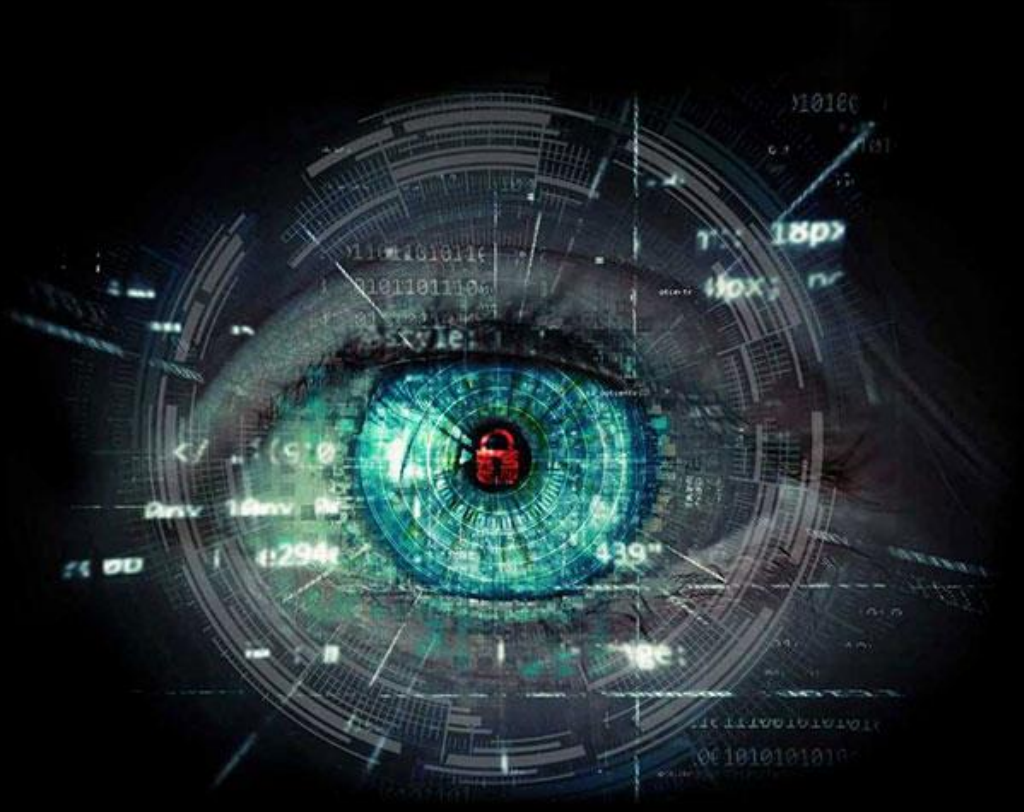
The Sony cyber attacks and it's recurrence

Emma Kelly, Aisha Ntuli, Kevin Osifo, Ayomide Idowu, Jane Keyes

Topics of discussion



01 **Introduction to cyber attacks**

- What is a cyber attack
- Motivation for cyber attacks
- How cyber attacks happen
- Cyber Attacks
- Cyber Attack Prevention

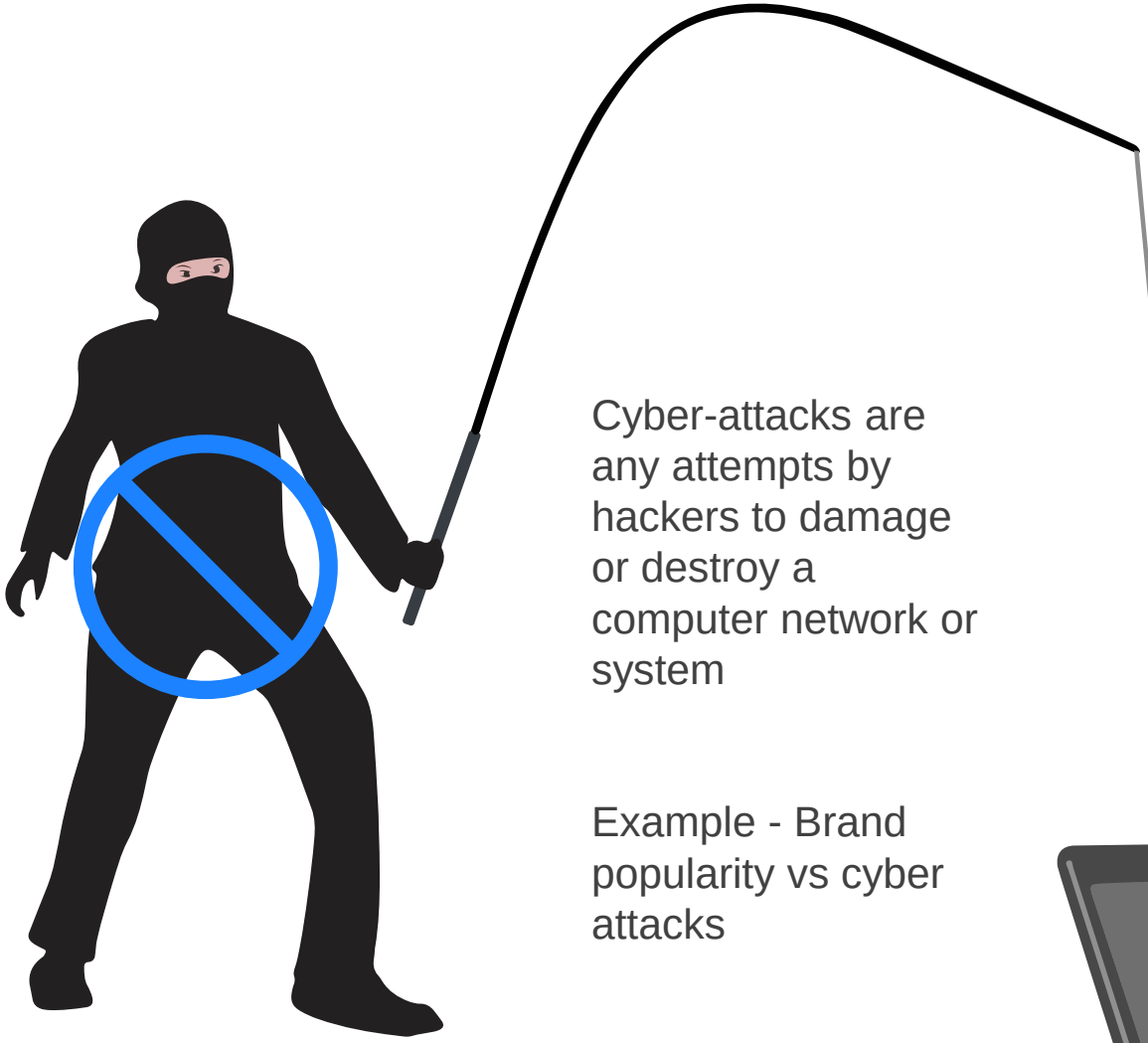
02 **Sony cyber attacks**

- Timeline
- 2011
- 2014
- 2017
- 2023

03 **Q&A Session**

Introduction to Cyber Attacks

What is a cyber-attack?



Cyber-attacks are any attempts by hackers to damage or destroy a computer network or system

Example - Brand popularity vs cyber attacks

Cyber-attacks are usually aimed at interrupting normal business processes.

Motivation for cyber attacks

Financial gain

Using phishing techniques, hackers can obtain credit/debit card details, banking login details, etc, to gain access to bank accounts and steal money.

Insider Threats

An organizations critical information may be sold to other organizations by someone who is working directly within the company. This may be for personal gain, to damage the company's reputation, or because of negligence (easily guessable/exposed passwords)

Recognition and notoriety

Individuals may hack systems in order to gain recognition by an individual or by the masses.

State-Sponsored Hackers

White or black hat hackers target terrorists, foreign governments, and corporations to steal their information. These hackers are often funded by and working for governments

Drugs

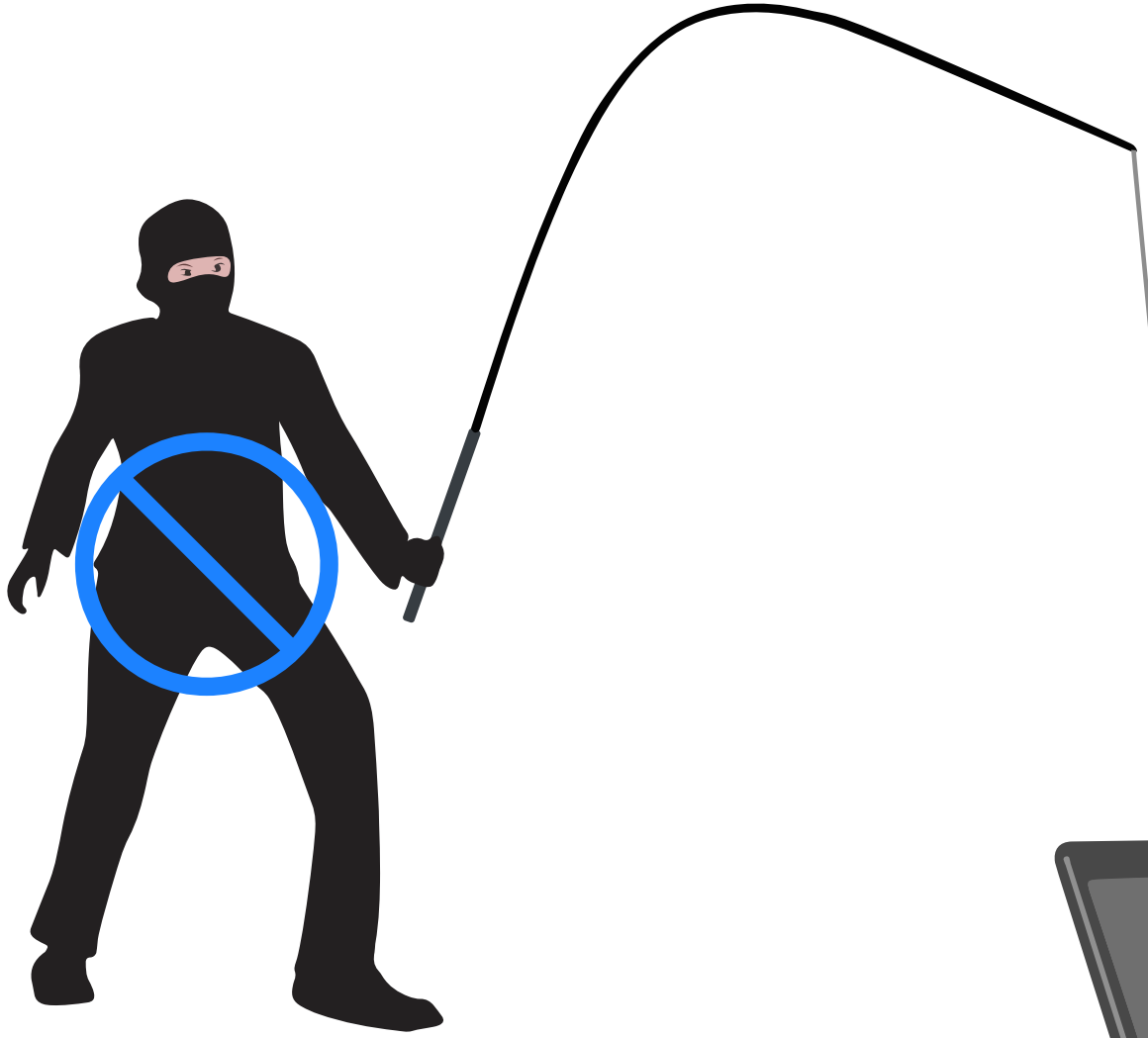
Using the darknet, people can carry out illegal activities such as selling drugs. The darknet is used as they do not open using normal browsers

Crackers

Programming applications are modified by hackers. This can be to make the application free to use, earn money with ads, or insert malicious code to collect user information.

How cyber attacks happen

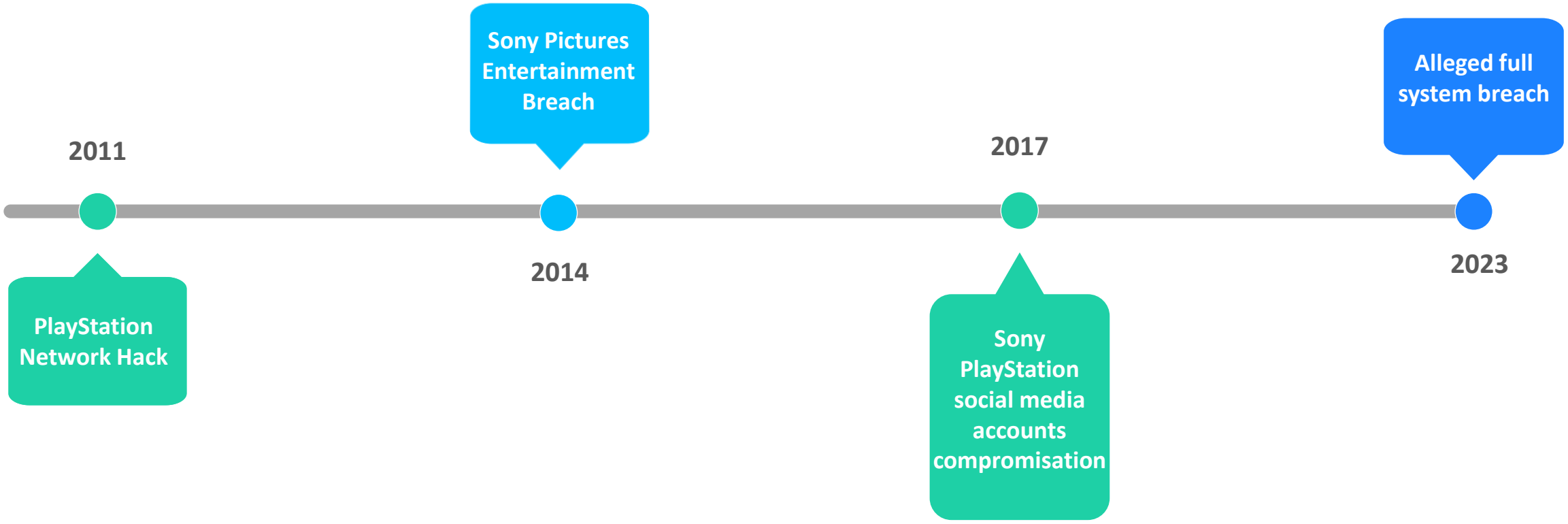
Cyber-attack Prevention



- Antivirus software
- Firewalls
- Stay alert
- Update your operating system.

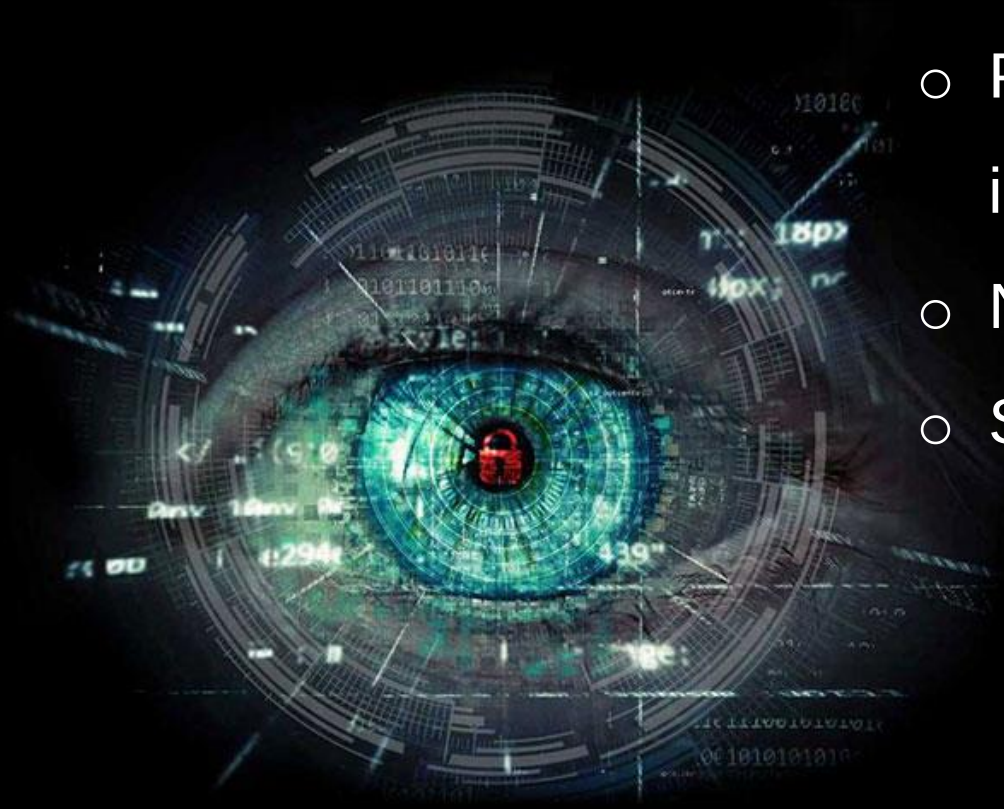
Sony Attacks

Sony Data Breaches Timeline



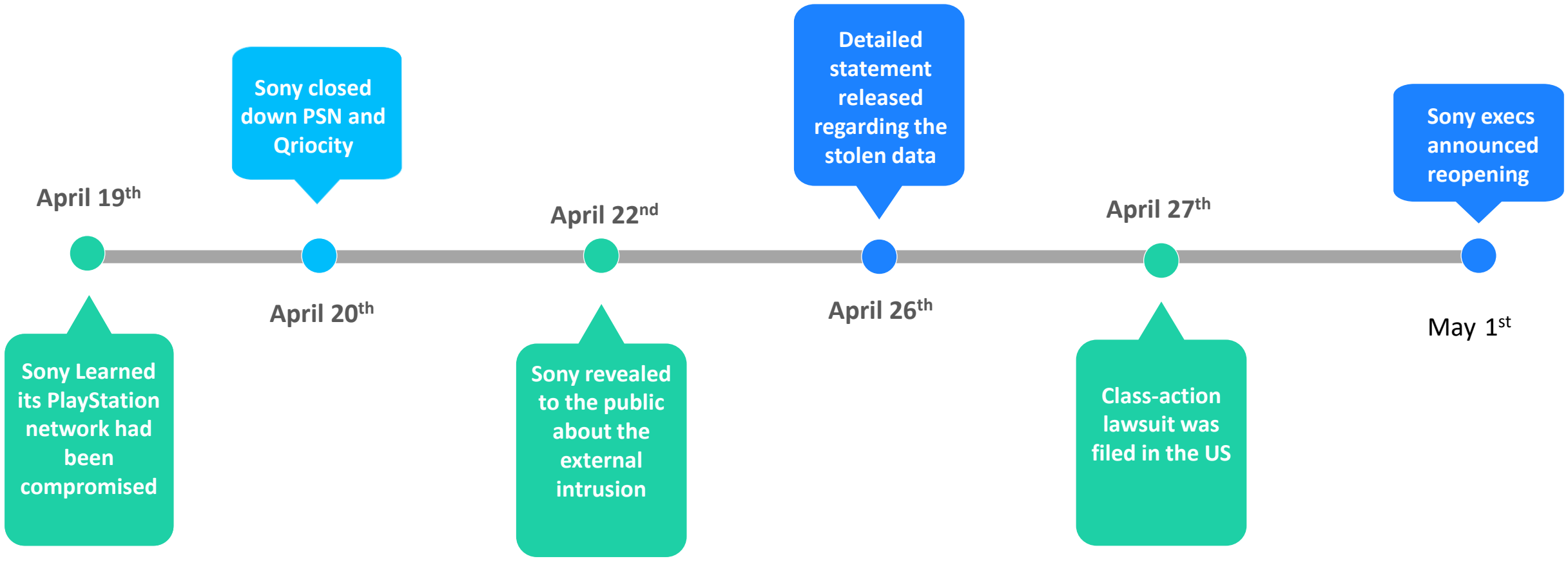
2011- PlayStation Network Hack

What happened?



- “Illegal and unauthorised person” got access to people's data
- PSN was one of the largest holders of card information in the world
- No evidence of Card Details stolen
- Sony PSN and Qriocity were down for 24 days

2011 PSN Hack Timeline



Consequences

- PlayStation network was down for 24 days
- Lost approx. 171 million following the network outage
- 70 million users' data was leaked
- Sony settled the US lawsuit for 15 million dollars (but not actually!)

How could this have been prevented?

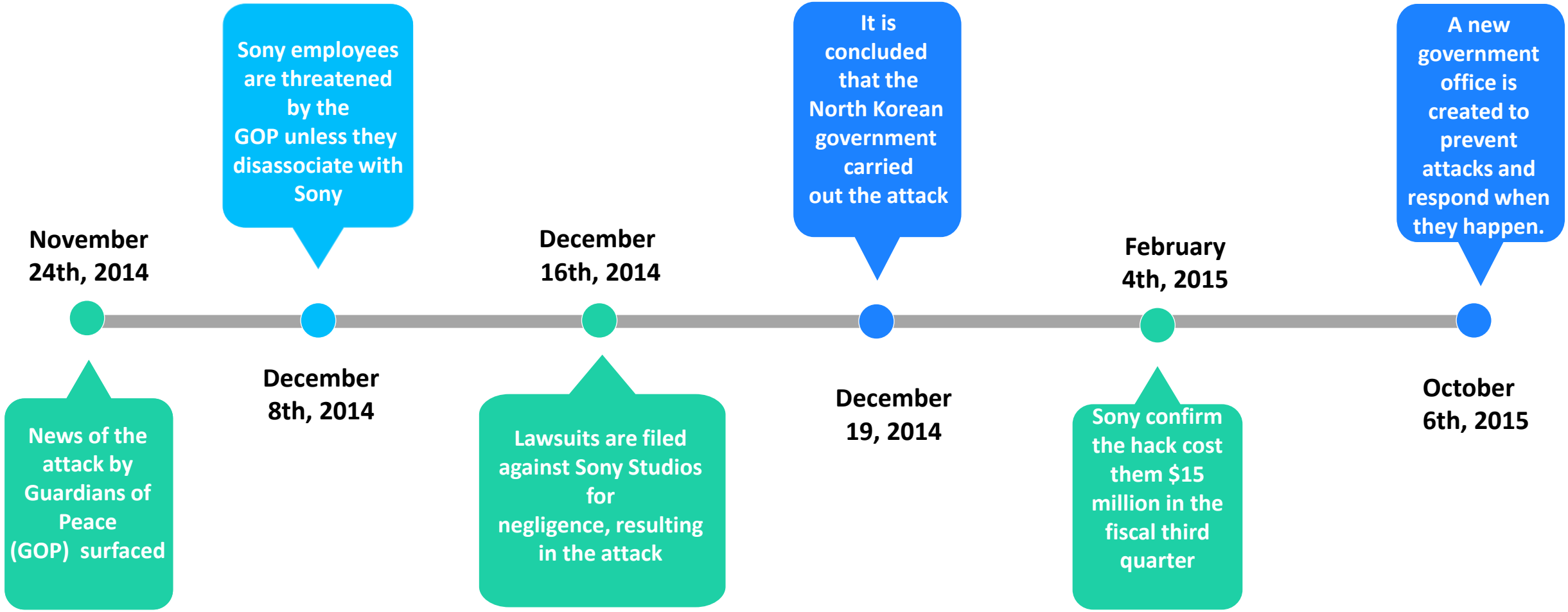
- Encrypted passwords better
- Grant need-to-know access
- Invest in DDoS, scraping & rate limiting tools to properly defend infrastructure
- Implement tools that contain malware and trojan
- If an attack happens, the network should be able to defend itself
- Strong incident response plan

2014 - **Sony Pictures Entertainment Breach**

What happened?

- A group called "Guardians of Peace", believed to be working with North Korea, hacked Sony Pictures Entertainment
- The hackers demanded a halt of the release of the movie "The Interview"
- When demands were not met:
  - Unreleased scripts and films were leaked
  - Employee social security numbers and records were stolen
  - salary lists, and sensitive emails were disclosed

2014 Hack Timeline



Consequences

- The attacked resulted in the piracy of five Sony films
- Digital files containing 47,000 Social Security numbers of current or former Sony employees, contractors, and actors were stolen
- The attack cost Sony $15 million in the third fiscal quarter
- Sony reached an $8 million settlement with their current and former employees to re-imburse them for identity-theft losses, preventative measures and legal fees

How could this have been prevented?

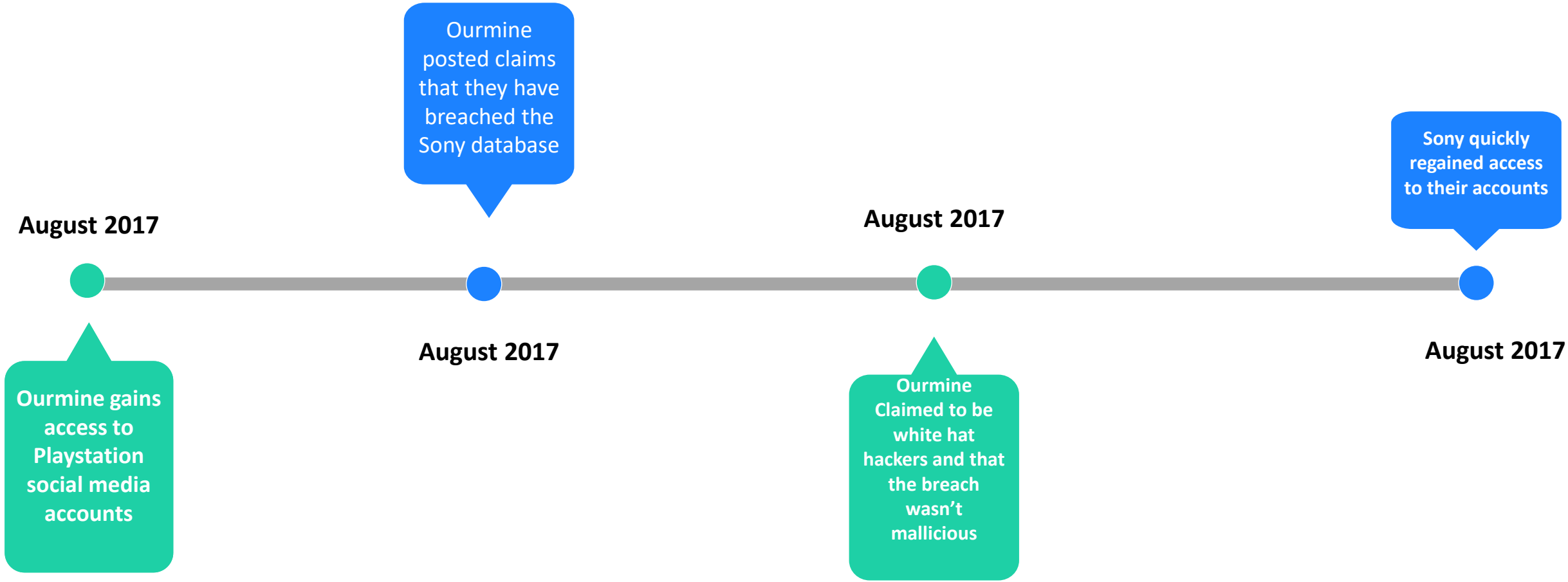
- If Sony Studios had not been negligent by ignoring computer system warnings that that the servers were prone to attack, the attack may have been prevented.
- Conducting regular employee training on cyber security could prevent an attack like this happening again
- As most of the confidential files were password protected, perhaps multi- factor authentication could have prevented sensitive information from being accessed

2017 -Sony PlayStation social media accounts compromisation

What happened?

- In August 2017 “Ourmine” gained access to Sony’s social media accounts.
- The claimed they had accessed the network database and collected log-in info usernames etc.
- They also claimed that they had no malicious intent.

2017 Hack Timeline



Consequences

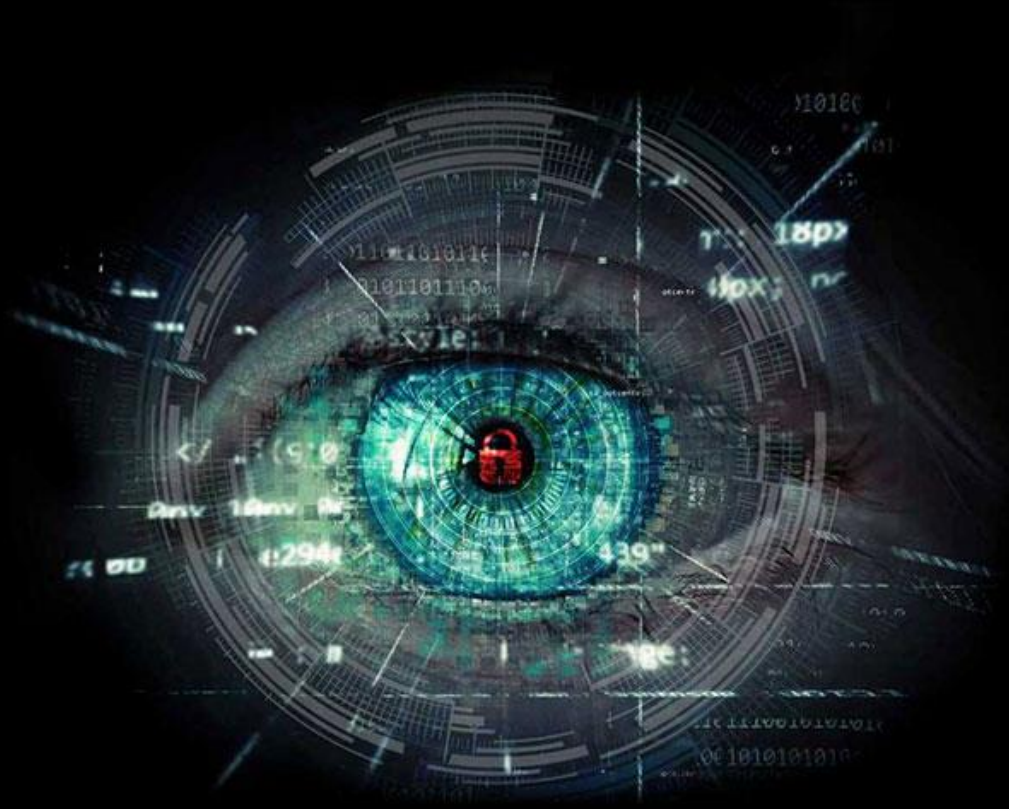
- PlayStation's integrity was stained.
- The breach showed how simple it was to gain access.
- Customer’s data were compromised.

How could this have been prevented?

- Sony should have employed their own personal white hat hackers to test the social security.
- Create a stronger encrypted password or different passwords for each media.

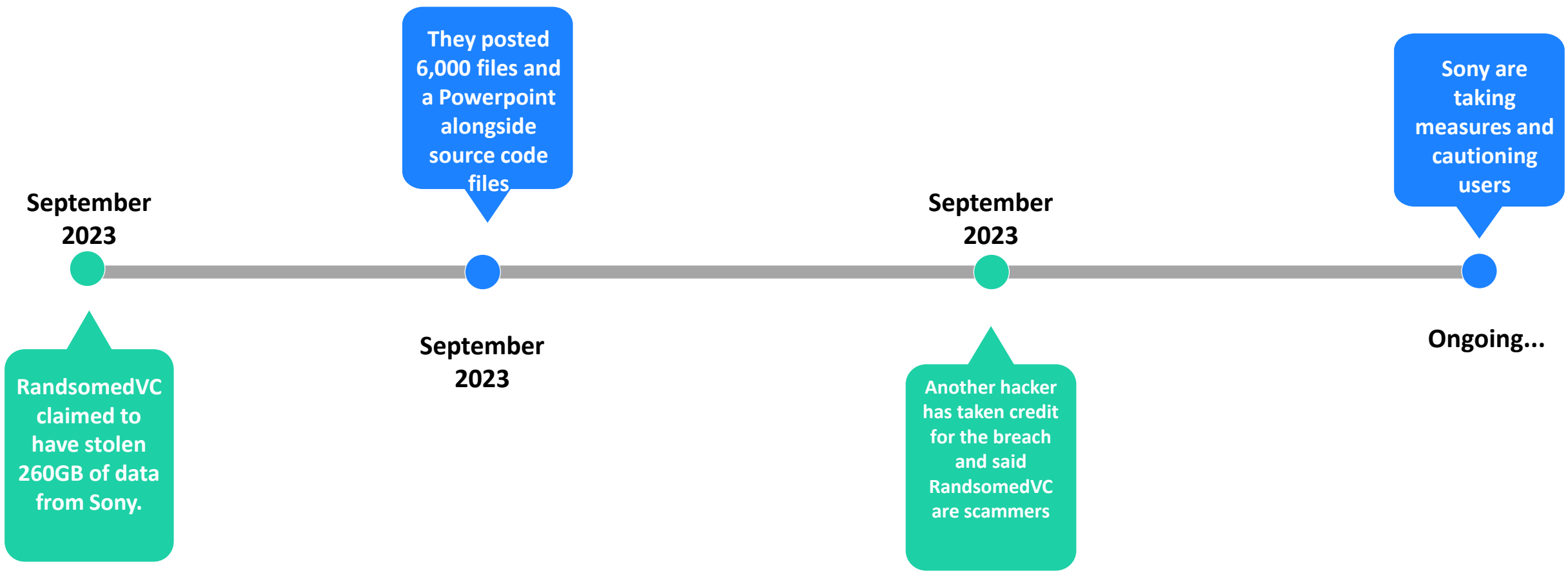
2023 -Alleged full system breach

What happened?



- On the 25th of September this year “RandsomedVC” claimed to have stolen 260GB of data from Sony.
- They posted 6,000 files as a sample of the data stolen.
- A hacker “MajorNelson” claimed that They were the ones who stole the data and that “RandomedVC” were scammers.
- Sony are currently investigating the matter.

2023 Hack Timeline



Consequences

- Sony are in a sticky situation.
- The claims may be true or false.
- All users are currently in limbo as they are unsure if their data is compromised.

How could this have been prevented?

- If the claims are false, not much as this could be a quick gimmick to steal money off Sony.
- If the claims are true, then a more secure database and some kind of reconciliation to customers.


Q & A

References

- https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data
- https://www.networkworld.com/article/2202583/playstation-network-hack-timeline.html
- https://www.wired.com/2011/05/sony-psn-hack-losses/
- The 2014 Sony hacks, explained - Vox
- https://coopwb.in/info/how-many-times-has-sony-been-hacked/
- https://firewalltimes.com/sony-data-breach-timeline/
- https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014)#:~:text=The%20hackers%20were%20taking%20retaliatory,the%20North%20Korean%20Supreme%20Leader.
- https://securityboulevard.com/2022/12/8-motives-of-cybercrime-hackers-world/#:~:text=Most%20of%20the%20hacker's%20primary,the%20money%20to%20their%20account.

THANK YOU