

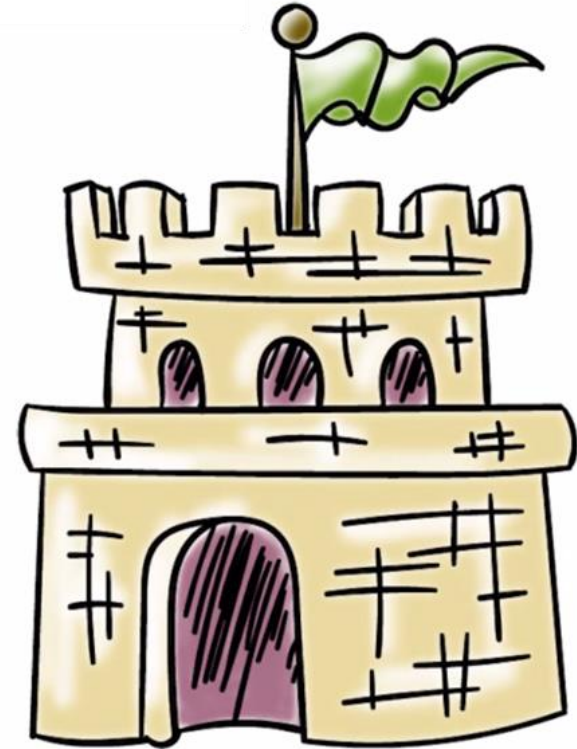
Security Mindset

Lesson Introduction

- Why is **cyber security** important?
 - How do we **understand cyber security**?
 - What needs to be done to **address cyber security**?
-

Why Cyber Security?

We worry about **security** when...



...we have **something of value** and there is a **risk it could be harmed**.

Why Cyber Security?



Individuals store a lot of sensitive data online

- if stolen, criminals can profit from it

Societies rely on the internet

nefarious parties could profit by controlling it

Why Cyber Security?



Smart Grids rely on cyber systems

- whoever controls the grid controls the community infrastructure

Business and government proprietary information is often stored on the internet

unauthorized access could be economically or politically disastrous



Security Impact Quiz

Each of these organizations **suffered data breaches** of more than 30,000 records. Check the companies that **you have patronized**:

- ☐ Home Depot
- ☐ Facebook
- ☐ Ebay
- ☐ Apple
- ☐ JP Morgan Chase
- ☐ Snapchat

- ☐ Anthem
- ☐ Target
- ☐ Twitter
- ☐ UPS
- ☐ Mozilla
- ☐ Nintendo

Cyber Assets at Risk

How do we understand the risk to our online information and systems?

We need to develop a security mindset

What is the security mindset?

Threats, vulnerabilities and attacks

Cyber Assets at Risk

Threat source: who wants to do harm to us in our online lives



Cybercriminals: want to profit from our sensitive data for financial gain.

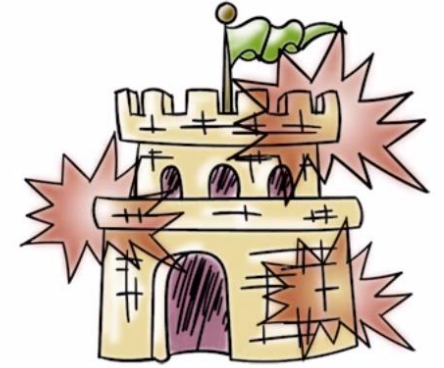


Hacktivists: activists who do not like something you are or something you do.



Nation-states: Countries do it for political advantage or for espionage.

Vulnerabilities and Attacks



- **threat actors** exploit vulnerabilities to launch attacks
- **attacks** lead to compromises or security breaches
- **vulnerabilities** can be found in software, networks, and humans.

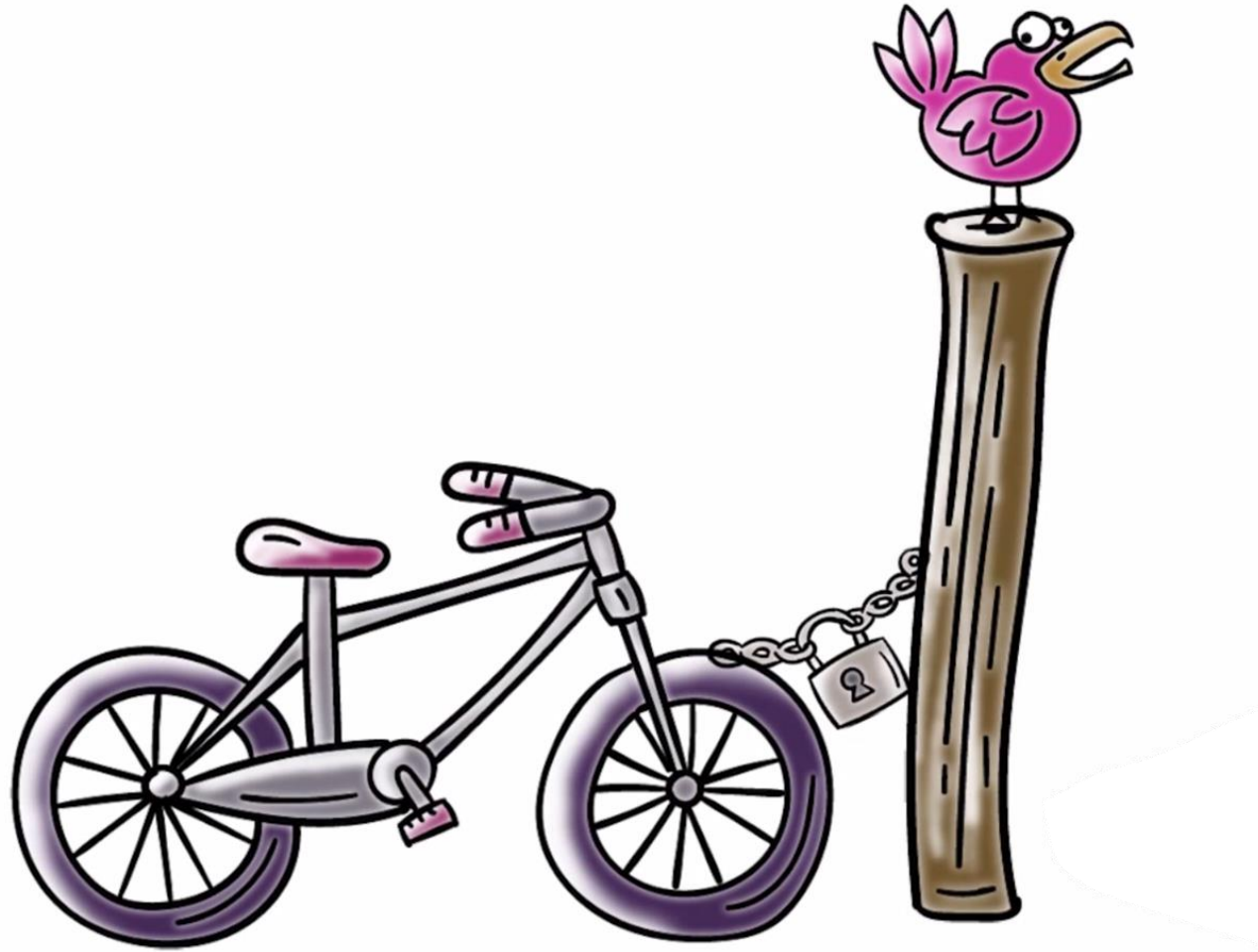
Vulnerabilities and Attacks



**Time to
take a break!**



Vulnerabilities and Attacks



Vulnerabilities and Attacks

A few hours later...

Vulnerabilities and Attacks



FAIL



A Real World Example:





Black Market Prices Quiz

What is your **hacked/stolen data worth** on the Black Market (as of March 2015)? Enter **dollar amounts** in the boxes next to the data.

3 digit security code on your credit card

Credit card information

PayPal/Ebay account

Health information



Sony Pictures Quiz

With regards to the “**The Interview**” (2014) related hack, answer the following questions. Put the number of the correct answer in the box next to the question:

● **The threat source was:**

[1] cybercriminals, [2] Hacktivists, or [3] Nation-State

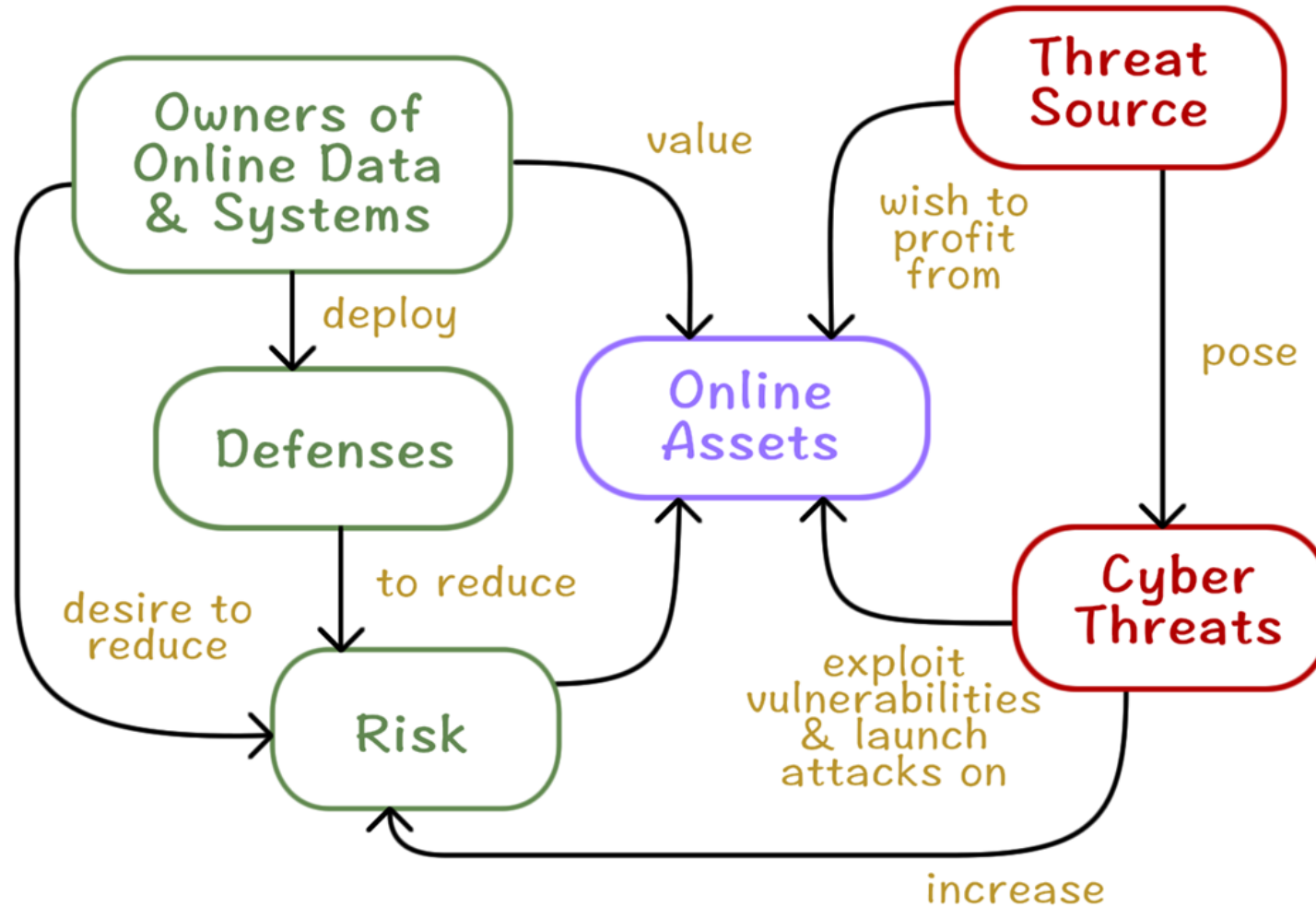
● **Goal of the attack was:**

[1] Monetize stolen information, [2] Stop Sony from releasing the movie “interview”), [3] Extort money from Sony

● **What did the attack accomplish:**

[1] Disclosed sensitive data, [2] Destroyed Sony computers


Revisiting Threats, Vulnerabilities, Attacks, and Risk



Relationship of Key Cyber Security Concepts

What Should We do in Cyber Security?

- Make threats go away (**crime should not pay**)
- Reduce vulnerabilities
- Strive to meet security requirements of sensitive information:

- **Confidentiality**
 - **Integrity**
 - **Availability**
 - Other consequences (stuxnet, physical)
- 
- CIA**
(not the intelligence agency)
- The diagram consists of three green arrows originating from the words 'Confidentiality', 'Integrity', and 'Availability' in the list above. These arrows converge and point towards the text 'CIA (not the intelligence agency)'.

What should the Good Guys Do?

- Prevention
- Detection
- Response
- Recovery and remediation
- Policy (**what**) vs. mechanism (**how**)



How Do We Address Cyber Security?

- Reduce vulnerabilities by following **basic design principles for secure systems**:
 - Complexity is the enemy (**economy of mechanism**)
 - Fail-safe defaults
 - Complete mediation
 - Open Design
 - Least Privilege
 - Psychological acceptability
 -





Mindset Quiz #1

What is the estimated value of **world-wide losses** due to **cybercrime**?

☐

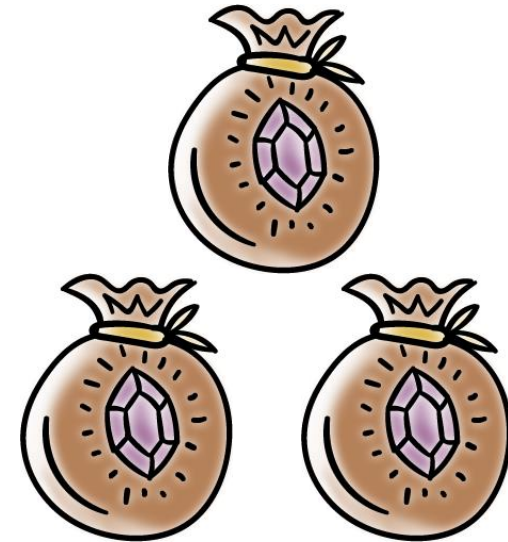
Less than \$10 Billion (US)

☐

Close to \$500 Billion (US)

☐

Trillions of US Dollars





Mindset Quiz #2

Data breaches violate which of the following **security requirements**?

☐

Integrity

☐

Availability

☐

Confidentiality



Mindset Quiz #3

What **security weakness** was exploited to enable **Stuxnet malware** to compromise **Iran's** nuclear plan networks?

☐

Out of date anti-virus system

☐

Disloyal employees or poor judgment by humans

☐

Weak security controls, such as easy to guess passwords

Security Mindset

Lesson Summary

- **Cyber Security:**

- HUGE problem for people, governments, companies, etc
- Enhance the **level of assurance** of systems

- **Security mindset** requires we know:

- **threats**
 - **actors/motivations**
 - how they **successfully attack**
-