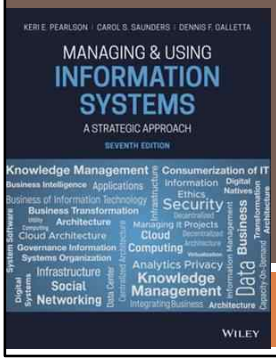
CHAPTER 7
SECURITY



Managing & Using Information Systems: A Strategic Approach (7th Edition), Pearlson, Saunders, & Galletta

Chapter Introduction

- Information technology (IT) security is one of the top issues of concern to businesses--hacked systems or stolen data can put a company out of business or cause physical damage to critical infrastructure.
- General managers must be knowledgeable participants in information security discussions to ensure continuance of operations.
- This chapter explores basic concepts for managing security including security planning, governance, culture, and metrics.

Chapter Introduction

3

- Lessons from some of the largest and most well-known breaches are covered as well as how they occurred according to security experts.
- The chapter also discusses common tools that aim to secure access, data storage, and data transmission to prevent these breaches and their advantages and disadvantages.
- Winding up the chapter is a discussion of how to answer the question "How secure are we?"

Case: U.S. Office of Personnel Management

4

- During lunchtime on June 6, 2015, a white van pulled in front of the U.S. Office of Personnel Management (인사국) in Washington, D.C.
- A team of three expert hackers entered the front door, displaying the credentials of three janitors who were bound and gagged (손과 발을 묶고 입에 재갈을 물린) back at their office.
- As the hackers stood at a supply room door next to a highly secure server room, the target of their attack, one feigned (pretend) having to crouch (bent) to tie his shoe, the other two stood in the way of the security cameras, and the crouching bandit used a lock-picking tool to gain access to the supply room.

Case: U.S. Office of Personnel Management

5

- They figured they had only a few minutes to clip a monitoring device to the network wires that led to the servers containing security clearance information (보안확인정보) for millions of employees and past employees.
- The device monitored electrical activity (전기 활성) right through the insulation (전열재/단열재) and transmitted it to the van.
- The hackers closed and relocked the supply room door, exited the building, and re-entered the van just as the clock struck 1 P.M.

Insulation: a thick layer of a substance that keeps something warm, especially a building.

Case: U.S. Office of Personnel Management

6

- The tallest of the three declared "right on schedule!" and set a timer for 10 minutes.
- He tuned his laptop into the monitoring device and the other two did the same.
- They watched communications to and from the server, waiting for an employee, any employee, returning from lunch to log-in.
- Monitoring was risky due to random sweeps (scopes) for rogue (독자적으로 행동하는) wireless connections, so after 10 minutes they would abort the mission.

Case: U.S. Office of Personnel Management

7

- The three typed frantically (madly) at their keyboards but nothing seemed to work for several agonizing (painful) minutes.
- Ten seconds before their time was up, one of the perpetrators hastily wrote some computer code and then smiled.
- He was just in time to reveal a log-in conversation complete with password.
- The hackers set the timer for another 10 minutes, which they had budgeted for the next phase.

Case: U.S. Office of Personnel Management

8

- The hackers searched frantically for large files that might contain the security clearance information (보안확인정보) they were hired to obtain.
- One of them found a large file called "SecurClearRecs," and the three cursed when they saw that the file was larger than anticipated.
- They immediately typed commands to upload the file through the Internet to a server in Shanghai, China.
- They kept one eye on the building and the other eye on the red "progress bar" that indicated "5% complete" for 20 full seconds before it changed to "10% complete."

Case: U.S. Office of Personnel Management

9

- The time required for each 5% seemed to vary widely; moving from 15% to 20% took almost an entire minute.
- They realized it would take the entire 10 minutes they had allocated or more.
- They could almost hear their own pulses pounding as they anticipated the million dollar reward that awaited them if they were successful but also dreaded (feel very anxious and unhappy) the fact that their overall budgeted 20 minutes might not be quite enough.
- Maybe they could chance it and go just a little longer.

Case: U.S. Office of Personnel Management

10

- A few terror-filled minutes past the budgeted 20 minutes, at 90% complete, they saw a guard step outside of the building and point at the van.
- Another officer joined him, and the pair started walking cautiously toward the van, trying to talk into his radio.
- The hackers had wisely jammed police channel communications and flattened the patrol cars' tires, but they wanted to avoid physical contact as much as possible.
- Trouble was certain to loom ahead; one of the officers turned to run back to the building.
- The tallest hacker jumped into the driver's seat and started the van.

Case: U.S. Office of Personnel Management

11

- The hackers looked down at the progress bar, which said "99% complete," just as an alarm sounded.
- The remaining guard began running to the van.
- Four flat tires would mean a 10-minute delay waiting for another officer from the security firm's headquarters.
- The hackers waited 5 more seconds for "100% complete" and then screeched (make an unpleasant high-pitched noise on the road) away to a secluded (quiet and private) clearing (a small area in a forest) a one-half mile away in the woods where a blue turbocharged Ford Mustang awaited them.

Case: U.S. Office of Personnel Management

12

- They pushed a red "self-destruct" button in the van to start a timer, jumped in the Mustang, and sped down back roads as distant sirens blared (makes a loud, unpleasant noise) and the van exploded.
- Two weeks later, on June 20, 2015, an article in *Computerworld* stated that "The U.S. government still isn't saying how much data it fears (우려하다) was stolen."
- This story is notable (unusual and worth noticing) for two reasons: (1) It is exactly the type of story that we would all imagine when hearing about data breaches, largely thanks to big-budget Hollywood movies.

Case: U.S. Office of Personnel Management

13

- However, (2) the story is almost completely false; the only true parts are that a large number of private security clearance files were indeed stolen from the Office of Personnel Management, and the June 20 article in *Computerworld* did display the preceding quote.
- If managers expect only such "urgent and frantic" physical attacks, they will focus their attention on the wrong threats.
- Instead, most attacks take place over months, going undetected until the damage is done and, often at that point, impossible to prevent.

Case: U.S. Office of Personnel Management

14

- Governmental officials learned in May 2015 that at least 4 million records likely had been stolen several months earlier.
- Subsequent estimates placed the number at 14 million records.
- The records contained much more than names, addresses, and social security numbers of current and former employees, possibly as far back as the 1980s.
- The 127-page dossier (file) for each person also included information on alcohol and drug use, financial, psychological, employment, and criminal history as well as sensitive personal information about contacts and relatives.

Case: U.S. Office of Personnel Management

15

- There were even comments from acquaintances, which could include neighbors, enemies, and potential enemies of each person.
- In short, according to the *International Business Times,* the stolen information was "invasive enough to ruin potentially millions of American lives."
- As a consequence, the Chairman of the U.S. House Oversight Committee (하원감독위원회) asked for the resignation of the person in charge, the Director of the Office of Personnel Management.

Case: U.S. Office of Personnel Management

16

- In reality, the following important issues are true for this case as well as many others:
  1. The hackers were far away and did not need any physical contact or any escape plan.
  2. They were able to spend an extended period of time--possibly over a year-to carry out their attack.

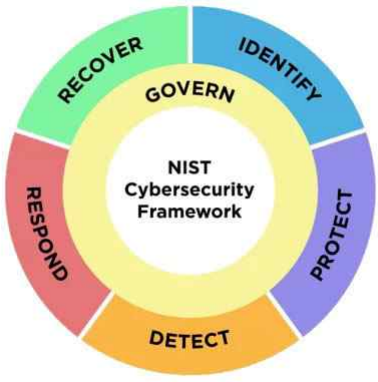
Case: U.S. Office of Personnel Management

17

3. It took the victim organization months to discover the breach, which enabled the hackers to cover their tracks.
   - ✓ In fact, a 2015 report from consulting firm Mandiant revealed that the median time that it took in 2014 for firms to detect a threat group's presence was 205 days, and the maximum was a whopping (very large) 2,982 days (11 years).
4. The hackers exploited a stolen password, likely obtained by various means described later in this chapter.

NIST Cybersecurity Framework (CSF)

18



NIST 사이버 보안 프레임워크란?

NIST의 사이버 보안 프레임워크 2.0에서 변경된 사항은 무엇이며 왜 관심을 가져야 합니까?

Figure 7.1 NIST CSF Framework

NIST: National Institute of Standards and Technology (미국국립표준기술연구소)

Functions	Definitions	Example Activities
Identify (식별)	• An organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	• Asset management, business environment, governance, risk assessment and management strategy
Protect (보호)	• Safeguards to ensure delivery of critical infrastructure services	• Access control, awareness and training, data security, information protection, maintenance, protective technology
Detect (탐지)	• Activities to identify the occurrence of a cybersecurity event	• Continuous monitoring, anomalies and events, detection processes
Respond (대응)	• Activities to take action regarding a detected cybersecurity incident	• Response planning, communication planning, analysis, mitigation, improvement
Recover (복구)	• Activities to maintain plans for resilience and to restore any capabilities or services that were impaired (damaged) due to a cybersecurity incident	• Business recovery planning, improvements, communication planning

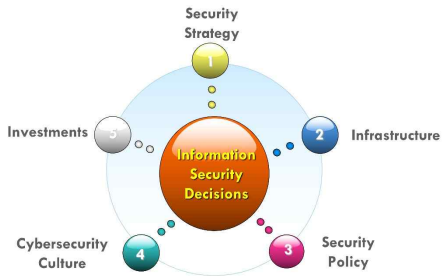
Figure 7.2 NIST CSF Functions and Their Definitions

19

IT Security Governance Framework

20

- The first step on the road to an effective security plan is for management to adopt a broad view of security.
- This can be done by establishing an information security strategy and then putting the infrastructure (tools) and policies (tactics) in place that can help the organization realize its strategy.
- The whole security picture can be reflected in five key information security decisions, presented in Figure 7.3.



- put something in place: (대책 등을) 수립, 준비 또는 실행하다

Information Security Decisions	Who Is Responsible	Rationale	Major Symptoms of Improper Decision Rights Allocation
Security Strategy	• Business leaders	• Business leaders have deep knowledge of the company's strategies on which security strategy should be based. • No detailed technical knowledge is required.	• Security is an afterthought and patched on to processes and products.
Infrastructure	• IT leaders (CISO)	• In-depth technical knowledge and expertise are needed.	• There is a misspecification of security and network typologies or a misconfiguration of infrastructure. • Technical security control is ineffective.
Security Policy	• Shared: IT and business leaders	• Technical and security implications of behaviors and processes must be analyzed, and trade-offs made, between security and productivity. • The firm's I T infrastructure needs to be understood.	• Security policies are written based on theory and generic templates. • They are unenforceable due to a misfit with the company's specific IT and users.
Cybersecurity Culture	• Shared: IT and business leaders	• Business buy-in and understanding, are needed to design programs. • Technical expertise and knowledge of critical security issues are needed to build them.	• User behaviors are not consistent with security needs. • Users bypass security measures, fail to recognize threats, or do not know how to react properly when security breaches occur.
Investments	• Shared: IT and business leaders	• They require financial (quantitative) and qualitative evaluation of business impacts of security investments. • A business case must be presented for competing projects. • Infrastructure impacts need to be evaluated.	• Under- or overinvestment in information security occurs. • The human or technical security resources are insufficient or wasted.

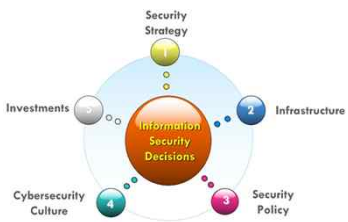
Figure 7.3 Key Information Security Decision

21

IT Security Governance Framework

22

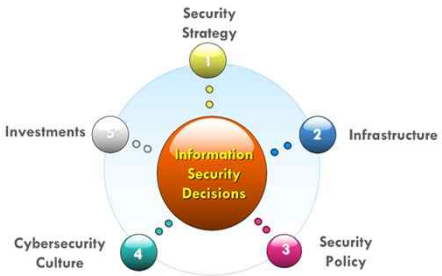
- Information security strategy
  - A company's information security strategy is based on such IT principles as protecting the confidentiality of customer information, strict compliance with regulations, and maintaining a security baseline that is above the industry benchmark.
  - Security strategy is not a technical decision.
  - Rather, it should reflect the company's mission, overall strategy, business model, and business environment.



IT Security Governance Framework

23

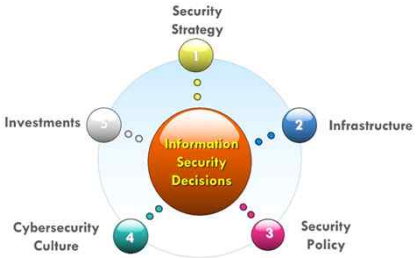
- Information security strategy
  - Deciding on the security strategy requires decision makers who are knowledgeable about the company's strategy and management systems.
  - An organization's information systems (IS) likely need to provide the required technical input for supporting the decision.



IT Security Governance Framework

24

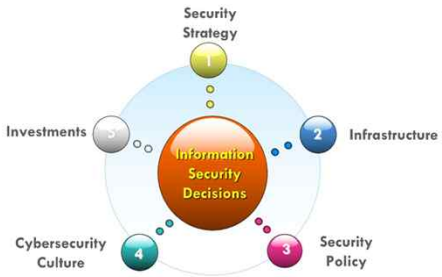
- Information security infrastructure
  - Information security infrastructure decisions involve selecting and configuring the right tools.
  - Common objectives are to achieve consistency in protection, economies of scale, and synergy among the components.
  - Top business executives typically lack the experience or expertise to make these decisions.



IT Security Governance Framework

25

- Information security infrastructure
  - For these reasons, corporate IT typically is responsible for managing the dedicated security mechanisms and general IT infrastructure, such as enterprise network devices.
  - Thus, corporate IT should take the lead and make sure that the technology tools in the infrastructure are correctly specified and configured.



IT Security Governance Framework

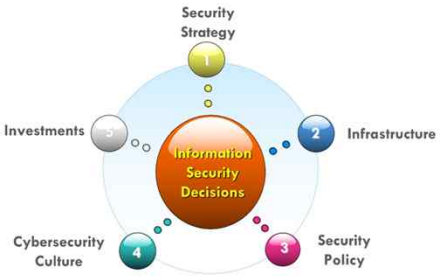
26

- Information security policy
  - Security policies provide guidelines for the organization's activities, both technical and organizational, to increase cyber resilience.
  - Following best practices, they broadly define the scope of and overall expectations for the company's information security program.
  - One of the most basic best practices is cybersecurity hygiene, or applying the basic system updates and patches offered from the vendors of systems, since these updates usually fix known bugs and vulnerabilities.

IT Security Governance Framework

27

- Information security policy
  - From these security policies, lower-level tactics are developed to control specific security areas (e.g., internet use, access control) and/or individual applications (e.g., payroll systems, telecom systems).
  - Policies must reflect the delicate balance between the enhanced information security gained from following them versus productivity losses and user inconvenience.



IT Security Governance Framework

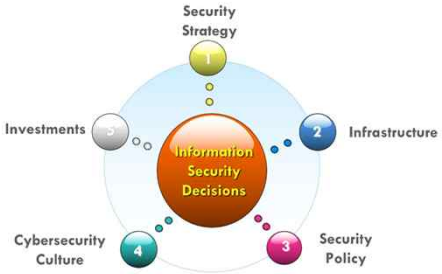
28

- Cybersecurity culture
  - Employees in an organization perform behaviors that they understand are important to the success of the business, and driving cyber-secure behaviors are no different.
  - Creating that understanding is a function of managerial practices.
  - It is very important to make business users aware of security policies and practices and to provide information security education, training, and awareness (SETA).

IT Security Governance Framework

29

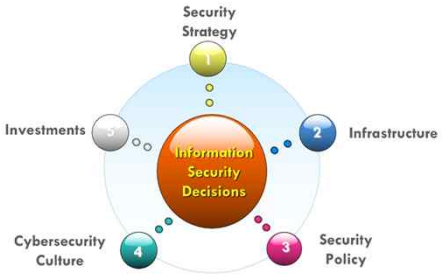
- Cybersecurity culture
  - Training and awareness programs provide team members with guidelines and sample behaviors to keep the organization secure.
  - IT and business managers have an additional role to model cybersecure behaviors and to emphasize the importance of cybersecurity.



IT Security Governance Framework

30

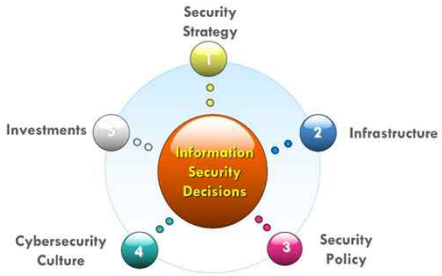
- Information security investments
  - The fear, uncertainty, and doubt ("FUD") factor once was all that was needed to get top management to invest in information security.
  - As information security becomes a routine concern in daily operations, security managers increasingly must justify their budget requests financially.



IT Security Governance Framework

31

- Information security investments
  - But it is difficult to show how important security is until there has been a breach- and even then it is hard to put a dollar amount on the value of security.
  - As when determining business needs, different units within the company may have rival or conflicting "wish lists (소원 목록)" for information security-related purchases that benefit their unique needs.



Cyberattacks and How They Occurred

32

Date Detected	Company	What Was Stolen	How
November 2013	• Target	• 40 million credit & debit cards	• Contractor opened virus-laden email attachment
May 2014	• Ebay #1	• 145 million user names, physical addresses, phones, birthdays, encrypted passwords	• Employee's password obtained
September 2014	• Ebay #2	• Small but unknown	• Cross-site scripting (XSS)
September 2014	• Home Depot	• 56 million credit card numbers • 53 million email addresses	• Obtaining a vendor's password/exploiting OS vulnerability

Figure 7.4.1 Well-Known Breaches, What was stolen, and How

Date Detected	Company	What Was Stolen	How
January 2015	• Anthem Blue Cross	• 80 million names, birthdays, emails, Social security numbers, addresses, and employment data	• Obtaining passwords from 5 or more high-level employees
July 2016 (but started August 2013)	• Yahoo (largest breach of all time	• For all 3 billion accounts: name, birthdate, answers to security questions, phone number, encrypted password, etc.	• An intruder forged cookies to fool Yahoo into thinking the password was already provided
September 2017	• Equifax	• 147 million records of personal information including social security numbers, names, birthdates, addresses, and credit information	• Hackers found vulnerability in an Equifax server that should have been fixed and used it to extent data for 76 days before being discovered

Figure 7.4.2 Well-Known Breaches, What was stolen, and How

33

Date Detected	Company	What Was Stolen	How
September 2018	• Facebook	• 87 million Facebook users profile information, friend information, private messages	• Cambridge Analytica illegally harvested users' information without their permission for political motivation to influence the 2016 political campaign.
September 2018 (but expected to have been going on since 2014)	• Marriot/ Starwood	• 500 million hotel guest names, addresses, passport numbers, account information, birthdates, hashed credit card information	• Chinese state hackers stole records from worldwide quests. • In 2017: A cybersecurity contractor downloaded a malware sample for analysis but it executed. • In 2016, Yahoo's new cloud-based system used an easily guessed password. • In 2014, an SQL injection bug was planted

Figure 7.4.3 Well-Known Breaches, What was stolen, and How

34

Breaches

35

- 80% of breaches are caused by stealing a password.
  - Phishing attack: sends a person a counterfeit e-mail that purports to be from a known entity.
    - ✓ The e-mail includes either a virus-laden attachment or a link that invites the user to click and visit a page to either solve a problem or accomplish a task.
  - Spear phishing: highlights the targeted nature of the attack, mimic a situation or relationship highly familiar to the targeted user.

Breaches

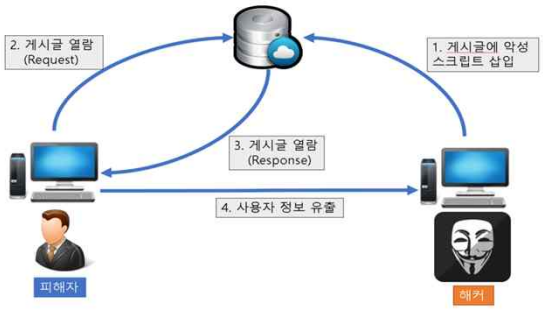
36

- 80% of breaches are caused by stealing a password.
  - Key logger: software that traps keystrokes and stores them for hackers to inspect later.
  - Weak passwords (123456 is most common)
  - Evil twin connection WiFi: By using an unsecured network at a coffee shop, hotel, or airport

Other Attack Approaches: Cross-Site Scripting(XSS)

37

- Malicious code pointing to a link requiring log-in at an imposter (e.g., a hacker) site



- 게시글과 같은 페이지에, 공격자가 악성 스크립트를 삽입하여, 사용자의 정보를 탈취, 악성코드 등을 유입시키는 공격
- 이 공격의 특징으로는 사용자(클라이언트) 대상으로 이루어 진다는 점

Other Attack Approaches: Third Parties

38

- The Target attackers broke into the network using credentials stolen from a heating, ventilation, and air conditioning (HVAC) contractor and installed malware on the retail sales system.
- The malware captured and copied the magnetic stripe card data right from the computer's memory before the system could encrypt and store it.
- Why would an HVAC contractor have access?
  - Security expert and blogger Brian Krebs reports that it is common for large retailers to install on their systems temperature and energy monitoring software provided by contractors.

Other Attack Approaches: Third Parties

39

- HVAC companies need to update and maintain their software, and are given access to their main systems so they don't have to endure delays in those updates.
- Access to the retailing system enabled the malware to spread to a majority of Target's cash registers, collecting information from debit and credit cards and sending it to various drop points in Miami and Brazil to be picked up later by hackers in Eastern Europe and Russia.

Other Attack Approaches: System Logs and Alerts

40

- Early news reports of Target's hack outraged customers when it was revealed that the newly installed, state-of-the-art $1.6 million security system detected what was going on.
- It sent several warnings to the IT department, even before the first files were transferred, but those alerts were unheeded (disregarded).
- However, some security experts explain that there are perhaps hundreds of generic alerts each day, and it is difficult to follow up on every one.
- One expert was quoted aptly: "it is completely understandable how this happened."

The Cost of Breaches

41

- A Ponemon study suggested that the cost of a data breach in 2018 was at an all-time high.
- Costs have been estimated at an average of $148 per record, overall, but reaching $408 per record in health-care organizations.
- In a so-called "mega-breach," exposing more than a million records, the costs could escalate to about $350 million.
- Surprisingly, there were 16 mega-breaches in 2017.
- Many firms facing such costs would find themselves in serious jeopardy.

The Cost of Breaches

42

- The Target breach cost $61 million in just two months, $162 million a year later, and potentially billions of dollars in damage control over the long run.
- The CIO resigned, fourth quarter profit fell 46%, and revenue declined 5.3%.
- The Home Depot breach cost $33 million (after insurance proceeds (returns) of $30 million reduced the initial outlays (expenses) of $63 million), and the company's stock price fell 2.1% the day after the breach was announced.
- Sales were not affected, however, which might indicate that customers have become numb (deprived of sensation) to these announcements.

The Impossibility of 100% Security

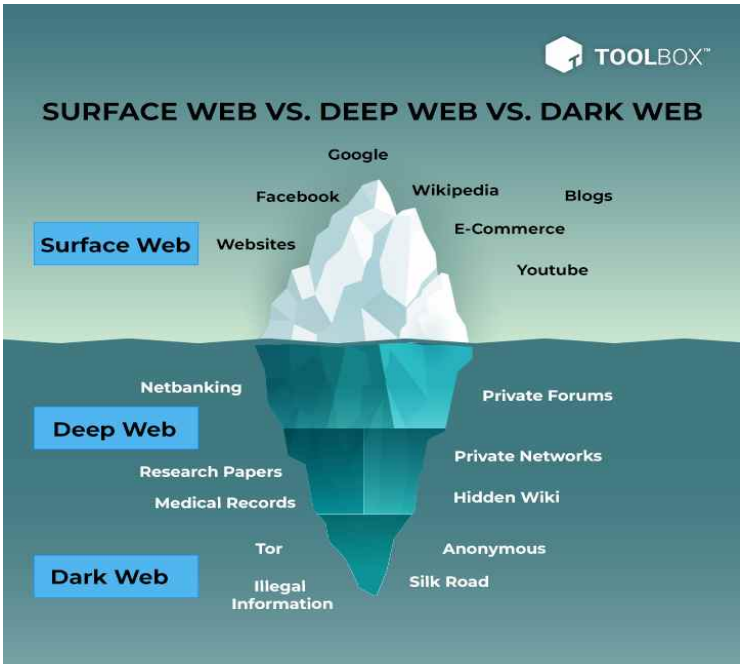
43

- Can you be safe?
- No, unless the information is permanently inaccessible.
  - "You cannot make a computer secure" – from Dain Gary, former CERT chief.
- 97% of all firms have been breached.
- Sometimes security makes systems less usable.

The Impossibility of 100% Security

44

- What Motivates the Hackers?
- Sell stolen credit card numbers for up to $50 each.
- 2 million Target card numbers were sold for $20 each on average.
- Street gang members can usually get $400 out of a card.
- Some "kits" (card number plus SSN plus medical information) sell for up to $1,000.
  - They allow opening new account cards.
- Stolen cards can be sold for bitcoin on the Deep Web.



45

What Should Management Do?

46

- Building on the model described above, managers must be informed and involved in decisions about five elements: security strategy, infrastructure, policies, culture, and investments.
- Security strategy needs to come first, and top management must determine the general strategy as well as investments that are needed.
- Infrastructure, policy, and culture decisions have to be made in more detail, and these three areas will now be discussed.
- Fortunately, general managers can easily understand key issues for each of these elements and participate fully in design and implementation of the resulting security plans.

Infrastructure

47

- Hackers have significant weapons to breach security barriers as previously described.
- In this rapidly escalating cyber war, management must use its own set of technologies and specialists to reduce risk and increase security.
- Tools can be divided into two categories:
  - Tools that provide protection from access by undesired intruders (Figure 7.5) and
  - Tools that provide protection for storage and transmission (Figure 7.6).

Access Tool	Concept
Physical locks	• Physically protect computing resources
Passwords	• Invent a set of characters known only by the user
Biometrics	• Scan a body characteristic, such as fingerprint, voice, iris, head, or hand geometry
Challenge questions	• Prompt with a follow-up question such as "model of first car"
Token	• Use small electronic device that generates a new supplementary passkey at frequent intervals
Text message	• Send a text message with a passkey
Multifactor authentication	• Couple two or more access techniques, for instance ✓ Passwords and phone call to phone number on file ✓ Biometrics and follow-up questions ✓ Passwords and text messaging

Figure 7.5 Common system access security tools and their advantages and disadvantages

48

Storage and/or Transmission Tool	Concept
Antivirus/antispyware	• Software scans incoming data and evaluates the periodic state of the whole system to detect threats of secret software that can either destroy data or inform a server of your activity
Firewall	• Software and sometimes hardware-based filter prevent or allow outside traffic from accessing the network
System logs	• They keep track of system activity, such as successful or failed login attempts, file alterations, file copying, file deletion, or software installation
System alerts	• System sends a warning when it detects unusual activity in the logs such as multiple failed login attempts, or large files being transferred out
Encryption	• System follows a complex formula, using a unique key (set of characters) to convert plain text into what looks like unreadable nonsense and then to decode back to plain text when presented with the decoding key
WEP/WPA (wired equivalent privacy and wireless protected access)	• Encryption used in a wireless network
VPN (virtual private network)	• Software provides a trusted, encrypted connection between your site and a particular server

Figure 7.6 Common storage and transmission security tools

49

Security Policies

50

- Management's approach to security emphasizes its importance and instructs users on what they need to do to achieve safety.
- Without sound management policy, access and storage technologies will be useless.
- If employees write their passwords on stick), notes and put them near their workstations, passwords will be ineffective from the start.
- Figure 7.7 provides a list of management policy tactics to prevent security weaknesses.

Policy	Concept
Perform security updates promptly	• Make sure all security updates are applied as soon as possible
Manage access of systems closely	• Remove former employees' credentials upon departure of the co mpany
Keep passwords secret	• Forbid users from sharing passwords
Perform mobile device management	• Provide a BYOD (bring your own device) policy on permitted pr oducts and required connection methods
Data disposal policies	• Require complete and secure disposal of documents after their u sefulness ends (deleting data is not "enough")
Test systems regularly for vulnerabilities	• Consultants or internal experts perform penetration tests to find vulnerabilities that need to be fixed or patched

Figure 7.7 Common used management security policies

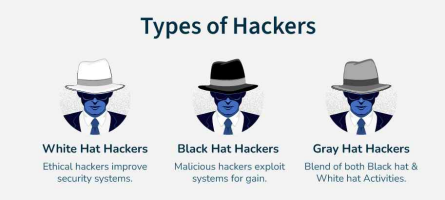
51

Security Policies

52

- Some managed security services provider (MSSP) firms offer the services of:

White hat hackers	• Break into a firm's systems to help it uncover weaknesses
Black hat hackers	• Break in for their own gain or to wreak (do) havoc (damage) on a firm.
Grey hat hackers	• Test organizational systems without any authorization and notify a company when they find a weakness. • Although they can be helpful, what they do is nevertheless illegal.



Cybersecurity Culture

53

- Managers can shape user behavior by creating a culture of cybersecurity.
- Culture is defined as the values, beliefs, and attitudes held by members of the organization.
- Culture is a set of unwritten rules that users value and follow even if they are not stated directly.
- Creating a cybersecurity culture is accomplished through management actions combined with environmental factors that managers do not control.
- Figure 7.8 summarizes the framework for driving cybersecure behaviors in organizations.

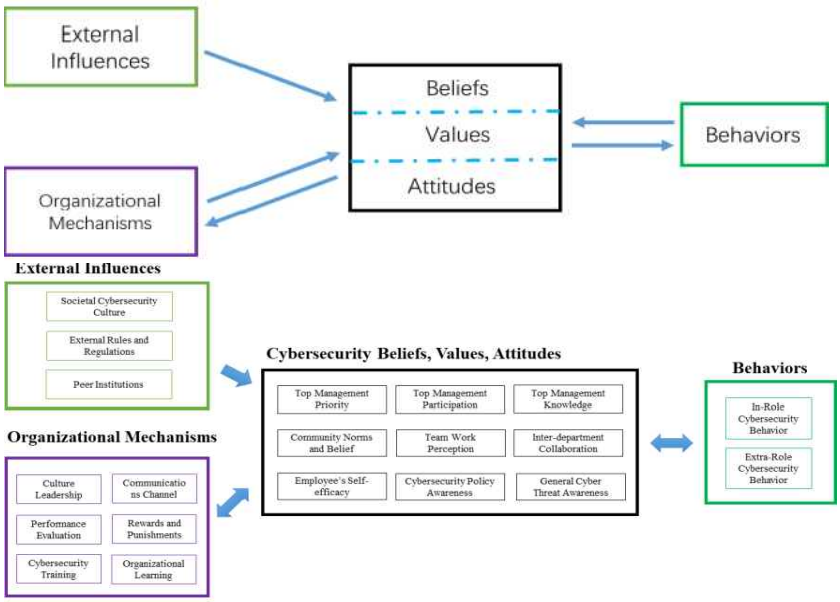


Figure 7.8 A model of organizational cybersecurity culture

54

SETA (Security Education, Training, and Awareness)

55

- Although awareness comes at the end of the SETA acronym, it is an important first step merely to let users know that security is a complex but important issue and that there are consequences when policies are not followed.
- Awareness includes an explanation of what might occur if users are relaxed about security.
- Education provides frameworks, reveals concepts, and builds understanding, while training covers procedures to follow and practice in following them.

SETA (Security Education, Training, and Awareness)

56

- Creating successful behaviors means that users need to know what to do, how to do it, and that they can actually complete the tasks.
- This last step is often lost in training programs.
- Sharing what and how gives the information needed, but if users do not feel they can implement these steps, then their behavior is not likely to change.
- See Figure 7.9 for a list of areas for education and training along with possible activities for each.

Subject	Sample Educational Activities	Sample Training Activities
Access tools	• Advantages and limitations of passwords • Why passwords should be complex and long • How often passwords should be changed • Strengths of multifactor authentication	• How to choose a password • How to change your password • How to use multifactor authentication • How to use a password manager
Bringing your own devices (BYOD)	• Why there are rules • What the rules are	• How to follow the rules • What to do if something goes wrong
Social media	• Why there are rules • Examples of issues that have occurred in the past • How those issues could have been avoided	• What to do in particular situations on social media • What to do if you need help or clarification on an issue
Vigilance	• What signals you might see under certain situations (warning messages; phishing e-mails; customer complaints) • What physical intrusions look like • What the signals mean • Which pieces of equipment have ports (USB, Ethernet)	• Where and how to look for warning signs • What to do when you see the various signals (for instance, a number to call or way to shut down) • How to protect your laptop when traveling

Figure 7.9 Major areas for education and training, with examples

57

Phishing

58

- One goal of education is to avoid the consequences of phishing by helping individuals identify ways to recognize these scams.
- Phishing = Private Data + Fishing

Classic Signs of Phishing

59

- An e-mail or bank account is closed, and the user needs to click to log-in and reactivate it.
- An e-mail inbox is too full, and the user is asked to click to increase storage.
- The user just won a contest or lottery and is asked to click to claim the prize.
- A user just inherited a fortune or will receive a commission to administer an inheritance after clicking to claim it.
- A product delivery failed, and the user needs to click to retry.

Classic Signs of Phishing

60

- An odd or unexpected Web address shows up when hovering a mouse pointer over a link in an e-mail.
- A familiar name in the "from" box is followed by an odd e-mail address.
- Poor grammar and spelling are in a note that purports to be from a large company.
- Goods or services are offered at an impossibly low price.
- An attachment is executable, often with an extension such of ZIP, EXE, or BAT.

Spoofing

61

- Phishing e-mails are the most common way for outsiders to gain access to company systems.
- But an unexpected e-mail, even from a known source, could breed viruses because of anyone of the following:
  1. The e-mail might not really be from the known source, and someone is spoofing (counterfeiting) the address.
  2. The e-mail might be from a known source's computer but the e-mail was secretly generated by a virus without knowledge of the owner, and it in turn contains a copy of the virus.
  3. Finally, the e-mail might have been sent from a familiar person who doesn't know that a virus is attached.

Defense in Depth

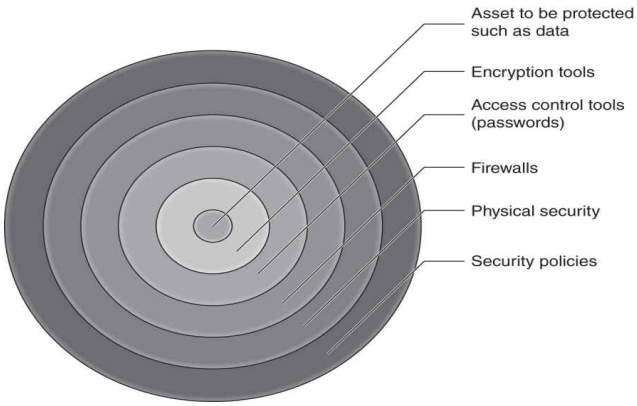
62

- Defense in depth is the concept of having multiple layers of different security policies and practices so when one layer fails to stop a perpetrator, another layer might be more effective.
- For example, even if a hacker is able to get past a firewall, not having the right fingerprint or password might stop the attack.
- Typical defense in depth plans have physical, technical, and administrative barriers.
- Figure 7.10 has an example of what multiple layers might look like.

"더 나은 보안을 위한 종합적인 접근" 심층 방어의 이해

Defense in Depth

63



심층 방어

[Azure-900]

Figure 7.10 Examples of defense in depth layers

How Do We Measure How Secure We Are?

64

- The big question for most managers is to know how secure their organization actually is.
- While many have come up with metrics and frequently collect them to help answer this question, there is no universal approach.
- Instead, the best approach is a type of balanced scorecard with several dimensions.
- Each measure, by itself, gives some information about how secure an organization is, but each falls short by not measuring enough of the areas of vulnerability faced by an organization.
- Figure 7.11 illustrates the scorecard categories.

How Do We Measure How Secure We Are?

65

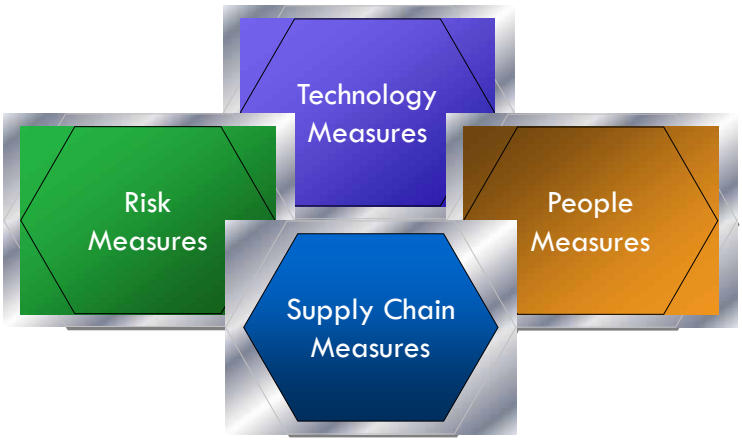


Figure 7.11 Cybersecurity Balanced Scorecard

How Do We Measure How Secure We Are?

66

- Technology measures give indication of the number of technical vulnerabilities in the organization's systems.
  - Many vendors offer tools to "calculate" this metric.
  - These tools go through the network and hardware of the organization and identify open ends, forgotten devices, and other potentially vulnerable points of entry for hackers.

How Do We Measure How Secure We Are?

67

- People measures are critical for understanding the security of a company.
  - One common practice is to conduct phishing exercises and report on results with the goal of reducing the number of employees who click on suspicious e-mails and increasing the number of employees who report them to the security team.

How Do We Measure How Secure We Are?

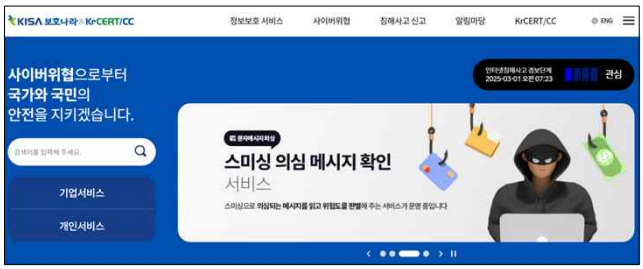
68

- Supply chain measures: As noted in the aftermath of the well-known Target breach in 2014, the malware affecting their systems was introduced by an unsuspecting HVAC vendor.
  - As supply chains increase the connectedness between buyers and suppliers, the vulnerabilities for cyber incidents increase.

How Do We Measure How Secure We Are?

69

- Risk measures: When leaders understand the risks associated with their cybersecurity plans and profile, they have a better understanding of the chances and potential costs of a breach.
  - Executives and Boards of Directors often focus on this part of security management wanting to know the company's risk profile or the risk that they are taking on from the different alternative decisions they might make.
  - Cyberinsurance is one way companies manage risk.



70