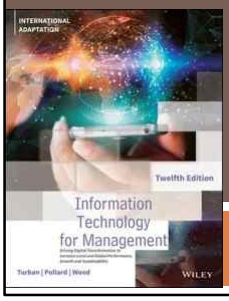
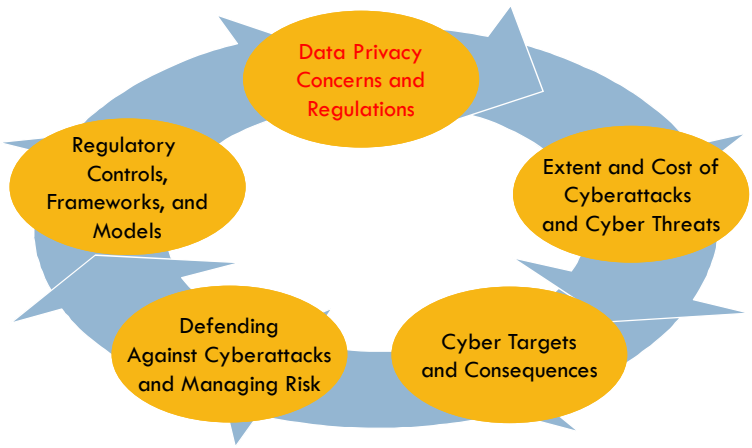
CHAPTER 5
DATA PRIVACY AND CYBER SECURITY



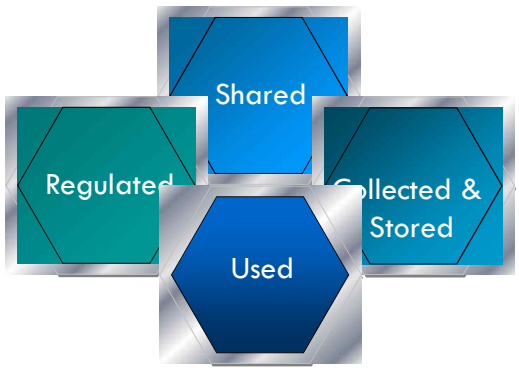
Chapter Outline (1 of 5)



Data Privacy Concerns and Regulations

3

- Data privacy is the right to self-determine what information about you is made accessible, to whom, when, and for what use or purpose.
- Four main concerns:
  1. How data are shared with third parties.
  2. How data are collected and stored.
  3. How data are used.
  4. How data are regulated.



Confused, Concerned, and Out of Control

4

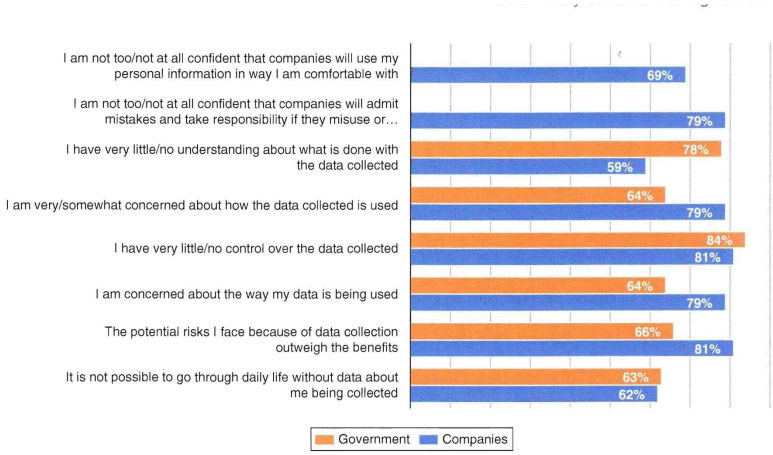


FIGURE 5.1 Americans are concerned, confused, and feel out of control about the collection of their personal information.

Confused, Concerned, and Out of Control

5

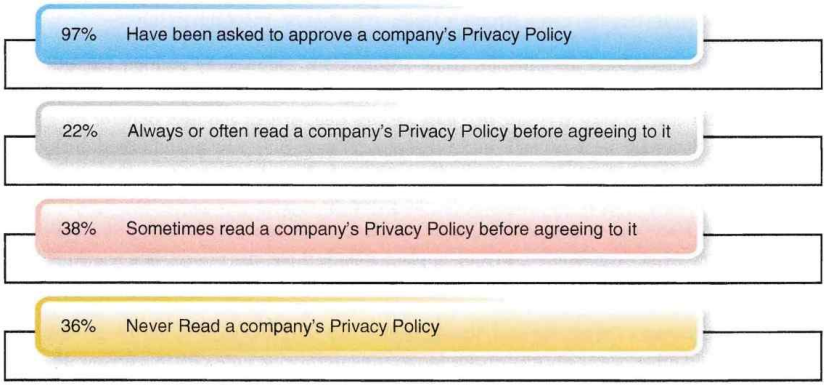


FIGURE 5.2 How many consumers read privacy policies?

The Privacy Paradox

6

- The inconsistency between the competing demands (경쟁적 수요) to use IT and have an online presence, while guarding against potential threats to personal safety and privacy resulting from misuse of personal information is known as the privacy paradox.
- Privacy paradox
  - The disconnect between how important people say their on line privacy is versus how they actually behave in real life.

Privacy Rights Are Civil Rights

7

- Data collection and analytics are increasingly vital to operating a business and are becoming integral to the way businesses deliver products and services to their customers.
- As a result, everything that is done online generates data, much of which is tracked.
- Tracked data is fed into powerful algorithms to deliver personalized ads and other services that appear on websites that we visit.
- While these are sometimes beneficial, these same algorithms can be used to facilitate discrimination in employment, housing lending, e-commerce, and voting.

U.S. Consumer Protection Data Privacy Regulations

8

- Privacy is a business-critical discipline for many organizations, enforced by multiple regulations.
- To protect the privacy rights and civil rights of consumers, governments around the world have created regulations and enacted laws to ensure that data are collected, shared, and used only for the purpose for which the data were made available in the first place (Figure 5.3).

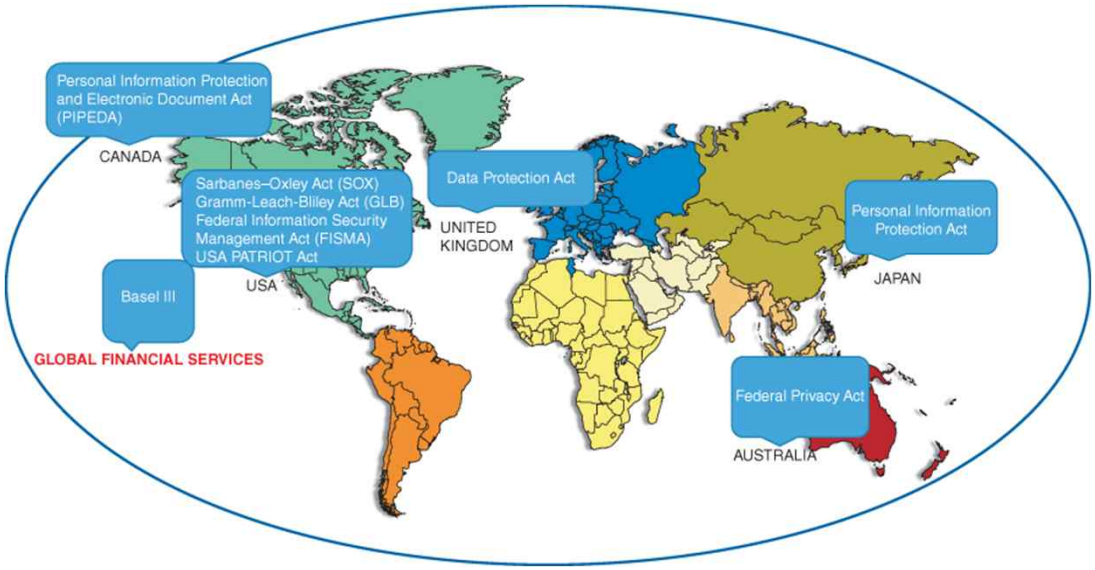


FIGURE 5.3 Global government regulations of PII (Personally Identifiable Information)

9

U.S. Consumer Protection Data Privacy Regulations

10

- Any unauthorized disclosure of personal information to third parties is normally considered a breach of privacy.
- Breach of privacy
  - The loss of, unauthorized access to, or disclosure of, personal information.
- U.S. Federal consumer protection data privacy regulations currently in place include those that protect data related to health care, finance, government, licenses, and credit.

U.S. Consumer Protection Data Privacy Regulations

11

- Health Insurance Portability and Accountability Act (HIPAA)
  - Protects the privacy of medical records and other personally identifiable healthcare information unless it's to a person who needs the information because they are involved in the person's care, processing payment for care, or the information is necessary to facilitate health-care operations.

  - 미국건강보험양도 및 책임에 관한 법(HIPAA): 건강 정보를 처리하고 보호하는 방법을 규제하는 연방법.
  - HIPAA에서는 전자 의료 정보에 대한 보안 통제를 요구하고 개인정보 보호 관행을 의무화하여 의료 정보 보호를 보장.

U.S. Consumer Protection Data Privacy Regulations

12

- Gramm-Leach-Bliley Act
  - Requires financial institutions that offer consumers financial products such as loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and to safeguard sensitive data.

  - 금융서비스현대화법: 금융기관이 보유하는 고객의 금융정보보호를 위해 제정.
  - 개인금융정보의 수집 이용 관련 고지 의무를 규정하는 프라이버시 원칙, 정보보호를 위한 세이프 가드 원칙, 고객 대상 기만적 정보 취득을 금지하는 프리텍스팅(pretexting)을 규정.

U.S. Consumer Protection Data Privacy Regulations

13

- Privacy Protection Act of 1980
  - Makes it unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of publication, in or affecting interstate or foreign commerce.
  - 프라이버시보호법: 언론인과 뉴스팀(신문사.방송사에서 뉴스를 받고 준비하는 곳) 보호를 위한 법으로, 언론인 및 언론 자료를 과도한 수색 및 압수 집행에서 보호하기 위해 제정.
  - 언론 자료의 범죄 연관성에 대한 개연성(probable cause)이 없는 한 개인의 작업산출물(work products) 및 문서 자료에 대한 수색이나 압수 금지.

U.S. Consumer Protection Data Privacy Regulations

14

- Driver's Privacy Protection Act (DPPA)
  - Protects the personally identifiable information of licensed drivers from improper use or disclosure.
  - 운전자 프라이버시 보호법: 차량관리국(DMV, Department of Motor Vehicle)의 기록에 포함된 개인정보의 대중 공개 제한.

U.S. Consumer Protection Data Privacy Regulations

15

- Fair Credit Reporting Act
  - Governs how a credit reporting agency can collect, access, use, and share credit information to ensure the accuracy, fairness, and privacy of the information in consumer credit bureau (소비자신용조사기관) files.

  - 공정신용조사법: 신용평가기관(Credit Reporting Agencies)에 의한 개인정보의 오남용 등 방지를 위한 신용정보보호 법률.
  - 신용평가기관은 은행, 신용카드사, 기업, 임대업자 등의 사업자가 개인의 신용 평가 목적으로만 정보를 사용한다는 합리적 믿음이 있는 경우 혹은 서면 동의가 있는 경우에만 정보 제공 가능.

U.S. State-Level Privacy Laws

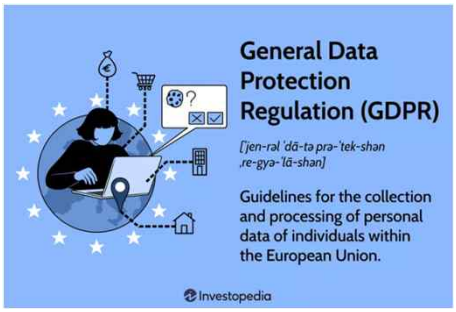
16

- Although the FTC (Federal Trade Commission: 미국연방통상위원회) has a broad level of authority over the enforcement of data protection regulations, there is no federal data privacy law or central data protection authority responsible for compliance with those regulations.
- Instead, most regulation is at the state level and the state attorneys general (법무장관) play a key role in enforcement.
- The number of state-level data privacy laws enacted across the United States is growing.

European Union's General Data Protection Regulation (GDPR)

17

- Recently, the European Union's General Data Protection Regulation (GDPR: 일반개인정보 보호법) spearheaded (leaded) a global movement of evolving privacy and data protection laws with very strict requirements.
- The GDPR is an EU-wide consumer Bill of Rights (권리 장전) enacted in May 2018 that empowers EU consumers by forcing retailers, marketers, and others to explicitly tell consumers how they are collecting, using, and storing consumers' personal data.



The EU-U.S. Privacy Shield

18

- Under the GDPR rules the EU does not allow the transfer of data on its citizens outside of the country unless the country is deemed to have adequate data privacy laws.
- The EU does not consider the data privacy laws currently in place in the United States to be adequate, so U.S. businesses must work around this requirement by adhering to the EU-U.S. Privacy Shield.
- A similar mechanism is available between Switzerland and the United States.

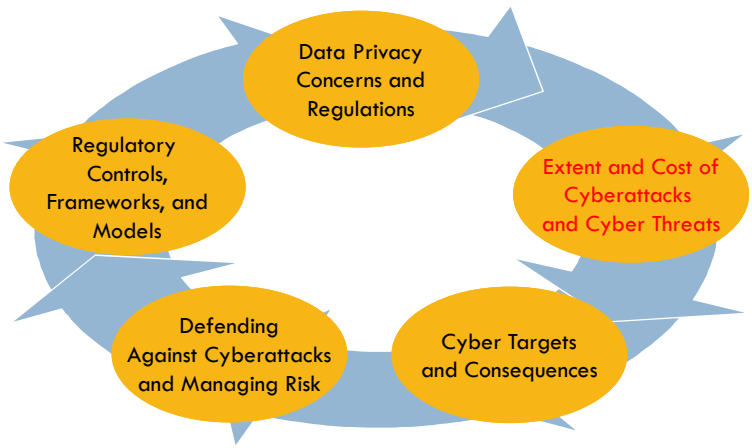
Public Lack of Understanding

19

- As governments around the globe continue to work to protect the handling and privacy of their citizens' data by adopting more powerful laws, organizations are being required to reconsider how they collect, store, and process personal information.
- Unfortunately, these data privacy regulations and laws that have been put in place to protect consumers are generally not well understood by the general public.

Chapter Outline (2 of 5)

20



Extent and Cost of Cyberattacks and Cyber Threats

21

- Cyberattack is an actual attempt to expose, alter, disable, destroy, steal, or gain unauthorized access to a computer system, infrastructure, network, or any other smart device.
- Cyber threat is the method used to commit a cyberattack that seeks to damage data, steal sensitive data, or disrupt digital life in general.
- Cyberattacks often include breaches in data privacy like the ones experienced by Yahoo and unfortunately are becoming a common occurrence.

Extent and Cost of Cyberattacks and Cyber Threats

22

- Table 5.1 lists the top five largest data breaches on record as of July 2019.

TABLE 5.1 Top Five Largest Data Breaches

Rank	Company	Records Exposed	Year	Cause
1	Yahoo	3 billion	2013	Hacking
2	First American Financial Corporation	885 million	2019	Poor Security
3	Facebook	540 million	2019	Poor Security
4	Yahoo	500 million	2014	Hacking
5	Marriott	500 million	2018	Hacking

Extent and Cost of Cyberattacks and Cyber Threats

23

- The industry sectors that were most heavily targeted by the cyberattacks are shown in Figure 5.4.

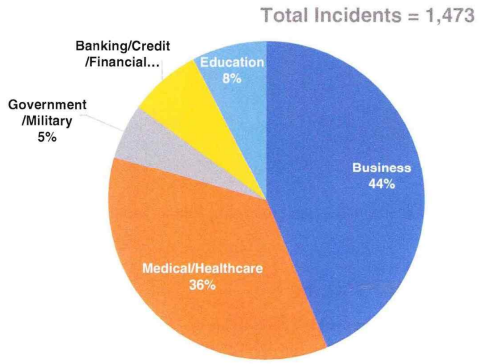


FIGURE 5.4 Number of 2019 U.S. data breaches by industry sector

Extent and Cost of Cyberattacks and Cyber Threats

24

- The types and extent of cyberattack experiences that companies suffered ranged from attempts to successful malicious attacks with organizational impacts such as:
  - Data corruption
  - Unrecoverable data
  - Tech-related business disruption with organizational impact as shown in Figure 5.5.

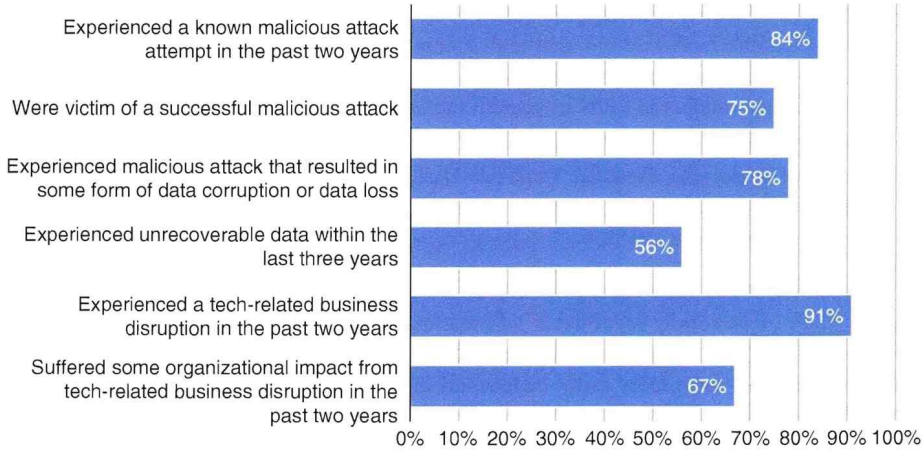


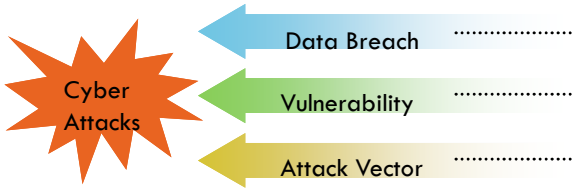
FIGURE 5.5 Percentage of companies across all industry sectors that have experienced cyberattacks

25

Extent and Cost of Cyberattacks and Cyber Threats

26

Data Breach	• The *successful retrieval* of sensitive information by an individual, group, or software system.
Vulnerability	• A gap in IT security defenses of a network, system, or application that can be exploited by a threat to gain unauthorized access.
Attack vector	• A path or means by which a computer criminal can gain access to a computer or network server in order to deliver a malicious outcome.



Extent and Cost of Cyberattacks and Cyber Threats

27

- Vulnerabilities threaten the confidentiality, integrity, or availability (CIA) of data and information systems, as defined in Figure 5.6, and leave organizations open to several types of unintentional and intentional cyber threats.

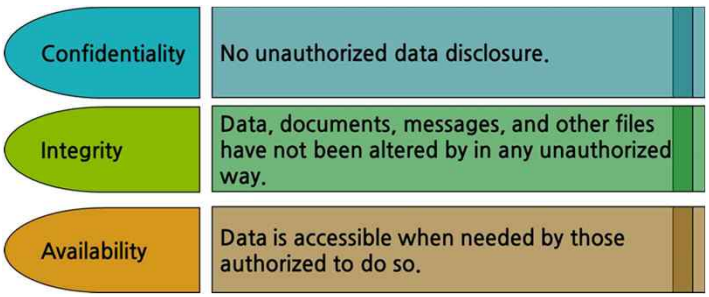


FIGURE 5.6. The three objectives (CIA) of data and information systems security

Intentional Cyber Threats

28

- Hacking
  - Broadly defined as intentionally accessing a computer without authorization or exceeding authorized access.
  - Various state and federal laws govern computer hacking.
- Hacktivist
  - Short for hacker activist or someone who performs hacking to promote awareness for or otherwise support a social, political, economic, or other cause.
  - Hacking an application, system, or network without authorization, regardless of motive, is a crime.
- In the Hacker culture there are three classes of hackers, shown in Table 5.2.

TABLE 5.2 Three Classes of Hackers

Type	Characteristics	Outcome
White hat	• Computer security specialist who breaks into protected systems and networks to test and assess their security.	• Use their skills to improve security by exposing vulnerabilities before malicious hackers (black hats) can detect and exploit them.
Black hat	• Person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons.	• Can inflict (impose/force) major damage on both individual computer users and large organizations by stealing personal financial information, compromising security of major systems, or shutting down or alerting the function of websites and networks.
Gray hat	• Person who may violate ethical standards or principles, but without the malicious intent ascribed to black hat hackers.	• May engage in practices that are less than ethical, but are often operating for the common good, e.g., exploits a security vulnerability to spread public awareness that the vulnerability exists.

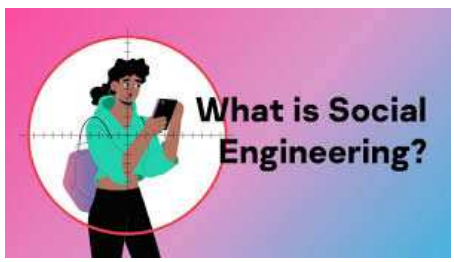
29

➢ ascribe to:~~의 결과라고 간주하다

Intentional Cyber Threats

30

- Social Engineering
  - Experts believe that one of the greatest cyber security dangers over the next few years will involve a hacker's clever use of deception or manipulation of people's tendency to trust, be helpful, or simply follow their curiosity on social media.
  - This phenomenon is called social engineering and it is difficult for even the most powerful IT security systems to defend against what can be made to appear to be authorized access.



Intentional Cyber Threats

31

- Phishing (Private Data + Fishing)
  - It is the oldest tool in a hacker's arsenal (무기고) and still the most effective social-engineering technique.
  - In a phishing attack, the attacker sends an e-mail to gain the victim's trust by evoking a sense of curiosity, urgency, or fear, to steal confidential information.
  - Spear phishing is a type of phishing that targets select groups of people who have something in common.
    - ✓ When spear phishing targets are executives or persons of significant wealth, power, influence, or control, the activity is known as "whaling (고래잡이)."

Intentional Cyber Threats

32

- Malware
  - It refers to various levels of intrusive or malicious software that can run undetected in the background on an IS or personal computer.
  - Less intrusive malware has more nuisance value than malicious intent.
  - More hostile malware is specifically designed to disrupt computer or mobile operations, gather sensitive information, and gain access to private computer systems.

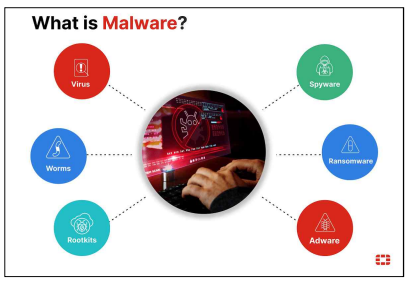


TABLE 5.2.1 Types of intrusive, but not necessarily, malicious software

Cookie	• A small piece of data sent from a website and stored in a user's Web browser while the user is browsing a website.
Spamware	• Software that enables attackers to search, sort, and compile a list of e-mail addresses, generate random addresses, insert fake headers into message, and use multiple mail servers simultaneously to broadcast unsolicited messages to unsuspecting recipients.
Adware	• Software that embeds advertisements in the application.
Spyware	• Tracking software that is not designed to intentionally damage or disable a system.

33

TABLE 5.2.2 Types of hostile malicious software

Zero-day	• Zero-day exploits prey upon system vulnerabilities that an attacker finds, but that the organization hasn't yet discovered.
Backdoor	• A difficult to detect malicious computer program used to provide an attacker with unauthorized remote access to a compromised PC by exploiting security vulnerabilities and works in the background hidden from the user.
Rootkit	• Set of software tools that enables an attacker to gain control of a computer system without being detected.
Boot record infector	• Attaches itself to the master boot record on a hard disk where it's loaded into memory when the system is started and can replicate itself to other drives or computers.
File infector	• Attaches itself to an executable code (.exe files) and is installed once the code is opened.

34

TABLE 5.2.3 Types of hostile malicious software

Keylogger	• A piece of software or hardware that logs every key pressed on a computer keyboard.
Virus	• Infects apps like Microsoft Word where it executes instructions once opened before transferring back control to the app.
Worm	• Doesn't attach itself to a host, like a virus, but it is a self-contained program that can replicate itself across computers and networks.
Trojan	• Hides in a useful program to infect the victim's system.
Remote access trojans (RATS)	• A form of Trojan horse that creates an unprotected backdoor into a system through which a hacker can remotely control that system.

35

Intentional Cyber Threats

36

- Ransomware
  - It is designed to block access to a computer system until a sum of money has been paid.
  - The use of ransomware began on a fairly small scale, targeting individual users, but the ransomware cyber threat is growing and attacks have become large scale.
  - Now, some executives fear entire companies will be shut down by ransomware until they pay up, or risk losing all their data.

Intentional Cyber Threats

37

- Cryptojacking
  - Cryptocurrency(암호화폐) + Hijacking(강탈)
  - It is a way that cybercriminals can make money with minimal effort.
  - It is a ransomware-like scheme to use other people's devices without their consent or knowledge to secretly syphon (빼돌리다) off cryptocurrency at the victim's expense.

Intentional Cyber Threats

38

- SQL Injection
  - It is one of the most dangerous vulnerabilities of a network app since attackers can use SQL injection to bypass application security measures.
  - The intent is to execute SQL code inside an app or Web page for personal gain or simply to be destructive.
  - By inserting malicious code into SQL statements, an attacker can manipulate an SQL query and force the query to return different data than was intended by the authorized user.

Intentional Cyber Threats

39

- Man-in-the-Middle (MitM)
  - These attacks are on the rise.
  - They occur when cyber criminals insert themselves between two parties in a transaction with the intention of stealing data.
  - One common MitM point of entry is an unsecured public Wi-Fi.
  - Once malware has breached a system, the attacker can install software to process the victim's information.

Intentional Cyber Threats

40

- The three common MitM attacks are:
  - Session hijacking
    - ✓ The attacker hijacks a session between the victim and a trusted network server.
  - IP spoofing
    - ✓ The attacker convinces the victim's computer system that it is communicating with a trusted, known entity to provide the attacker with system access.
  - Replay
    - ✓ The attacker intercepts messages and saves them with the intention of sending them later impersonating one of the trusted message participants.

Intentional Cyber Threats

41

- Denial-of-Service (DoS)
  1. Distributed Denial-of-Service (DDoS) crashes a network or website by bombarding it with traffic (i.e., requests for service) and effectively denying services to all those legitimately using it and leaving it vulnerable to other threats.
  2. Telephony Denial-of-Service (TDoS) floods a network with phone calls and keeps the calls up for long durations to overwhelm an agent or circuit and prevents legitimate callers such as customers, partners, and suppliers from using network resources.
  3. Permanent Denial-of-Service (PDoS) completely prevents the target's system or device from working.

Intentional Cyber Threats

42

- Botnets
  - The term botnet is derived from the words robot and network.
  - Cyber criminals use trojan viruses to breach the security of several user computers, take control of each computer, and organize all of the infected machines into a network of "bots" they can remotely control for malicious purposes.
  - Botnets are typically used to send spam and phishing e-mails and launch DDoS attacks.

Insider Threats and Privilege Misuse

43

- A method often used by insiders is data tampering (부당변경), a common means of cyberattack that is overshadowed by other types of attacks.
- Data tampering is a cyberattack during which someone enters false or fraudulent data into a computer, or changes or deletes existing data.
- Data tampering is extremely serious because it may not be detected.

Insider Threats and Privilege Misuse

44

- Physical Theft or Loss
  - It can be defined as the threat of an information asset going missing, whether through negligence or malice, that can send companies into a panic.
- Miscellaneous Errors
  - The main concern related to this source of cyber threat is a shortage of capacity that prevents information from being available where and when needed (Table 5.3).
- Table 5.4 lists some ways that organizations can guard against the various intentional and unintentional cyber threats we have discussed.

TABLE 5.3 Threat Actions Classified as Miscellaneous Errors

Threat Action	Description
Shortage of capacity	• Insufficient computer capacity to make information available where and when needed
Misdelivery	• Information delivered to the wrong person, when e-mails or documents are sent to the wrong people
Publishing error	• Information published to an unintended audience, such as the entire Internet, enabling them to view it
Misconfiguration	• A firewall rule is mistyped allowing access to a sensitive file server from all internal networks rather than a specific pool of hosts
Disposal error	• A hard drive is not "wiped" on decommissioned devices
Programming error	• Code is mistyped or logic is flawed
Date entry error	• Data is entered incorrectly or into the incorrect file or duplicated
Omission	• Data is not entered; document is not sent

- Decommission:
  - ✓ To officially stop using (a ship, weapon, dam, etc.);
  - ✓ To remove (something) from service

45

TABLE 5.4.1 How to Guard Against Intentional and Unintentional Cyber Threats

Source/Type	Solution	
Hacking	• Train your staff • Change password frequently	• Have "strong" passwords
Social Engineering	• Don't trust.	• Validate the source.
Phishing	• Train your staff	• Monitor activity
Spear Phishing	• Use a verbal password • Implement a quality spam filter	• Only allow e-mail from authorized server
Malware	• Use antimalware/AV(antivirus) software	• Patch promptly
Ransomware	• Monitor change and watch key indicators; back-up system regularly • Capture data on attacks	• Practice principle of least privilege
Cryptojacking	• Add an extension to Web browser like NoCoin, minerlLock or NoScript	

46

TABLE 5.4.2 How to Guard Against Intentional and Unintentional Cyber Threats

Source/Type	Solution	
SQL Injection	• Use a type-safe parameter encoding mechanism	• Validate input strings on server side
Man-in-the-Middle	• Use strong encryption between client and server	
Denial-of-Service	• Segregate key servers • Choose your providers carefully	• Test your anti-DDoS service
Insider and Privilege Misuse	• Monitor user behavior • Track mobile media usage	• Know your data
Physical Theft	• Encrypt your data • Train your staff	• Reduce use of paper
Physical Loss	• Encrypt your data	• Train your staff
Miscellaneous Errors	• Learn from your mistakes • Strengthen controls	• Ensure all assets go through a rigorous check by IT before they are decommissioned or disposed of

47

What Motivates Cybercriminals?

48

- "High Profile" Cyberattacks
  - Hackers and hacktivists with personal agendas carry out high-profile attacks to gain recognition and notoriety.
  - Hacktivist groups, such as Anonymous, a loosely associated international network of activist and hacktivist entities and its spin-off hacker group, LulzSec, have committed daring data breaches, data compromises, data leaks, thefts, threats, and privacy invasions.

✓ High Profile: 세간의 이목을 끄는

What Motivates Cybercriminals?

49

- "Under-the-Radar" Cyberattacks
  - Not all cyber criminals seek notoriety.
  - Some are profit motivated like advanced persistent threat (APT, 지능형지속공격) attackers who typically operate in stealth mode.
  - Advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an attacker gains access to a network and remains undetected for a period of time.

✓ Under-the-Radar: 은밀한

Unintentional Cyber Threats

50

Human error (a majority of internal security issues)	• Poorly designed systems • Faulty programming • Neglecting to change passwords • Unaware users
Environmental hazards	• Natural disasters • Faulty HVAC(Heating, Ventilation, and Air Conditioning) systems
Computer systems failure	• Poor manufacturing or maintenance

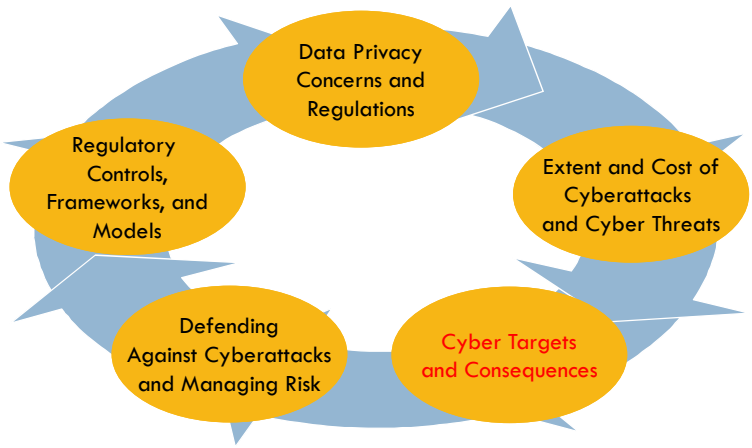
How Much Does a Cyberattack Really Cost an Organization?

51

Detection and escalation	• This involves costs to conduct activities that enable a company to detect the breach and report it to the appropriate personnel.
Notification	• This involves costs to perform activities that enable the company to notify regulators and individuals who had their data compromised in the breach.
Post data breach response	• This involves costs to create, operate, and maintain processes set up to help customers communicate with the company, such as call centers, as well as costs associated with redress (보상) and reparation (배상).

Chapter Outline (3 of 5)

52



Cyberattack Targets and Consequences

53

- Every enterprise has data that profit-motivated criminals target.
- Customer data, networks, websites, proprietary information systems, and patents are examples of valuable digital assets that need to be protected.
- The most prevalent and deadly targets that cybercriminals attack in companies and governmental agencies include: weak passwords, critical infrastructure; theft of IP; identity theft; shadow IT; bring your own device (BYOD); and social media.

➢ Shadow IT: 미인증 IT 환경, 기업이 구성원에게 사용을 허가하지 않은 IT 기기와 소프트웨어가 사내에서 사용되는 것

Weak Passwords

54

- One of the greatest cyber security weaknesses that cyber criminals like to target is users who ignore the dangers of weak passwords and password reuse.
- The capture and misuse of credentials (자격 인증서), such as user's IDs and passwords, is one of the foundation skills hackers use to execute numerous types of cyber threats, such as phishing, leaving organizations open to data breaches.
- For example, an attacker can inject some SQL code into a Web from input box such as submit box or editable payment textbox to gain access to a user's account to gather resources or make changes to data.

Critical Infrastructure

55

- Critical infrastructure is defined as, "systems and assets, whether physical or virtual, so vital to a country that the incapacity (inability) or destruction of such systems and assets would have a debilitating (making weak) impact on security, national economic security, national public health or safety, or any combination of those matters".
- Figure 5.7 shows 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation (무력화) or destruction would have a debilitating effect on a country's security, national economic security, national public health or safety, or any combination thereof.

Critical Infrastructure

56

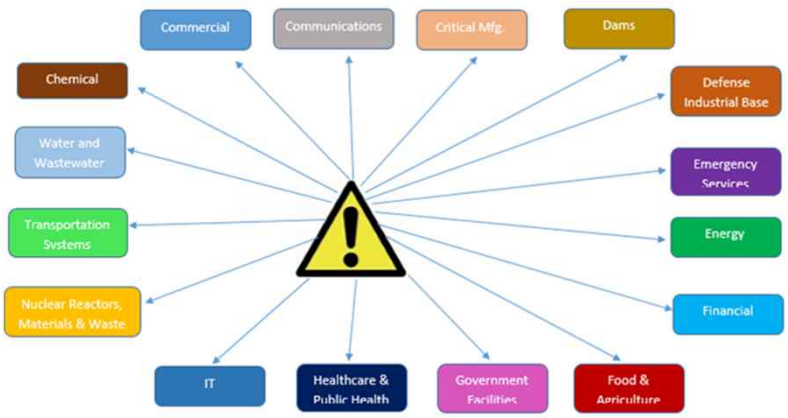


FIGURE 5.7 U.S. Critical Infrastructure Sectors.

Critical Infrastructure

57

- Intellectual property (IP) is a work or invention that is the result of creativity that has commercial value, including copyrighted property such as a blueprint, manuscript, or a design, and is protected by law from unauthorized use by others.
- Advancements in technology, increased mobility, rapid globalization, and the anonymous nature of the Internet create growing challenges in protecting IP.
- Hackers' preferred modus operandi (method of working, 작업 방식) is to break into employees' mobile devices and leapfrog into employers' networks--stealing trade secrets without a trace.

Identity Theft

58

- Identity theft is also on the rise.
- Thefts where individuals' Social Security and credit card numbers are stolen and used by thieves are not new.
- Criminals have always obtained information about other people--by stealing wallets or dumpster diving.
- But widespread electronic sharing and databases have made the crime worse.

Shadow IT

59

- Shadow IT, sometimes known as stealth IT, introduces security risks when unsupported hardware and software used by individuals or departments circumvent (avoid) IT security measures that apply to approved technology.
- Shadow IT is the use of IT-related hardware or software by an individual or a department without the knowledge of the IT department within the organization.

Shadow IT

60

- Figure 5.9 summarizes how shadow IT apps, mobile devices, and cloud services can put organizations at a greater risk of cyberattack.

FIGURE 5.9 Shadow apps, mobile devices, and cloud services put companies and users at risk

Bring Your Own Device

61

- It's an appealing concept because BYOD enables companies to cut costs by not having to purchase and maintain employees' mobile devices.
- Unfortunately, many companies have rushed into it without considering how these policies relate to IT security.
- The BYOD trend is driven by employees using their own devices for business purposes because they are more powerful than those the company has provided.
- Another factor is mobility.

Bring Your Own Device

62

- BYOD Raises Serious and Legitimate Areas of Concern
  - Hackers break into employees' mobile devices and leapfrog into employers' networks--stealing secrets without a trace.
  - New vulnerabilities are created when personal and business data and communications are mixed together.
  - Another serious problem arises when an employee's mobile device is lost or stolen.

Consumerization of IT (CoIT) Overview Demo

Social Media

63

- Companies' poor social media security practices put their brands, customers, executives, and entire organizations at serious risk.
- Social networks and cloud computing increase vulnerabilities by providing a single point of failure and attack for organized criminal networks.
- To combat these types of cyber threats and prevent widespread outbreaks, Web filtering, user education, and strict policies are key.

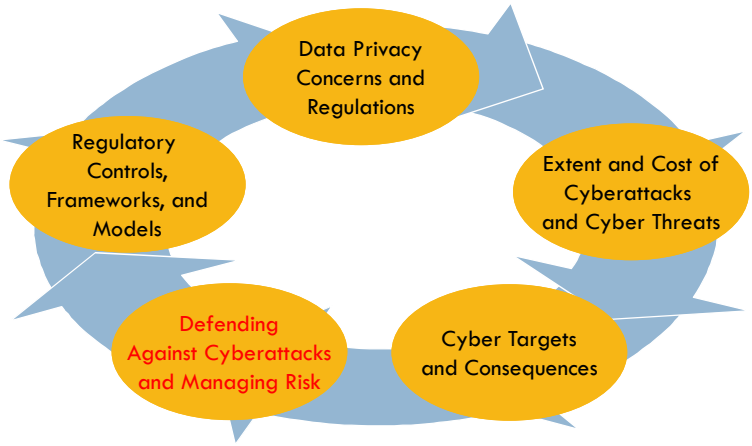
Social Media

64

- Networks and Services Increase Exposure to Risk
  - An overriding (most important) reason why networks and services increase exposure to risk is the time-to-exploitation of today's sophisticated spyware and mobile viruses.
  - Time-to-exploitation is the elapsed time between when a vulnerability is discovered and when it is exploited.
  - Patch is a software program that users download and install to fix a vulnerability.

Chapter Outline (4 of 5)

65



Defending Against Cyberattacks and Managing Risk

66

- The first step in a cyber security initiative is to choose a cyber defense strategy, then adopt risk mitigation strategies specific to different types of assets, and deploy robust security measures that are not just the responsibility of IT and top management, but the ongoing duty of everyone in an organization.
- The cyber security field has its own terminology, which is summarized for quick reference in Table 5.5.

Defending Against Cyberattacks and Managing Risk

67

TABLE 5.5.1 Cyber Security Terminology

Term	Definition
Access control	• Security feature designed to restrict who has access to a network, IS, or data
Asset	• Something of value that needs to be protected. • Customer data, trade secrets (영업비밀), proprietary formulas, and other intellectual property
Audit	• Procedure of generating, recording, and reviewing a chronological record of system events to determine their accuracy
Authentication	• Method (usually based on username and password) by which an IS validates or verifies that a user is really who he or she claims to be

Defending Against Cyberattacks and Managing Risk

68

TABLE 5.5.2 Cyber Security Terminology

Term	Definition
Biometrics	• Methods to identify a person based on a biological feature, such as a fingerprint or retina
Ciphertext	• Encrypted text
Encryption	• Transforming data into scrambled code to protect them from being understood by unauthorized users
Exploit	• A program (code) that allows attackers to automatically break into a system through a vulnerability • To attack or take advantage of a vulnerability
Exposure	• Estimated cost, loss, or damage that can result if a threat exploits a vulnerability

✓ Biometrics: 생체인식기술 / 지문, 홍채, 피부 등 개인의 생체정보를 이용한 인증 방식

Defending Against Cyberattacks and Managing Risk

69

TABLE 5.5.3 Cyber Security Terminology

Term	Definition
Fault tolerance	• The ability of an IS to continue to operate when a failure occurs, but usually for a limited time or at a reduced level
Firewall	• Software or hardware device that controls access to a private network from a public network (Internet) by analyzing data packets entering or exiting it
Plaintext or clear text	• Readable text
Risk	• Probability of a threat exploiting a vulnerability and the resulting cost of the loss, damage, disruption, or destruction • Risk = f(Threat, Vulnerability, Cost of the Impact)

Cyber Defense Strategies

70

Strategic Intelligence

- Informs HOW an organization will defend itself.
- This includes analyzing the gaps in an organization's cyber security tools and processes to ensure they can adequately defend themselves against aggressive cyber threat and make it easier for an organization to protect against threats before they occur.

Tactical Intelligence

- Informs WHAT an organization needs to do when it is attacked.
- This might include identifying threatening domains, malware, and IP addresses and getting information from other organizations who have suffered similar cyberattacks.

Cyber Defense Strategies

71

TABLE 5.6 Cyber Defense Strategies

Action	Details
Prevention and Deterrence	• Properly designed controls may prevent errors from occurring, deter criminals from attacking the system, and, better yet, deny access to unauthorized people.
Detection	• Like a fire, the earlier an attack is detected, the easier it is to combat, and the less damage is done.
Containment	• This objective involves minimizing or limiting losses once a malfunction has occurred.
Recovery	• A recovery plan explains how to fix a damaged information system as quickly as possible.
Correction	• Correcting the causes of damaged systems can prevent a problem from occurring again.
Awareness/ Compliance	• All organization members must be educated about the hazards and must comply with the security rules and regulations.

Managing Risk

72

- The higher the value of the asset to the company and to cybercriminals, the greater the risk is to the company and the higher the level of security needed.
- To do this, a company can use one of the four risk management approaches to assess its risk tolerance relative to different computing resources and their environment.
- Figure 5.10 identifies and describes the four different risk mitigation strategies that apply to business continuity and disaster recovery.

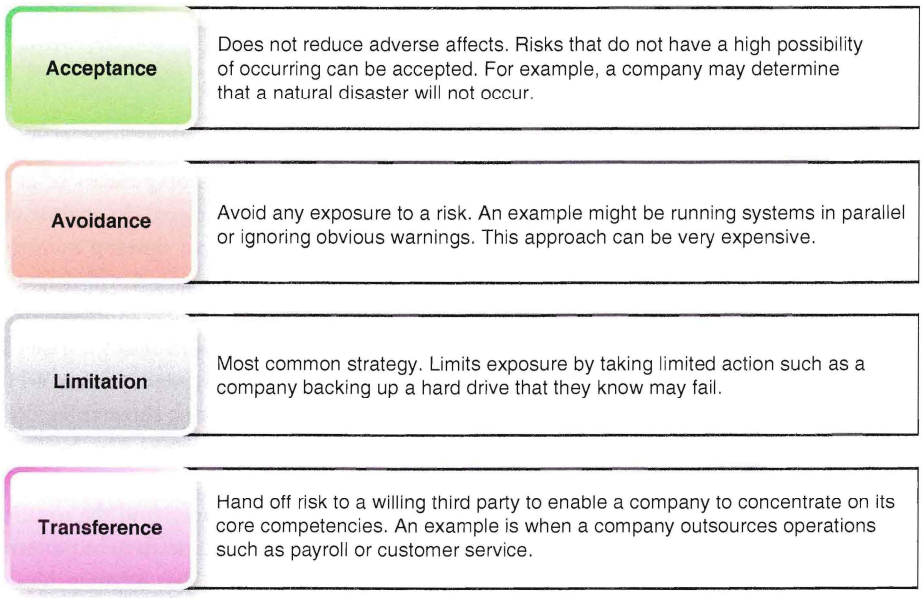


FIGURE 5.10 Risk mitigation strategies

73

Acceptance	• Does not reduce adverse affects. • Risks that do not have a high possibility of occurring can be accepted. • For example, a company may determine that a natural disaster will not occur.
Avoidance	• Avoid any exposure to a risk. • An example might be running systems in parallel or ignoring obvious warnings. • This approach can be very expensive.
Limitation	• Most common strategy. • Limits exposure by taking limited action such as a company backing up a hard drive that they know may fail.
Transference	• Hand off risk to a willing third party to enable a company to concentrate on its core competencies. • An example is when a company outsources operations such as payroll or customer service.

74

Securing Systems

75

- Cyber Defense Tools

Antivirus software	• Anti-malware tools are designed to detect malicious codes and prevent users from downloading them.
Intrusion detection systems (IDSs)	• As the name implies, an IDS scans for unusual or suspicious traffic.
Intrusion prevention systems (IPSs)	• An IPS is designed to take immediate action-such as blocking specific IP addresses--whenever a traffic-flow anomaly is detected.
IP intelligence services	• Being able to detect and block cyber threats before they occur is a huge advantage in protecting a network against attack.

Securing Systems

76

- Protecting Against Malware Reinfection, Signatures, Mutations, and Variants
  - Malware is very difficult to remove from infected computers.
  - When a host computer is infected, attempts to remove the malware can fail and the malware may re-infect the host for two reasons:
    1. Malware is captured in backups or archives.
       - ✓ Restoring the infected backup or archive also restores the malware.
    2. Malware infects removable media.
       - ✓ Months or years after the initial infection, the removable media may be accessed, and the malware could attempt to infect the host.

Securing Systems

77

- Protecting Against Malware Reinfection, Signatures, Mutations, and Variants
  - Most antivirus (AV) software relies on malware signatures to identify and then block malware.
  - Malware signature is a unique value that indicates the presence of malicious code.
  - Zero-day exploit is malicious software that exposes a vulnerability in software or hardware and can create complicated problems well before anyone detects it.

Securing Systems

78

- Protect Mobile Devices
  - Mobile biometrics, such as voice and fingerprint biometrics, can significantly improve the security of physical devices and provide stronger authentication for remote access or cloud services.
  - Voice biometrics is an effective authentication solution across a wide range of consumer devices including smartphones, tablets, and TVs.

✓ Biometrics: 생체인식기술 / 지문, 홍채, 피부 등 개인의 생체정보를 이용한 인증 방식

Securing Systems

79

- Protect Mobile Devices
  - Rogue (fake) application monitoring is used to detect and destroy malicious applications.
  - Mobile kill switch or remote wipe capability as well as encryption are needed in the event of loss or theft of a device.
  - Encryption is process of converting information or data into a code and is essential to prevent unauthorized access to sensitive information transmitted online.

Securing Systems

80

- Develop Do-Nat-Carry Rules
  - U.S. companies, government agencies, and organizations are now imposing do-not-carry rules, which assume that devices will inevitably be compromised according to Mike Rogers, current chairman of the House Intelligence Committee.
  - For example, House members can bring only "clean" devices and are forbidden from connecting to the government's network while abroad.

Securing Systems

- Becoming IT Resilient
  - IT resilience involves effectively mitigating the risk to data and apps of any kind of planned or unplanned disruption.
  - IT resilience is the ability to protect data and apps from any planned or unplanned disruption to eliminate the risk of downtime to maintain a seamless customer experience.
  - Figure 5.11

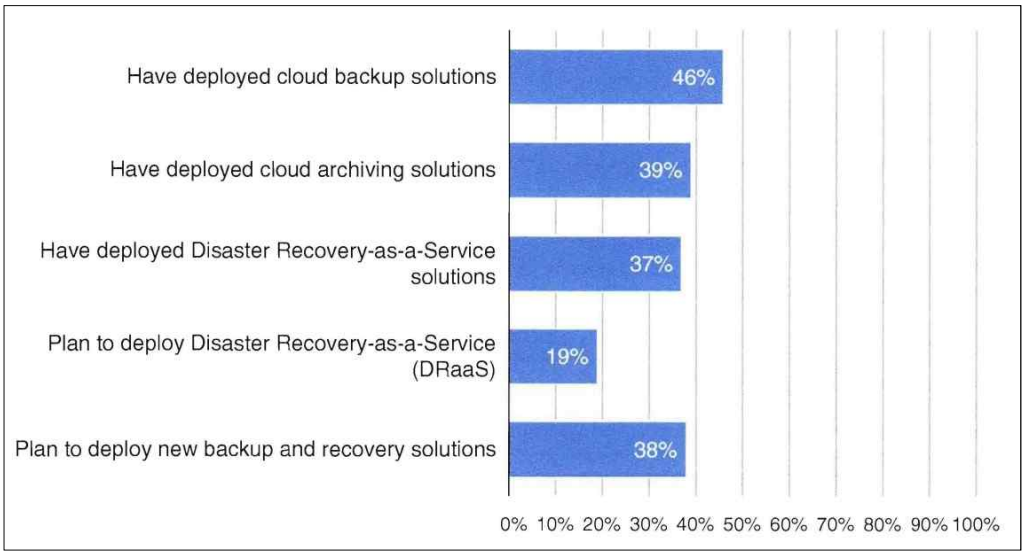


FIGURE 5.11 Companies deployed and planned IT resilience initiatives

Backup and Recovery

83

- An effective IT resilience strategy should consist of four elements:
  1. Availability to keep customers continuously connected to their data and apps.
  2. Mobility to be able to move apps and workloads while keeping them fully protected.
  3. Agility to maintain the freedom to choose your own cloud and be able to move to, from and between clouds.
  4. Training of IT and non-IT employees.
     - They must understand their roles in case of a disruption or disaster and must be trained in how to respond.

Backup and Recovery

84

- Policies and Procedures for IT Resilience and Disaster Recovery
  - Business policies, procedures, and disaster recovery plans around computing resources are critical to IT resilience and cyber security.
  - Acceptable use policy (AUP, 허용가능사용정책) is a document that lists the constraints and practices a user must agree to for access to a corporate network or the Internet.
  - Table 5.7 lists the characteristics of an effective cyber security program.

TABLE 5.7 Characteristics of an Effective Cyber Security Program

• Make data and documents available and accessible 24/7 while simultaneously restricting access.
• Implement and enforce procedures and AUPs (Acceptable Use Policy, 사용가능사용정책) for data, networks, hardware, and software that are company or employee owned, as discussed in the opening case.
• Promote secure and legal sharing of information among authorized persons and partners.
• Ensure compliance with government regulations and laws.
• Prevent attacks by having network intrusion defenses in place.
• Detect, diagnose, and respond to incidents and attacks in real time.
• Maintain internal controls to prevent unauthorized alteration of data/records.
• Recover from business disasters and disruptions quickly.

85

Business Continuity Planning

86

- Business continuity refers to maintaining business functions or restoring them quickly when there has been a major disruption.
- The plan covers business processes, assets, human resources, business partners, and more.
- Fires, earthquakes, floods, power outages, malicious attacks, and other types of disasters hit data centers.
- The purpose of a business continuity plan is to keep the business running after a disaster occurs.

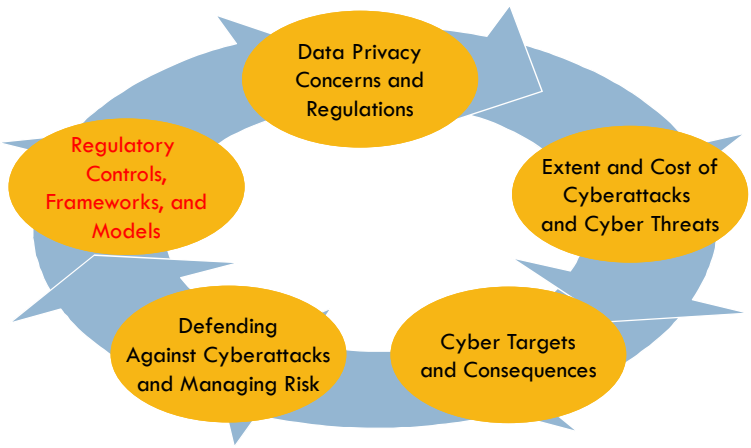
Disaster Recovery Services

87

- Another effective way to recover normal computer and network operations disrupted by a natural or other disaster such as a hurricane, earthquake, or explosion is to set up a secure, off-site disaster recovery space.
  - Hot site. It has all the necessary equipment including office space, furniture, communications capabilities and computer equipment.
  - Warm site. It provides a fully equipped physical data center, but it has no customer data.
  - Cold site. It provides office space but requires the customer to provide and install the equipment needed to continue operations.

Chapter Outline (5 of 5)

88



Regulatory Controls, Frameworks, and Models

89

- Figure 5.12 illustrates the two major categories of cyber defense controls that used to guide the execution of a cyber defense strategy.

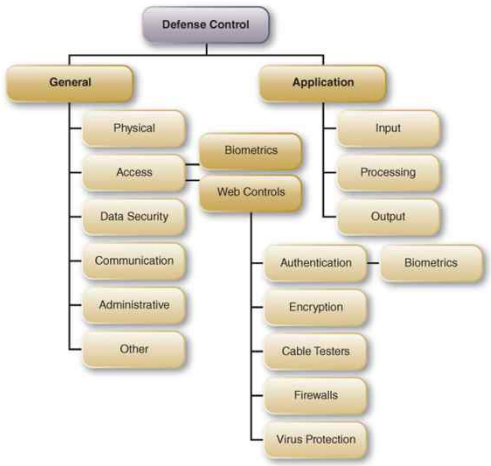
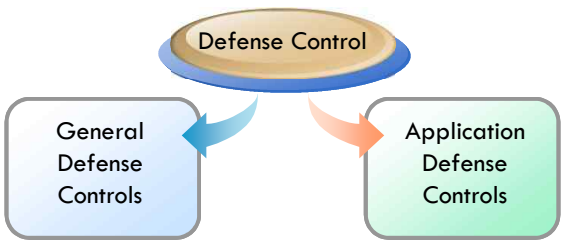


FIGURE 5.12 Major cyber defense controls

Regulatory Controls, Frameworks, and Models

90

General Defense Controls	• Established to protect the system regardless of the specific application. • For example, protecting hardware and controlling access to the data center are independent of the specific application.
Application Defense Controls	• Safeguards that are intended to protect specific applications.



General Defense Controls

91

Physical Controls	• Protect physical computer facilities and resources.
Access Control	• The major line of defense against unauthorized insiders as well as outsiders.
Data Security Controls	• Needed to protect sensitive data throughout the five stages of its life cycle, from creation to disposal.
Communications Controls	• Restrict access to devices on the network to endpoint devices that comply with the organization's security policy and secure the flow of data across networks.
Administrative Controls	• Deal with issuing guidelines and monitoring compliance with an organization's security guidelines.

Application Defense Controls

92

1. Completeness checks to ensure records processing from start to finish
2. Validity checks to ensure only valid data is input or processed
3. Authentication to identify users
4. Authorization to ensure appropriate permissions
5. Input controls to ensure data integrity of all data entered
6. Availability to ensure that the app is available as needed
7. Whitelisting to document appropriate apps
8. Blacklisting to block inappropriate apps

Auditing Information Systems

93

1. Are there enough controls in the system?
2. Which areas are nor covered by controls?
3. Which controls are not necessary?
4. Are the controls implemented properly?
5. Are the controls effective? That is, do they check the output of the system?
6. Is there a clear separation of duties of employees?
7. Are there procedures to ensure compliance with the controls?
8. Are there procedures to ensure reporting and corrective actions in case of violations of controls?

Government Regulations

94

1. Implement training or specific types of security policies and practices.
2. Create cyber security task forces and commissions.
3. Restructure government for improved security.
4. Provide for the security of utilities and critical infrastructure.
5. Study the use of block chain for cyber security.
6. Address the security of connected devices.
7. Address cyber security threats to elections.
8. Provide funding for improved security measures.

Risk Management and IT Governance Frameworks

95

- Enterprise Risk Management Framework
  - ERM is a risk-based approach to managing an enterprise developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
  - The ERM consists of eight components, listed in Table 5.8.

TABLE 5.8 Enterprise Risk Management Framework Components

Components	Description
Internal environment	• Assess risk management philosophy and culture
Objective setting	• Determine relationship of risk to organizational goals
Event identification	• Differentiate between risks and opportunities; negative/positive impact
Risk assessment	• Assess risk probability and impact
Risk response	• Identify and evaluate risk responses
Control activities	• Develop policies and procedures to ensure implementation of risk responses
Information and communication	• Identify, capture, and communicate information
Monitoring	• Conduct ongoing and separate evaluations of risk-related activities

96

Risk Management and IT Governance Frameworks

97

- The COBIT 2019 Framework
  - COBIT 2019 is a globally recognized governance framework that integrates security, risk management, and IT governance developed by ISACA-the International Systems Audit and Control Association.
  - Its purpose is to enable management, users, and IS audit, control, and security practitioners to bridge the gap between control requirements, technical issues, and business risks.
  - Figure 5.13

FIGURE 5.13 COBIT 2019 principles and components

98

Industry Security Standards

99

- Industry groups impose their own standards to protect their customers and their members' brand images and revenues.
- One example is the Payment Card Industry Data Security Standard (PCI DSS) created by Visa, MasterCard, American Express, and Discover.
- The purpose of the PCI DSS is to improve customers' trust in e-commerce, especially when it comes to online payments, and to increase the Web security of online merchants.

IT Security Defense-In-Depth Model

100

- The Defense-in-Depth Model (심층방어모델) is based upon the premise that no organization can ever be fully protected by a single layer of security.
  - Figure 5.14
- The Model's objective is to provide redundancy to buy an organization more time in the event of a cyberattack or other vulnerability and involves people, processes, technology and the system's physical environment.

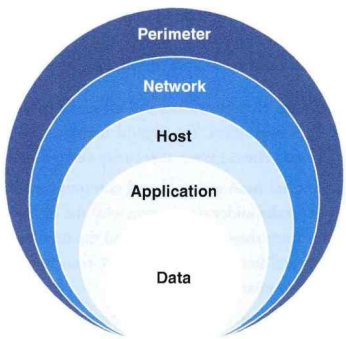


FIGURE 5.14 Multiple layers of defense


"더 나은 보안을 위한 종합적인 접근" 심층 방어의 이해

'심층 방어(Defense in depth)'란 하나가 실패하면 다른 것이 버틸 것이라고 가정해 여러 개의 보안 도구, 메커니즘, 정책을 배치하는 보안 전략이다. 예컨대 해커들이 네트워크에 침투하지 못하도록 방화벽에만 의존하는 대신, 엔드포인트 보안 소프트웨어와 IDS(Intrusion Detection System)를 배포해 방화벽을 통과한 공격자를 찾아낸다.

IT Security Defense-In-Depth Model

101

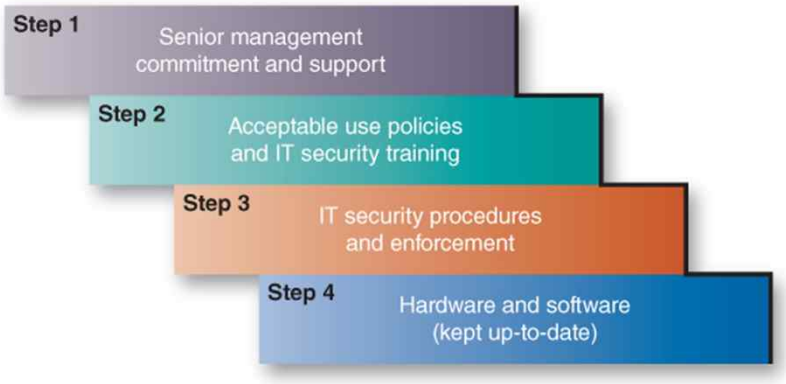


FIGURE 5.15.1 IT security defense-in-depth model

IT Security Defense-In-Depth Model

102

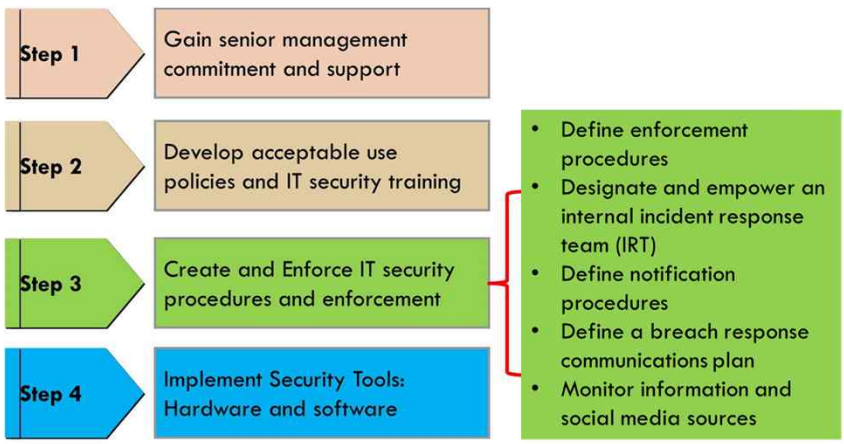


FIGURE 5.15.2 IT security defense-in-depth model