Before learning about cybersecurity breaches, you will first need to know important technology definintions of parts explained in the paper.

Cybersecurity breach- This is when non granted access has entered into technology platforms or data.

Vulnerability- This is a weakness on the technology system side.

Exploit- This is when something can be used and benefited from.

Patch- These are technology fixes to vulnerabilities.

Cyber insurance- This is a policy that will cover cyber breaches and attacks.

Research Paper #1

Mandy Lancaster

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Joseph Kovacic

May 21, 2023

Cybersecurity breaches occur when vulnerabilities are put in place to allow unwanted individuals to get granted access. There are so many instances that occur each day of cybersecurity attacks. The level of significance deals a lot with the vulnerabilities and damage that has occurred in a particular time frame.

In 2017, a significant cybersecurity breach occurred called NotPetya allowing computers to be affected by vulnerabilities created. The NotPetya malware became larger by an update to the MeDoc tax software. This was a software utilized by a lot of Ukrainian businesses (International cyber law: interactive toolkit, 2022). The big cybersecurity vulnerability consisted of this update and granting access to the computer afterwards. The threats that exploited the vulnerabilities consisted of NotPetya malware using the EternalBlue exploit that had never been patched. This was from the patch being granted to be fixed two months prior to that cyberattack and being held off. Individuals in a group took advantage of the time period being basically left open (*Notpetya: Looking back three years later*). This major cybersecurity breach was committed by the government. This attack was also thought of as "war". The problem is how to officially classify the attack as war for the insurance to cover the damage. It is a main issue regarding the realm of cyber insurance and coverage. A main contributor is the need for cyber insurance. If they are all outside of what is covered, then no coverage is needed. This was a main fight that could change the outcome of cyber insurance just from this one attack. There also is a main business regarding repercussions from the NotPetya cyber breach. It leaves cyber insurance companies questioning their language and restrictions to coverage. This attack brought customers questioning as well if the insurance is even worth it. It is hard to change the language so much and then still advertise it as a crucial need. It really hurt a lot of cyber insurance companies this way (Wolff, 2021).

The NotPetya cyber breach had many flaws that were just left alone for some time. The affect was $10 billion of global damage that should have tried to have been stopped beforehand. It made such an international impact and changed the way cyber insurance works and is looked at (Wolff, 2021). Cybersecurity measures such as vulnerability management and organizations applying the patch on time instead of waiting would have prevented this major attack. The time of the patch placement still might have allowed a window of access; however, vulnerability management could have mitigated that (*Notpetya: Looking back three years later*).

References

Notpetya: Looking back three years later. Claroty. (n.d.). https://claroty.com/blog/notpetya-looking-back-three-years-later#:~:text=Poor%20vulnerability%20management%3A%20Since%20the,organizations%20had%20applied%20the%20patch.

International cyber law: interactive toolkit. (2022, November 14). *Notpetya (2017)*. International cyber law: interactive toolkit. https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)#:~:text=The%20NotPetya%20malware%20was%20spread,and%20repurposed%20by%20the%20GRU.

Wolff, J. (2021, December 1). *How the notpetya attack is reshaping cyber insurance*. Brookings. https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/