand, monetize through subscriptions or ads, and seek to serve all users across all devices."[2]

The type of business model your company uses informs a number of decisions that drive the organization's overall strategy.

References

[1] https://stratechery.com/2013/the-dropbox-opportunity/

[2] https://stratechery.com/2013/understanding-google/

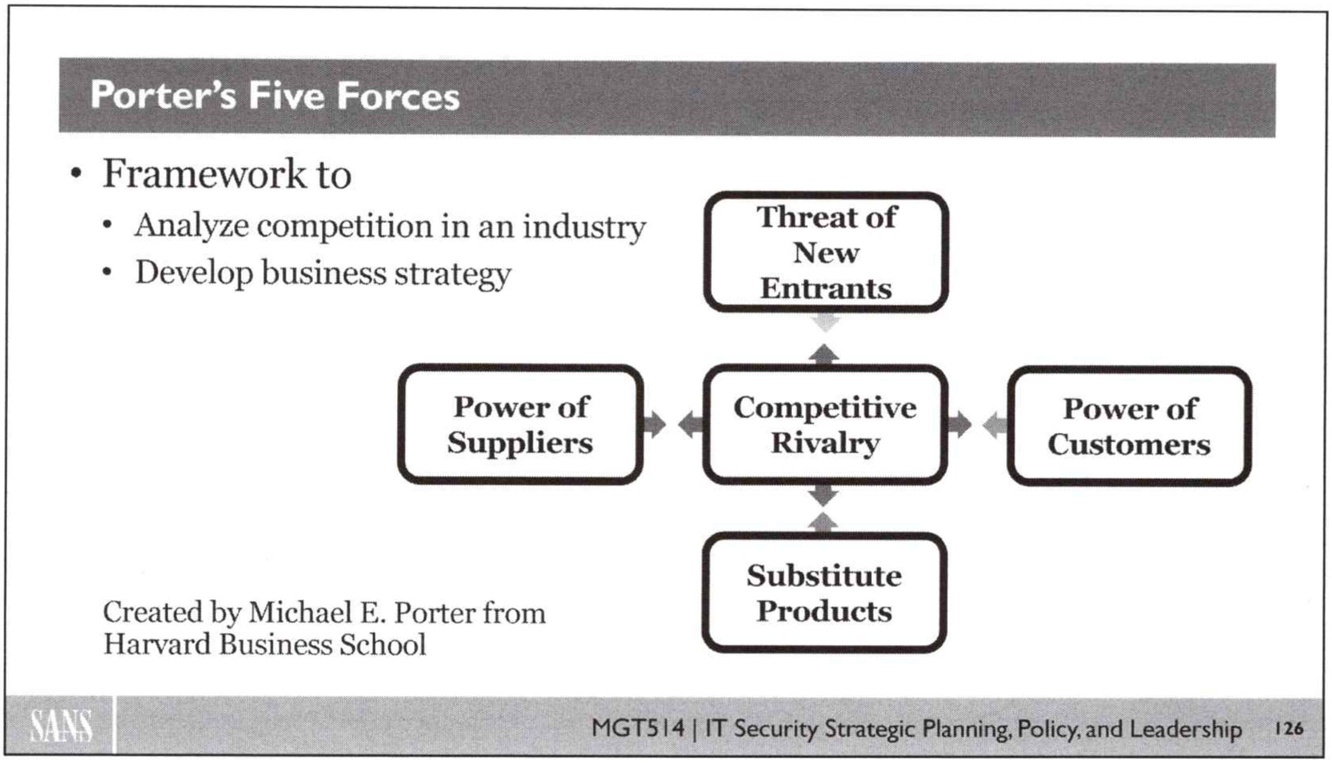
Business Strategy

- Business model
  - Describes what your company does to generate revenue and profit
- Business strategy
  - How you build competitive advantage
  - How you will do better than your rivals
  - Actions to implement your business model

If a business model describes what your company does to generate revenue and profit, then what describes *how* your company accomplishes this feat?

Many companies have similar business models, but only some survive and thrive. Why did Microsoft dominate the PC market where other operating system vendors failed? Why did Google come to dominate search in the face of many competing search engines like Yahoo!, Bing, and countless others? Why has Facebook become the king of social networking despite the large head start that MySpace enjoyed?

Having a solid business model alone is not enough. How did organizations like the ones mentioned above build competitive advantage and do better than their rivals? This is where an understanding of business strategy, actions that can be taken to implement your business model, come into play.



Porter's Five Forces is a powerful method used to develop business strategy by understanding where power lies in a business situation. By looking at the internal and external pressures that exist within an industry sector, you can determine whether or not an industry is attractive and if you will have a defensible niche. It's a checklist of sorts that leads you through the identification and consideration of five forces that determine competitive intensity and, ultimately, how you can make a profit.

Porter's Five Forces also aids in the understanding of how markets may change, and narrows the factors that could bring about change. A change in any of the forces normally requires a business unit to re-assess the market. The balance or net effect of these five forces determines your relative strength in the marketplace.

Porter's Five Forces was developed in 1979 by Michael E. Porter, who is a leading authority on competitive strategy and economic development. Porter has authored 18 books and numerous articles and is one of the most-cited authors in business and economics. Porter's Five Forces method has been applied to a diverse range of problems from helping businesses become more profitable to helping governments stabilize industries. You can learn more about Porter's research and other business tools in his book *Competitive Strategy: Techniques for Analyzing Industries and Competitors.*[1]

Below is a summary of each of the five forces:

- **Power of Customers:** Here, you look at the impact your customers have on your business. As an example, this force is driven by the number of customers you have, the importance of each individual customer to your business, and the cost involved for them to switch from your products and services to another company or organization. In other words, you are looking at the ability your customers have to put your firm under pressure.

- **Substitute Products**: Here, you look at the ability of your customers to find substitute products or alternative ways of doing what you, your team, or your company does. If substitution is easy and viable, this weakens your power.

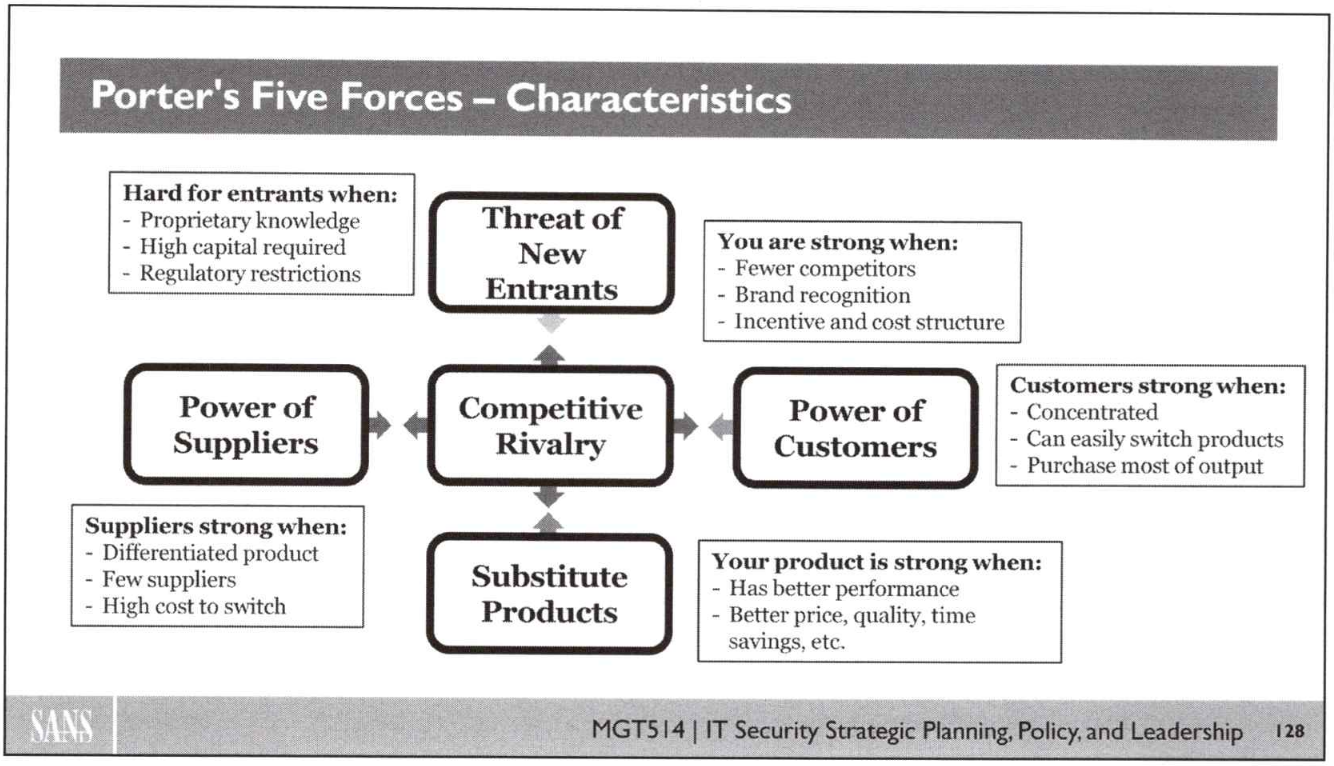
- **Power of Suppliers**: Here, you look at how easy it is for suppliers to influence and drive up prices; the uniqueness of their product or service; their strength and control over you, your organization, and/or your company; and the cost of switching from one supplier to another. The fewer suppliers you have, and the more you need suppliers, the more powerful the suppliers are.

- **Threat of New Entrants**: Here, you look at how easy it is for people to enter your market. New competitors can easily become a threat if it costs little time and money to enter your market and effectively compete with your company, if there are few economies of scale in place, or if you have little protections for your key technologies; new competitors can quickly enter your market and weaken your position. If you have strong barriers to entry, you can maintain leverage and maintain a favorable position. The thing you have to remember in this area is profitable markets will always attract new firms.

- **Competitive Rivalry**: Here, you will look at the number of competitors and their capabilities. You will have less power in the market if you have many capable competitors that have equally attractive products and/or services. On the other hand, if no one else can do what you do, or provide the services you can provide, you will have tremendous strength.

Reference

[1] http://www.amazon.com/Competitive-Strategy-Techniques-Industries-Competitors/dp/0684841487



Power of Customers

This force looks at the impact your customers have on your business. It is driven by the number of customers you have, the importance of each individual customer to your business, and the cost involved for them to switch from your products and services to another company or organization. In other words, you are looking at the ability your customers have to put your firm under pressure.

Customers have the power to demand lower-price or higher-quality products when their bargaining power is strong. Lower price means lower revenue for the company, while higher quality typically raises production costs. Customers have strong bargaining power when they buy in large quantities, control access points to the final customer, or where only a few buyers exist. They also have power when the switching costs to other suppliers are low, or there are many options for products and/or service, or finally if customers are price sensitive.

Substitute Products

Here, you look at the ability of your customers to find substitute products or alternative ways of doing what you, your team, or your company does. If substitution is easy and viable, this weakens your power. This force typically impacts an industry through price competition; as more substitutes become available, the demand becomes more elastic because customers now have more alternatives to choose from.

This force is especially threatening when customers can easily find alternatives or substitutes for their desired products and/or services with attractive pricing and/or better quality and when customers can easily switch from one product and/or service to another with little to no cost. As an example, switching from coffee to tea costs you little to nothing, whereas switching from a bicycle to a car for transportation will cost more.

Power of Suppliers

Here, you look at how easy it is for suppliers to influence and drive up prices, the uniqueness of their product or service, their strength and control over you, your organization and/or your company, and the cost of switching from one supplier to another. The fewer suppliers you have, and the more you need suppliers, the more powerful the suppliers are. The more potential but realistic sources of supply, the stronger the bargaining power for your company will have.

Threat of New Entrants

Here, you look at how easy it is for people to enter your market. New competitors can easily become a threat if it takes relatively little time and money to enter your market, if there are few economies of scale in place, or if you have little protections for your key technologies. If you have strong barriers to entry, then you can leverage and maintain a favorable position. Remember that profitable markets will always attract new firms.

It is difficult to enter a market if your products are patented, proprietary know-how is required, you have a strong brand, or there are restricted distribution channels or economies of scales are difficult to achieve.

Competitive Rivalry

With this force, you must consider the number and capabilities of your competitors. You will have less power in the market if you have many capable competitors that have attractive products and/or services. If more companies are competing with each other, the resulting competitive pressures will mean that prices, profits, and strategy will be driven by it. Competitive rivalry might be higher when similar-sized companies operate in one market, when companies have similar strategies, when products offered have similar features and offer the same benefit, when the growth in the industry is slow, or there are high exit barriers or low entry barriers.

Porter's Five Forces – Antivirus Example

Force	Antivirus
Customers	• Customers have no choice but to purchase, but can switch who they purchase from • High-volume customers can negotiate more favorable terms and pricing
Substitute Products	• No acceptable substitutes seen by most of market, though endpoint white listing may be on the horizon • High barrier to switching
Suppliers	• Product is dependent on intellectual capital, not material inputs, so suppliers have little power • Employees have some power collectively, but not individually
New Entrants	• High costs to develop and market a new competitive product • Strong brand loyalty • Customers resistant to switching
Competitors	• Market dominated by a few large competitors, very fragmented remainder of market • Customers see little differentiation in core product, just in support and ease of use

Let's take a summary view of how we would apply Porter's Fiver Forces analysis to a security vendor for antivirus. Performing this method of analysis should be a prerequisite to establishing the right components for your strategy because it will enable more informed decisions about your security investments such a security products and or services purchases.

Power of Customers

When you are looking at current or potential suppliers for your security products, you may want to consider additional questions with a slight twist. In relation to suppliers in the marketplace, as a customer, what does our spend represent as an overall percentage of their turnover? Are we a large or small buyer of their security products and/or services? Could we send a typical supplier in the marketplace into liquidation if we moved our business from one supplier to another? In the antivirus example, customers have no choice but to purchase, but they can switch which supplier they purchase their product from. High-volume customers can negotiate more favorable terms and pricing.

The higher your spend is against the spend of other customers in the marketplace, the stronger bargaining power you have for your security products and/or services. You may want to consider procurement auctions for categories in which your business is significant enough to be attractive, you have clearly defined requirements, and there are ample suppliers attracted to your business to ensue competition.

Substitute Products

You'll want to determine if other products are available that could fulfill the same purpose or if technology advancements provide an alternative way of fulfilling the same need and how likely new inventions are to get to market and lastly, whether new products are delayed in getting to the market for fear of disrupting the market. In the antivirus example, there are not acceptable substitutions seen by most of the market, although endpoint whitelisting may be on the horizon, and there is a high barrier to switching.

Power of Suppliers

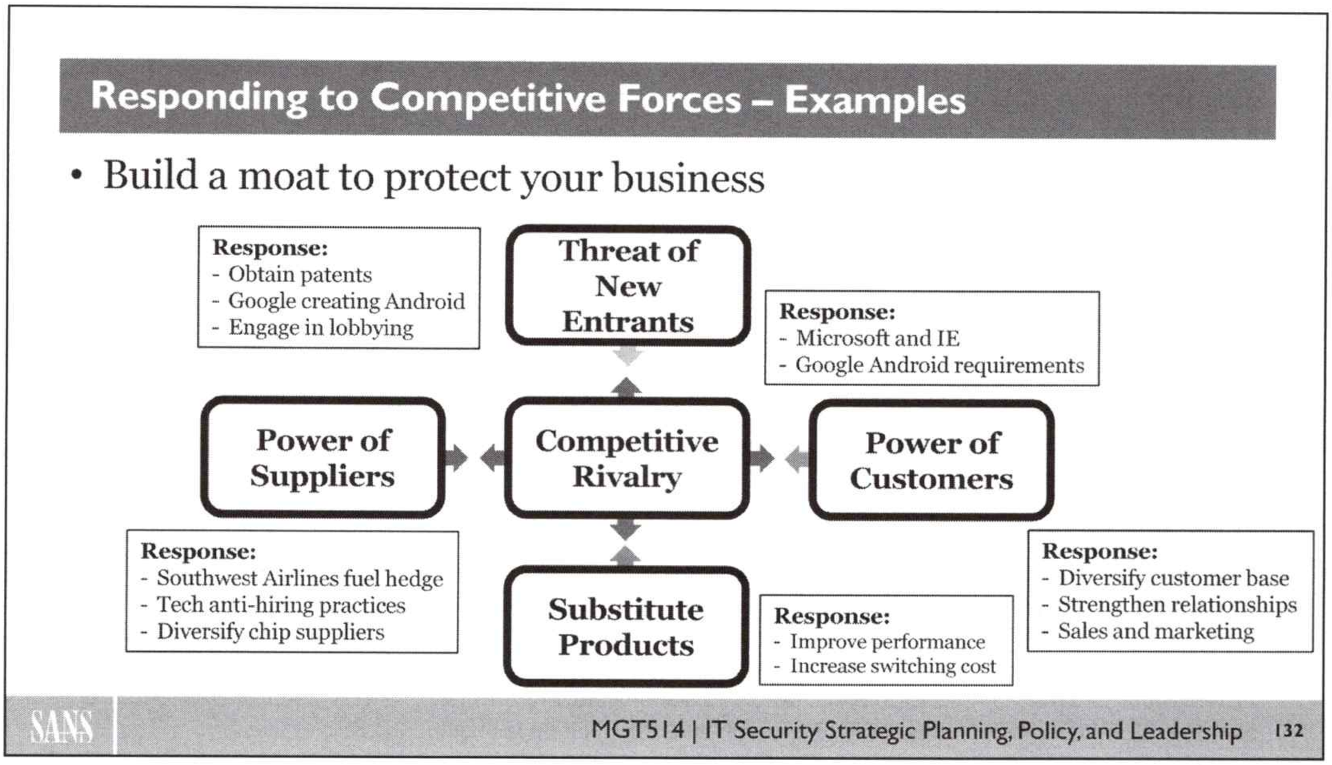
You'll want to determine how many sources of supply there are in the market for a particular product, how stable the market is, and if the same suppliers have dominated the market for years. You'll also want to consider if there is supplier consolidation taking place or if current suppliers are enjoying high profits or they are going out of business. In the antivirus example, products are dependent on intellectual capital, not material inputs, so suppliers have little power, and employees have some power collectively, but not individually.

Threat of New Entrants

You'll want to determine if the market is profitable for current and potential suppliers, or if there are barriers to entry for a new firm, such as regulation, high fixed cost, or strong brand equity. You'll also want to determine if a new entrant can add value to the product or create a differentiation, and lastly, how quickly new products are introduced. In the antivirus example, there are high costs to develop and market a new competitive product, and there is a strong brand loyalty; therefore, customers are resistant to switching.

Competitive Rivalry

The more fierce the competition between existing firms, and the more firms that reside in the marketplace, the stronger bargaining power you have for your security products and/or service needs. This should be balanced against the number of customers in the marketplace. If there are a lot of customers and a lot of suppliers, then suppliers can change their customers as can customers change their suppliers. In the antivirus example, the market is dominated by a few large competitors, and the remainder of the market is very fragmented. Customers see little differentiation in core products but recognize differentiation in support and ease of use.



When you have an understanding of the competitive forces that affect your industry and company, the next step is to translate this understanding into action. The idea is to build a moat that protects your business. By quickly building favorable synergies and rigid consequences, companies can strengthen their own virtuous cycles and block the cycles of others. Ultimately, the goal is to create defensible business positions that enable you to capture more value than competitors.

Power of Customers

Because customers can potentially walk away from your business at any time, it is important to broaden, diversify, and strengthen your customer base. For example, customers can, in theory, easily switch computing devices—whether it be from a Mac to a PC or from an iPhone to an Android phone. To help combat this, Apple has focused on creating synergies among its various products. After the iTunes Store was made available on PCs, existing iPod customers started buying more Macs. This "halo effect" has since been seen in relation to iPhone customers who also buy Macs and other Apple products. To further strengthen customer relationships, Apple created the Genius Bar in its stores. This customer support desk is not a profit center but is instead designed to engage with customers, provide them needed support, and make them happier about the use of Apple's products. All of this is further strengthened by Apple's marketing, which often focuses on emotional appeals and helps strengthen long-term relationships with customers.

Substitute Products

Customers can switch away from your product and use something else entirely. In transportation, people can choose to take planes, trains, buses, boats, cars, bicycles, and so on. Each of these options has trade-offs in terms of time, cost, and convenience. To ensure that customers prefer your particular product, you can, of course, continue to improve it over time. A better product often means happier and more loyal customers. One way to engineer "loyalty" is to increase switching costs. If it is extremely expensive or time consuming to switch products, then you are less likely to do so. This is why technology vendors like Microsoft worked to create dependencies among their various products. To run Exchange, you had to have Windows Server, which includes

ActiveDirectory (AD). With large parts of the Microsoft stack in place, it's much more likely that other Microsoft product like SQL Server and Sharepoint would be used.

Power of Suppliers

Suppliers have a key role in your value chain. They can determine how quickly you can get product to market and how profitable you may be. If the costs of your key inputs go up drastically, this will obviously impact your bottom line. In the airline industry, this is exactly why Southwest Airlines enters into fuel hedging contracts. By better controlling the volatility of one of its key inputs, the company is able to keep fares lower than competitors. In the technology industry, skilled labor (for example, developers, security professionals) is a key input for many companies. To keep costs down, a number of technology companies like Adobe, Apple, Google, Intel, Intuit, and others entered into illegal anti-poaching agreements that restricted the recruitment of their high-tech employees. In response, the Department of Justice brought an anti-trust action against these companies, resulting in settlement payouts of hundreds of millions of dollars. In addition to cost, suppliers can determine whether or not updated products get to market. For many years, the availability of newer Intel chips determined when new, more powerful PCs could be brought to market. In recent years, Apple has tried to diversify supply of its A Series chips from multiple manufacturers like Samsung and Taiwan Semiconductor Manufacturing Co. (TSMC) to better manage risk from key suppliers.

Threat of New Entrants

It is often beneficial to make it difficult for new entrants to join your market. This can be accomplished by developing new, proprietary technology that others do not have and patenting it. Because creating new inventions and patents is difficult and time consuming, some organizations have simply bought large patent libraries from other companies. In the competitive mobile space, this is a big reason that Google bought Motorola for $12.5 billion. This is also why a consortium of Apple, Microsoft, Blackberry, and others bought Nortel's patents for $4.5 billion. All this patent acquisition is a hedge against attacks from competitors. In fact, that is why Google originally created Android itself. It was concerned about Microsoft, with its leading mobility efforts at the time, controlling an operating system that would exclude Google Search. Google didn't know it at the time, but its investment in Android wound up being more of a hedge against Apple's iOS. Many companies also engage in political lobbying to create or update regulations to their benefit. This includes items like patent reform, corporate tax reform, privacy, and cyber security.

Competitive Rivalry

To win in the market, companies often try to create barriers for other firms. This is what Microsoft was accused of when it bundled its Internet Explorer (IE) web browser and Windows Media Player with its Windows operating system. Regulators argued that Microsoft used its monopoly power in PC operating systems to unfairly gain an advantage in other markets.[2] Shifting from PCs to mobile devices, Google is now accused of anti-trust violations in the European Union (EU) because it required manufacturers to pre-install Google Search and Chrome, provided financial incentives for favoring Google Search, and provided access to the Google Play Store only to manufacturers who agreed to make Google Search the default and agreed not to create forked versions of Android. These tactics helped strengthen Google's dominant position and built barriers that protected its core business.

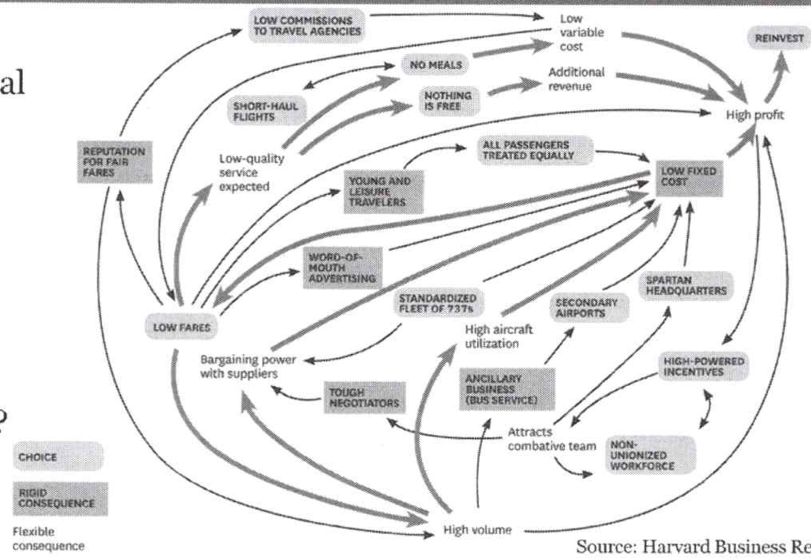
References

[1] https://en.wikipedia.org/wiki/High-Tech_Employee_Antitrust_Litigation

[2] https://en.wikipedia.org/wiki/United_States_v._Microsoft_Corp.

Strategic Objectives – Ryanair

- Strategic objectives
  - Long-term organizational goals
  - Convert vision and mission into more specific plans
- Ryanair
  - Vision to become a low-cost airline
  - What are the next steps?



Source: Harvard Business Review

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 134

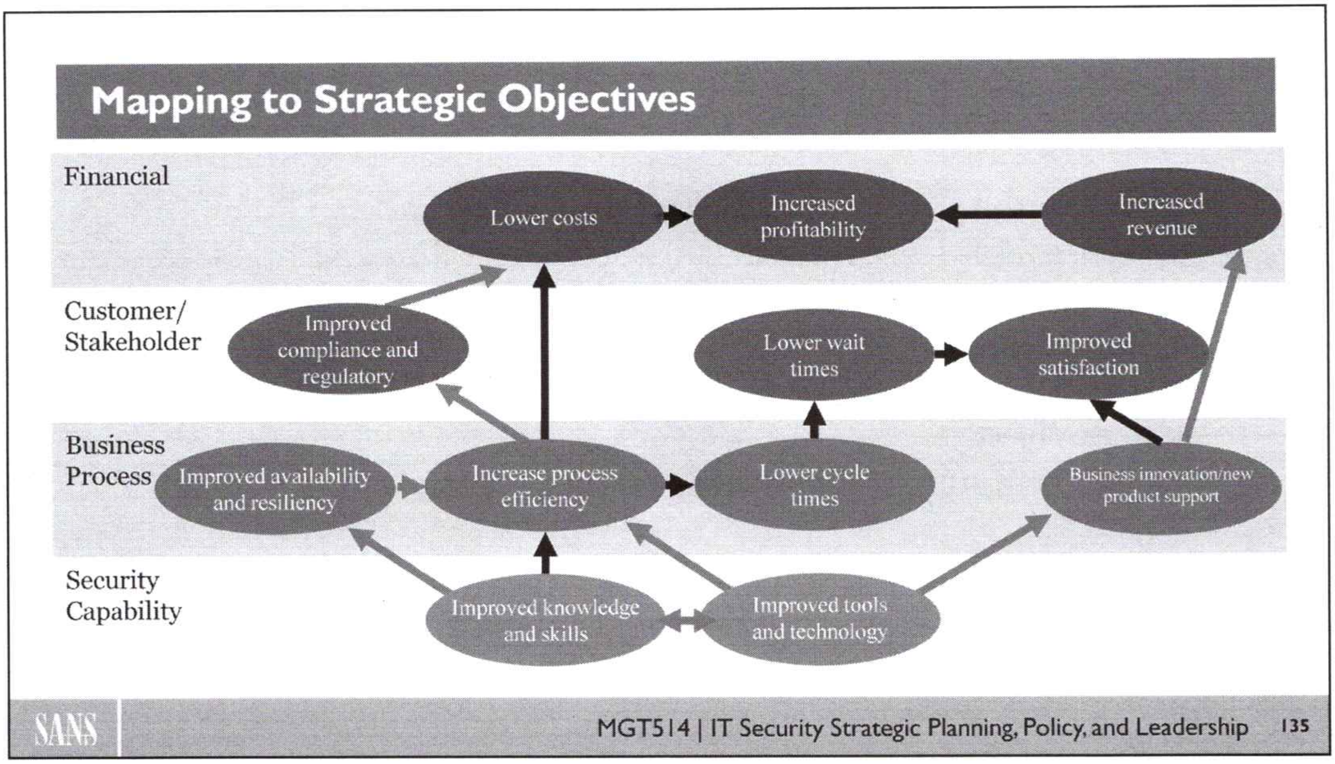
Organizations create strategic objectives to clearly define how they should respond to the competitive forces in the marketplace. These strategic objectives are long-term organizational goals that help turn high-level mission and vision statements into more concrete goals. In other words, strategic objectives are actions you take to implement your business strategy.

Ryanair had a vision to become a low-cost airline. It wanted to move away from its traditional business model, which had become unprofitable. So, Ryanair took steps to implement a number of strategic objectives to help it achieve its plan of becoming a low-cost airline. The company defined the following critical strategic objectives:

- **Maintain Low Fixed Costs:** This included flying out of secondary airports, choosing a nonunionized workforce, operating out of a spartan headquarters, and utilizing a standardized fleet of Boeing 737s.
- **Attract Young and Leisure Travelers:** The company chose to treat all passengers equally. By catering to only one class of passenger, it could charge for all additional services, serve no meals, and focus on short-haul flights. This objective not only reduced costs but also drove additional revenue because now customers had to pay for all checked bags, snacks, and so on.
- **Be Tough Negotiators:** The company decided to hire an aggressive management team by offering high-powered incentives for performance. This enabled the company to more effectively bargain with suppliers and the workforce.
- **Build a Reputation for Fair Fares:** As a result of these strategic objectives, Ryanair reduced variable and fixed costs while driving up volume because of its reputation for reasonable fares. It has created a virtuous cycle in which all the parts of its business help deliver acceptable service at low prices.

Reference

https://hbr.org/2011/01/how-to-design-a-winning-business-model



As security professionals, we are often focused on the bottom row of this diagram—improving our security capabilities by increasing our knowledge and skills or improving our tools and technologies. As security leaders and managers, we have to remember how these security activities support the overall strategic objectives for the organization as a whole. For example, improving security tools and technologies can help support new products that the company is trying to bring to market. These may be new mobile apps, websites, or other technology products in which security can contribute new features or capabilities. These new products have a direct correlation, improving customer satisfaction and ultimately increased revenue. Similarly, by improving our security capabilities, we can improve business processes around efficiency and availability, leading to improved compliance and ultimately lower costs.

The goal of any organization is to create value for its key constituents. Usually, this means increasing revenue and overall profitability. Whatever the key strategic objectives are for your organization, a key component to your success as a security business leader will be mapping your security activities to those overall strategic objectives.

In Summary

- Security leaders and managers must understand
  - Business model
    - What the organization does to create value
  - Business strategy
    - How the organization competes
  - Strategic objectives
    - Specific goals to implement strategy

A business model describes how your company or organization operates. It is the plan for how you will generate revenue and actually make a profit from that revenue. This is, of course, done by delivering something of value to your customers. However, it's not enough to simply have a business model. Successful businesses have a strategy that defines how the organization will respond to the various competitive forces in the marketplace. To win in the market, an organization will define strategic objectives which are specific goals that help the company implement the overall strategy. As security leaders and managers, we must understand how our businesses operate so that we can provide services that help drive value for the overall organization.

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 1

- Background
  - About This Course
  - Need for Strategic Planning
    - Exercise #1: Case Scenario
- Understand the Business
  - Vision & Mission
    - Exercise #2: Mission Statement
  - Stakeholder Management
  - PEST Analysis
    - Exercise #3: PEST
  - Business Strategy
- *Understand the Threats*
  - Threat Actors
    - Attack case studies
  - Asset Analysis
    - Exercise #4: Attacker Motivation
  - Threat Analysis
    - Exercise #5: Intrusion Kill Chain

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 137

This page intentionally left blank.

Why We Need to Understand the Threats

- By understanding the threats and threat landscape, we can
  - Better plan our defenses
  - Learn how we can improve against actual threats
  - Understand where attackers are weak

> "If you know the enemy and know yourself you need not fear the results of a hundred battles."
> - Sun Tzu

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 138

Sun Tzu (544–496 BC) was a Chinese military general, strategist, and philosopher who is best known for writing *The Art of War*. It presents a philosophy of war that is widely accepted as a masterpiece of strategy. Its lessons have been applied not only to military affairs, but also to business, politics, and, of course, information security.

In the previous section, we covered topics to help us understand the business ("know yourself"). In this section, we cover topics to help us understand the threats ("know the enemy"). By understanding the threats, we can improve our defenses and understand where attackers are weak. As Sun Tzu notes, it is only by understanding both that we can hope to build a successful information security program.

How to Develop an Understanding of the Threats

1) Understand threat actors
   - Their motivations and mindset
2) Understand key business assets
   - What is important to the business
3) Analyze threats
   - Understand tactics, techniques, and procedures using Kill Chain Analysis

This understanding of the threats comes from:

1) Understanding threat actors

Being able to think like your adversaries requires an understanding of their motivations and mindset.

2) Understanding business assets

With your knowledge of the business from the previous sections, you should have a sense of what the organization considers to be critical business assets. If you think these assets are important, then it is possible that your adversaries may consider them to be valuable also.

3) Analyzing threats

If an adversary is attempting to gain access to your critical assets, then it will need to mount an attack. Understanding its tactics, techniques, and procedures will help you better plan your defense and understand where your current defenses may be lacking.

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 1

- Background
  - About This Course
  - Need for Strategic Planning
    - Exercise #1: Case Scenario
- Understand the Business
  - Vision & Mission
    - Exercise #2: Mission Statement
  - Stakeholder Management
  - PEST Analysis
    - Exercise #3: PEST
  - Business Strategy
- Understand the Threats
  - *Threat Actors*
    - Attack case studies
  - Asset Analysis
    - Exercise #4: Attacker Motivation
  - Threat Analysis
    - Exercise #5: Intrusion Kill Chain

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 140

This page intentionally left blank.

Understanding Threat Actors

- Goals of this section
  - Learn about the different types of threat actors
  - Understand their motivations
  - Understand the tactics used by two common threat actors
    - By walking through two cases of real-world attacks

In this section, we cover the different types of threat actors, their motivations, and the tactics used by two common threat actors by walking through two examples of real-world attacks.

About VERIS

- VERIS
  - Vocabulary for Event Recording and Incident Sharing
  - Defines a schema to describe security incidents in a structured and repeatable manner
    - Available at http://veriscommunity.net
- Used by the Verizon DBIR
  - Standard way to analyze incidents
  - Mapped and recoded incidents from other frameworks
- VERIS Community Database (VCDB)
  - Free repository of publicly reported security incidents
    - Available at http://vcdb.org

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 142

VERIS is the Vocabulary for Event Recording and Incident Sharing.[1] It defines a schema and set of metrics to describe security incidents in a structured and repeatable manner. It is most famously used by Verizon as part of its annual Data Breach Investigations Report (DBIR).

The VERIS Community Database (VCDB) is a free repository of publicly reported security incidents. Both the raw incident data and a nice dashboard for searching historical incidents are available online.[2]

By utilizing a standard mechanism for talking about security incidents, the VERIS framework helps us describe threat actors and their motivations.

References

[1] http://veriscommunity.net

[2] http://vcdb.org

VERIS Threat Actors

Category	Description	Actor	
External	Threats from sources outside the organization and its partners. This includes criminal groups, lone hackers, former employees, and government entities as well as "Mother Nature" and chance.	• Acquaintance • Activist • Auditor • Competitor • Customer • Force majeure	• Former employee • Nation state • Organized crime • State affiliated • Terrorist • Other
Internal	Threats that arise from within the organization. This includes full-time employees, contractors, interns, and other staff.	• Auditor • Call center staff • Cashier • Developer • End user • Executive • Finance	• Help desk • HR • Maintenance staff • Manager • Security guard • System admin • Other
Partner	Any third party that has a business relationship with the organization. These business partners usually have some level of trust or privilege.	• Supplier • Vendor • Hosting provider • Outsourced IT • Other	

VERIS has three categories for threat actors:

- **External:** Threats from sources outside the organization and its partners
- **Internal:** Threats that arise from within the organization
- **Partner:** Any third party that has a business relationship with the organization

Each category has a comprehensive list of potential threat actors that an organization may encounter.

Sample Threat Actors and Motivations

Threat Actor	Description	Motivation
Hacktivist	Activist groups target organizations because of real or perceived slights. Their goal is to damage the brand and embarrass the organization.	• Ideology or protest • Fun, curiosity, or pride • Grudge or personal offense
Organized Crime	Criminals want to make money using stolen data and access to systems. They use malware, phishing, and application attacks to steal data.	• Financial gain
Nation State	Countries attempting to gain economic or military advantage over their adversaries and economic competitors by stealing data and sabotaging equipment.	• Espionage • Competitive advantage • Fear or duress
Competitor	Other organizations in the same or similar industries seeking proprietary information.	• Espionage • Competitive advantage
Insider	Employees who put data at risk by violating policies and standards or through negligence.	• Espionage • Grudge or personal offense • Convenience or expediency
Partner	Vendors that are relied upon to store and process sensitive information. Partners may have elevated levels of access to sensitive data or systems.	• Espionage • Convenience or expediency

Let's look at some common threat actors and their motivations.

Hacktivists: Activist groups who target organizations for real or perceived slights

Organized Crime: Criminals who want to make money using stolen data and access to systems

Nation State: Countries that attempt to gain economic or military advantage over their adversaries

Competitor: Other organizations that may seek proprietary information for competitive advantage

Insider: Employees who put data at risk through malicious or negligent actions

Partner: Vendors who knowingly or unknowingly put data and information at risk

Threat actor motivations defined in VERIS:

Espionage: Espionage or competitive advantage

Fear: Fear or duress

Financial: Financial or personal gain

Fun: Fun, curiosity, or pride

Grudge: Grudge or personal offense

Ideology: Ideology or protest

Convenience: Convenience of expediency

Unknown: Unknown

Other: Other

Hacktivist Case

This page intentionally left blank.

Anonymous

- Hacktivist collective
  - Ideologically motivated
  - Driven by social and political agendas
  - Seeks publicity to humiliate and embarrass targets
  - Not profit driven
- Some high-profile attacks
  - Sony attacked after it filed suit against PS3 hacker George "GeoHot" Hotz
  - Amazon, PayPal, MasterCard, Visa attacked for anti-WikiLeaks behavior

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 146

Anonymous is a loosely associated network of hacktivists that has attacked various government, religious, and corporate entities as a result of ideological differences.[1] The entity is driven by social and political agendas and often seeks to humiliate and embarrass its targets by exposing sensitive data and conducting denial-of-service attacks. In 2012, *Time* magazine called Anonymous one of the 100 most influential people in the world.[2]

Numerous high-profile attacks are attributed to Anonymous, including:

- **Sony PlayStation Network hack:** After George "GeoHot" Hotz compromised the security of the PlayStation 3 (PS3) to allow any software to run on the device and subsequently published the root keys on his website, Sony filed suit against him for violating the Digital Millennium Copyright Act (DMCA), computer fraud, and copyright infringement.[3] In response, Anonymous announced its intent to attack Sony websites due to Sony gaining access to the IP addresses of everyone who visited Hotz's website, calling this action "an offensive against free speech and Internet freedom." Shortly thereafter, the Sony PlayStation Network was hacked, resulting in the theft of 77 million accounts and a site outage that lasted 23 days.

- **Operation Payback:** After WikiLeaks published 250,000 U.S. diplomatic communications, various organizations, including Amazon, PayPal, MasterCard, and Visa, withdrew their services from WikiLeaks. In response, Anonymous began Distributed Denial-of-Service (DDoS) attacks against these companies.[4]

References

[1] http://en.wikipedia.org/wiki/Anonymous_(group)
[2] http://content.time.com/time/specials/packages/article/0,28804,2111975_2111976_2112122,00.html
[3] http://en.wikipedia.org/wiki/Sony_Computer_Entertainment_America,_Inc._v._Hotz
[4] http://www.bbc.com/news/technology-11935539

HBGary Background

- HBGary
  - CEO Greg Hoglund
  - Computer security company that sells products and services
- HBGary Federal
  - CEO Aaron Barr
  - Affiliated with HBGary but sells products to U.S. federal government
- Aaron Barr claimed he could unmask Anonymous
  - Using social media analysis and IRC

One of the most well-publicized Anonymous attacks was conducted against HBGary, a computer security consulting and product company. HBGary's CEO, Greg Hoglund, is a well-known security researcher. The company also had a sister organization called HBGary Federal to provide products and services to the U.S. federal government that might require security clearance. In 2010, HBGary Federal's CEO, Aaron Barr, claimed that he could unmask Anonymous by using social media and IRC analysis. He planned to publish the identities of Anonymous members and sell this information and his techniques to potential clients.

Hacked HBGary Home Page

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 148

Anonymous was not happy with Greg Hoglund's announcement and within a matter of days compromised the HBGary website, replaced the contents with this message, and provided a link to download all of HBGary's e-mail messages.

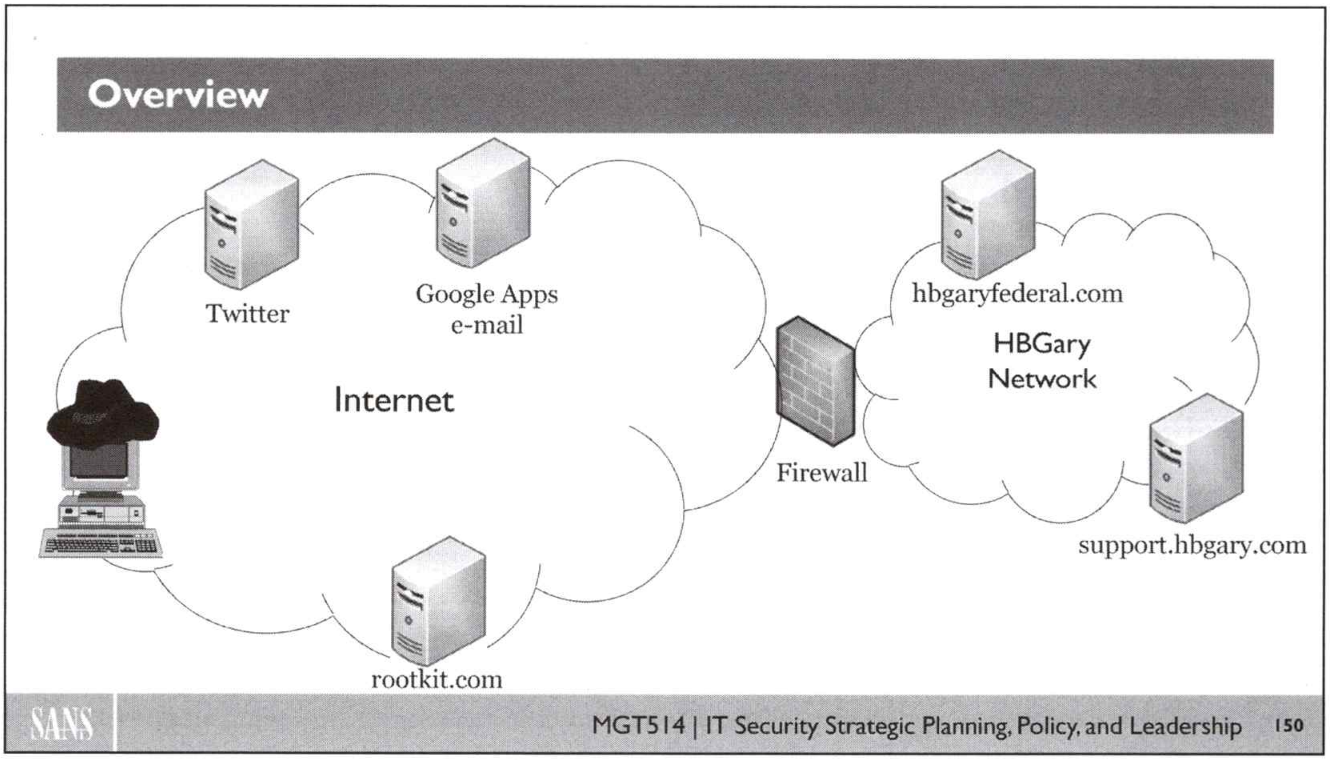
What Happened?

- Within two days
  - hbgaryfederal.com hacked
  - rootkit.com hacked
  - 40,000 e-mails stolen
  - Downloaded and then deleted 1TB of backup data
  - Hacked Aaron Barr's Twitter and LinkedIn
  - Claimed to have remotely wiped Aaron Barr's iPad

Within two days, Anonymous compromised much of HBGary's infrastructure:

- hbgaryfederal.com was hacked.
- rootkit.com (Greg Hoglund's research site) was hacked.
- 40,000 corporate e-mails were stolen and published online.
- One terabyte of backup data was stolen and deleted.
- Aaron Barr's Twitter and LinkedIn accounts were hacked.
- For kicks, the attackers even attempted to remotely wipe Aaron Barr's iPad.

Details in this section are from the Ars Technica story published at http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars.



How did the attack occur. As the diagram shows, the attacker used a relatively small number of systems to compromise HBGary.

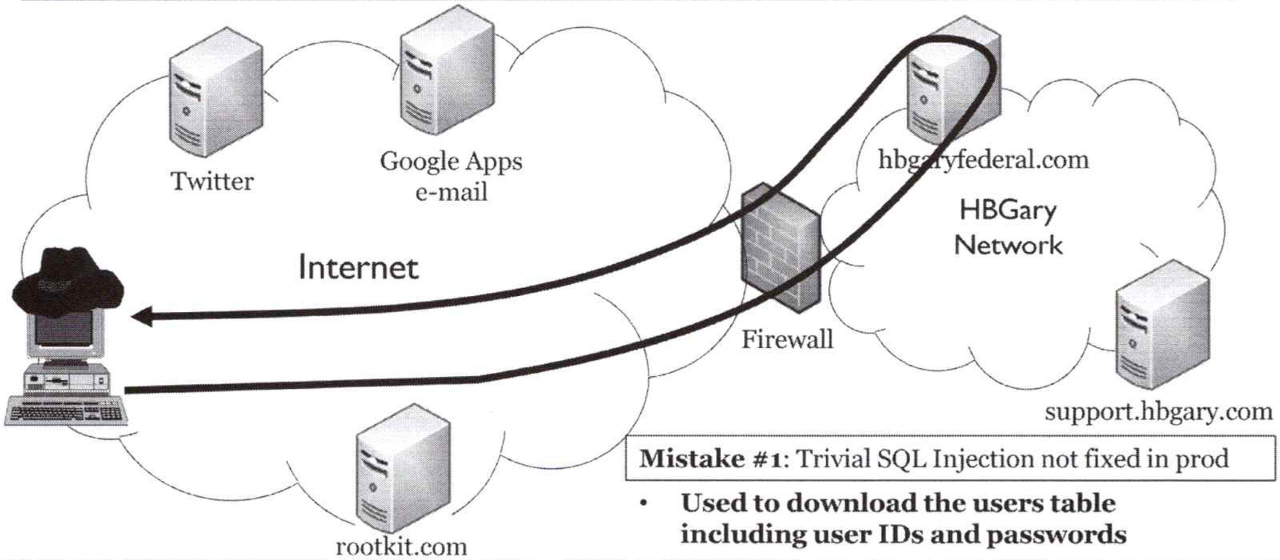
On the HBGary internal network, two systems were accessible to the Internet:

- hbgaryfederal.com
- support.hbgary.com

Outside the HBGary network, the attack targeted:

- rootkit.com (Greg Hoglund's research site)
- cloud services from Twitter and Google utilized by the company

SQL Injection on Custom CMS



Mistake #1: Trivial SQL Injection not fixed in prod

- **Used to download the users table including user IDs and passwords**

As a first step, the attacker discovered a trivial SQL Injection vulnerability in the Content Management System (CMS) used for hbgaryfederal.com. This simple security vulnerability was not fixed in the production website and allowed the attacker to download every single record in the entire database. This included all the user IDs and passwords for the system.

Mistake #1 was not fixing this trivial vulnerability on the website.

Password Issues

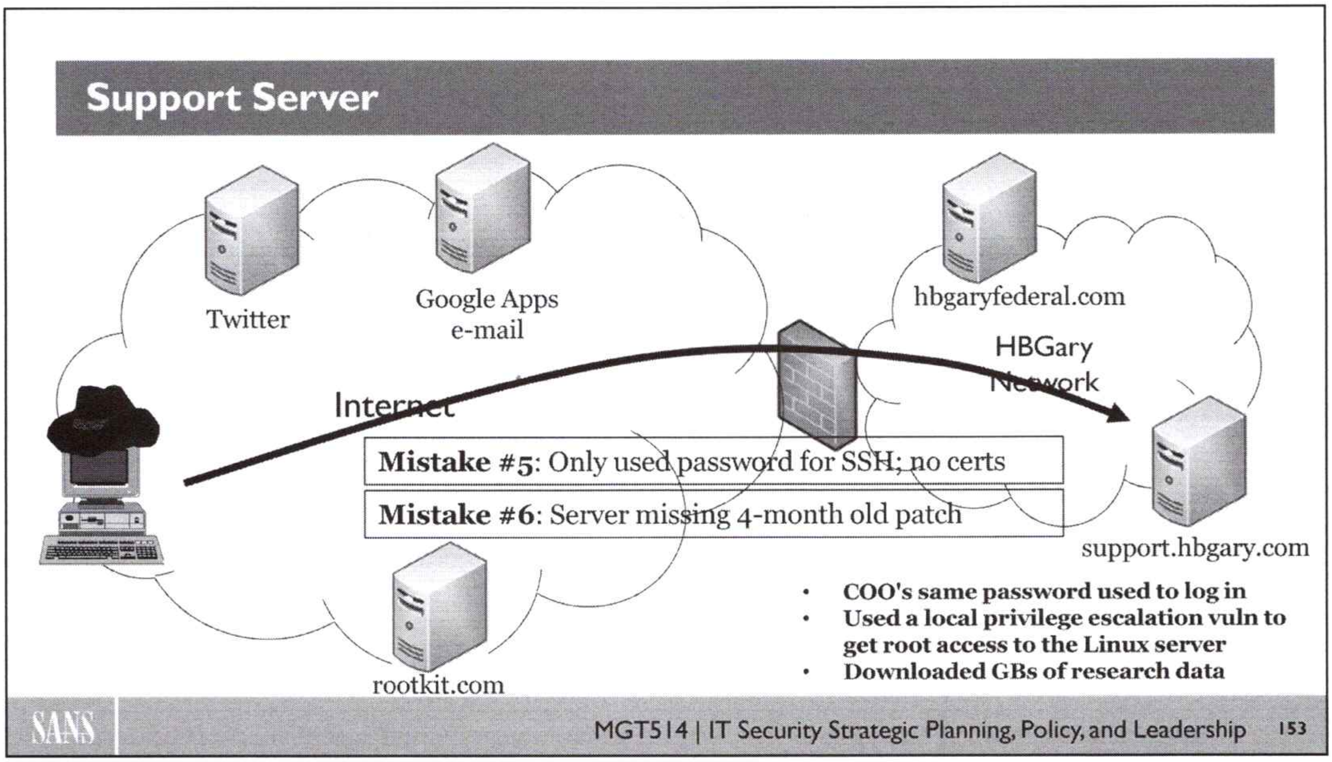
- Passwords were stored hashed
  - Mistake #2: Used unsalted MD5 hashes
  - Trivial to crack using rainbow tables
- Attacker discovered all user passwords
  - Mistake #3: Weak password policy
  - CEO Aaron Barr and COO Ted Vera used 8-character passwords with 6 lowercase letters and 2 numbers
- Access other systems
  - Mistake #4: Password reuse
  - Weak passwords used on other systems also

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 152

After downloading all the user IDs and passwords, the attackers discovered that the passwords were stored in a hashed format using the MD5 algorithm. Although better than storing the password in plaintext without any protection, using this simple algorithm alone does not provide sufficient protection against password-cracking attacks. Mistake #2 was using a weak algorithm without a "salt" to add additional protection to the password. This allowed the attackers to quickly crack all the passwords in the HBGary database.

After cracking all the passwords, the attackers discovered that many users had very simple passwords. Specifically, the CEO and the COO both used eight-character passwords with six lowercase letters and two numbers. Mistake #3 was not enforcing a stronger password policy.

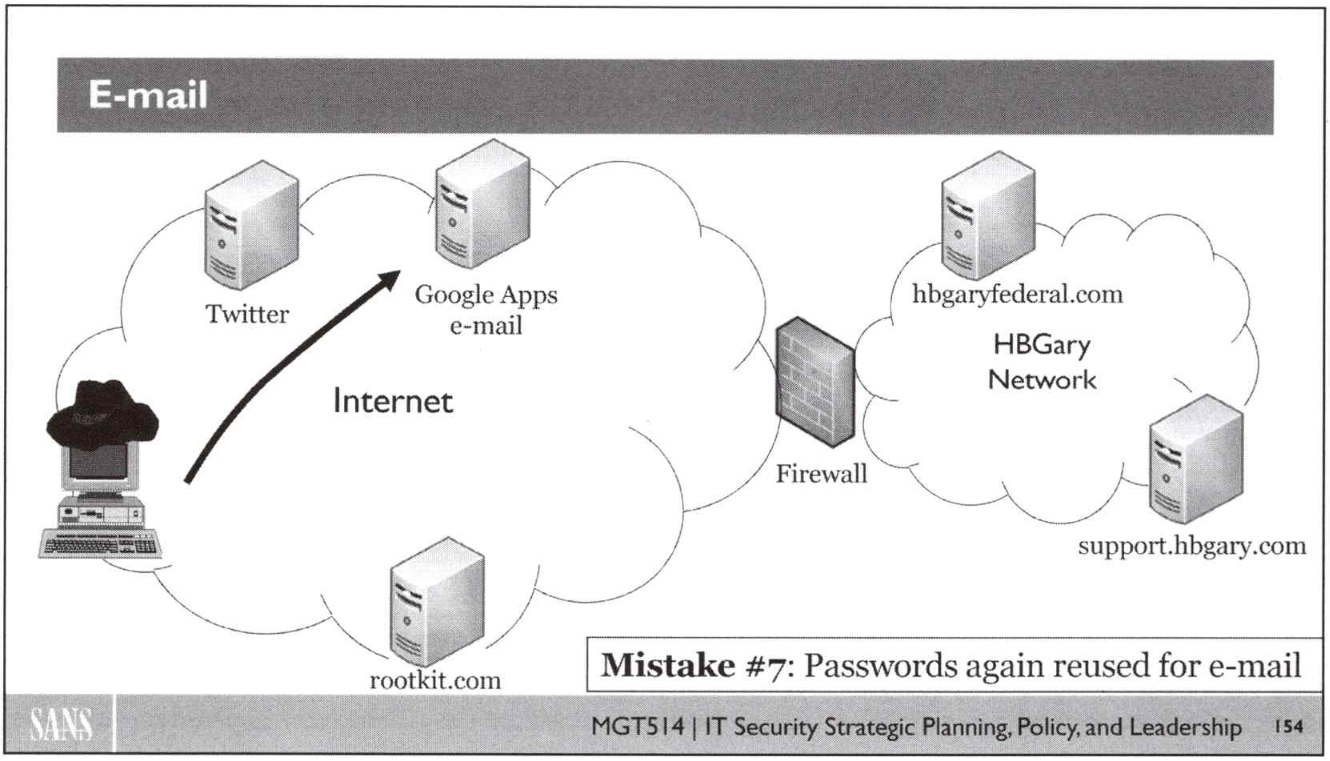
The attackers then discovered that many of these passwords were also used on other systems. Mistake #4 was allowing these weak passwords to be reused across sensitive systems.



By using the COO's same password, the attackers then logged in to the support.hbgary.com system using SSH. Mistake #5 was exposing sensitive SSH functionality on the Internet and protecting it with only a simple password (and not using certificates).

After the attackers logged in, they discovered that the COO's account was just a regular user. To get additional access, they used a local privilege escalation exploit for the Linux server. This was possible only because of Mistake #6: The server was missing a four-month-old patch that would have fixed the vulnerability.

After gaining elevated access, the attackers downloaded gigabytes of research data and backups. As a parting gesture, they then deleted all the data and backups from the server.



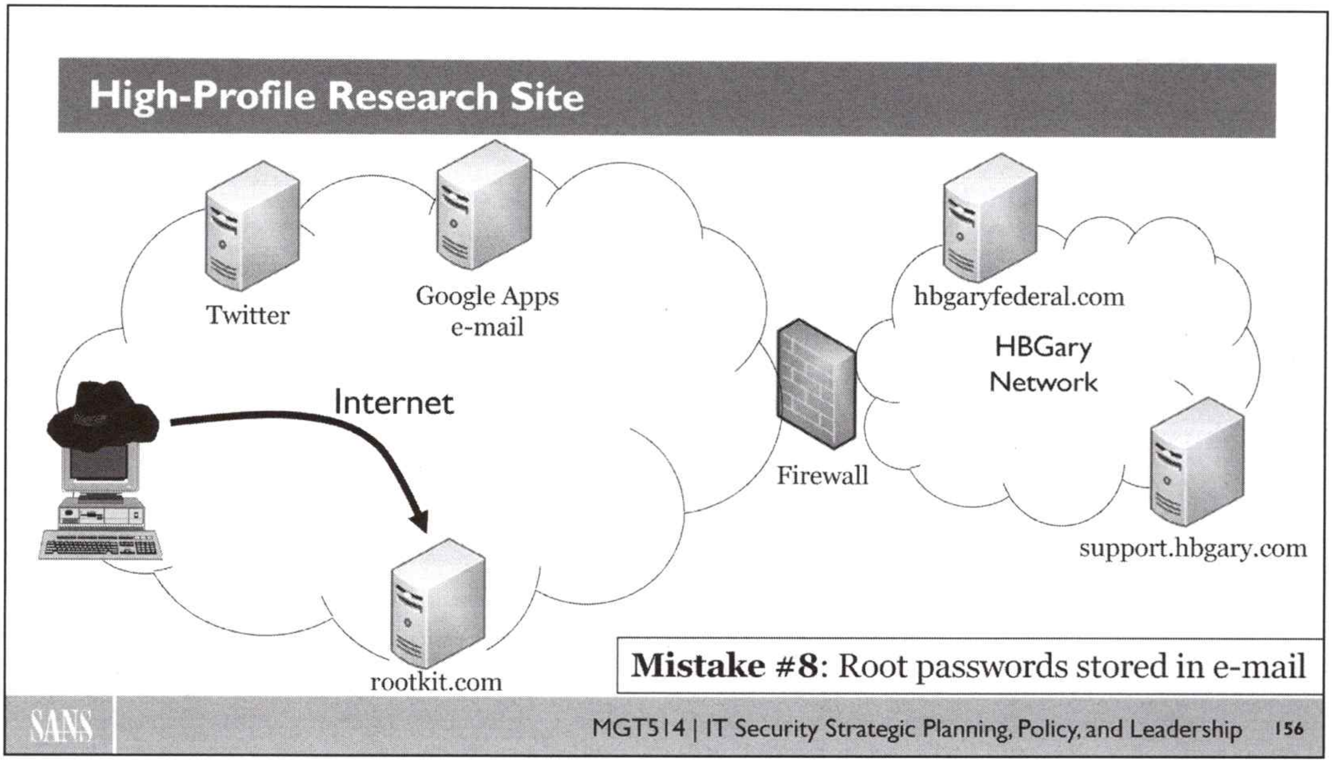
Not satisfied with gaining access and stealing a terabyte of data, the attackers then moved on to other targets. They realized that HBGary was hosting its e-mail using a Google Apps for business account.

Google Apps for E-mail

- Used same password
  - Downloaded HBGary Federal CEO's e-mail
  - But Aaron Barr was also the Google Apps admin!
  - Used to access all other e-mails
  - Also used to reset passwords and send e-mails *as* that person
- Another target
  - Access e-mail of HBGary CEO, Greg Hoglund

The HBGary Federal CEO, Aaron Barr, used the same password for his e-mail that the attackers used to gain access to all of his e-mail communications. It also turned out that, as the CEO, Aaron Barr was also a Google Apps administrator with full access to all corporate e-mail communications. Using this access, the attackers downloaded all 40,000 corporate e-mails and used the administrative console to reset passwords. This allowed them to log in as any user and send e-mails *as* that person.

Using this access, the attackers decided to target HBGary CEO Greg Hoglund.



The attackers knew that Greg Hoglund ran a security research site called rootkit.com. In reviewing his e-mails, they discovered that the root passwords for rootkit.com were sent and stored in e-mail. This was mistake #8.

Info in E-mails

- Sensitive data stored in e-mail
  - Root password for rootkit.com was:
    - `88j4bb3rw0cky88` or `88Scr3am3r88`
  - Someone named Jussi who also had root access
- Attackers had access to Greg Hoglund's e-mail
  - What would you do?

The root passwords for rootkit.com were `88j4bb3rw0cky88` or `88Scr3am3r88`. However, this server was not accessible over the Internet because the firewall was configured to block remote login via SSH.

By reading Greg Hoglund's e-mails, they discovered that someone named Jussi also had root access to the server.

At this point, the attackers decided to utilize some basic social engineering using Greg Hoglund's e-mail account.

Social Engineering

```
From: Greg
To: Jussi
Subject: need to ssh into rootkit

im in europe and need to ssh into the server. can
you drop open up firewall and allow ssh through
port 59022 or something vague?
and is our root password still
88j4bb3rw0cky88 or did we change to
88Scr3am3r88 ?
thanks
```

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 158

The attackers crafted this message to Jussi. It's brilliant in its simplicity. Not only is Jussi inclined to trust this message because (1) it was sent from Greg Hoglund's actual e-mail address, but (2) it also contains some information that presumably only Greg would know (the actual root passwords).

Based on this trust, the attackers asked Jussi to open a port on the firewall to allow SSH access via the Internet.

Can't SSH as root

- Jussi opened up the firewall to accept SSH connections on the specified port
- Reset the password to `changeme123` as requested
- But the attackers still couldn't log in
  - The "root" ID wouldn't let them in
  - They didn't know the user ID!

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 159

Of course, Jussi did just that by configuring the firewall to accept SSH connections on the specified port. He also reset the password to provide access.

However, the attackers still couldn't log in. The "root" user ID was not allowed to sign on. As a result, the attackers did not know the user ID associated with the new password. They could have tried to guess all the potential user IDs, but that could have taken a long time. So, they went back to social engineering via e-mail.

More Social Engineering

```
From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
yes jussi thanks

did you reset the user greg or?

-------------------------------------

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit

nope. your account is named as hoglund
```

What's the user ID?

Here it is!

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 160

The attacker simply asked Jussi what the user ID was. Helpfully, Jussi provided the answer by responding that the user ID was "hoglund."

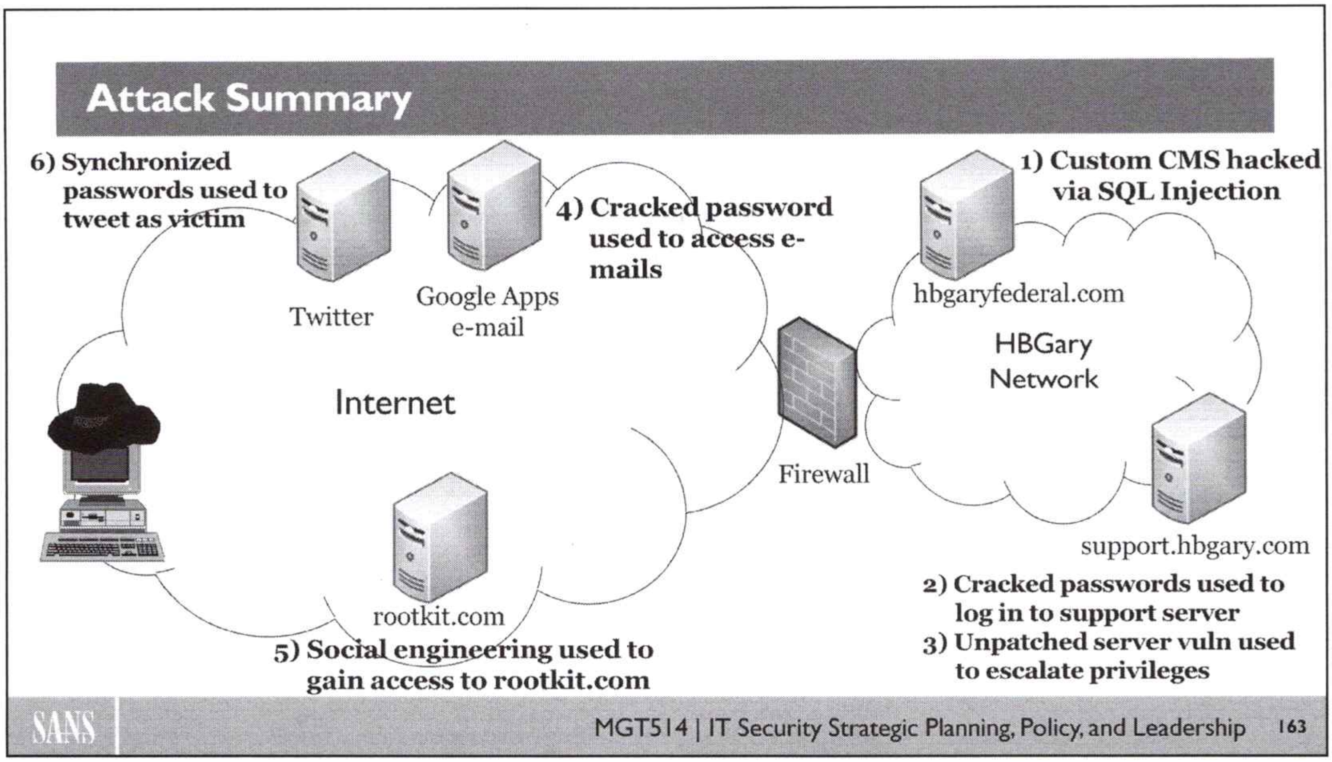
Hack rootkit.com

- Dump database containing e-mails and passwords
  - Again crack MD5 hashes
- Deface website
- Use synchronized passwords to tweet about the compromise

Now, with full root access, the attackers proceeded to dump the database containing e-mails and passwords for rootkit.com, crack additional MD5 password hashes, deface the website, and use additional synchronized passwords to tweet about the compromise.

Twitter Hacked

Screenshot showing Aaron Barr's hacked Twitter account.



In summary, the attackers used a simple SQL Injection vulnerability in a custom CMS system as the initial entry point of compromise. By stealing passwords and cracking them, they were able to log in to a support server and escalate their privileges due to a missing patch. Using these same passwords, the attackers then gained access to all corporate e-mails in the Google Apps for business account for the company. Using this e-mail access, the attackers then used basic social engineering attacks to trick a system administrator into providing root access to an important research system. After stealing 1TB of data, deleting the backup files, and harvesting 40,000 e-mail addresses, the attackers then used the same stolen passwords to log in to Twitter and publicize the attack.

Organized Crime Case

This page intentionally left blank.

Organized Crime

- Criminal Gangs
  - Driven by profit
  - Seek data that can be easily monetized
    - U.S. credit cards are a popular target
    - Magnetic stripe data can be used to create counterfeit cards
  - Run as a business with different specialties
    - Researchers: exploit developer
    - Farmers: maintain botnet and compromised systems
    - Dealers: conduct attacks and steal data
    - Consumers: monetize stolen data, commit fraud, hire money mules

Organized crime groups are driven by profit. They seek data that can be easily monetized. This includes credit card information that can be sold, used to create counterfeit cards, or used to buy physical goods that can then be sold for cash. Many of these criminal gangs are highly organized and run like legitimate businesses.[1] People are hired based on their specialties. Researchers may be hired to actually develop exploits. Farmers are hired to maintain botnets and compromised systems. Dealers conduct attacks and steal sensitive data. Consumers monetize this stolen data, commit fraud, and hire money mules, who ship products purchased with stolen credit cards overseas.[2]

References

[1] http://www.securityweek.com/structure-crybercrime-organization-hackers-have-supply-chains-too

[2] http://krebsonsecurity.com/2014/08/white-label-money-laundering-services/#more-27008

Target Corporation

- One of the largest retail chains in the U.S.
  - Nearly 1,800 stores across the country
- Suffered one of the biggest retail hacks in U.S. history
  - 40 million credit cards stolen
  - 70 million PII records stolen
- Information in this section from Brian Krebs
  - krebsonsecurity.com

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 166

Target Corporation is one of the largest retail chains in the United States. In 2013, it was the victim of one of the largest hacks in history. The hack was first reported by investigative journalist Brian Krebs. Unless otherwise noted, information about the Target hack described in this section comes from his website. [2, 3, 4, 5, 6]

References

[1] http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

[2] http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/

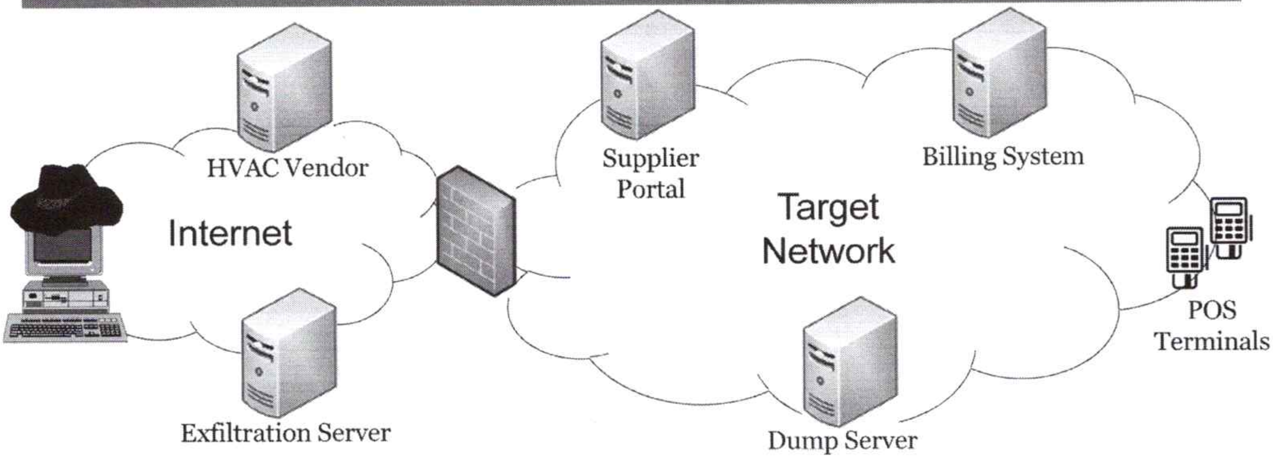
[3] http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/

[4] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[5] http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

[6] http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

Overview



Information based on reporting by Brian Krebs - krebsonsecurity.com

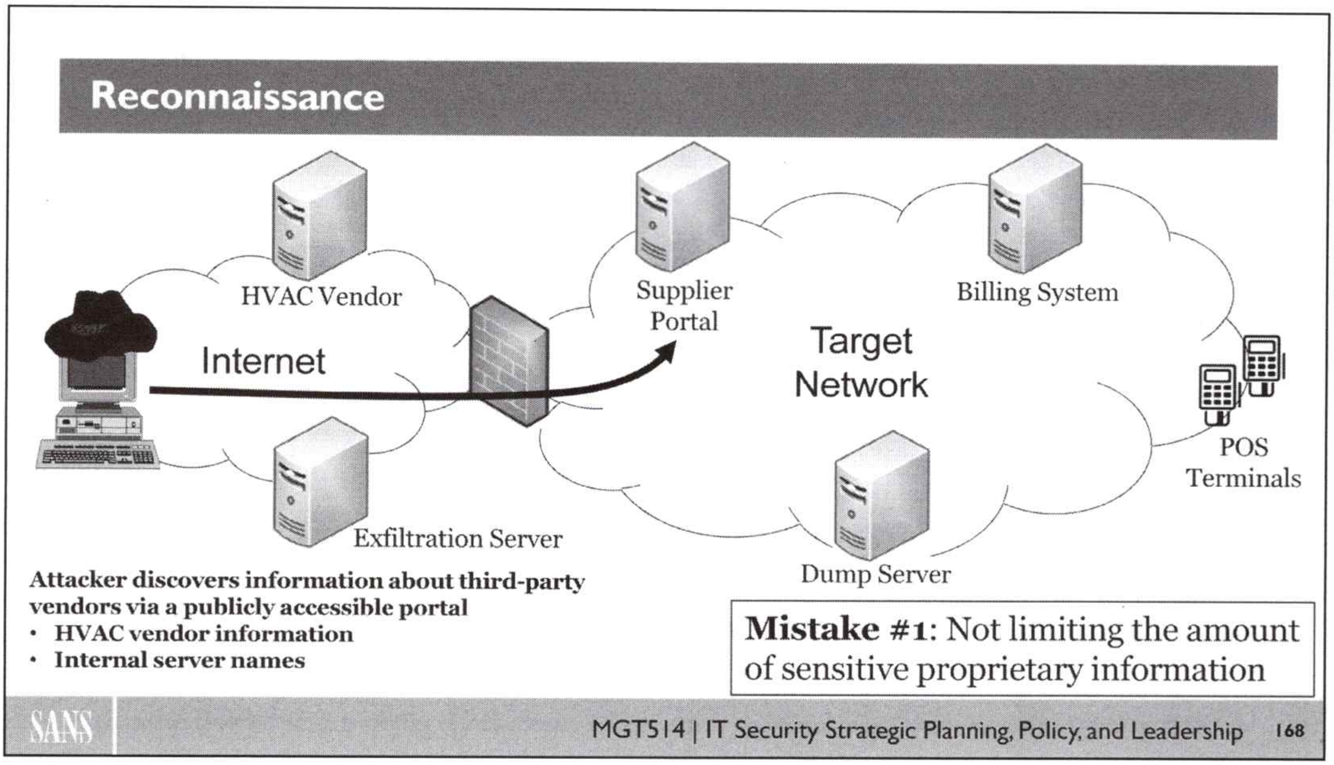
Before we discuss the details of the Target breach, let's start with an overview of the key systems involved in the attack.

Inside the Target network, there were the following systems:

- **Supplier Portal:** This system provides information to vendors who want to do business with Target.
- **Billing System:** Vendors use this system to request payment from Target for services rendered.
- **POS Terminals:** The Point of Sale (POS) systems are located at various Target retail locations.
- **Dump Server:** This internal server, discovered by the attackers, was used as a temporary storage location for stolen data.

Outside the Target network, there were the following systems:

- **HVAC Vendor:** This vendor supplies Target with services related to its heating, ventilation, and air conditioning (HVAC) systems.
- **Exfiltration Server:** These servers were used as the destination for stolen data.

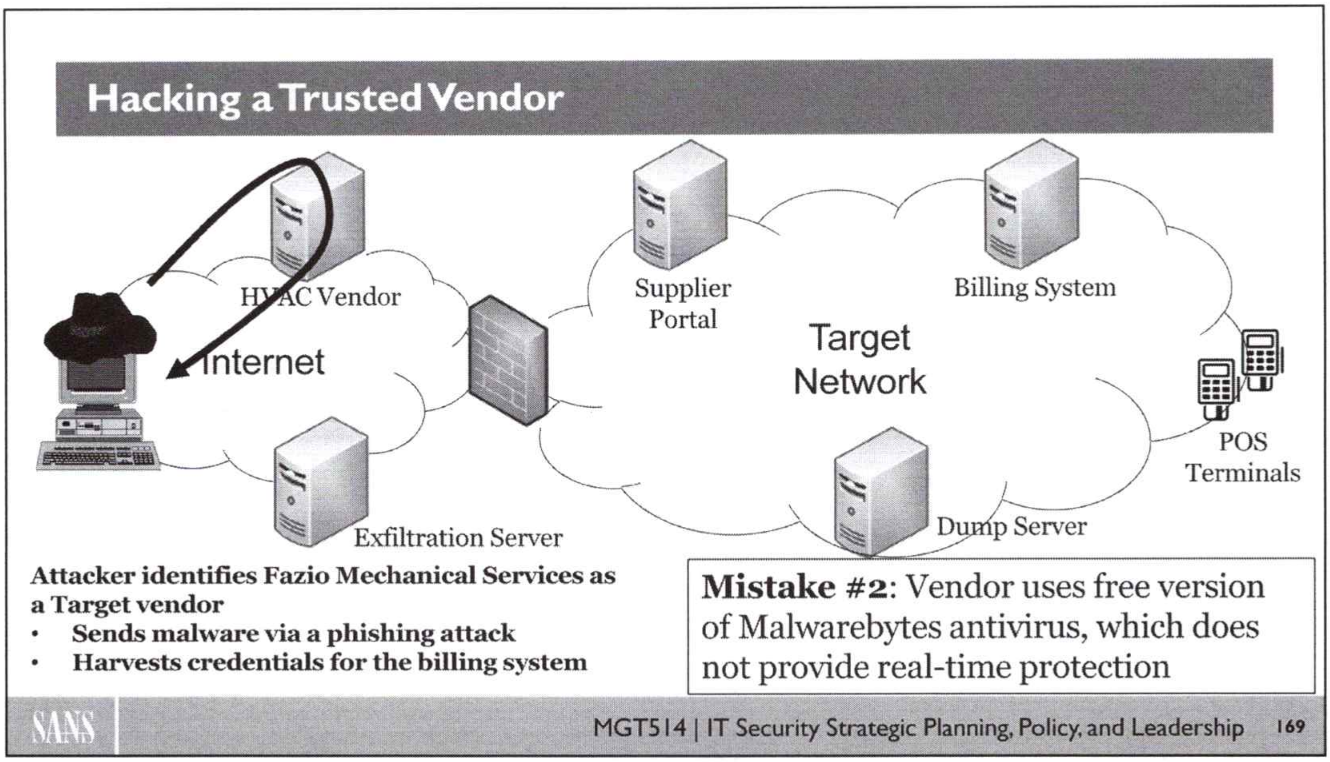


Successful attackers know that reconnaissance is one of the most important phases of an attack. In this case, the attackers discovered information about Target's process for working with third-party vendors via a publicly accessible portal. This portal contained information for new vendors and the process for submitting invoices and work orders. The "supplier downloads" page contained a list of resources for HVAC and refrigeration companies, along with Excel files containing metadata with internal server names. For example, one Excel file showed that a document was recently printed to the server named \\TCMPSPRINT04P. It was later revealed that attackers moved data to an internal server named \\TTCOPSCLI3ACS.

On its own, much of this information appears benign. However, taken as a whole, this information proved to be valuable to attackers in understanding where Target might have some weak spots in its defenses. Mistake #1 was not limiting the amount of sensitive, proprietary information available to the public about important internal process and vendors.

Reference

http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

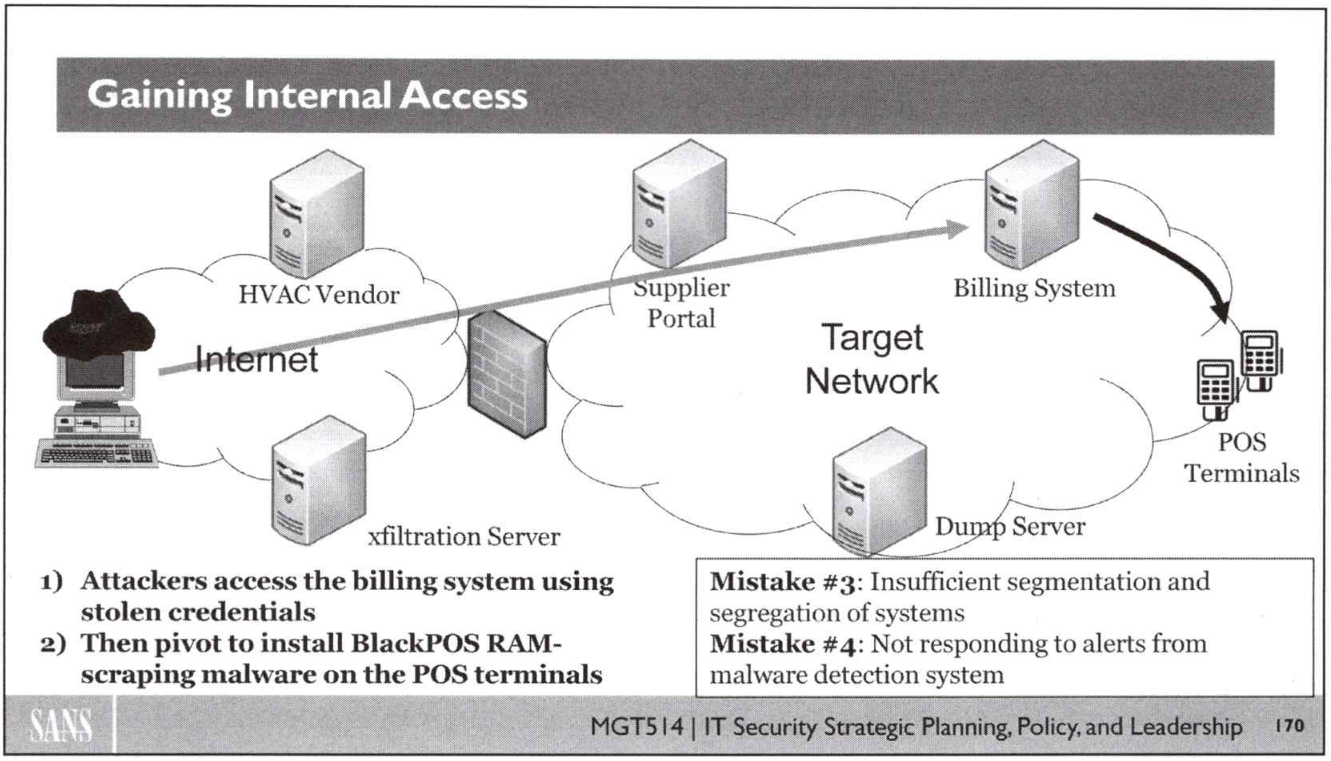


With the information about Target's third-party vendors, the attackers identified Fazio Mechanical Services as a Target vendor. Using a simple phishing e-mail, the attackers sent malware to a Fazio employee and hacked into the vendor's computer systems using the Citadel malware, a password-stealing bot program that is a derivative of Zeus. With this access, the attackers then harvested credentials Fazio used to access the Target billing system.

As a small company, Fazio did not have the resources in place to prevent, detect, or respond to potential cyber intrusions. Mistake #2 actually came from this vendor. It used a free version of Malwarebytes antivirus software, which did not provide real-time protection against any malware attacks.

Reference

http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/



With the stolen credentials, the attackers proceeded to access the billing system running Ariba software. It is unclear how the attackers then moved from the billing system to gain access to the various POS terminals, but that is exactly what they did. Krebs cites a former Target employee who indicated that the billing system may have had more network access than necessary.[1] Mistake #3 was a lack of sufficient segmentation that could have prevented the attackers from moving from the billing system to the in-store networks where the POS terminals were located.

By pivoting to the POS terminals, the attackers were able to install the BlackPOS memory-scraping malware on the terminals themselves. BlackPOS is a specialized piece of malware for POS systems that records all credit and debit cards swiped through the system. At the time, the basic version sold for $1,800; with the full version, which has an option to encrypt stolen data, selling for $2,300.

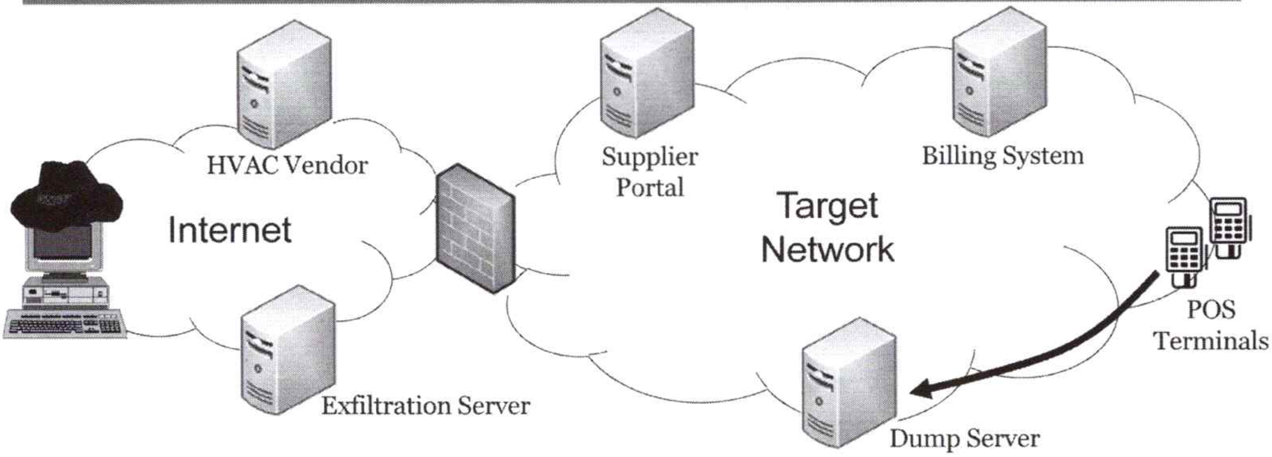
Target actually had advanced malware detection software that detected the BlackPOS malware. Security analysts in India reportedly saw the alerts and informed the Security Operations Center (SOC) in the United States.[2] However, Mistake #4 was not responding appropriately to alerts from the malware detection system.

References

[1] http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

[2] http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Storing Stolen Data



Attackers store data on internal dump servers
- **Using default Best1_user account for Performance Assurance software by BMC**

Mistake #5: Not deleting or modifying default accounts

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 171

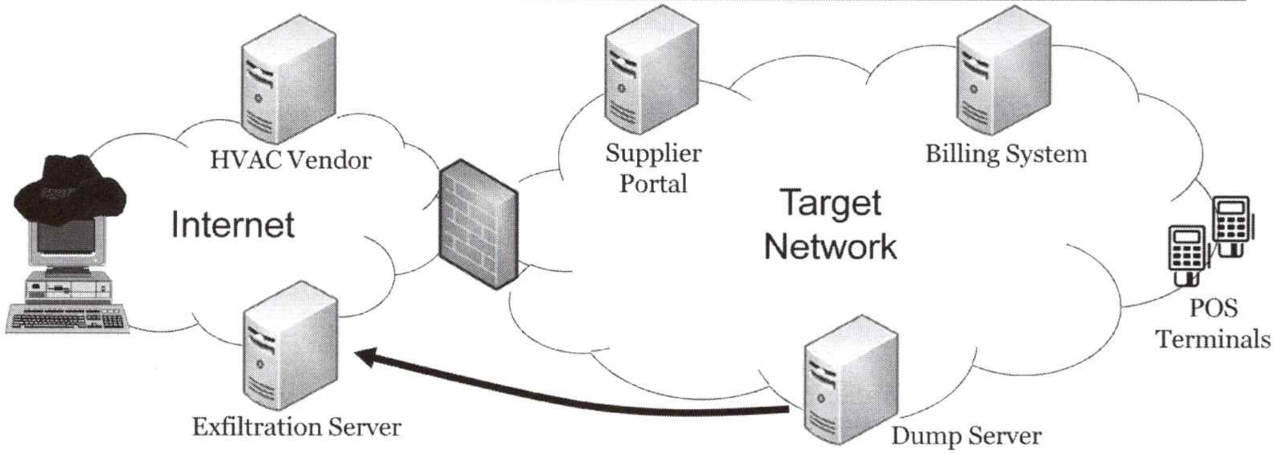
Now that the attackers were stealing millions of credit cards using the malware installed on the POS terminals, they needed a place to temporarily store this information. This is when they discovered an internal Windows share at 10.116.240.31. Analysis of the Target malware revealed that attackers were connecting to this share with a user ID of "Best1_user" and password of "BackupU$r."[1] This user ID indicated that the server was running Performance Assurance for Microsoft Servers from BMC Software. According to BMC's product documentation, the "Best1_user" was an administrative-level account that should never be used to log on to the system because it was not part of any Windows groups. The password was essentially hard-coded. We know this because: "Perform Technical Support does not have the password to this account and this password has not been released by Perform Development. Knowing the password to the account should not be important as you cannot log into the machine using this account. The password is known internally and used internally by the Perform agent to assume the identity of the 'Best1_user' account."

Mistake #5 was not being able to delete or modify default accounts to a system used by attackers to temporarily store stolen data.

Reference

http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/

Stealing the Data



Attackers exfiltrate 11GB of data via FTP

- **To servers in Russia, Brazil, and Miami**

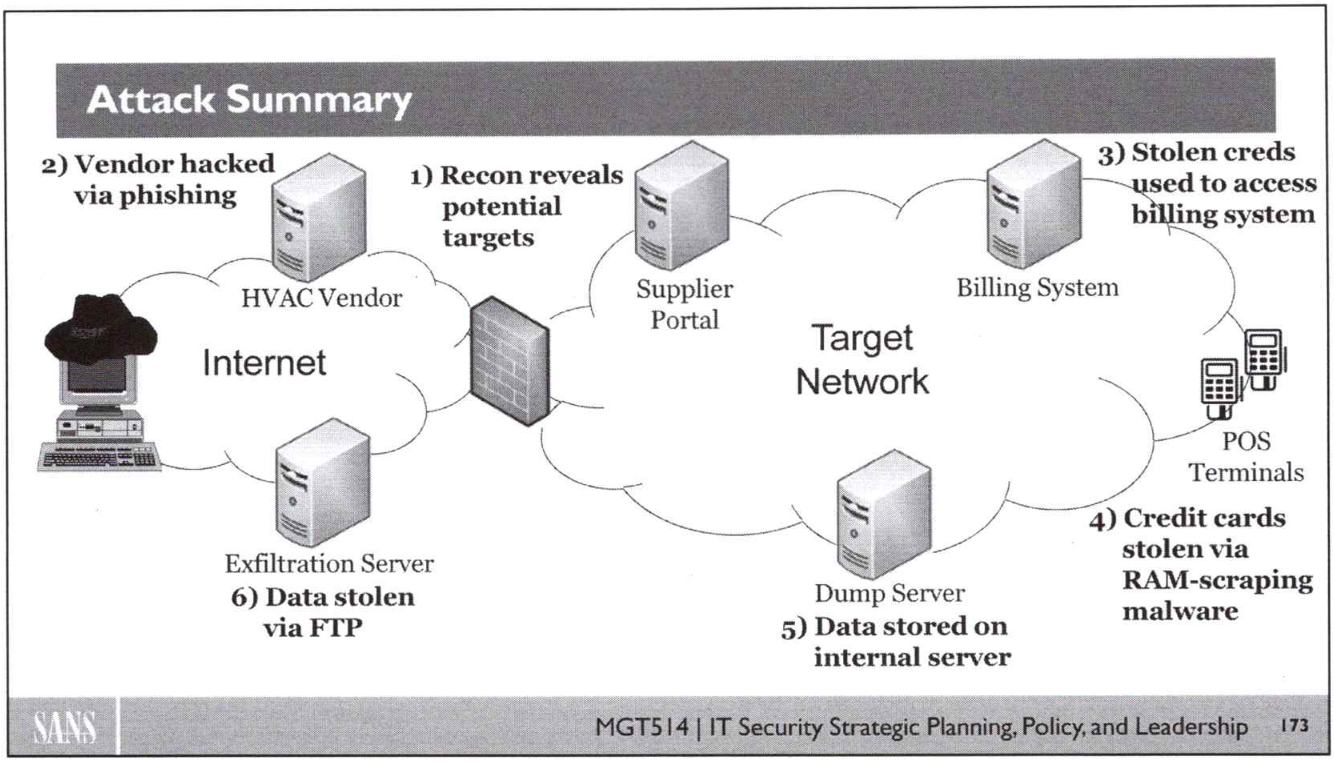
Mistake #6: Not blocking unauthorized outbound data transfers and connections

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 172

With the stolen data sitting on the internal dump server, the attackers then proceeded to exfiltrate 11 gigabytes[1] of cardholder information via FTP to servers in Russia, Brazil, and Miami. Mistake #6 was not being able to detect and then block this unauthorized data transfer.

Reference

http://www.seculert.com/blog/2014/01/pos-malware-targeted-target.html



In summary, attackers started by gathering publicly available information about Target's third-party vendors. This reconnaissance revealed proprietary information that helped attackers compromise an HVAC vendor used by Target. After stealing credentials from the HVAC vendor, the attackers logged on to the Target billing system and then pivoted to install malware on POS terminals to steal credit card data. This information was stored temporarily on an internal dump server and then exfiltrated to external servers via FTP.

Attacker Motivations

Motivation	Description
Espionage	State spying or industrial espionage for competitive advantage
Fear	Use of fear or duress
Financial	Theft of sensitive data for financial or personal gain
Fun	Activities conducted for fun, curiosity, or pride
Grudge	Retaliation based on a grudge or personal offense
Ideology	Actions based on ideology or in protest of a cause
Convenience	Actions conducted out of convenience or expediency
Other	"Some men just want to watch the world burn."

This slide lists this attacker motivations defined in the VERIS framework. It is important to understand why attackers would want to target your organization. In some cases, there may be multiple motivations. In other cases, you may not be able to determine why you were targeted. This conversation between Bruce Wayne and his butler Alfred Pennyworth from the movie *The Dark Knight* illustrates this point:

- **Bruce Wayne:** Criminals aren't complicated, Alfred. Just have to figure out what he's after.
- **Alfred Pennyworth:** With respect, Master Wayne, perhaps this is a man that *you* don't fully understand, either. A long time ago, I was in Burma. My friends and I were working for the local government. They were trying to buy the loyalty of tribal leaders by bribing them with precious stones. But their caravans were being raided in a forest north of Rangoon by a bandit. So, we went looking for the stones. But in six months, we never met anybody who traded with him. One day, I saw a child playing with a ruby the size of a tangerine. The bandit had been throwing them away.
- **Bruce Wayne:** So why steal them?
- **Alfred Pennyworth:** Well, because he thought it was good sport. Because some men aren't looking for anything logical, like money. They can't be bought, bullied, reasoned, or negotiated with. Some men just want to watch the world burn.

Reference

http://m.imdb.com/title/tt0468569/quotes?qt=qt0507146

Section Summary

- Reviewed two cases of real-world attacks
  - To understand the tactics and motivations of two common threat actors
- Other threat actors have varied goals and motivations
  - Important to keep them in mind as you plan your defenses
    - Asset analysis
    - Threat analysis

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 175

In this section, we reviewed two cases of real-world attacks to understand the tactics and motivations of two common threat actors. It's important to keep these threat actors in mind as you plan your defenses. In the upcoming sections, we will discuss Asset Analysis and Threat Analysis. An understanding of attacker motivations and goals will be important to frame those discussions.

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 1

- Background
  - About This Course
  - Need for Strategic Planning
    - Exercise #1: Case Scenario
- Understand the Business
  - Vision & Mission
    - Exercise #2: Mission Statement
  - Stakeholder Management
  - PEST Analysis
    - Exercise #3: PEST
  - Business Strategy
- Understand the Threats
  - Threat Actors
    - Attack case studies
  - *Asset Analysis*
    - Exercise #4: Attacker Motivation
  - Threat Analysis
    - Exercise #5: Intrusion Kill Chain

This page intentionally left blank.

Goals of This Section

- Discuss different types of assets
  - What is most valuable to your organization?
    - What is most critical to the mission?
  - What is most valuable to the attacker?
    - What does the attacker want to accomplish?

A key first step of any security program is to identify your key business assets. It's no accident that the first two Critical Security Controls are conducting an inventory of authorized and unauthorized devices and software.

In this section, we will discuss different types of assets and what may be most valuable to your organization. This is informed by an understanding of what is most important to the mission and vision of the organization. By extension, if something is valuable to you, it will likely also be valuable to attackers. Depending on the attackers' motivation, what they want to accomplish, they may want to target different assets.

Reference

https://www.sans.org/critical-security-controls/

Tangible Assets

- Cyber action can have significant kinetic impact in the physical world
  - Must understand key physical assets of the org
- Critical infrastructure is connected to all aspects of society:
  - Power plants
  - Hospitals
  - Transportation
  - Water treatment facilities
  - Financial
  - Retail
  - Residential

As information security professionals, we are primarily focused on protecting digital assets. However, it is important to keep in mind that cyber action can have significant kinetic impact in the physical world. The Stuxnet worm[1] is a prime example of this. It was designed to attack the programmable logic controllers (PLCs) used in Iranian nuclear facilities. By changing the speeds of centrifuges used to process uranium, Stuxnet reportedly damaged one-fifth of Iran's nuclear centrifuges. Similarly, cyber attacks against Industrial Control Systems (ICS) and SCADA systems used to manage power plants could have large impacts on the physical world.

If your organization has important tangible assets such as buildings, data centers, hospitals, transportation infrastructure, water treatment facilities, or even residential centers, it is important to consider how cyber attacks could disrupt your business. As the virtual and physical worlds converge with the Internet of Things (IoT), this becomes even more relevant. For example, Apple iBeacon[2] is an indoor positioning system that provides precise location information. It is being deployed at retail and other outlets to more accurately track customers and provide personalized service. It will be important to consider the security implications of such systems as IoT continues to be more widely adopted.

Additionally, incorporating alerts from physical security systems into your information security monitoring capability will help identify anomalous activities.

There are a number of reasons that information security has to stay abreast of the key tangible assets of an organization.

References

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

[2] http://en.wikipedia.org/wiki/IBeacon

Intangible Assets

- Customer data
  - PII, credit cards, mailing lists
- Employee data
  - PII, HR data, payroll, e-mails
- Intellectual property
  - Patents, trademarks, copyrights, trade secrets
- Business proprietary
  - Business processes, contracts, M&A activity

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 179

Organizations have many different types of intangible assets:

- **Customer data:** Includes personally identifiable information (PII), credit cards, and contact information. This contact information can be one of the most valuable assets that an organization has. Mailing lists are still one of the most effective ways to inform customers of new products or services. Competitors would love to get access to current and potential customer lists.

- **Employee data:** Includes personal information, human resource data such as salary and benefits, and even internal e-mail communications.

- **Intellectual property:** Includes any "creation of the mind," such as music, literature, source code, and courseware. These inventions are protected by intellectual property laws and include patents, trademarks, copyrights, and trade secrets.

- **Business proprietary information:** Includes business processes, contracts, mergers and acquisitions activity, and even general business know-how.

Employee Example – Payroll Theft

- Professor at Western Michigan University
  - Ray Cool had his paycheck stolen
- Attackers accessed online HR portal
  - Changed the bank routing information
  - Deposit was made directly into an attacker-controlled account
  - Some attackers even change the number of deductions to avoid detection

This slide relates an example, not of employee data theft, but of employee payroll theft. Ray Cool, professor at Western Michigan University, thought something was wrong when his bank showed his paycheck direct deposit to be only $11.08. Attackers had gained access to his online HR account, changed the bank routing information, and had his pay of $1,581.00 direct deposited to a separate account in Utah.[1, 2]

Unfortunately, this type of attack is common, with more sophisticated attackers avoiding detection by siphoning off smaller amounts of money and changing the number of payroll deductions to make it appear that the remaining direct deposit did not change.

This example highlights that it is not only data that needs to be protected but also key systems. These systems are also important intangible assets for the organization.

References

[1] http://www.computerworld.com/article/2475732/cybercrime-hacking/hacker-steals-teacher-s-direct-deposit-paycheck--university-says-too-bad-so-sad.html

[2] http://www.mlive.com/news/kalamazoo/index.ssf/2014/02/hackers_stole_western_michigan.html

Patent Example – Cenzic

- Cenzic
  - Web application scanning vendor
  - Granted patent for "Fault injection methods and apparatus"
    - Patent No. 7,185,232
- Highly controversial patent
  - "Method of creating a fault-inducing transaction"
  - How web app testing has always been conducted
- Has since been licensed by other vendors with web application scanning products

Cenzic was a web application scanning vendor that was acquired by Trustwave. One of its patents involved a "method of creating a fault-inducing transaction." Basically, the patent was for sending bad data to a web application to make something bad or unexpected happen. In other words, it was a patent for how application testing has always been conducted! This is what made it such a controversial patent.

Despite the fact that it was arguably not a new invention, it has since been licensed by a number of other vendors with web application scanning products.

Reference

http://www.networkworld.com/article/2228588/opensource-subnet/the-curious-case-of-patent-232.html

Trade Secret Example – Theft of RC4

- RC4
  - Commonly used stream cipher
  - Designed by Ron Rivest
- Trade secret
  - Owned by RSA Security
  - Did not patent because it can be used in other cryptographic implementations
- Stolen and leaked to a mailing list
  - Immediately became public domain
  - Drastically reducing its value to RSA

RC4 is a commonly used stream cipher designed by Ron Rivest for RSA Security. RSA did not patent it because it can be used in other cryptographic implementations like WEP and WPA for wireless communications. It was initially a trade secret, but in September 1994, the algorithm was anonymously posted to the Cypherpunks mailing list. From there, it was published on many other websites and immediately became public domain. Because the algorithm is known, it is no longer a trade secret.[1, 2]

The name "RC4" is trademarked, so RC4 is often referred to as "ARCFOUR" or "ARC4" (meaning Alleged RC4) to avoid trademark problems.

RSA Security has never officially released the algorithm.

References

[1] http://en.wikipedia.org/wiki/RC4

[2] https://blogs.rsa.com/news-media-2/rsa-response/

Business Proprietary Example – Aloha Airlines

- Mesa Airlines
  - Competitor to Aloha Airlines
  - Met with Aloha executives to consider a partnership
- Instead formed Go!
  - By stealing proprietary route and cost information from Aloha
- Aloha filed suit
  - Won $2 million and 10% of Mesa stock
  - But still went bankrupt

Aloha Airlines was one of the leading airlines in Hawaii. One of its competitors, Mesa Airlines, approached Aloha about a partnership. After initial rounds of due diligence, Mesa stole Aloha's proprietary route and cost information and, instead of partnering, formed Go! airlines.[1, 2]

Aloha filed suit and won $2 million and 10% of Mesa stock, but the company still went bankrupt (it still does business as a commercial carrier).

This example highlights the importance of business proprietary information and the need for information security teams to understand what is valuable to the business.

References

[1] http://www.bizjournals.com/pacific/stories/2006/10/09/daily61.html?jst=b_ln_hl

[2] http://www.airlinepilotforums.com/regional/33956-mesa-air-group-settles-aloha-lawsuit.html

Example – Intangible Assets

Customer Data	Employee Data	Intellectual Property	Business Proprietary
Credentials	Personally Identifiable Information (PII)	Patents	Financial information
Personally Identifiable Information (PII)	HR information	Copyrights	Contracts
Protected Health Information (PHI)	Payroll data	Trademarks	Mergers & Acquisitions Data
Payment Card Information	Tax information	Trade secrets	Customer mailing lists
		Research & Development	E-mail communications
		Source code & systems	

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 184

This slide shows a simple summary of the different types of intangible assets that the security team might have to protect.

Asset Analysis Example

- You have been hired by a mid-size healthcare provider to
  - Brief senior executives (CEO, General Counsel, etc.) on the healthcare threat landscape
- You decide to start with an understanding of the organization's critical assets
  - Mapping them to importance and attacker motivations

You recently quit a comfortable day job to start your own information security consulting company. It's Monday afternoon on your first official day of operation when you get a call from a mid-size healthcare provider. The company wants you to create a strategic plan for its information security program. However, as a first step, it wants your help explaining to the CEO and General Counsel why someone might even want to target the organization. After reviewing the vision and mission of the organization, you decide to start by developing an understanding of its critical assets and how they relate to the evolving threat landscape.

Example – Healthcare Assets

Asset	Description	Business Importance Impact	Attacker Motivation Likelihood
PHI (Protected Health Information)	Organized crime uses PHI to commit healthcare fraud Nation states target sensitive personal data to profile targets Insiders may leak or mistakenly use sensitive data	High	Financial Espionage Grudge Convenience
PII (Personally Identifiable Info)	Organized crime uses PII to commit healthcare fraud Nation states target sensitive personal data to profile targets Insiders may leak or mistakenly use sensitive data	High	Financial Espionage Convenience
PCI (Cardholder data)	Organized crime easily monetizes stolen cardholder information	High	Financial
Research data	Competitors and nation states utilize intellectual property to advance their own programs	High	Espionage
Key systems	Attackers target key systems like the Member Portal, Health Information Exchange (HIE), Health Insurance Exchange (HIX), Claims Systems for political/economic advantage or to cause business disruption	High	Financial Espionage Ideology, Fun

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 186

This slide lists key assets that are typically found in healthcare organizations.

Protected Health Information (PHI)

PHI is extremely valuable because it offers many opportunities for financial, credit, and medical fraud. The black market value of stolen healthcare credentials is reported to be ten times more than a stolen credit card,[1] whereas a stolen medical record is reported to be worth up to $50.[2] It shouldn't be a surprise that organized crime is becoming more interested in the theft of electronic health records. Additionally, nation states are reportedly targeting healthcare records to steal the personal information of military and government workers to profile targets.[3] Also, employees and other insiders have accidentally disclosed sensitive health records.

Personally Identifiable Information (PII)

Healthcare organizations hold a wealth of personal information about their members. Sometimes, this data is not appropriately protected, as was evidenced in the Sutter Health data breach,[4] where an unencrypted desktop computer was stolen containing the personal information of over 4 million patients. In this case, the data was not appropriately protected by the company due to convenience and/or negligence. However, attacker motivations would be much more malicious.

Payment Card Industry (PCI)

Many healthcare organizations rely on credit cards to sell prescriptions, process co-pays and premiums, and sell food in the cafeteria and flowers in the gift shop. Much like retail companies, point of sale (POS) terminals are accessible at various locations to process payments. This is a big target for organized crime groups that want to monetize large amounts of stolen cardholder data.

Research Data

Some healthcare organizations and research hospitals are unique in that they have large amounts of research data from patient interactions and research studies. Pharmaceutical companies also have drug and clinical trial information that can be very valuable to competitors and nation states that want to advance their own programs.

Key Systems

Healthcare organizations rely on key systems like Health Information Exchange (HIE) to share patient records with other organizations to provide better care and Health Insurance Exchange (HIX) to open up new channels to sell coverage. Attackers may target these systems to steal data or even just to cause business disruption due to a disagreement over the way care is delivered.

Reference

[1] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[2] http://hipaahealthlaw.foxrothschild.com/2015/03/articles/privacy/hacked-health-records-prized-for-their-black-market-value/

[3] http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

[4] http://www.healthcareitnews.com/news/1b-suit-filed-against-sutter-health-over-data-breach

Exercise 1.4 – Attacker Motivation

Estimated Time: 10 Minutes

- Goal of this exercise
  - Identify key assets at your organization
  - Map them to attacker motivations
- On your own, write down
  - Important assets that are unique to your company or industry
    - Key business assets
  - Why attackers would want this information
    - What they would do with this asset

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 188

The goal of this exercise it to identify some of the key assets at your organization and think about why attackers would want this data.

On the next page, write down (1) assets that are unique to your company or industry and (2) what attackers would want with this asset.

Asset Analysis Worksheet

Asset	Description	Business Importance Impact	Attacker Motivation Likelihood

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 189

Use this worksheet to write down the following:

- Key assets in your organization
- Description of the asset and its value to attackers
- Ranking of business importance
- Motivation of attackers

In Summary

- Understanding critical business assets
  - Enables you to have meaningful conversations with business leaders
  - Creates an understanding of attacker motives
  - Helps determine how assets should be protected

Understanding critical business assets is an extremely important step in the strategic planning process. Without an understanding of what is important to the business, you will not be able to do the following:

- Have meaningful conversations with business leaders
- Understand why attackers would target your organization
- Develop appropriate defenses to mitigate risk associated with those assets

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 1

- Background
  - About This Course
  - Need for Strategic Planning
    - Exercise #1: Case Scenario
- Understand the Business
  - Vision & Mission
    - Exercise #2: Mission Statement
  - Stakeholder Management
  - PEST Analysis
    - Exercise #3: PEST
  - Business Strategy
- Understand the Threats
  - Threat Actors
    - Attack case studies
  - Asset Analysis
    - Exercise #4: Attacker Motivation
  - *Threat Analysis*
    - Exercise #5: Intrusion Kill Chain

This page intentionally left blank.

Goals of This Section

- Understand how attackers work
  - By applying the Intrusion Kill Chain
- Learn how threat intelligence can
  - Create a feedback loop that can be used to disrupt attackers

In previous sections, we discussed *why* attackers want to target your organization and *what* assets they might be most interested in stealing. In this section, we discuss *how* attackers work and the steps that they take to conduct attacks by analyzing the Intrusion Kill Chain. You will also learn how Cyber Threat Intelligence can be used to better understand attackers and disrupt their attacks.

Risk Analysis

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$
$$\text{Risk} = \text{Vulnerability} \times \text{Threat}$$

- Security has traditionally focused on the vulnerability component of risk
  - Conventional tools like IDS, Antivirus, etc., are focused on vulnerabilities that inform the impact
- Risk cannot be fully understood without considering the threat component of risk
  - Analysis of threat actors and their motivations informs the likelihood

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 193

Risk is commonly defined as the combination of the impact and likelihood of an event. Another way to look at risk is to analyze the vulnerability (security vulnerabilities in your systems) and threat (attacker motivations) components.

Security has traditionally focused on the vulnerability component. Because critical vulnerabilities increase risk, much work has been done to mitigate and prevent vulnerabilities using tools like Intrusion Detection and Prevention Systems (IDS/IPS) and Antivirus as well as patching of important issues. This is certainly a good and valuable approach to reduce risk. However, many organizations struggle to keep up with zero-day exploits and unpatched systems.

To reduce risk, we must also focus on the threat component of risk. By analyzing threat actors and their motivations, we can reduce the likelihood of successful attacks.

Threat Analysis

- To mitigate the threat component of risk, we need to
  - Acknowledge that traditional incident response methodology assumes an intrusion has already occurred
  - Understand the Tactics, Techniques, and Procedures (TTPs) of threat actors
  - Utilize these Indicators of Compromise (IOC) to create intelligence-driven computer network defense
- Intrusion Kill Chain described in a seminal paper
  - "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain"
    - By Hutchins, Cloppert, and Amin

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 194

Traditional incident response methodology assumes that an intrusion has already occurred. How can the likelihood of successful intrusion be decreased, thereby reducing overall risk?

By understanding the Tactics, Techniques, and Procedures (TTPs) of threat actors, various Indicators of Compromise (IOCs) can be identified to create "intelligence-driven computer network defense." This approach was described in a seminal paper by Hutchins, Cloppert, and Amin[1] and serves as the foundation for much of the modern work on threat analysis.

Reference

[1] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

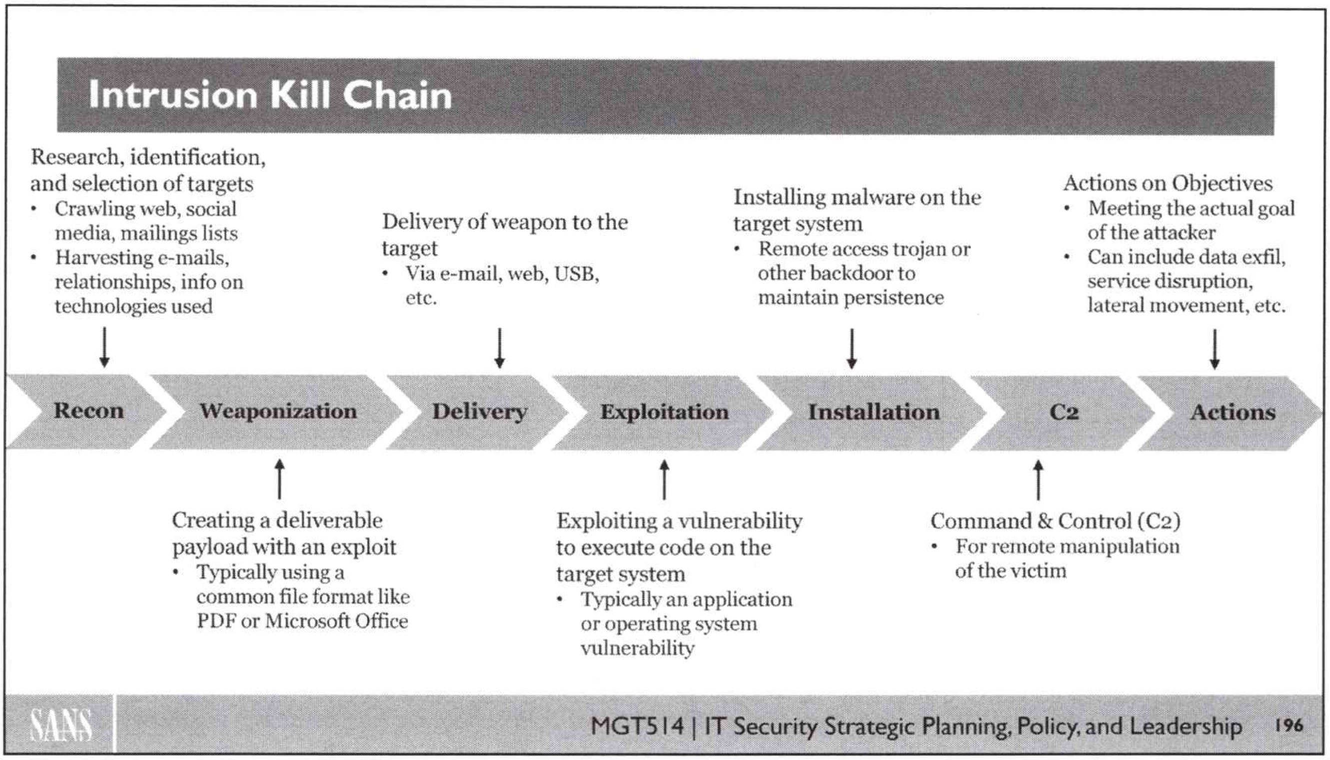
Intrusion Kill Chain

- Attackers must progress through each phase of the chain to achieve their goal
  - Breaking just one link in the chain disrupts the adversary
  - By understanding the attackers' perspective, defenders can gain an edge
    - Against even the most sophisticated attackers
    - Protect against zero-day exploits
      - Which is just one link in the chain

Recon → Weaponization → Delivery → Exploitation → Installation → C2 → Actions

The Intrusion Kill Chain defines a seven-step process that attackers follow to achieve their goal. By breaking just one link in the chain, breaking just one step in the attack process, the defender can disrupt the adversary and stop the attack. Understanding in detail the attackers' perspective and approach enables defenders to gain an advantage against even the most sophisticated attackers. This means that you can more easily protect against zero-day exploits, which are just one phase of the overall Kill Chain (that is, Exploitation), by identifying and blocking attackers before they ever reach their ultimate goal in the final Actions step.

Note that "Intrusion Kill Chain" is also referred to as the "Cyber Kill Chain." However, this second term is trademarked by Lockheed Martin.



The seven steps of the Intrusion Kill Chain are as follows:

Reconnaissance

In this phase, the attackers conduct research and identify targets. This can be accomplished by searching websites, social media, and mailing lists to harvest information about relationships and technologies used by the target.

Weaponization

At this point, the attackers create a payload that can be delivered to the target. This is typically in PDF or Microsoft Office format and will leverage some of the information identified in the previous step to personalize the payload.

Delivery

In this phase, the attackers deliver the payload to the target typically via e-mail or the web. In some cases, it may also be delivered via USB.

Exploitation

Once the payload is delivered, it will be executed to exploit a vulnerability on the target system.

Installation

By gaining access via an exploited vulnerability, the attackers can now install malware on the system to maintain persistence.

Command & Control (C2)

The backdoor allows for command and control capabilities that enable remote manipulation by the attackers.

Actions on Objectives

Now, with access to the target system, the attackers can accomplish their ultimate goal. This can include data exfiltration, service disruption, or even lateral movement to other areas of the organization.

Lockheed Martin Case Study

- Case study is taken from Lockheed Martin paper
  - By Hutchins, Kloppert, and Amin
- Over three weeks, Lockheed Martin detected three similar intrusion attempts
  - E-mail sent to five users
  - From an individual claiming to be an employee of a well-known aeronautics conference
  - E-mail contained a malicious PDF with legitimate content
    - First two attempts contained exploits for known but unpatched PDF vulnerabilities
    - The third attempt contained zero-day PowerPoint exploit

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 198

To illustrate how the Kill Chain works, we'll review the case study presented in the paper by Hutchins, Cloppert, and Amin.[1]

Over three weeks, Lockheed Martin detected three very similar intrusion attempts. All three intrusions attempted to gain access by delivering a malicious e-mail to five different users at the company. The attackers had personalized these e-mails so that they appeared to contain valid communications in which the targeted users would be interested. For example, one e-mail came from an individual claiming to be an employee of a well-known aeronautics conference in which the targeted user might be interested. These e-mails contained malicious PDF documents with this legitimate content. However, the malicious PDFs contained exploits for known but unpatched PDF vulnerabilities. A third e-mail even contained a previously unknown zero-day PowerPoint exploit.

By analyzing various Indicators of Compromise (IOC), the Lockheed Martin team was able to successfully repel these attacks.

Reference

[1] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Case Study Indicators of Compromise

Phase	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	Recipient List #1 Benign File: tcnom.pdf	Recipient List #2 Benign File: MDA_Prelim_09.pdf	Recipient List #3 Benign File: new.ppt
Weaponization	Trivial encryption algorithm		
	Key #1		Key #2
Delivery	Subject: AIAA Technical Committees E-mail Body #1	Subject: 7th Annual U.S. Missile Defense E-mail Body #2	Subject: Celebrities Without Makeup E-mail Body #3
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Exploitation	CVE-2009-0658 [shellcode]		[PPT zero-day] [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp		
C2	202.abc.xyz.7 [HTTP request]		
Actions	N/A	N/A	N/A

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 199

This slide shows the Indicators of Compromise for the three different intrusion attempts against Lockheed Martin mapped to the seven phases of the Intrusion Kill Chain:

Reconnaissance

In this phase, the attackers gather information about potential targets and search the Internet for valid PDF files that can be used in the attack. In all three intrusion attempts, the attackers utilized different recipient lists and originally benign files.

Weaponization

In this phase, the attackers modify the benign files to create a payload with an exploit. In the first two intrusion attempts, the attackers utilized the same encryption key but changed to a different key in the third attempt. However, an important element noted by the Lockheed Martin team was the repeated use of the same trivial encryption algorithm across all three intrusion attempts. This was one of the valuable Indicators of Compromise that helped the team detect and block the attacks.

Delivery

In all three intrusions, the attackers attempted to use e-mail to deliver the weaponized PDFs. In all three cases, the attackers utilized different e-mail subject lines and body text. However, in two of the cases, the same target user and source IP addresses were utilized. This information provided some clues that the e-mails were actually part of an attack.

Exploitation

In the first two intrusion attempts, the attackers utilized the same known but unpatched PDF vulnerability (CVE-2009-0658). In the third attempt, the attackers utilized a previously unknown zero-day PowerPoint vulnerability.

Normally, this would result in a successful attack. But, because other Indicators of Compromise retrieved from the Weaponization and subsequent Installation and C2 phases helped identify these e-mails as actual intrusions, even the zero-day vulnerability was successfully blocked.

Installation

All three intrusions attempted to install the same malware (fssm32.exe, IEUpd.exe, IEXPLORE.hlp) on the target system. This was an obvious Indicator of Compromise that helped detect and block the attack.

Command & Control (C2)

All three intrusions also attempted to have the malware connect back to the same command and control server (202.abc.xyz.7) over HTTP. This was another obvious Indicator of Compromise.

Actions on Objectives

Because all three intrusion attempts were successfully identified by analyzing reused IOCs, they were all blocked, which prevented the attackers from achieving their ultimate goal (that is, Actions on Objectives).

Threat Analysis

- Threat analysis based on Kill Chain indicators
  - Creates an intelligence feedback loop
    - "Enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt"
  - Forces the attacker to make constant adjustments to Tactics, Techniques, and Procedures (TTPs)
    - Prevents attackers from reusing tools and infrastructure
    - Increases the cost of a successful intrusion by causing attackers to change every phase of the operation
  - Results in an increased level of resilience
    - By utilizing indicators across the entire Kill Chain
    - Instead of focusing only on post-compromise indicators

Analyzing the Lockheed Martin case highlights that threat analysis based on the Kill Chain and corresponding Indicators of Compromise (IOCs) can help defenders create an intelligence feedback loop that establishes "a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt."

This effort forces the attackers to make constant adjustments to their Tactics, Techniques, and Procedures (TTPs) and increases the cost of a successful intrusion. Instead of being able to reuse attack infrastructure and tools, the attackers now have to change every phase of their operation to avoid detection. This drastically increases the effort required by attackers and results in an increased level of resilience. By understanding that attackers leave evidence of an attack even before the compromise itself, defenders can gain an edge against even the most sophisticated adversaries.

Cyber Threat Intelligence

- Techniques that collect, classify, and use knowledge about adversaries
- This knowledge can be shared using well-known frameworks
  - STIX – Structured Threat Information eXpression
    - Language that describes the full range of cyber threat information including adversary TTPs, campaigns, and courses of action
    - Open community effort sponsored by the U.S. Department of Homeland Security
    - Commonly used in confidential information sharing organizations
  - TAXII – Trusted Automated eXchange of Indicator Information
    - Transport mechanism that standardizes automated exchange of cyber threat info
    - Supports a number of sharing models
      - Hub and Spoke
      - Source/Subscriber
      - Peer to Peer

SANS MGT514 | IT Security Strategic Planning, Policy, and Leadership 202

Cyber Threat Intelligence (CTI) is the collection, classification, and exploitation of knowledge about adversaries that helps defenders reduce the adversary's likelihood of success with each subsequent intrusion attempt.[1] There are three levels of threat intelligence:

1. **Strategic:** Executives and senior leaders seek to understand the larger threat landscape to identify risks and make investment and strategic decisions.
2. **Operational:** Operational staff look for trends in an adversary's operation or campaign.
3. **Tactical:** This level shows foundational consumption and sharing of Indicators of Compromise (IOCs) and attacker Tactics, Techniques, and Procedures (TTPs).

As the Lockheed Martin case shows, gathering even basic IOCs about adversaries and their TTPs can greatly aid in disrupting intrusion attempts. Building profiles of adversary groups and sharing intelligence with other organizations further enhances an organization's ability to detect and disrupt attacks.

STIX and TAXII are two well-known frameworks used for defining and sharing threat information.

STIX is a language that enables you to specify and communicate standardized cyber threat information. It is an XML schema sponsored by the U.S. Department of Homeland Security (DHS) as an open community effort. As a result, it is widely used in confidential information sharing organizations such as the Financial Services Information Sharing and Analysis Centers and National Health Information Sharing and Analysis Centers (FS-ISAC and NH-ISAC).

STIX[2] defines the cyber threat information, whereas TAXII[3] provides a standard way to share that threat information. It is flexible enough to support a number of sharing models, including these:

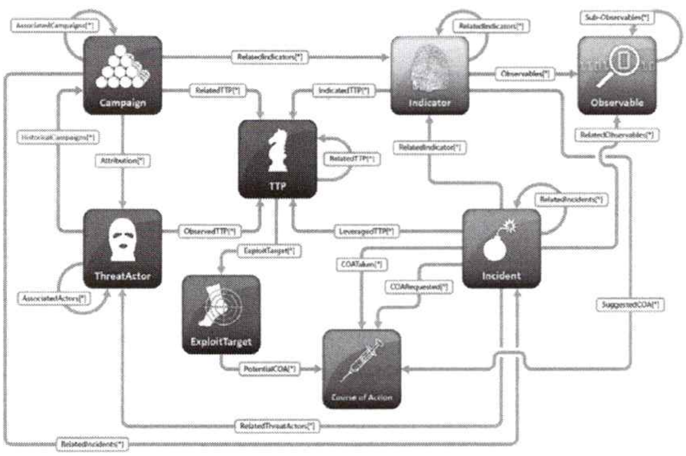
- **Hub and Spoke:** One organization serves as the central hub of information while a partner organization can choose to consume and/or provide information.
- **Source/Subscriber:** One organization provides information to the subscribers.
- **Peer to Peer:** Two or more organizations share information directly with each other.

References

[1] https://www.sans.org/course/cyber-threat-intelligence
[2] http://stixproject.github.io
[3] http://taxiiproject.github.io

STIX Architecture

Structured Threat Information eXpression (STIX)
v1.0 Architecture



This STIX Architecture[1] consists of eight core constructs:

Threat Actor: Information about who was conducting the attack

Campaign: Data about why they were conducting the attack

TTP: Details about how they conducted the attack

Exploit Target: Information about what was targeted

Incident: Details about the result of the attack

Indicator: Details about Indicators of Compromise

Observable: Items that you can look for in the attack

Course of Action: Details about what you should do about the attack

Reference

[1] http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf

External Threat Intelligence Sources

- Open:
  - SANS
  - OSINT
  - Mitre
  - US-CERT
- Private forums:
  - FS-ISAC
  - NH-ISAC
  - REN-ISAC
- Commercial:
  - AlienVault
  - Crowdstrike
  - CyberUnited
  - Dell SecureWorks
  - FireEye/Mandiant
  - iSight Partners
  - McAfee
  - OpenDNS
  - Palo Alto
  - Recorded Future
  - ThreatStream
  - Verisign iDefense

SANS | MGT514 | IT Security Strategic Planning, Policy, and Leadership 205

You can utilize many external threat sources to enhance your intelligence program. This slide lists some examples of open and commercial sources.

Internal Threat Intelligence Sources

- Many internal log sources that can be analyzed for intelligence:
  - Database
  - Directory
  - DLP
  - DNS
  - E-mail
  - Firewall
  - HR information
  - IDS/IPS
  - Malware
  - Physical access
  - VPN
  - Web/WAF

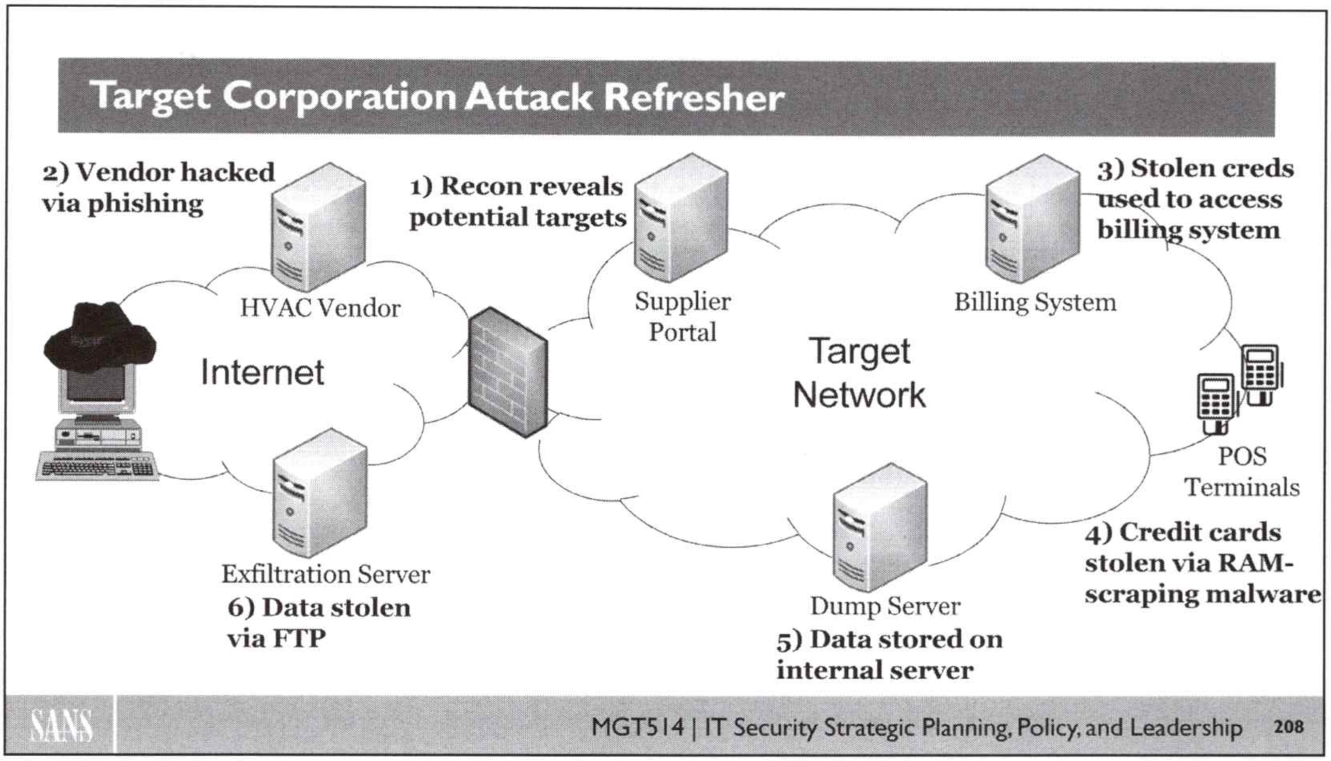
Many internal data sources also can be analyzed for intelligence. Typically, organizations already collect large amounts of this data but do not fully mine it to provide intelligence about adversaries. Especially in large organizations, even starting to consolidate this data is a large undertaking.

Cyber Threat Intelligence Key Elements

- What your team should look for from threat intelligence sources:
  - Can be consumed and parsed automatically
  - Use of a standard framework like STIX
  - IOCs that can be shared internally and externally
  - Capability to normalize indicators
  - Meaningful indicators:
    - Not just hashes, IP addresses, and domain names
    - Insight into Tactics, Techniques, and Procedures (TTPs)

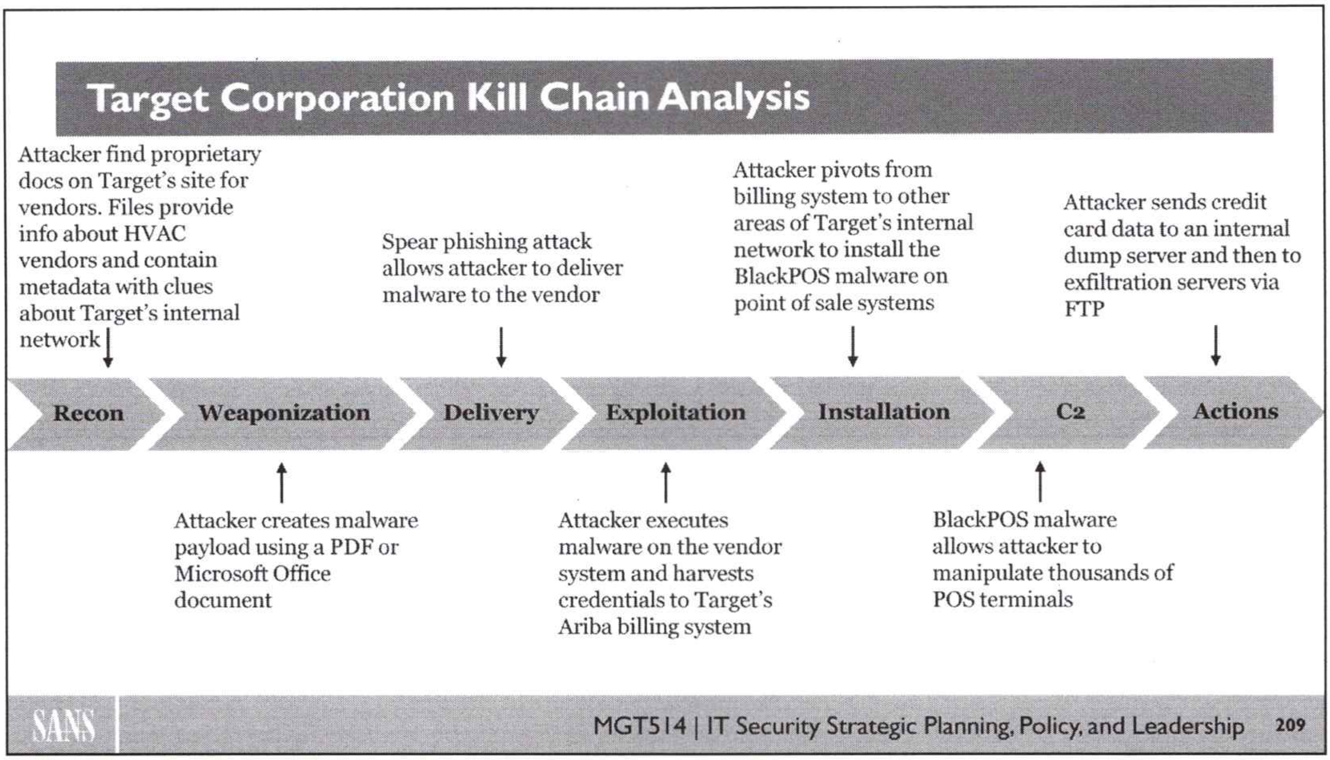
You should consider a number of elements before utilizing a new threat intelligence source. One of the key elements is automation. Can data be consumed and parsed automatically? Is it available via an API in a structured format like STIX? Can IOCs be shared both internally and externally?

Most importantly, are the indicators you receive meaningful? You will likely start with hashes, IP addresses, and domain names, but what additional insight can you gain into various threat groups that might be targeting your organization or industry? What TTPs are being used, and *why* is your company being targeted?



In an earlier section, we walked through the attack on Target Corporation and the theft of millions of credit cards. We will now map the attack to the various phases of the Kill Chain. Before we do that, though, let's briefly summarize the attack.

Attackers started by gathering publicly available information about Target's third-party vendors. This reconnaissance revealed proprietary information that helped attackers compromise an HVAC vendor used by Target. After stealing credentials from the HVAC vendor, the attackers logged on to the Target billing system and then pivoted to install malware on POS terminals to steal credit card data. This information was stored temporarily on an internal dump server and then exfiltrated to external servers via FTP.



This analysis is based on a paper by the U.S. Senate's Committee on Commerce, Science, and Transportation titled "A 'Kill Chain' Analysis of the 2013 Target Data Breach."[1]

Reconnaissance

In this phase, attackers discovered proprietary documents on Target's site for vendors. These files provided information about HVAC vendors and contained important metadata with clues about Target's internal network. Using this information, the attackers identified an HVAC vendor providing services to Target.

Weaponization

The attackers then created a malware payload using a PDF or Microsoft Office document.

Delivery

The malware was then delivered to the HVAC vendor via e-mail.

Exploitation

Once the victim received and opened the malicious document, the attackers' malware executed on the vendor system and harvested credentials to Target's billing system.

Installation

The attackers then pivoted from the billing system to other areas of the Target network to install the BlackPOS malware on various Point of Sale systems.

Command & Control (C2)

This BlackPOS malware enabled the attackers to scrape credit card numbers from memory and manipulate thousands of Point of Sale systems.

Actions on Objectives

The attackers achieved their ultimate goal of data exfiltration when they sent millions of credit card numbers to external servers via FTP.

Reference

http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883

Exercise 1.5 – Target Case

Duration Time: 15 Minutes

- Goals of this exercise
  - Identify courses of action that can be taken to prevent the attack from occurring
- For each phase of the Kill Chain, write down
  - What Target could do going forward
- Use the blank worksheet on the next slide

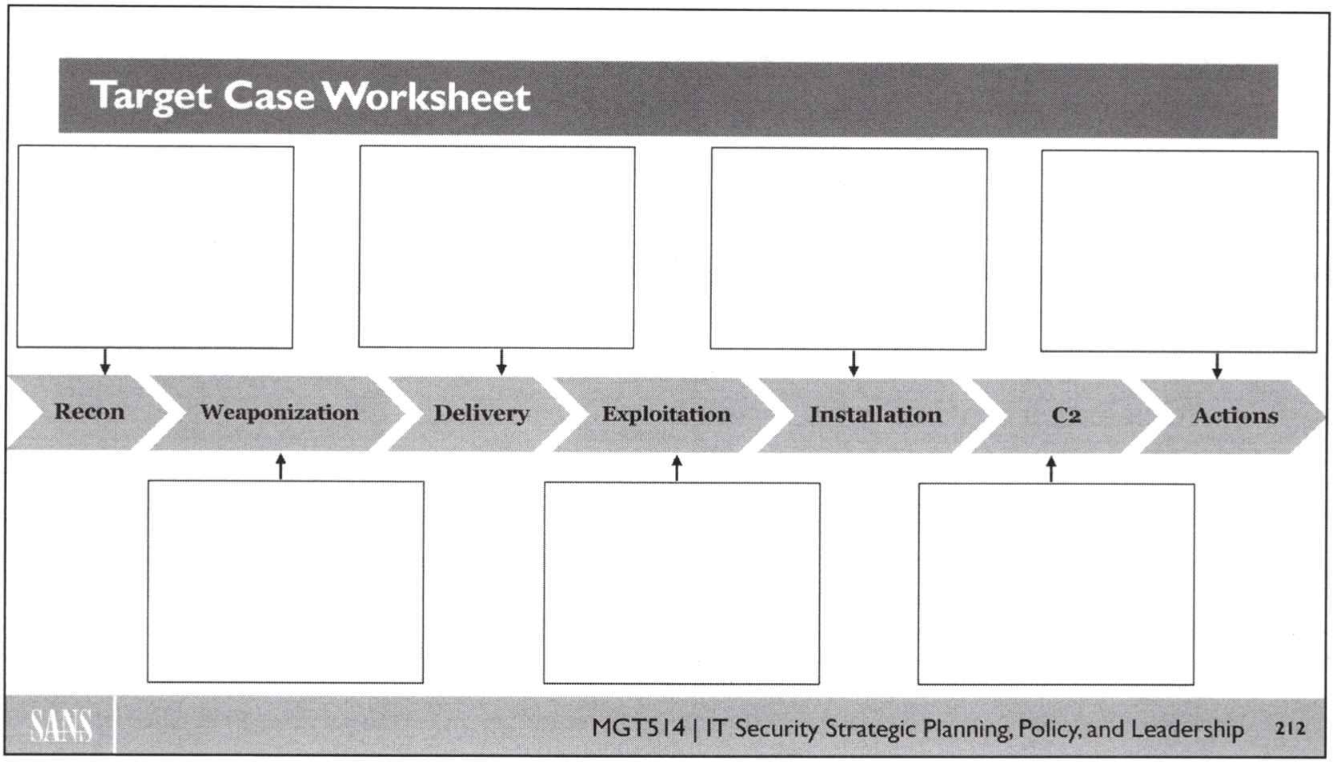
NOTE

Don't read the next section

It contains a debrief and potential exercise answers

Imagine that it has been two days since the Target breach was made public. Two weeks before that, you had excitedly accepted an offer to join Target's Information Security team. Now, you're not sure if you should still be excited. Today is your first day of work, and your boss, who is obviously a little flustered, calls you in to his office. He wants you to analyze what can be done to protect the organization going forward.

The goal of this exercise is to identify courses of action that can be taken to prevent attacks from occurring in the future.



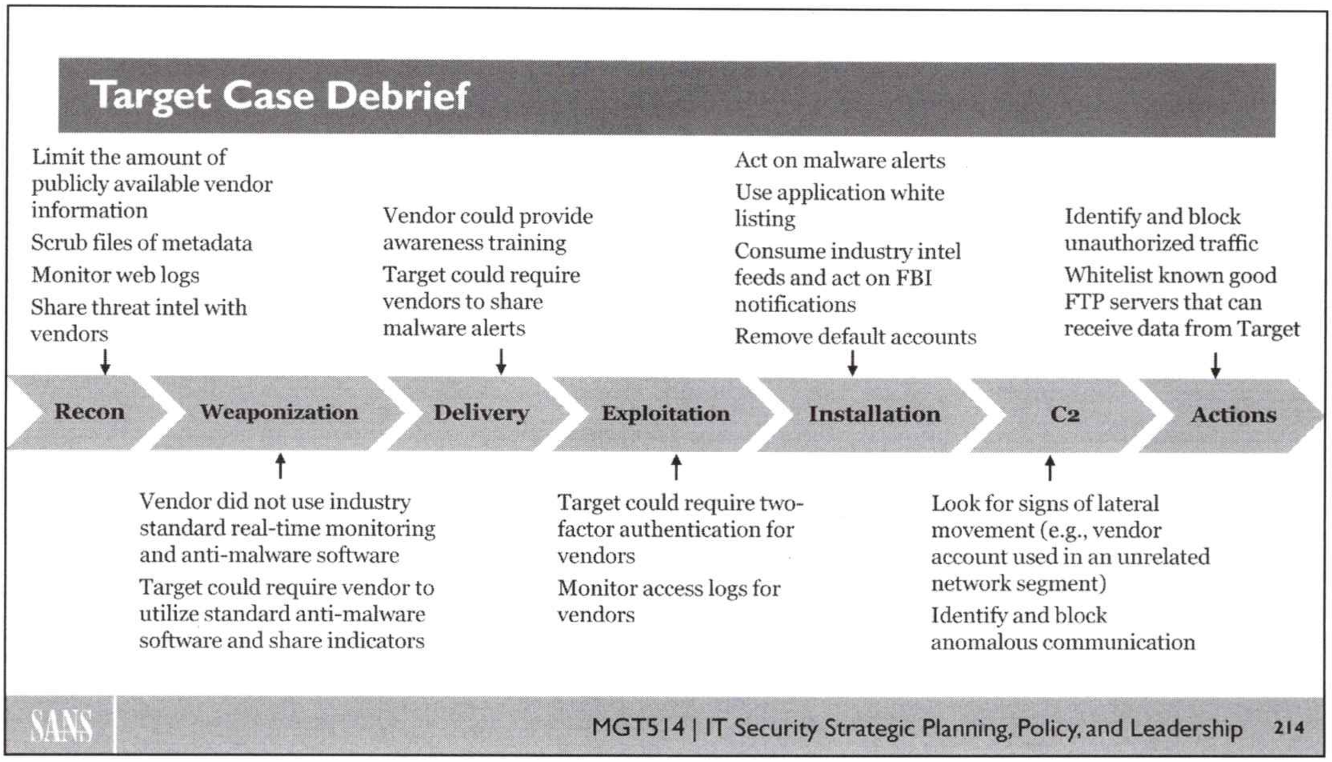
Use this worksheet to write down actions that could have been taken to prevent the attack for each phase of the Kill Chain.

Exercise Debrief

Note that this section contains a debrief and potential exercise answers

SANS 213

This page intentionally left blank.



A number of actions could have been taken to disrupt the attack.

Reconnaissance

By limiting the amount of publicly available vendor information and removing sensitive metadata from files, Target could have made it more difficult for attackers to identify potential targets. Additionally, monitoring web logs could have identified additional IOCs, like the IP addresses used by attackers and PDFs used in the attack. Sharing this information with vendors could have helped them be more prepared for targeted attacks that were conducted.

Weaponization

The attackers crafted a malicious PDF document that could have been detected by standard malware detection software. Target could require vendors to utilize standard anti-malware software and share IOCs.

Delivery

As part of a vendor risk management program, Target could provide awareness training to vendors about the risks of spam and phishing.

Exploitation

After the victim received and opened the malicious document, the attackers' malware executed on the vendor system and harvested credentials to Target's billing system. Target could require two-factor authentication and monitor access logs for vendors.

Installation

The attackers pivoted from the billing system to other areas of the Target network to install the BlackPOS malware. Target could have utilized application whitelisting to prevent installation of unauthorized software and more effectively consume and act on malware alerts. Additionally, FBI intelligence had previously identified the BlackPOS malware. By acting on FBI intelligence and consuming industry intelligence, Target could have disrupted the attacks. Finally, part of the attack relied on utilizing default accounts built into commercial software. Target could monitor usage of default accounts and, ideally, remove them entirely.

Command & Control (C2)

The attackers temporarily stored data on an internal dump server. Target could have looked for signs of lateral movement and blocked anomalous communication and the user of a vendor account in unrelated network segments.

Actions on Objectives

The attackers exfiltrated data using FTP. By blocking unauthorized traffic and whitelisting known good FTP servers, Target could have disrupted the attacks.

Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall AV	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Source: Lockheed Martin paper

SANS

From a technical perspective, a number of techniques can be used against attackers across various phases of the Kill Chain. The Lockheed Martin paper[1] lists a number of technical controls that can be used to detect, deny, disrupt, degrade, and deceive attackers.

Detect

Web and audit logs, along with Network Intrusion Detection (NIDS) and Host Intrusion Detection (HIDS) systems, provide a wealth of information about potential attacker activity. Additionally, vigilant users are often the first ones to notice signs of anomalous activity. Training them to report suspicious activity can provide a great early warning sign to potential attacks.

Deny

Capabilities such as firewalls, access control lists (ACLs), Network Intrusion Prevention (NIPS), proxy filtering, and Antivirus can be effective means of blocking attacks. Patching vulnerabilities and running in a "chroot" jail,[2] which prevents software from accessing files outside of its own root directory, are also effective means of preventing attacks.

Disrupt

Attacks can also be disrupted using a number of techniques such as in-line Antivirus and Network Intrusion Prevention (NIPS). To disrupt the Exploitation phase, software can also be built with the Data Execution Prevention (DEP) feature.[3] DEP is a security feature available on modern operating systems that marks certain areas of memory as "nonexecutable." This helps disrupt certain types of malware from executing.

Degrade

Attackers can also be slowed down to buy defenders more time to respond. This can be accomplished by queuing requests or decreasing the quality of service by using tarpits to purposely delay connections.[4]

Deceive

Attackers can also be deceived by DNS redirects or honeypots that appear to be part of a real system but are actually isolated systems that are specifically monitored to analyze attacks.

References

[1] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[2] http://en.wikipedia.org/wiki/Chroot

[3] http://en.wikipedia.org/wiki/Data_Execution_Prevention

[4] http://en.wikipedia.org/wiki/Tarpit_(networking)

In Summary

- Defenders must
  - Move detection and analysis up the Kill Chain
  - Implement defenses across the entire Kill Chain
- The Intrusion Kill Chain provides a structure
  - To analyze intrusions, extract indicators, and drive defensive courses of actions

Understanding the Tools, Techniques, and Procedures (TTPs) of adversaries and the corresponding Indicators of Compromise (IOCs) helps defenders move detection and analysis across the entire Kill Chain. By using the Kill Chain as a structure to analyze intrusions, defenders can drive defenses across the entire attack lifecycle. This helps defenders gain an edge against more sophisticated threats.

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 1

- Background
  - About This Course
  - Need for Strategic Planning
    - Exercise #1: Case Scenario
- Understand the Business
  - Vision & Mission
    - Exercise #2: Mission Statement
  - Stakeholder Management
  - PEST Analysis
    - Exercise #3: PEST
  - Business Strategy
- Understand the Threats
  - Threat Actors
    - Attack case studies
  - Asset Analysis
    - Exercise #4: Attacker Motivation
  - Threat Analysis
    - Exercise #5: Intrusion Kill Chain

This page intentionally left blank.

