CIT 270: SYSTEMS SECURITY I

CHAPTER 1: INTRODUCTION TO SECURITY

BYU IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

INTRODUCTION

Attacks can be successful with little skill:

- See: *Today's Attacks and Defenses*

Security personnel are greatly needed:

- Chief Information Security Officer (CISO)
- Security Manager
- Security Administrator
- Security Technician

CompTIA Security+

- ISO 17024
- DoD 8570.01-M
- FISMA

↑18%
2015 projection

↑28%
2019 projection

BYU IDAHO

CHALLENGES OF SECURING INFORMATION

Widespread Vulnerabilities:

- lack of vendor support
- end-of-life (EOL) systems

Configuration Issues:

- weak default configurations
- misconfiguration
- improperly configured accounts

Poorly Designed Software:

- architecture / design weakness
- improper input / error handling
- race conditions

Poorly Designed Software

Tchap the not so secure and private messaging app for the French Government.

CHALLENGES OF SECURING INFORMATION

Faster Detection of Vulnerabilities

- zero day

Delays in Security Updating

- hardware
- software
- vendors
- you / companies

Weak Security Update Distribution

Distributed Attacks

Use of Personal Devices

User Confusion

- untrained users

WHAT IS INFORMATION SECURITY?

The word *security* comes from Latin and means to be *free from care*. This leads to a modern day interpretation of *the state of being free from danger*.

Security is proportional. As security increases convenience is often decreased. If security is decreased (lowered) convenience is usually increased.

Security is not a war to be won or lost. Threats and attacks will never be completely eradicated.

WHAT IS INFORMATION SECURITY?

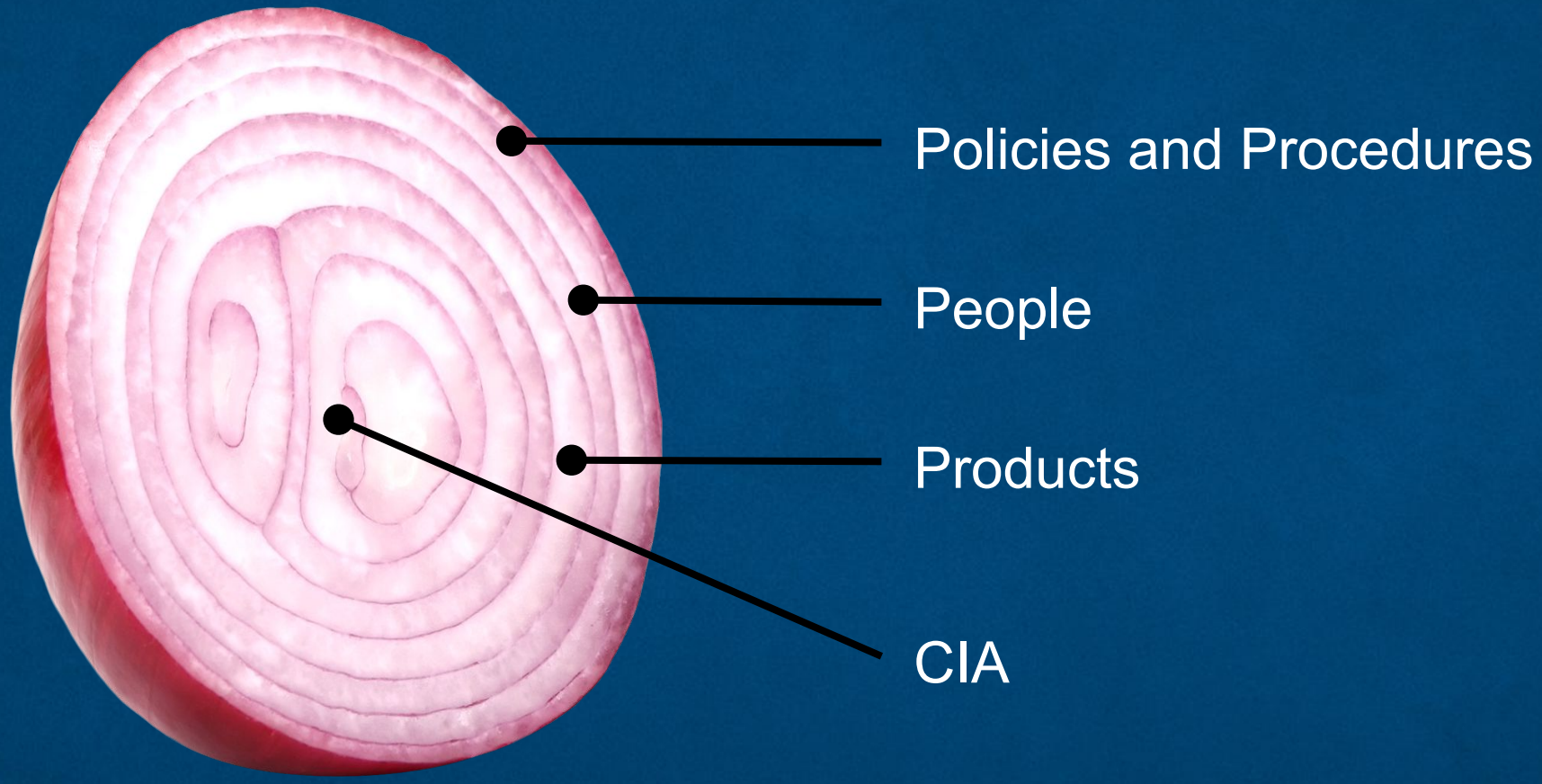
Information Security is about protecting information (data) that provides value to people and business'. Remember:

C Confidentiality: Only authorized parties can view and alter data

I Integrity: Data is correct and unaltered

A Availability: Data is accessible to authorized users

WHAT IS INFORMATION SECURITY?



Information Security Layers

INFORMATION SECURITY TERMINOLOGY

Assets: An item that has value to the enterprise and is not easily replaced.

- information (data)
- customized software
- system software
- physical items
- outsourced services

Threat Actor: A person or element that has power to carry out a threat.

- person or group
- software
- nature

INFORMATION SECURITY TERMINOLOGY

Vulnerability: A flaw or weakness that allows someone to bypass security.

Attack Vector: Means by which an attack can occur; exploiting a vulnerability.

Risk: Situation that involves exposure to some type of danger.

Risk Response Techniques:

- accept: risk is acknowledged and no steps taken to avoid it.
- transfer: risk is transferred to someone else; insurance.
- avoid: risk is identified and a decision is made not to engage in an activity.
- mitigate: risk is identified and attempts are made to make it less serious.

THE IMPORTANCE OF INFORMATION SECURITY

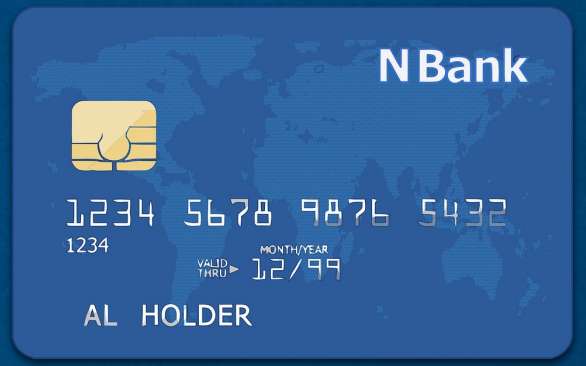
Information Security (Info Sec) is important to business' and individuals because it helps prevent:

- data theft
- identity theft
- legal consequences
- productivity loss
- cyberterrorism

THE IMPORTANCE OF INFORMATION SECURITY

Information Security (Info Sec) is important to business' and individuals because it helps prevent:

- data theft
- identity theft
- legal consequences
- productivity loss
- cyberterrorism



- proprietary information
- private information

- existing-card fraud
- new-account fraud
- card-not-present fraud

THE IMPORTANCE OF INFORMATION SECURITY

Information Security (Info Sec) is important to business' and individuals because it helps prevent:

- data theft
- identity theft
- legal consequences
- productivity loss
- cyberterrorism

HIPAA

$50,000 per violation fine

$1.5 Million per year max

10 years in prison

THE IMPORTANCE OF INFORMATION SECURITY

Information Security (Info Sec) is important to business' and individuals because it helps prevent:

- data theft
- identity theft
- legal consequences
- productivity loss
- cyberterrorism

ILOVEYOU

The love bug attack was a computer worm that cost an estimated $8.7 billion to fix. Imagine the time it took every business and user to fix their computers and recover data.

WHO ARE THE THREAT ACTORS?

Threat Actor is a generic term for individuals who launch attacks against other users of *computers*.

Attributes or characteristics of threat actors vary widely:

- simple
- curious
- little or no funding
- sophisticated with a high degree of complexity
- funded and resourced
- internal
- external
- motivation

WHO ARE THE THREAT ACTORS?

Script Kiddies: someone who wants to attack a computer but lacks the knowledge to do so successfully.

Hacktivists: an individual or group motivated by ideology; principles or beliefs.

Nation State Actors: state-sponsored attacks against a nation's foes.

STUXNET

Malicious computer worm, thought to have been in development since at least 2005. Believed to be responsible for causing substantial damage to Iran's nuclear program.

WHO ARE THE THREAT ACTORS?

Insiders: an enterprises own employees, contractors, or partners.

There are many more types:

- competitors
- organized crime
- brokers
- cyberterrorists

DEFENDING AGAINST ATTACKS

Multiple defenses are necessary to withstand an attack. Traditionally there are five fundamental security principles:

- layering
- limiting
- diversity
- obscurity
- simplicity

DEFENDING AGAINST ATTACKS

Multiple defenses are necessary to withstand an attack. Traditionally there are five fundamental security principles:

- layering
- limiting
- diversity
- obscurity
- simplicity

Layered security, also called defense-in-depth, can be useful in resisting a variety of attacks. This provides the most comprehensive protection.

DEFENDING AGAINST ATTACKS

Multiple defenses are necessary to withstand an attack. Traditionally there are five fundamental security principles:

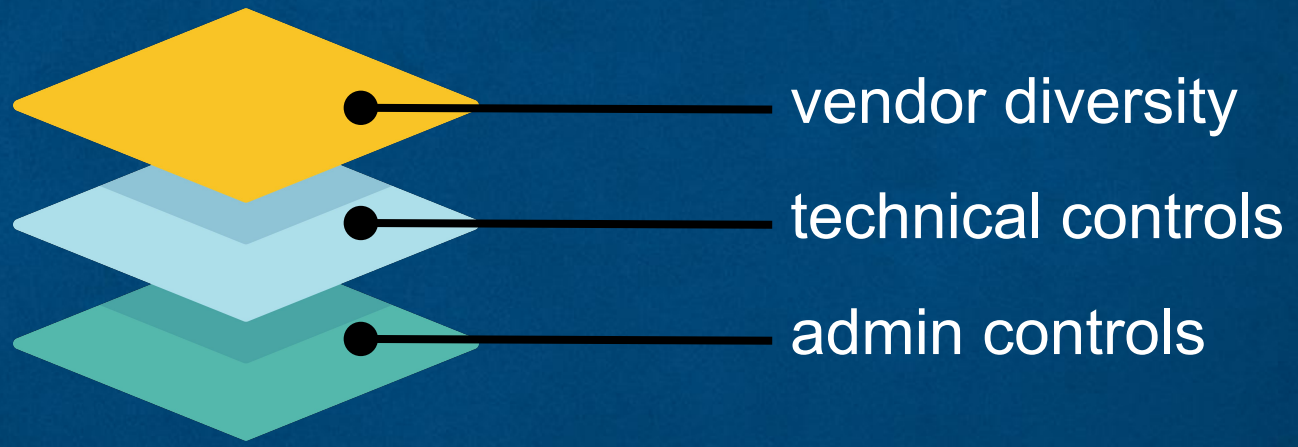
- layering
- limiting
- diversity
- obscurity
- simplicity

You can limit with technology: file permissions
You can limit with procedure: secure document room

DEFENDING AGAINST ATTACKS

Multiple defenses are necessary to withstand an attack. Traditionally there are five fundamental security principles:

- layering
- limiting
- diversity
- obscurity
- simplicity



Similar to layering, your security protections must be diverse. If you have 10 layers of the same type of security an attacker only has to break 1 level.

DEFENDING AGAINST ATTACKS

Multiple defenses are necessary to withstand an attack. Traditionally there are five fundamental security principles:

- layering
- limiting
- diversity
- obscurity
- simplicity

Security by obscurity means to obscure to the outside world what is on the inside making it difficult to plan an attack.

DEFENDING AGAINST ATTACKS

Multiple defenses are necessary to withstand an attack. Traditionally there are five fundamental security principles:

- layering
- limiting
- diversity
- obscurity
- simplicity

Keep security complexity from the inside simple and from the outside complex; if these books are your security policy no one will ever do your security right.

REFERENCES

Ahkâm. Slice Onion [PNG]. Free Icons Png, Aug. 2019, www.freeiconspng.com/img/38744.

Blue Vespa Scooter [PNG]. Png Find, Aug. 2019,
https://www.pngfind.com/mpng/hbbTbx_scooter-png-vespa-png-transparent-png.

Caduceus Medical Snake [PNG]. Pixabay, Aug. 2019,
https://pixabay.com/vectors/medicine-caduceus-medical-snake-295067.

Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.). Boston, MA: Cengage.

ElisaRiva. Business Buildings [PNG]. Pixabay, Aug. 2019,
https://pixabay.com/illustrations/palaces-city-palazzo-windows-1856386.

Iceberg [PNG]. Pin Clipart, Sep. 2019,
https://www.pinclipart.com/pindetail/ihhThwo_transparent-background-iceberg-clipart-png-download.

“Information Security Analysts.” Bureau of Labor Statistics, Aug. 2019,
www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

REFERENCES

Maklay62. Don’t Touch Reminder Post Note [PNG]. Pixabay, Sep. 2019, https://pixabay.com/illustrations/don-t-touch-reminder-post-note-1433095.

Multimedia. Chain Link [PNG]. Share Icon, Aug. 2019, www.shareicon.net/multimedia-connection-link-chain-linked-ui-tools-and-utensils-855208.

Naalexander. Credit Card [PNG]. Pixabay, Aug. 2019, https://pixabay.com/vectors/credit-card-credit-card-mastercard-3643710.

Nickbratton. Layers [PNG]. Icons PNG, Sep. 2019, https://www.iconspng.com/image/86543/layer.

Stack of Books [PNG]. Trzcacak, Sep. 2019, https://www.trzcacak.rs/imgm/hbxiwJx_pile-of-books-png-transparent-background-stack-of.