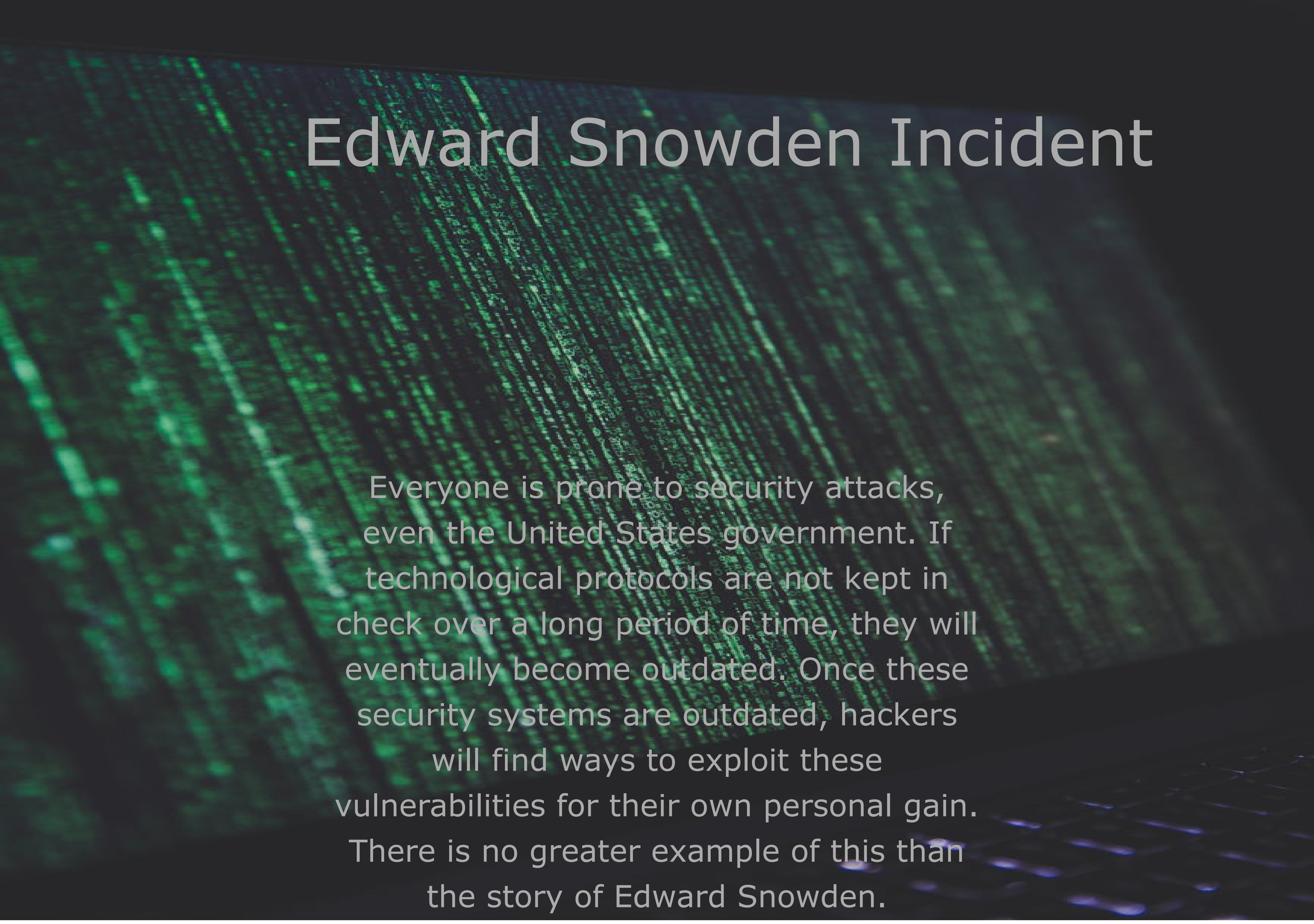

Edward Snowden Incident

Everyone is prone to security attacks, even the United States government. If technological protocols are not kept in check over a long period of time, they will eventually become outdated. Once these security systems are outdated, hackers will find ways to exploit these vulnerabilities for their own personal gain. There is no greater example of this than the story of Edward Snowden.

Who Is He And Why Is He Famous?

Edward Snowden is notoriously known as America’s most famous whistleblower. He was able to compromise millions of files without leaving a trace of evidence. Not only did he steal classified information from the U.S. government, he also revealed many of the top secret files for all to see in 2013. This all could have been prevented by the NSA if they regularly updated their security protocols. Snowden would not have been able to swipe such files if the system he extracted the files from traced his computer activity.

How Did He Steal Information From NSA Servers?

To avoid a long and drawn out story of Snowden’s entire career beforehand, he secured himself a job at Booz Allen Hamilton doing contract work for the NSA. This allowed Snowden access to an array of classified files within the NSA’s servers. At the time, the physical servers were accessed by employees through a “thin client”. A thin client is essentially a low-performance computer that is optimized for utilizing a main server’s computing power. In essence, the computer Snowden was using had access to nearly everything within the NSA’s servers.

Regardless of how easy it was to access the files, most people would get caught trying to view these files, but not Snowden. Because Snowden was a system administrator, he was allowed special privileges that nearly no one else had. A normal user on the network would have their activity logged for other higher-ups to view. But Snowden's permissions within the NSA's system allowed him to browse confidential files with no trace left behind. The NSA failed to account for a physical breach of their facility and Snowden exploited it.

The last piece of Snowden's puzzle was to avoid the eyes of in person spectators. If Snowden was located at the NSA's main headquarters, there would be numerous people walking by him. These people would see Snowden's flash drives and suspect his intentions to be harmful. This is why Snowden was sure to get somewhere more remote, where not as many people worked. The company he was hired by, Booz Allen Hamilton, and the NSA worksite he extracted this data from are both based in Honolulu, Hawaii. Snowden was able to hide his shady activities because there were not that many people to hide from in the first place.

The Aftermath

Because of these poor security measures, Edward Snowden was able to compromise approximately over 1.7 million files of sensitive data. After Snowden eventually leaked some of the data, he outed himself to the public, admitting it was him who stole the information. He says he did this so the government could not falsify a mock story, but some disagree, and believe he just wanted the credit. To this day, Snowden lives in Russia under temporary asylum and the Russian government has denied the U.S. government's request to hand him over. Because of Snowden's actions, U.S. intelligence officials have confirmed that they beefed up their security, starting with limiting the number of individuals with such high privileges on these classified servers.

ONWARD

This page is created and brought to you by Sean Rogawski and Nicholas Kafarski. Additional resources can be found in the following links.

OUR LINKS

Github - Sean
Github - Nicholas
Linkedin - Sean
Linkedin - Nicholas