Chapter 1: Introduction to Security

Gonzalo De La Torre Parra, Ph.D.

Fall 2021

Objectives

- Explain the challenges of securing information
- Define information security and explain why it is important
- Identify the types of threat actors that are common today
- Describe how to defend against attacks

1.1 Challenges of Securing Information

- Tens of billions of dollars are spent annually on computer security yet, the number of successful attacks continues to increase.
- Cyber Security Events:
  - Remote control of a Jeep Cherokee
  - Probing aircraft systems while in flight (United airlines)
  - 500 million compromised accounts (Yahoo)
  - Rubber duckies (USB Flash drives containing malware)
  - Lock down its administrator account and wireless network settings on voting machines (WinVote)

1.1 Breaches on Personal Information

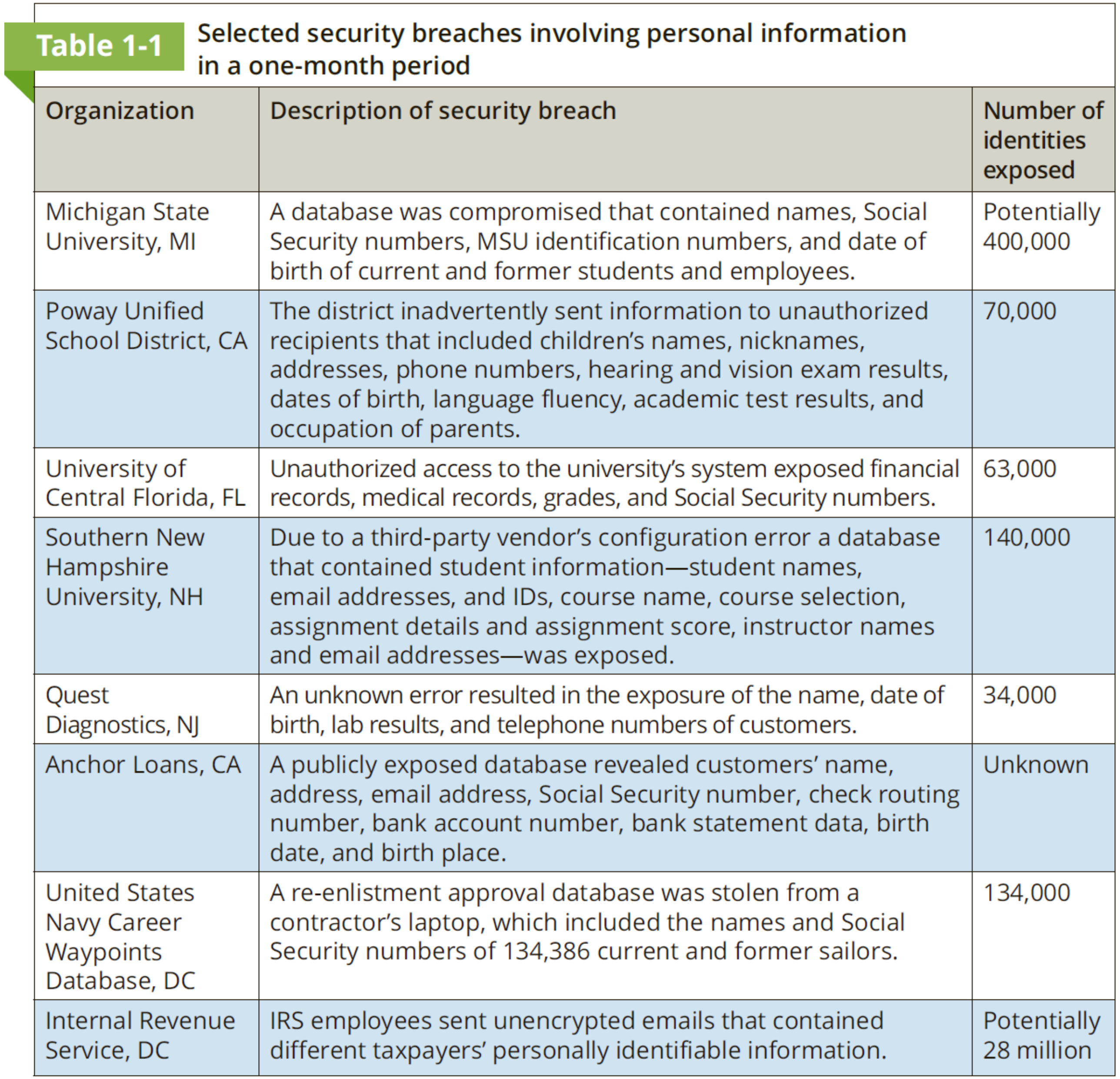


Table 1-1 Selected security breaches involving personal information in a one-month period

Organization	Description of security breach	Number of identities exposed
Michigan State University, MI	A database was compromised that contained names, Social Security numbers, MSU identification numbers, and date of birth of current and former students and employees.	Potentially 400,000
Poway Unified School District, CA	The district inadvertently sent information to unauthorized recipients that included children's names, nicknames, addresses, phone numbers, hearing and vision exam results, dates of birth, language fluency, academic test results, and occupation of parents.	70,000
University of Central Florida, FL	Unauthorized access to the university's system exposed financial records, medical records, grades, and Social Security numbers.	63,000
Southern New Hampshire University, NH	Due to a third-party vendor's configuration error a database that contained student information—student names, email addresses, and IDs, course name, course selection, assignment details and assignment score, instructor names and email addresses—was exposed.	140,000
Quest Diagnostics, NJ	An unknown error resulted in the exposure of the name, date of birth, lab results, and telephone numbers of customers.	34,000
Anchor Loans, CA	A publicly exposed database revealed customers' name, address, email address, Social Security number, check routing number, bank account number, bank statement data, birth date, and birth place.	Unknown
United States Navy Career Waypoints Database, DC	A re-enlistment approval database was stolen from a contractor's laptop, which included the names and Social Security numbers of 134,386 current and former sailors.	134,000
Internal Revenue Service, DC	IRS employees sent unencrypted emails that contained different taxpayers' personally identifiable information.	Potentially 28 million

Why are these attack successful?

- Widespread vulnerabilities
- Configuration issues
- Poorly designed software
- Hardware limitations
- Enterprise-based issues

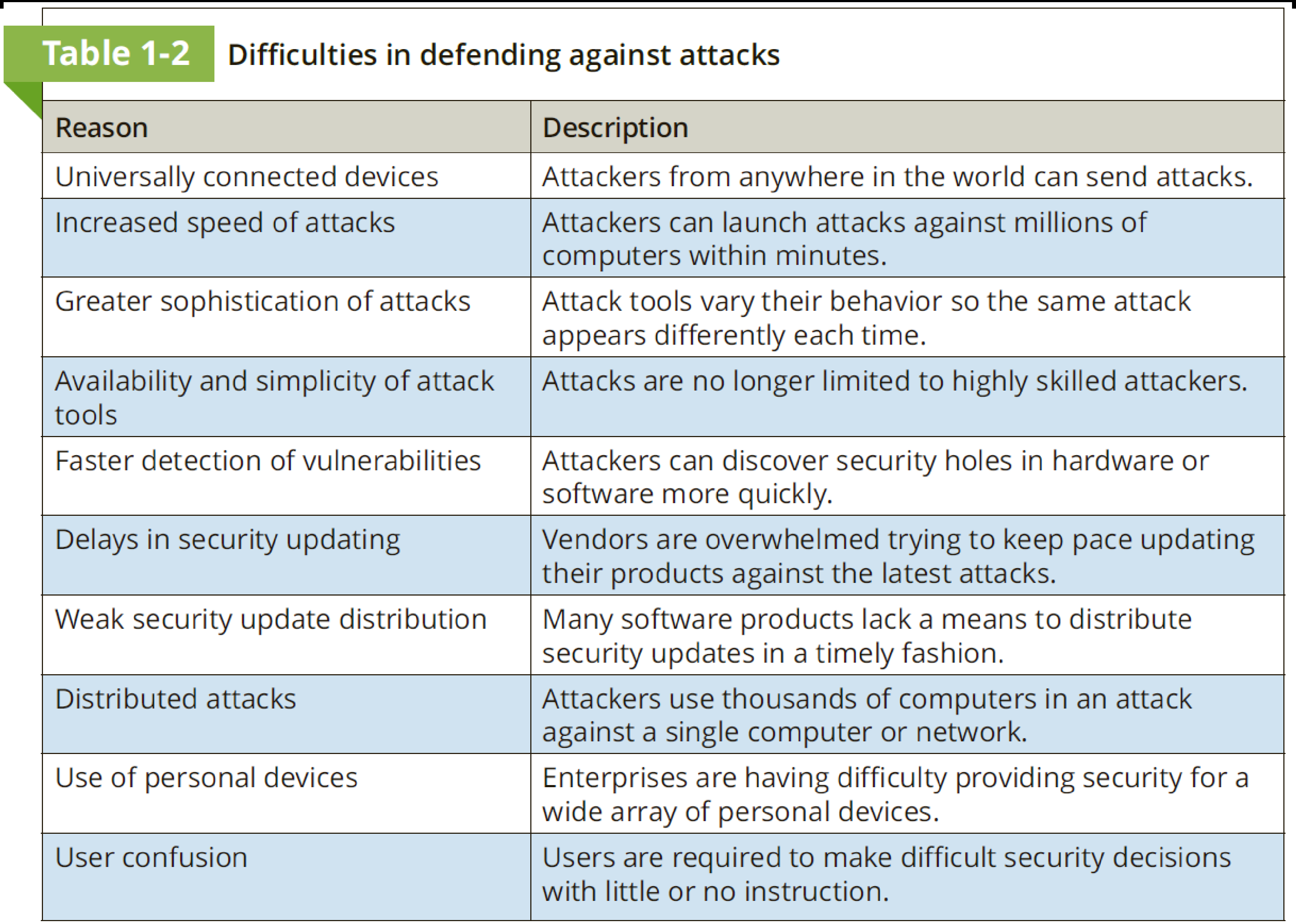
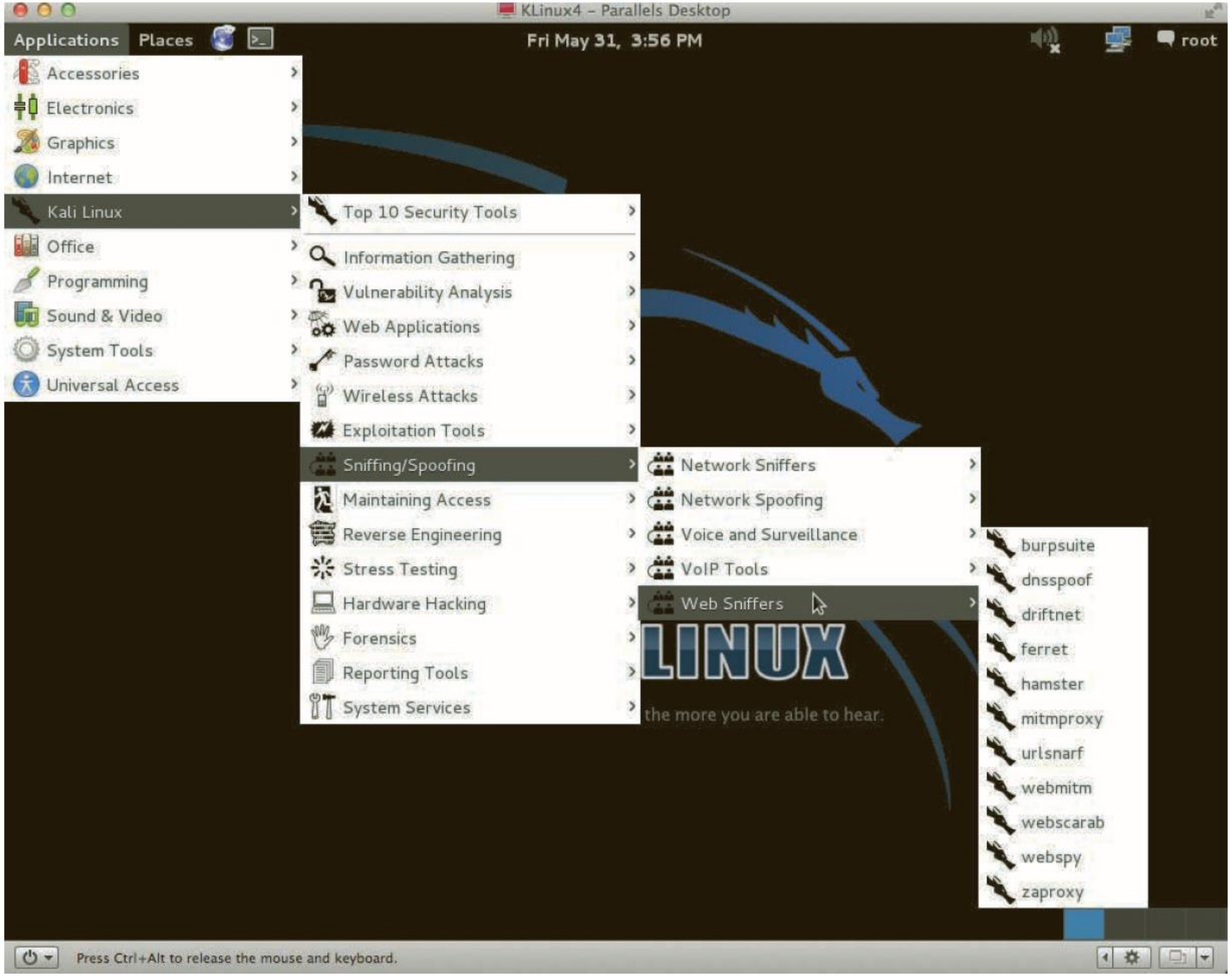


Table 1-2 Difficulties in defending against attacks

Reason	Description
Universally connected devices	Attackers from anywhere in the world can send attacks.
Increased speed of attacks	Attackers can launch attacks against millions of computers within minutes.
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time.
Availability and simplicity of attack tools	Attacks are no longer limited to highly skilled attackers.
Faster detection of vulnerabilities	Attackers can discover security holes in hardware or software more quickly.
Delays in security updating	Vendors are overwhelmed trying to keep pace updating their products against the latest attacks.
Weak security update distribution	Many software products lack a means to distribute security updates in a timely fashion.
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network.
Use of personal devices	Enterprises are having difficulty providing security for a wide array of personal devices.
User confusion	Users are required to make difficult security decisions with little or no instruction.

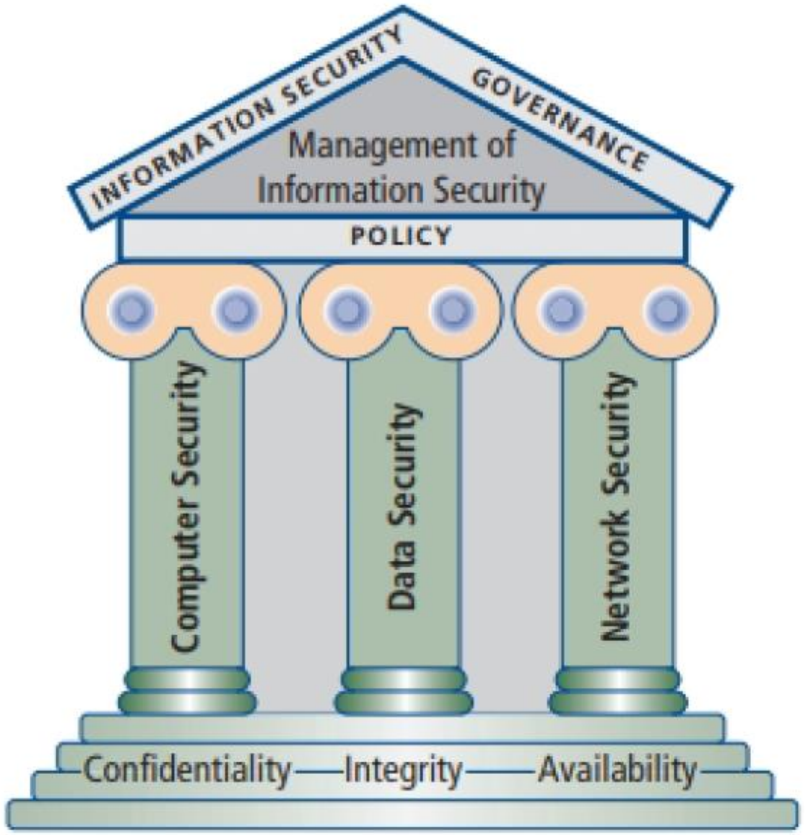
E.g. Kali Linux



Press Ctrl+Alt to release the mouse and keyboard.

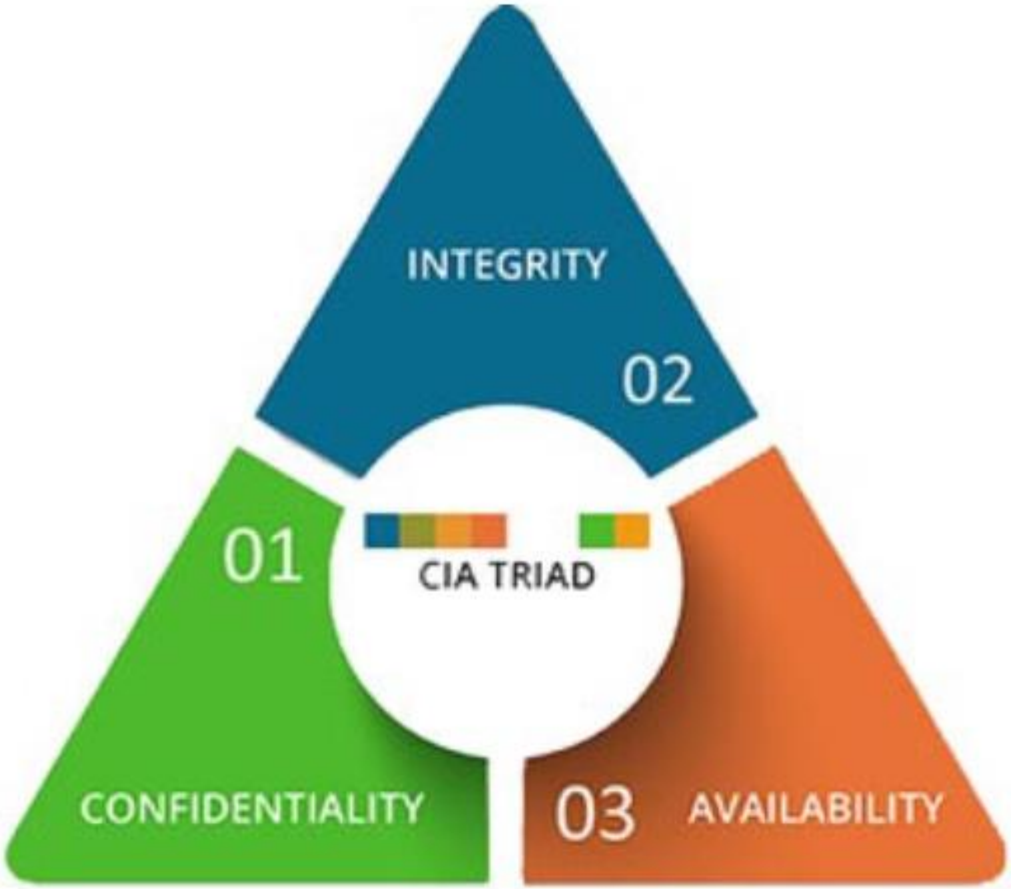
Understanding Security and Information Security

- Security:
  - The measures taken to ensure safety
  - The necessary steps to protect from harm
- Information Security
  - Ensure that protective measures are properly implemented to ward off attacks and prevent the total collapse of the system when a successful attack does occur
  - Protect information that provides value to people and enterprises



CIA Triad

- CIA: Three protections that must be extended over information
- Information security revolves around the three key principles: confidentiality, integrity and availability (CIA).
- Key characteristics of information that make it valuable to an organization



What is Confidentiality?

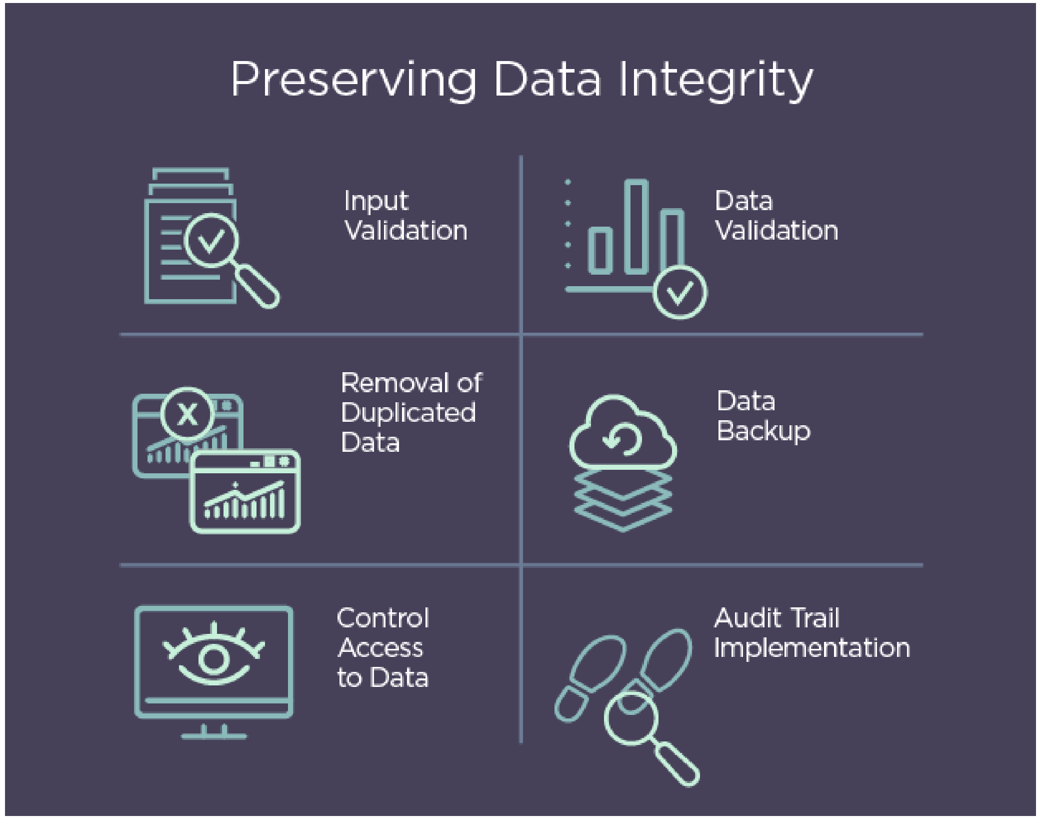
- Confidentiality measures are designed to protect against unauthorized disclosure of information. The objective of the confidentiality principle is to ensure that private information remains private and that it can only be viewed or accessed by individuals who need that information in order to complete their job duties.

What is Confidentiality?

- While U.S. federal agencies have had lapses that resulted in unwanted data disclosures, an event in July 2015 eclipsed all previous similar lapses.
- The loss of 21.5 million federal background-check files rocked the Office of Personnel Management (OPM)
- Revealing names, addresses, financial records, health data, and other sensitive private information
- Chinese hackers (Believed to be responsible)

What is Integrity?

- Integrity involves protection from unauthorized modifications (e.g., add, delete, or change) of data. The principle of integrity is designed to ensure that data can be trusted to be accurate and that it has not been inappropriately modified.



Preserving Data Integrity

Input Validation

Data Validation

Removal of Duplicated Data

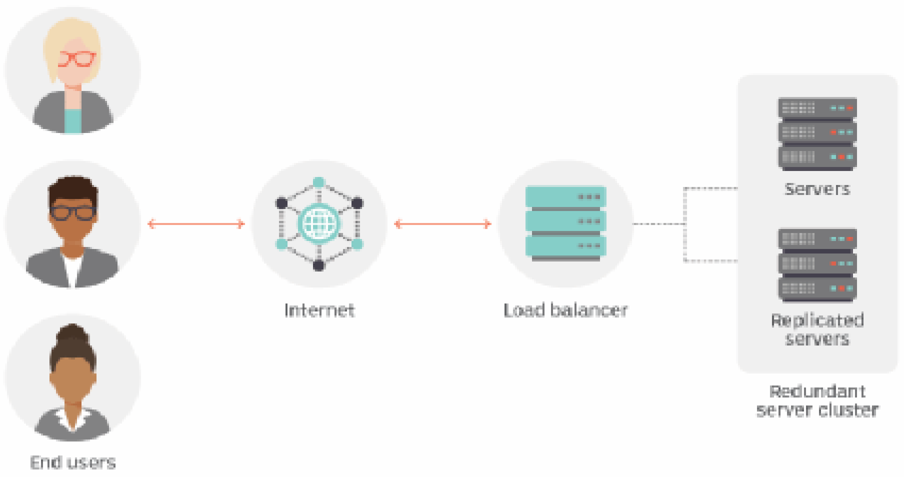
Data Backup

Control Access to Data

Audit Trail Implementation

What is availability?

- Availability is protecting the functionality of support systems and ensuring data is fully available at the point in time (or period requirements) when it is needed by its users. The objective of availability is to ensure that data is available to be used when it is needed to make decisions.



Information Security Layers

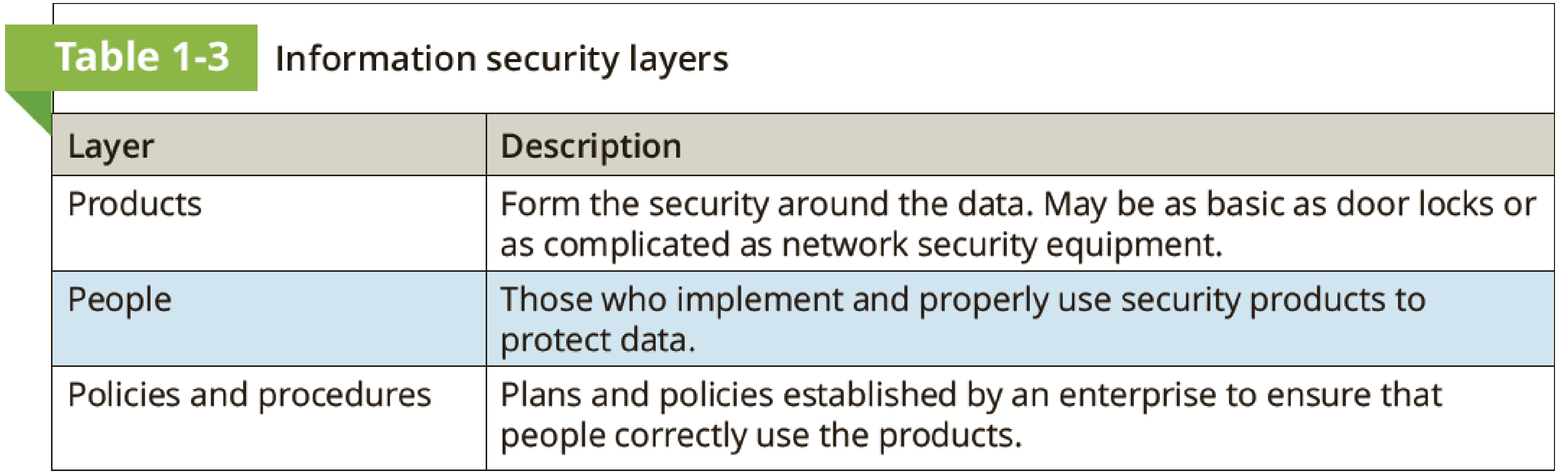


Table 1-3 Information security layers

Layer	Description
Products	Form the security around the data. May be as basic as door locks or as complicated as network security equipment.
People	Those who implement and properly use security products to protect data.
Policies and procedures	Plans and policies established by an enterprise to ensure that people correctly use the products.

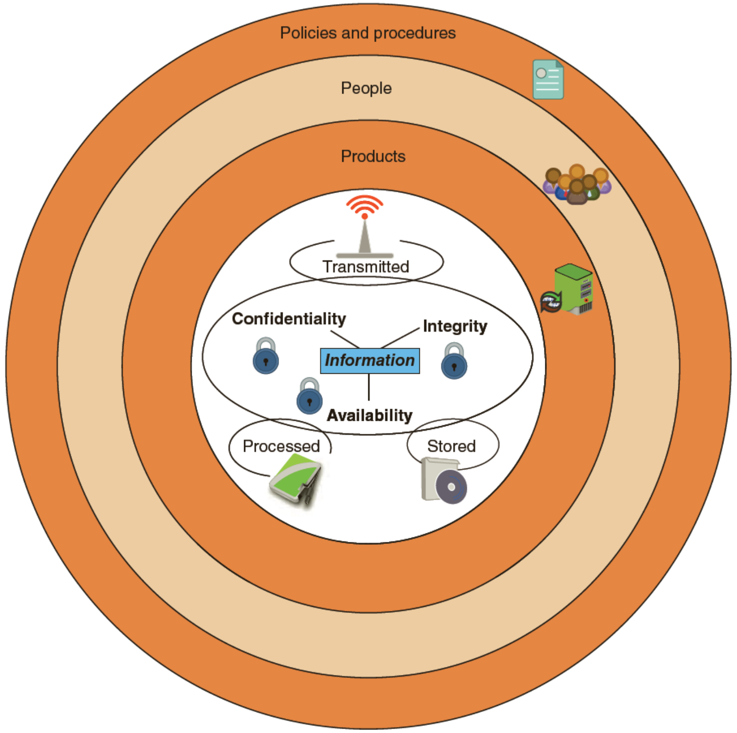


Figure 1-3 Information security layers

Information Security Components Analogy

- Suppose that Ellie wants to purchase a new motorized Italian scooter to ride from her apartment to school and work. However, because several scooters have been stolen near her apartment she is concerned about its protection. Although she parks the scooter in the gated parking lot in front of her apartment, a hole in the fence surrounding the apartment complex makes it possible for someone to access the parking lot without restriction.
- Which is the *asset*?
- What is the *vulnerability*?
- What is the *attack vector*?
- What is the threat?
- Who is the *threat actor*?
- What is the *risk*?

Information Security Components Analogy

- Which is the *asset*?
- What is the *vulnerability*?
- What is the *attack vector*?
- What is the threat?
- Who is the *threat actor*?
- What is the *risk*?

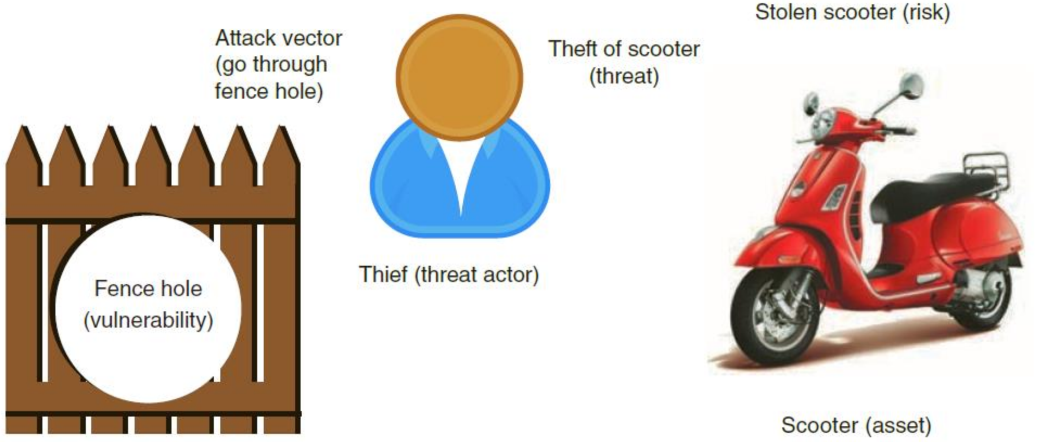

Attack vector (go through fence hole)
Fence hole (vulnerability)
Thief (threat actor)
Theft of scooter (threat)
Stolen scooter (risk)
Scooter (asset)

Figure 1-4 Information security components analogy

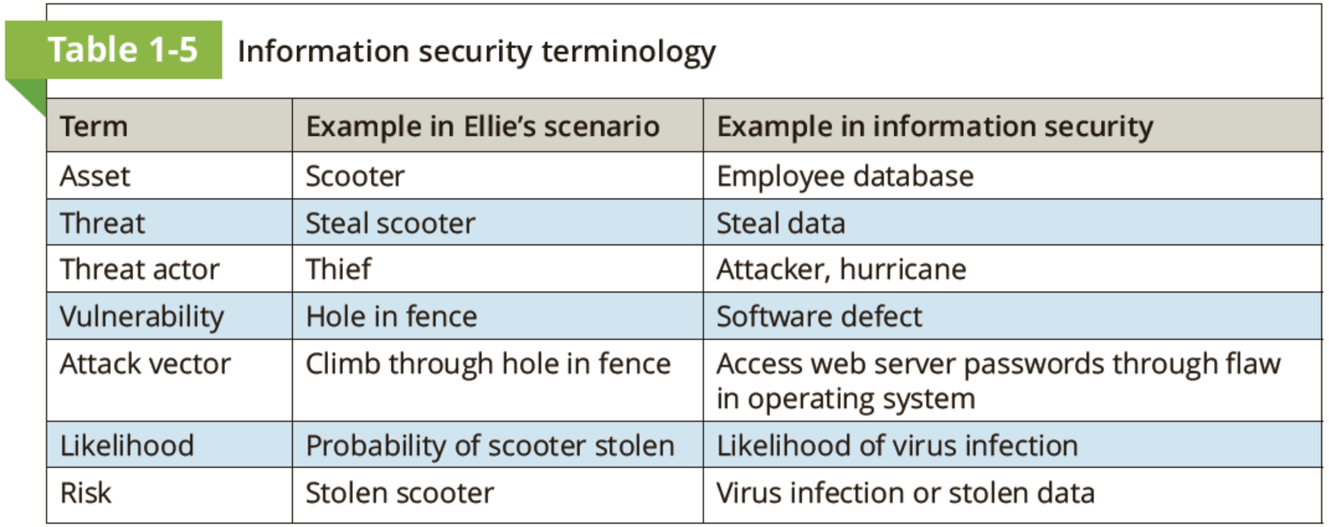


Table 1-5 Information security terminology

Term	Example in Ellie's scenario	Example in information security
Asset	Scooter	Employee database
Threat	Steal scooter	Steal data
Threat actor	Thief	Attacker, hurricane
Vulnerability	Hole in fence	Software defect
Attack vector	Climb through hole in fence	Access web server passwords through flaw in operating system
Likelihood	Probability of scooter stolen	Likelihood of virus infection
Risk	Stolen scooter	Virus infection or stolen data

Should everything be considered an asset?

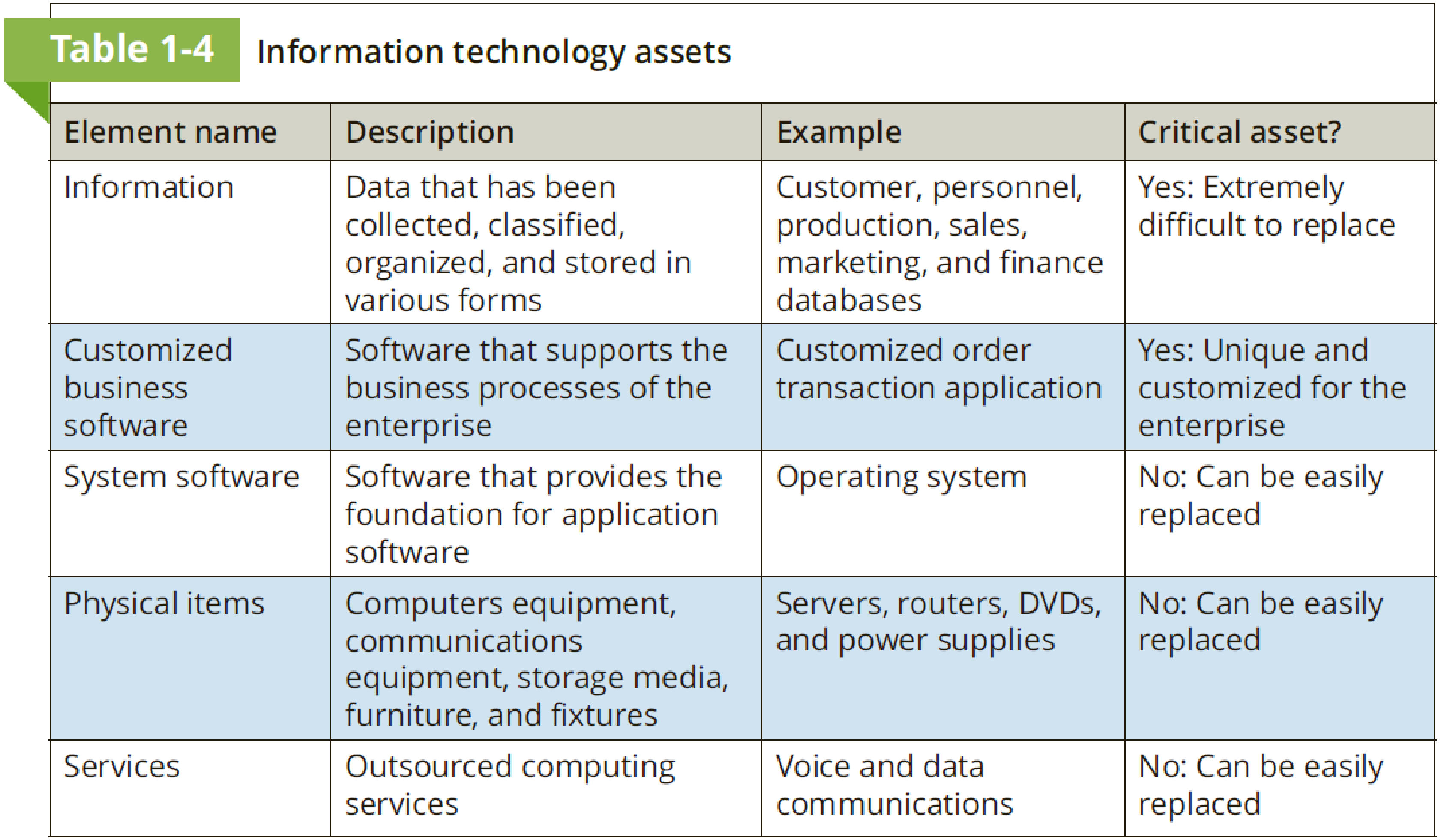


Table 1-4 Information technology assets

Element name	Description	Example	Critical asset?
Information	Data that has been collected, classified, organized, and stored in various forms	Customer, personnel, production, sales, marketing, and finance databases	Yes: Extremely difficult to replace
Customized business software	Software that supports the business processes of the enterprise	Customized order transaction application	Yes: Unique and customized for the enterprise
System software	Software that provides the foundation for application software	Operating system	No: Can be easily replaced
Physical items	Computers equipment, communications equipment, storage media, furniture, and fixtures	Servers, routers, DVDs, and power supplies	No: Can be easily replaced
Services	Outsourced computing services	Voice and data communications	No: Can be easily replaced

Risk response techniques

1. Accept
2. Transfer
3. Avoid
4. Mitigate

Risk response techniques

1. Accept: Risk acknowledgement – no steps are taken to address it
2. Transfer: Pass the risk to a third party (E.g., Insurance)
3. Avoid: Not acquiring the asset
4. Mitigate: Address the risk

Importance of Information Security

- Preventing data theft
- Thwarting Identity Theft
- Avoiding Legal Consequences (Data Protection Federal and State Laws)
  - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - The Sarbanes-Oxley Act of 2002 (Sarbox)
  - The Gramm-Leach-Bliley Act (GLBA)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - State notification and security laws

Maintaining Productivity

- Cleaning up after an attack diverts time, money, and other resources away from normal activities.

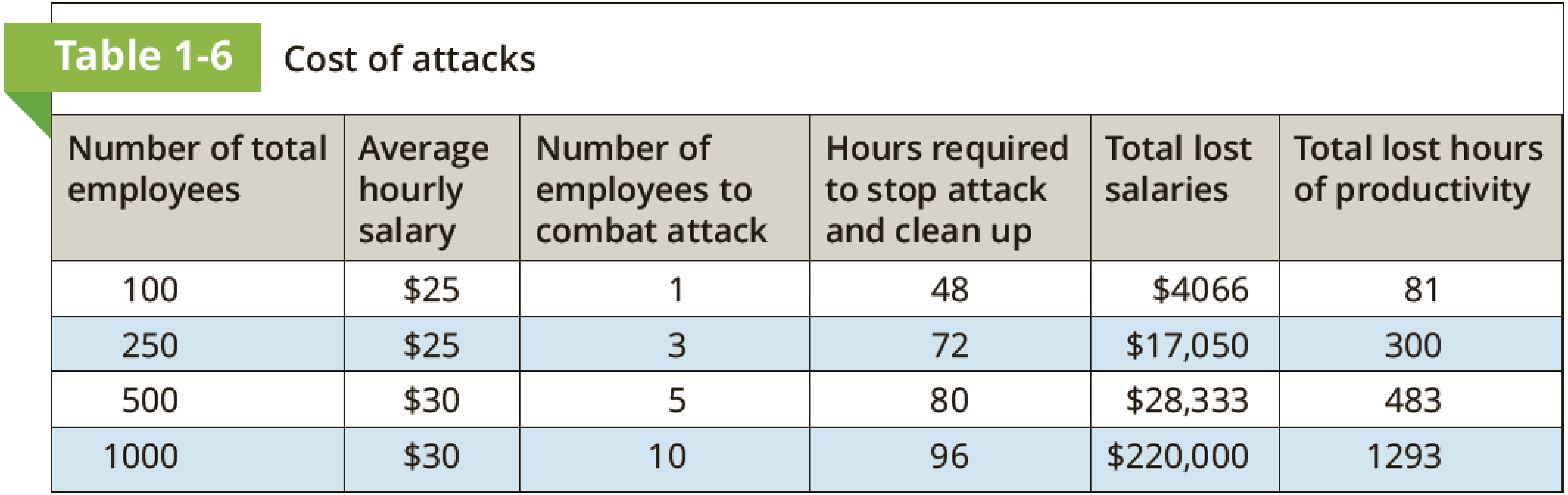


Table 1-6 Cost of attacks

Number of total employees	Average hourly salary	Number of employees to combat attack	Hours required to stop attack and clean up	Total lost salaries	Total lost hours of productivity
100	$25	1	48	$4066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1000	$30	10	96	$220,000	1293

Cyberterrorism

- The FBI defines cyberterrorism as any “premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents.”
- Objective
  - Cause panic or provoke violence among citizens

Threat Actor

- Threat actor is a generic term used to describe individuals who launch attacks against other users and their computers (another generic word is simply attackers).
    - Script Kiddies
    - Hacktivists
    - Nation State Actors
    - Insiders
    - Competitors
    - Organized crime
    - Brokers
    - Cyberterrorists

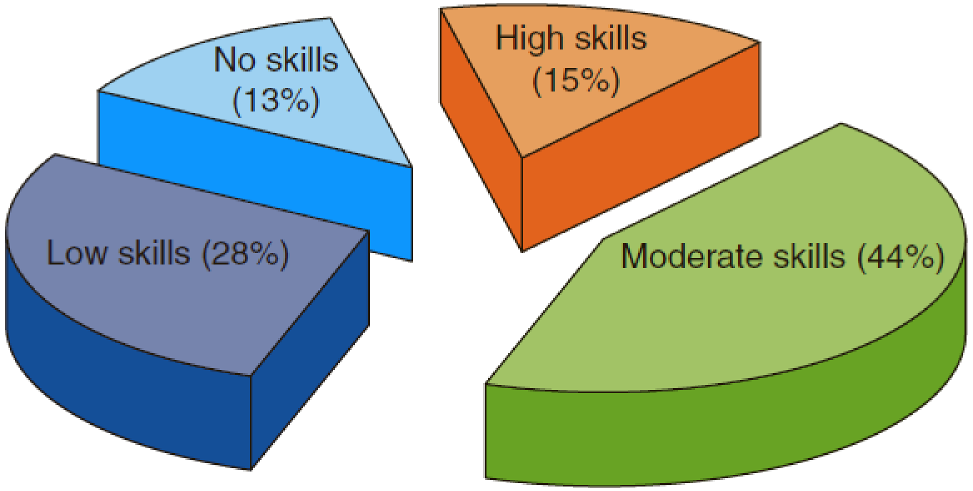
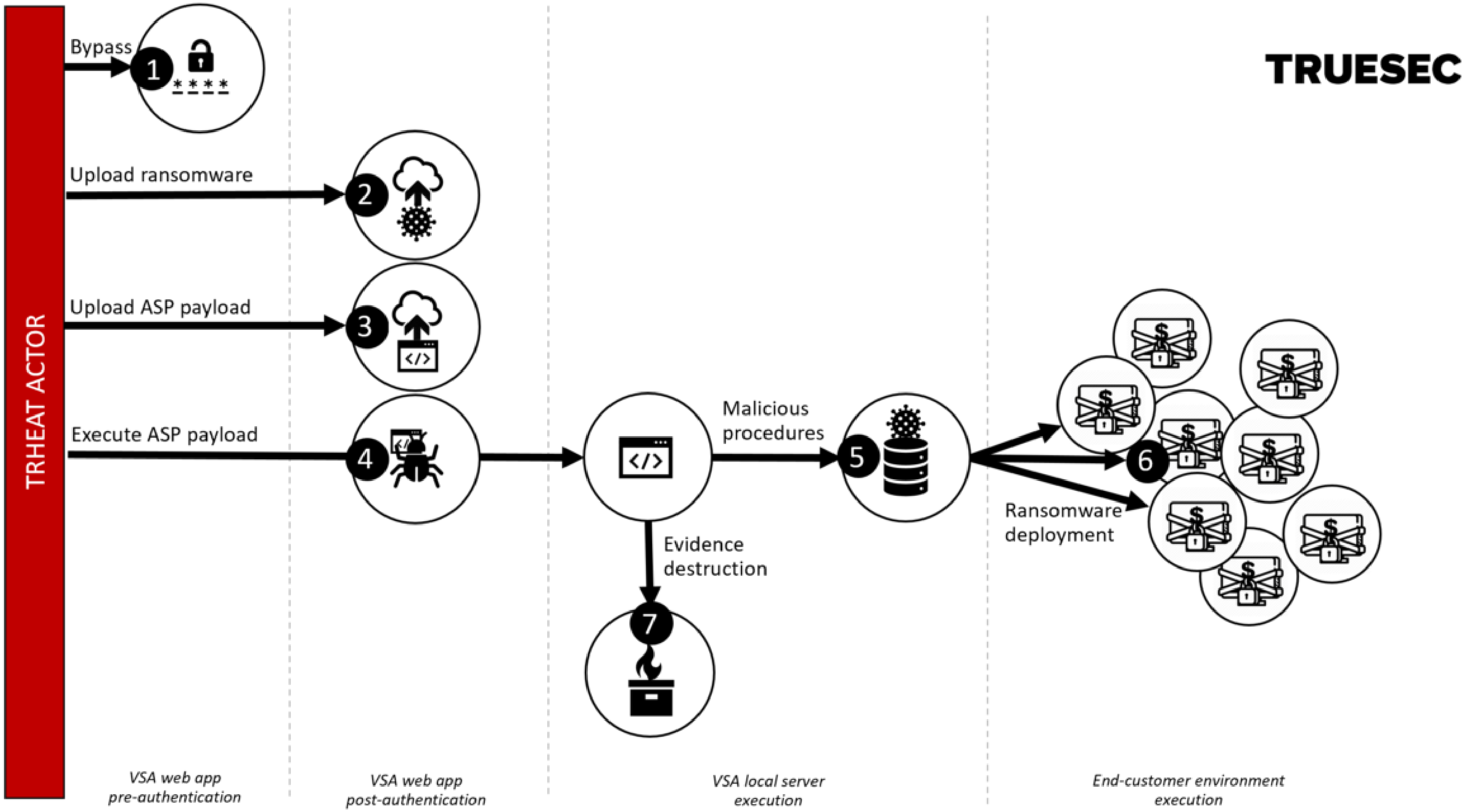


Figure 1-5 Skills needed for creating attacks

Fundamental Security Principles

- Layering: A layered security approach, also called defense-in-depth, can be useful in resisting a variety of attacks. If only one defense mechanism is in place, an attacker only has to circumvent that single defense.
- Limiting: Limiting access to information reduces the threat against it. This means that only those personnel who must use the data should have access to it.
- Diversity: Multiple types of security mechanisms (E.g., Access control, technical controls, administrative controls, etc.)
- Obscurity: Not revealing the type of computer, version of operating system, or brand of software that is used.
- Simplicity: As much as possible, a secure system should be simple for those on the inside to understand and use. Yet, it should be complex from the outside.

Kaseya Attack Timeline



https://blog.truesec.com/2021/07/06/kaseya-vsa-zero-day-exploit/