Motivation

Security = !?

Security

> The state of being free from danger or threat. [^1]

Vulnerability = ⁉

Vulnerability

> A **flaw or weakness in system** security procedures, design, implementation, or internal controls **that could [...] result in a security breach** or a violation of the system's security policy [^2]

Exploit = !?

Exploit

> A piece of software, a chunk of data, or a sequence of commands that **takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior** to occur on computer software, hardware, or something electronic (usually computerized) [^3]

Zero Day = ⁉

Zero-Day

> **A zero day vulnerability** refers to a hole in software that **is unknown to the vendor**.
>
> This security hole is then **exploited by hackers before the vendor becomes aware** and hurries to fix it—this exploit is called a zero day attack. [...]
>
> The term **"zero day" refers to the unknown nature** of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. [^4]

Exercise 1.1 (📌)

Brainstorming Attackers

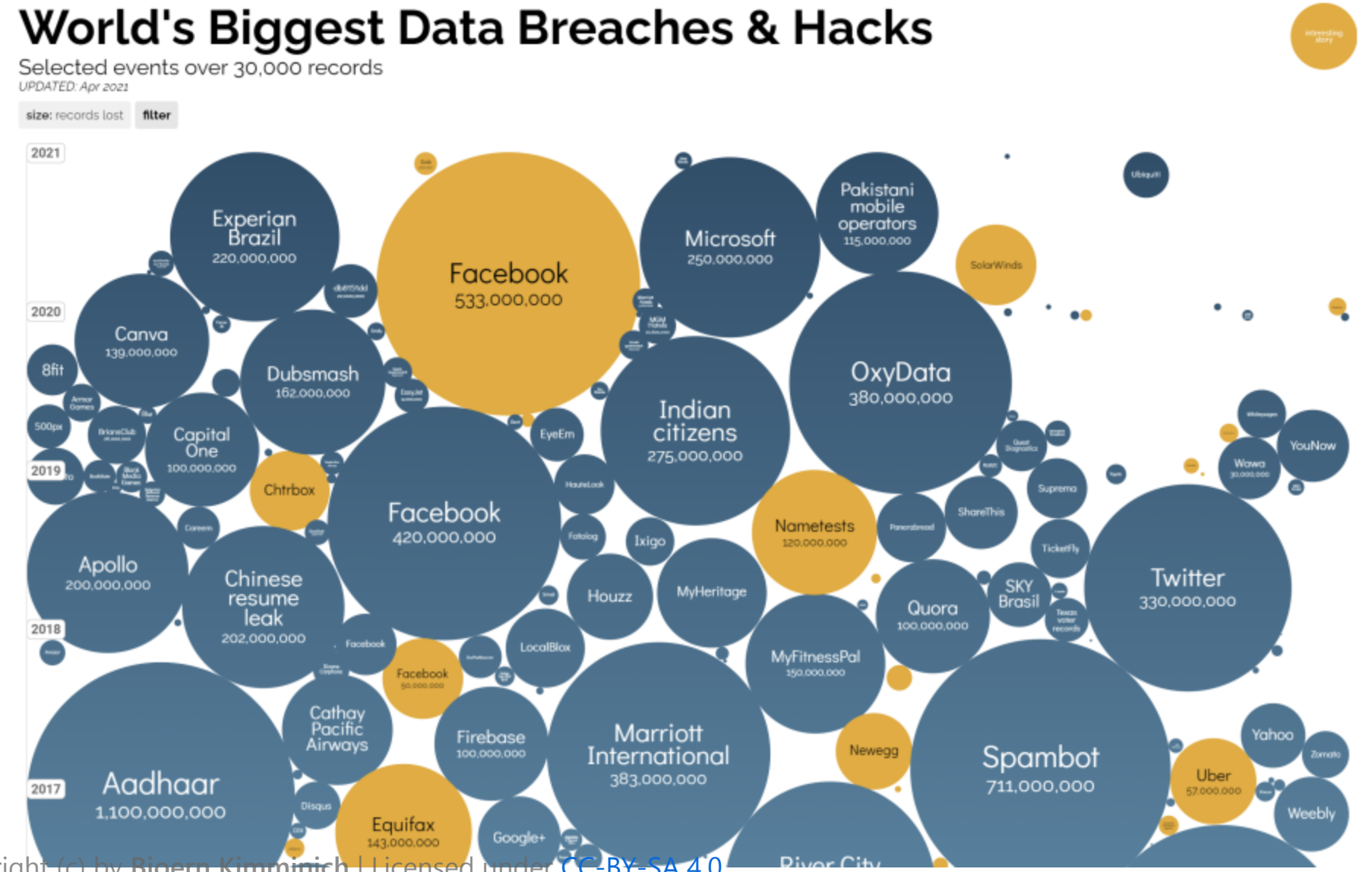
1. Identify and describe possible **Attackers** and their motivation
2. Rate the danger posed by each attacker type (💀 to 💀💀💀)
3. Estimate the risk (high/medium/low) of your own organization being targeted by each identified attacker type
4. Which attacker types are likely to work together and how does this impact their danger rating?

Advantage of the Attacker

- Attacker must **succeed once**
  - Defender must get it right *all the time*
- Attacker can choose the **weakest spot**
  - Defender must defend *all places*
- Attacker can leverage **zero-days**
  - Defender can only defend against *known attacks*
- Attacker can **play dirty**
  - Defender needs to *play by the rules*

Case Studies

Data Breaches



Peloton (May 2021)

> Peloton provides a line of network-connected stationary bikes and treadmills. The company also offers an online service that allows users to join classes, work with trainers, or do workouts with other users. In October [2020], Peloton told investors it had a community of 3 million members. Members can set accounts to be public so friends can view details such as classes attended and workout stats, or users can choose for profiles to be private. [^7]

> Researchers [...] reported that a flaw in Peloton's online service was making data for all of its users available to anyone anywhere in the world, even when a profile was set to private. All that was required was a little knowledge of the faulty programming interfaces that Peloton uses to transmit data between devices and the company's servers.
>
> Data exposed included: User IDs, Instructor IDs, Group Membership, Workout stats, Gender and age, Weight and if they are in the studio or not. [^7]

The initial fix let anyone who subscribed to the online service still obtain the private details of any other subscriber. 🕵

Marriot (November 2018)

> The hotel chain asked guests checking in for a treasure trove of personal information: credit cards, addresses and sometimes passport numbers. On Friday, consumers learned the risk. Marriott International revealed that hackers had breached its Starwood reservation system and had stolen the personal data of up to 500 million guests. [^5]

> [...] Starwood's data has not popped up on the so-called dark web, according to Recorded Future, a cybersecurity firm, and Coalition, a cyber insurance provider, which suggested that the hotel attackers weren't looking to sell what they took.
>
> "Usually when stolen data doesn't appear, it's a state actor collecting it for intelligence purposes," [...] information could be fed, for example, into an analysis program run by a country's state security apparatus [...]. Using "big data" technology similar to what marketers use in targeted advertising, the country could try to pinpoint the comings and going of intelligence agents from other nations. Did they stay, for example, in the same hotel as a potential source for that country? [^5]

The intrusion went unnoticed for four years by Starwood. 📅

Equifax (September 2017)

> If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies. [^6]

> Here are the facts, according to Equifax. The breach lasted from mid-May through July. The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people. And they grabbed personal information of people in the UK and Canada too. [^6]

Recommended steps for protection include "monitor your existing credit card and bank accounts closely" but also "consider placing a credit freeze" 🍦 *or "placing a fraud alert on your files".*

CloudPets (February 2017)

> [...] There were a lot of news headlines about how Germany had banned an internet-connected doll called "Cayla" over fears hackers could target children.
>
> [...] Just before that, we had the VTech data breach which exposed a huge amount of very personal information.
>
> Which brings us to CloudPets [...] which is a toy that represents the nexus of both the problems discussed above. [^8]

> [...] Put yourself in the shoes of the average parent, that is one who's technically literate enough to know the wifi password but not savvy enough to understand how the "magic" of daddy talking to the kids through the bear (and vice versa) actually works. They don't necessarily realise that every one of those recordings – those intimate, heartfelt, extremely personal recordings – between a parent and their child is stored as an audio file on the web. They certainly wouldn't realise that in CloudPets' case, that data was stored in a MongoDB that was in a publicly facing network segment without any authentication required and had been indexed by Shodan (a popular search engine for finding connected things). [^8]

Impacted parents were never notified by CloudPets. 😱

Missouri Dept. of Elementary and Secondary Education (October 2021)

> Through a multi-step process, an individual took the records of at least three educators, decoded the HTML source code, and viewed the SSN of those specific educators.
>
> We notified the Cole County prosecutor and the Highway Patrol's Digital Forensic Unit will investigate. [^9]

> [...] the St. Louis Post-Dispatch ran a story about how its staff discovered and reported a security vulnerability in a Missouri state education website that exposed the Social Security numbers of 100,000 elementary and secondary teachers.
>
> [...]
>
> The newspaper said it found that teachers' Social Security numbers were contained in the HTML source code of the pages involved. In other words, the information was available to anyone with a web browser who happened to also examine the site's public code using Developer Tools or simply right-clicking on the page and viewing the source code.

... 🤦 🤦 🤦

Exercise 1.2 (*optional* 📌)

Have I been pwned?

1. Visit https://haveibeenpwned.com/
2. Type in your email address
3. Hit the `pwned?` button
4. How many pwnages do you get for your private and/or organization email? (📌)

Exercise 1.3 (📝 🏠)

1. Mark potentially malicious items in the Press Kit from the *Trump-Kim Summit* (2018) in the image on the next slide (➡️)
2. Explain possible ways how these items might actually be malicious
3. Reason about potential attackers behind this and explain their most likely motivations
4. Come up with a least two more additions to the Press Kit and explain how they could be used maliciously

ℹ️ *Speculation is allowed, but still be as specific as possible!*