Introduction to Information Security

CISC 3325 — CUNY Brooklyn College
Lecture Notes

Recently From the News

A news report from Jun 15, 2023:

https://www.youtube.com/watch?v=UYID9JKDhA8

Recently from the News

Follow-up discussion:

What feelings did you experience while watching this video?

(E.g., anger 😠, disappointment 😞, worrying 😟, confusion 😕, indifference 🙄)

Why?

Recently from the News

Another short report, dated Jul 14, 2023:

https://www.youtube.com/watch?v=bp17wuKD-nM

Recently from the News

Follow-up discussion:

1. What feelings did you experience while watching this 2nd video? Why?
   (E.g., anger 😠, disappointment 😞, worrying 😟, confusion 😕, indifference 🙄)
2. Which of the two videos is more personally concerning to you? Why?
3. How would you react if you learned you were affected by a similar cyber-attack?
   (E.g., ignore it 😑, panic 😱, think what to do 🤔, call a person/organization 📞)

Recently from the News

Follow-up discussion:

1. What feelings did you experience while watching this 2nd video? Why?
   (E.g., anger 😠, disappointment 😞, worrying 😟, confusion 😕, indifference 😳)
2. Which of the two videos is more personally concerning to you? Why?
3. How would you react if you learned you were affected by a similar cyber-attack?
   (E.g., ignore it 😑, panic 😱, think what to do 🤔, call a person/organization 📞)

Recently from the News

Follow-up discussion:

1. What feelings did you experience while watching this 2nd video? Why?
   (E.g., anger 😠, disappointment 😞, worrying 😟, confusion 😕, indifference 😳)
2. Which of the two videos is more personally concerning to you? Why?
3. How would you react if you learned you were affected by a similar cyber-attack?
   (E.g., ignore it 😑, panic 😱, think what to do 🤔, call a person/organization 📞)

Information Security

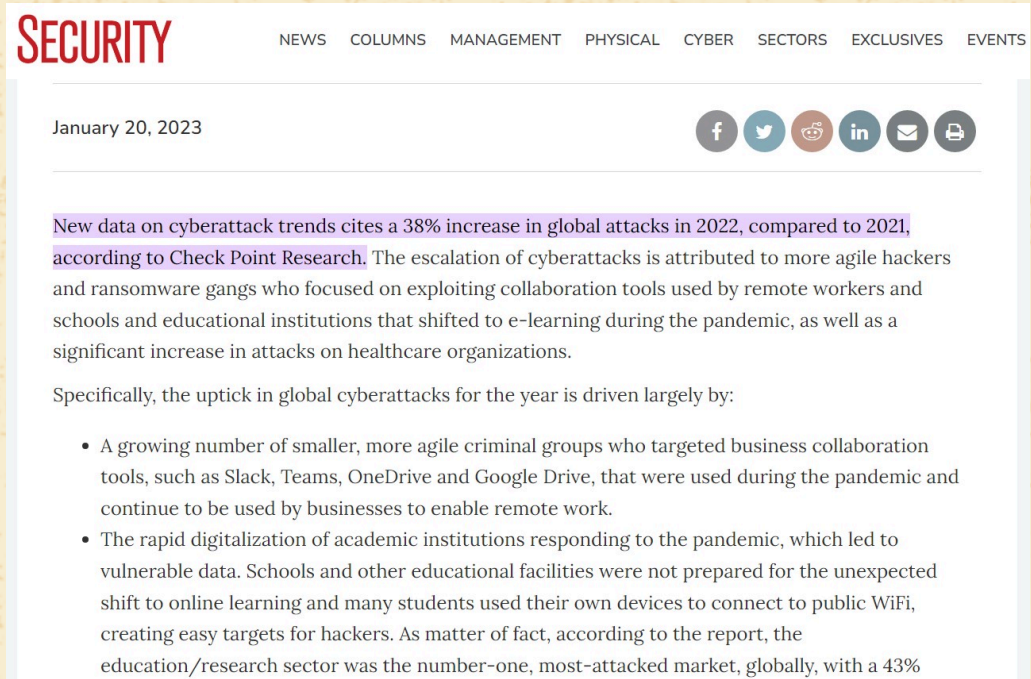
The number of cyber-attacks and other security breaches increases every year, so it isn't surprising that we hear about such incidents more and more often in the news.

Security breaches have different forms:

- Intentional vs. Accidental.
- Done for profit vs. done for ideology or fun.
- Carried out by a single person vs. organization vs. government.

Regardless, the damage inflicted by a security breach (financial, medical, reputational, etc.,) can be significant, irreversible, and even catastrophic.

Information Security



SECURITY

NEWS COLUMNS MANAGEMENT PHYSICAL CYBER SECTORS EXCLUSIVES EVENTS

January 20, 2023

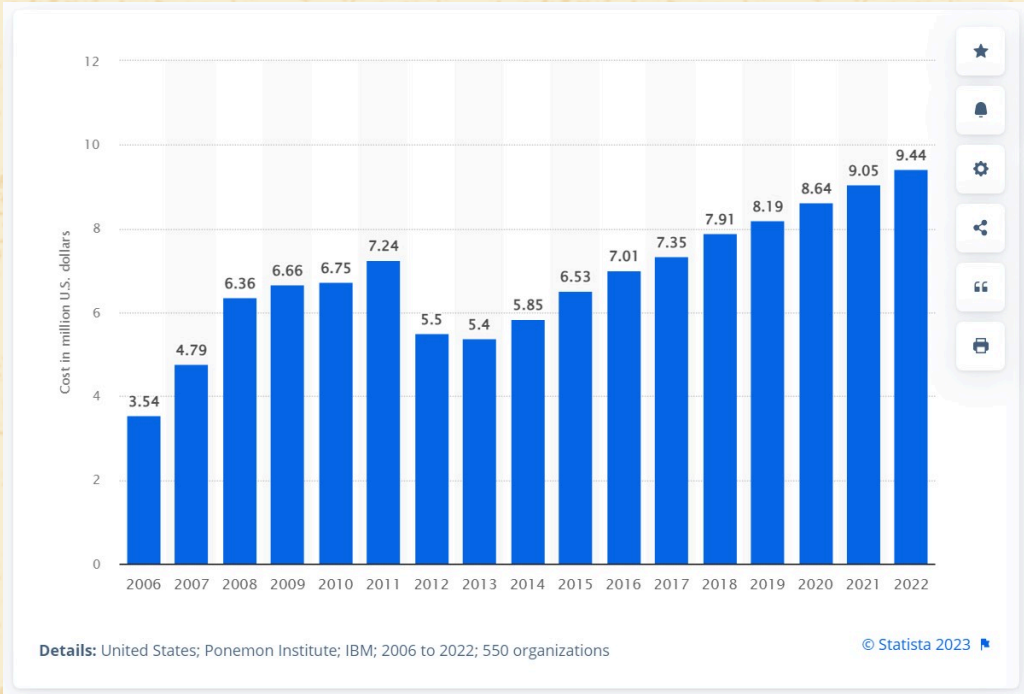
New data on cyberattack trends cites a 38% increase in global attacks in 2022, compared to 2021, according to Check Point Research. The escalation of cyberattacks is attributed to more agile hackers and ransomware gangs who focused on exploiting collaboration tools used by remote workers and schools and educational institutions that shifted to e-learning during the pandemic, as well as a significant increase in attacks on healthcare organizations.

Specifically, the uptick in global cyberattacks for the year is driven largely by:

- A growing number of smaller, more agile criminal groups who targeted business collaboration tools, such as Slack, Teams, OneDrive and Google Drive, that were used during the pandemic and continue to be used by businesses to enable remote work.
- The rapid digitalization of academic institutions responding to the pandemic, which led to vulnerable data. Schools and other educational facilities were not prepared for the unexpected shift to online learning and many students used their own devices to connect to public WiFi, creating easy targets for hackers. As matter of fact, according to the report, the education/research sector was the number-one, most-attacked market, globally, with a 43%

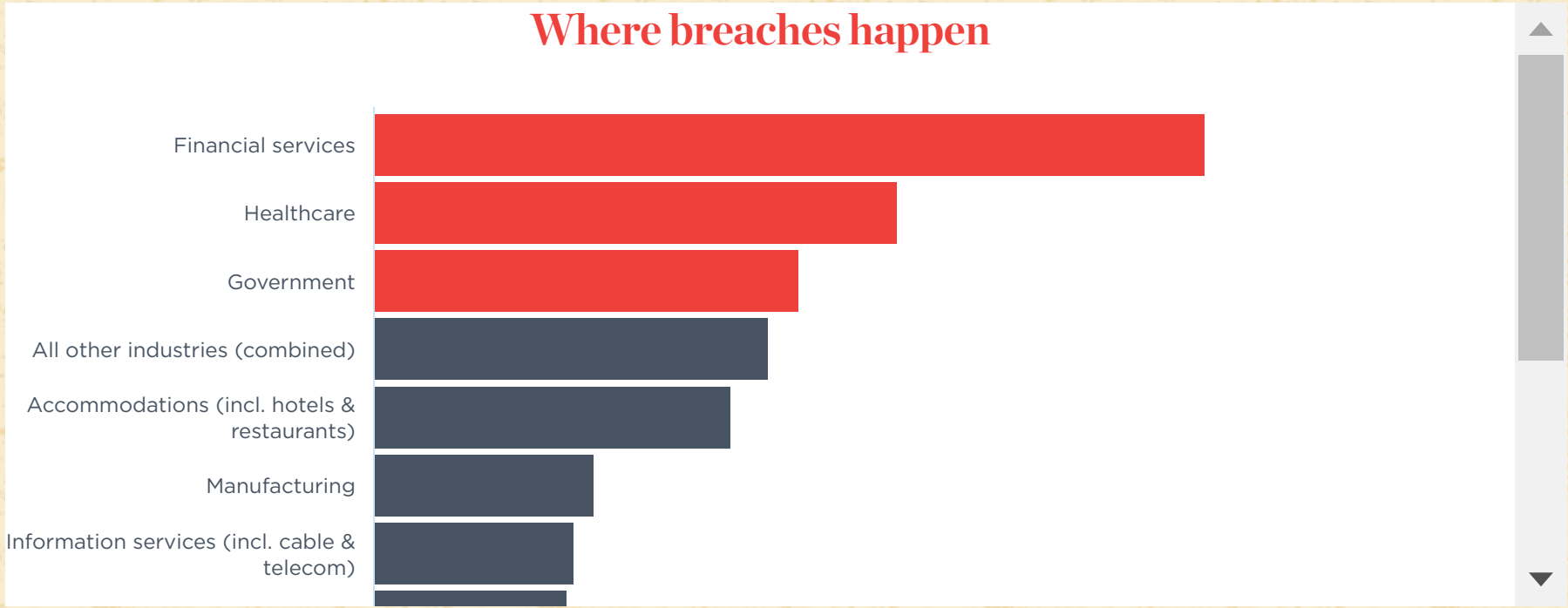
An increase in global cyber attacks in 2022. https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022.

Information Security



Average cost of a data breach in the United States from 2006 to 2022. https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/.

Information Security



Distribution of security breaches by industries. Taken from the National Retail Federation's Data Secuity page at https://nrf.com/data-security.

Why Studying Information Security?

- Sourrounded by an increasing number of phones, computers, and other smart devices with Internet connection capabilities, we store precious data on these devices, which we definitely want to learn how to protect.
- Other "Internet of Things" (IoT) devices, including home appliances, can connect to the Internet and other devices. No one wants a hacker to damage your home through your appliances (fire, gas leaks, high electricity bills, etc.)
- Everyone should learn how to shield themselves from cyberattack damages and effects.
- Jobs in cybersecurity are prestige and high-paying. Specialists are always in demand!

Information Security

Our goals in this course are to:

- Learn what information security is, and why it is crucial to care about security.
- Understand how security breaches come into existence, and how/why attackers use such situations to bring harm.
- Equip ourselves with knowledge and tools on how to prevent security breaches, in the first place, from happening.

As a first step, let's define some terms, including our course title, *Information Security*.

Information Security: Definitions

Definitions related to Information:

- **Data** (singular: **datum**) are sequences of symbols, such as bits (`0`s & `1`s), numbers, text strings, etc., that are used for reasoning, calculations, and decision-making.
- **Information** is a *meaningful* collection of data (i.e., data in context.)
- **Knowledge** is a human's understanding on a subject acquired from education or experience. Knowledge exists only in the context of humans/living beings.

Data do have some meaning, but it is very basic, limited, and contextless.

Information Security: Definitions

Examples:

- The zip code: `11210`, by itself, tells you nothing aside from being a zip code. As such, `11210` is a datum.
- Conversely, the senstence: `"The zip code of Brooklyn College is 11210"` conveys a context for `11210`, so we categorize this sentence as information.
- Your cognitive ability to recognize that the zip-code area for `11210` is located in the Brooklyn borough is knowledge you gained.

Information Security: Definitions

Another example of the difference between information and data. Miriam Briskman, CC BY-NC 4.0.

Note: click the GIF amination above to open and play it in a browser window.

Information Security: Definitions

Any questions?

Information Security: Definitions

Definitions related to Security:

- **Security** is the state of being free from external dangers and threats.
- **Protection** is the state of being free from internal dangers and threats.
- **Privacy** is keeping one's information away from people who shouldn't obtain it.

In our class, whenever we say 'security', we mean 'security, protection, and privacy' since we strive to keep sensitive information secure from both external and internal threats as we see next in Topic 2.

Information Security: Definitions

Examples:

- When a person connect to a network without being allowed ('unauthorized'), such as by hacking it, we have a security issue.
- When a person who received permission to use a device accidentally delete valuable data, we have a protection issue.
- When you allow your physician to access your medical information, but don't want your neighbor to access it, such medical information is considered private.

Information Security: Definitions

Information Security, therefore, is defined as:

- The practice of keeping information safe by addressing information risks.

Another handy definition:

- The practice of defending information from disallowed or unwanted access, use, disclosure, disruption, modification, inspection, recording, deletion, or destruction.

Information Security: Definitions

Definitions of a few more basic security-related concepts:

Vulnerability	An existing flaw or weakness in a computer system
Threat (n.)	A scenario of potential harm to a system
Attack (n.)	(Also: a **Breach**) An action of harming a system
Exploit (n.)	A tool (e.g., software) that misuses a vulnerability to attack a system
Control (n.)	(Also: a **Security Patch**) An action or tool that removes or reduces a vulnerability

- A **threat** is materialized when a person **exploits** a **vulnerability**, thereby **attacking** the system.
- To prevent this from happening, an InfoSec specialist would implement a **control** that remedies the **vulnerability** and thereby blocks the **threat**.

Information Security: Definitions

Example: Creating an email account, Joe Smith decided to set his account password to: '`12345`'.

Fun Class Activity: Match the items below to the concepts (one concept per item:)

	Items
1	Someone might guess the password and break into Joe's account.
2	Programming the email server to accept only strong passwords.
3	A password too short and too easy to guess.
4	Mal Waring, a hacker, guesses Joe's password and breaks in.
5	A program running password combinations against Joe's password to break it.

	Concepts
A	a vulnerability
B	a threat
C	an attack
D	an exploit
E	a control

Information Security: Definitions

The tasks of an information security specialist are to:

- Actively Look for and identify vulnerabilities in a system,
- Monitor for threats related to the discovered vulnerabilities,
- Recognize what types of attacks could exploit these vulnerabilities, and
- Take countermeasures or use methods to control or prevent an attack.

Any questions?

History of Security Attacks

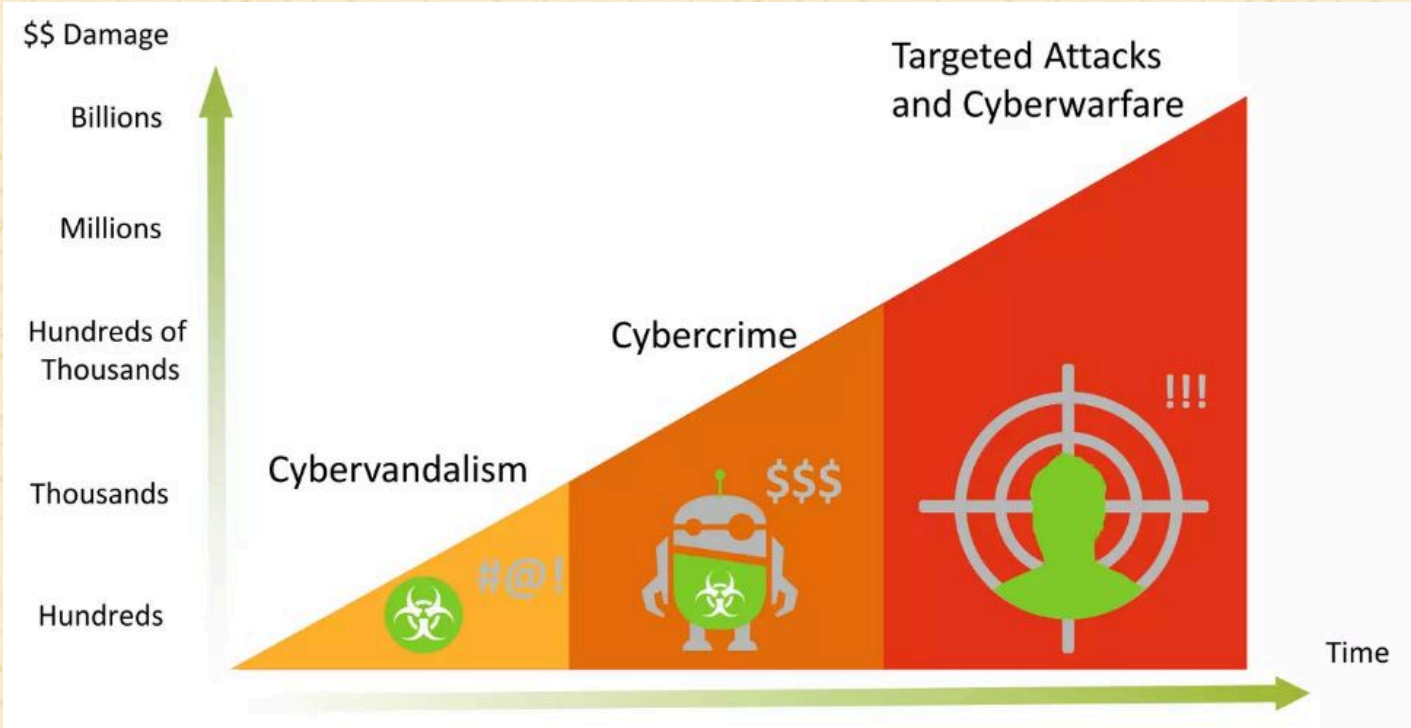
Attacks on modern infrustructure evolved over the decades:

- **1940s and WWII**: The use of the Enigma message encryption machine by the Nazi Germany, and its deciphering by Alan Turing.
- **1970s**: People known as phreakers (e.g., John Draper) exploited the weakness of digital-switching telephone systems for fun and free calls.
- **1980s and 1990s**: The earliest attacks on modern day computers. There were few attacks, but the attackers gain fame. Examples: Robert Morris, Markus Hess, Vladimir Levin, Jonathan James, and Kevin Mitnick.

History of Security Attacks

- **2000s**: An increase in attacks, which became financially motivated (pharms, financial, identity theft.) Attackers found out and use personal information about their victims to build trust and lure them into giving out confidential information (e.g., passwords, credit card numbers, etc.,) an activity called spear-phishing.
- **2010s to Present**: Attacks, now made by attacker groups rather than individuals, became mainly politically and sometimes financially motivated. They further divide into government-driven attacks, example of which are Stuxnet, Flame, Aurora, and private activism, such as Anonymous and Wikileaks.

History of Security Attacks



The Evolution of Cyber Attacks. https://www.slideshare.net/lastlinesecurity/ip-expo-oct-2014.

History of Security Attacks

Video about the top 10 computer hacks of all times:

https://www.youtube.com/watch?v=oOoMqgnvZaY

History of Security Attacks

One more video, this time about the 10 of the most dangerous hackers:

https://www.youtube.com/watch?v=TCwHfFu0R_E

History of Security Attacks

Any questions?

Introduction to Information Security: Sources

Rao, Umesh Hodeghatta, and Umesha Nayak. "Chapter 1: Introduction to Security." *The InfoSec handbook: An introduction to information security.* Springer Nature, 2014, pp. 3-12. URL: https://link.springer.com/content/pdf/10.1007/978-1-4302-6383-8.pdf#chapter+1:+introduction+to+security

Rao, Umesh Hodeghatta, and Umesha Nayak. "Chapter 2: History of Computer Security." *The InfoSec handbook: An introduction to information security.* Springer Nature, 2014, pp. 13-25. URL: https://link.springer.com/content/pdf/10.1007/978-1-4302-6383-8.pdf#chapter+2:+history+of+computer+security