An investigation of times that a lack in good physical security practices led to a cyber security issue

ISAAC BOAZ, Western Washington University, USA

Cybersecurity involves many layers and aspects of security to be achieved. This article analyzes and reviews historical occurences where a lack of physical security lead to a lack of cybersecurity. In addition to introduction, an analysis and review of such occurences will be presented.

CCS Concepts: • **Security and privacy** → **Security services**; **Systems security**; • **Social and professional topics** → *Network access restrictions*; **Social engineering attacks**; Universal access; Malware / spyware crime.

Additional Key Words and Phrases: Cybersecurity, Security, Software, Physical, Breaches

1 ARTICLE INTRODUCTION

In the world of software and programs, many people in the cybersecurity field focus on the security and practices used in their software and programs. However, one of the most well-known ideas for security is the idea that a system's security is only as strong as its weakest link. Just as electricity follows the path of least resistance, hackers and cybercriminals need only find a single weak point in a system to gain access to the rest of it.

Physical security is a part of cybersecurity. The act of protecting and securing IT assets, data, and resources from physical attacks is a part of cybersecurity. This article will review and analyze both fictional and non-fictional occurences where a lack of physical security lead to a lack or breach of cybersecurity.

A potential opinion of cybersecurity could fail to see (or underestimate) how a company's corporate culture could impact the security of the company. Password policies, access control, logging, and properly following security procedures must stem from a cybersecure-forward culture.

2 PHYSICAL SECURITY

Regardless of what a device is doing, it is always important to understand the physical environment and security that the device is in. Even the best anti-virus software cannot be protected from a malicious actor uninstalling it. Physical access could mean a man in the middle attack, power outages, or even a keylogger being installed.

Some basic physical security practices include:

- Locking a device when not in use
- Restricting physical access to those that need it
- Locking the doors and windows of a building
- Scanning and limiting who can enter a building
- Ensuring that all devices are up to date

Ultimately, physical security is necessary to ensure proper cybersecurity.

2.1 Cyber Secure Culture and Physical Security

The importance of a cyber secure culture cannot be understated. A company that does not have a cyber secure culture will not have employees that are aware of the dangers of social engineering, phishing, or plugging in unauthorized devices.

Author's address: Isaac Boaz, boazi@wwu.edu, isaac.k.boaz@gmail.com, Western Washington University, Seattle, Washington, USA.

Employee training, security protocols, and procedures are all dependent on a culture that is aware, attentive, and proactive about security; which you can only get from a cyber secure culture.

For instance, Google's Cyber Security Culture is stringent on including physical security, one example being how they handle their data centers [1]. Google made a video describing the security of their centers. To emphasize why the culture of cyber-security is important, Stephanie Wong (a Google employee) admitted she "could talk all day about cloud security, (but) physical security (at Google) is still pretty new to me" [2].

Google's Data Centers are a good example of how physical security is an important aspect of cybersecurity.

3 GOOGLE'S PLASMA GLOBE

One of the best ways to test security is by testing, verifying, and self-auditing how well the security system holds up. Google went about this by creating a "Red Team" [3], a team of white-hat hackers that were tasked with trying to hack Google (a testament to their cyber-security culture). Though this job includes software-based attacks, one of the successful attacks was a physical attack.

3.1 Google's Plan of Attack

The Red Team designed a Plasma Globe that had a USB cable attached to it for power. Only five plasma globes were created with a malicious modification to them. The Red Team added an internal chip that would emulate a USB keyboard when plugged in to a computer. After approximately 5-10 minutes, the device would quickly type out a command to download a larger payload from the internet [4]. In order to give the device to Google's employees, the Red Team disguised the device as an anniversary gift from Google (using LinkedIn to find anniversaries) [5].

While not everyone that received the device plugged it in, it only took one of Google's employees to plug it in for the attack be successful. Upon successful execution of the script, the Red Team had access to the employee's credentials. Through this, they were able to send emails to other employees which had higher privileges. Through these emails with attachments, the Red Team was able to gain access to Google's Glasses internal documentation [5].

Finally, the Red Team attempted to obtain a physical build of the Google Glasses. Unfortunately, due to a few typos, the Red Team caused a few red flags to be raised, and instead of going to pick up the build, they were met with Google's Chief Security Officer [5].

3.2 Attack Analysis

Ultimately, this attack was a phishing attack. The Red Team was able to convince Google's employees to plug in a USB device that was given to them. The Red Team was able to gain access to Google's Glasses internal documentation by using the employee's credentials [5].

Google's physical security culture did not account for the dangers of plugging in unauthorized devices. While Google's employees may have been aware of the dangers of USB devices, mistakes can happen or people can forget about security. Re-inforcing the importance of a cyber secure culture and the dangers of social engineering is important.

This attack also highlights the importance of physical security. If Google employees were not allowed to bring in unauthorized external devices, this attack would not have been successful.

3.3 Mitigation and Response

Google learned from this breach and created a software that would listen to extremely fast keystrokes from USB devices and block them. This software was then installed on Google's computers, and the software was publicly released [3, 6].

While a software solution is a good start, it is not a complete solution. A theoretically slow USB device could still be used to bypass this software. Cybersecurity hinges on a solid cyber secure culture, and humans are the core of that culture.

Whether a USB device is found in the parking lot or given as a gift, it is important to ensure that employees are aware of the dangers of plugging in unauthorized devices. Thankfully, the source of the attack was not a malicious actor, a testament to Google's cyber secure culture.

4 REMOTE HACKING OF OLDSMAR'S WATER TREATMENT SYSTEM

An interesting idea of physical security is the idea of remote physical security. The Oldsmar water treatment plant in Florida was hacked in February 2021. The attacker was able to remotely access the system "through a dormant software called TeamViewer" [7]. Unfortunately, not much is known about the attack, and Martina Dier (a spokeswoman for TeamViewer) stated "Based on cooperative information sharing, a diligent technical investigation did not find any indication for suspicious connection activity via our platform" [7].

4.1 Method of Attack

It is believed that the attacker was able to remotely access the system (supposedly) through TeamViewer. The attacker was able to increase the amount of sodium hydroxide (lye) in the water from 100 parts per million to 11,100 parts per million. Thankfully, the system's operator noticed the change and reverted it back to the normal levels.

[7] ultimately concludes that the attack was done remotely. The water treatment system was outdated and not kept up-to-date to proper security standards. "Gualtieri said the water treatment facility currently uses a Google Chrome product for remote access. The Oldsmar water treatment system is also using the Windows 7 operating system, which was released in 2009" [7].

4.2 Attack Analysis

The allowance of remote access to Oldsmar's water treatment system was a major security concern. A lack of proper security standards and outdated software contributed to the attack being successful [7]. A cyber secure-forward culture would have ensured that any remote access was authenticated, validated, logged, and audited.

Physical elements of a cyber secure culture could include requiring a physical security key, VPN, or timed access to the system. The Hill [8] admits that "Unfortunately, that water treatment facility is the rule rather than the exception. When an organization is struggling to make payroll and to keep systems on a generation of technology created in the last decade, even the basics in cybersecurity often are out of reach."

Ultimately a cyber secure culture needs to take into account maintenance and upkeep of the physical systems.

4.3 Mitigation and Response

A follow-up article by CyberScoop [9] reveals that it may not have been a cyber-attack at all, and that it could have been an unintentional action by an employee.

"The FBI concluded there was nothing, no evidence of any access from the outside, and that it was likely the same employee that was purported to be a hero for catching it, was actually banging on his keyboard" [9].

Even though this may not have been an actual outsider attack, the potential was certainly still present. According to [9], "a data leak containing the email addresses and passwords with two domains belonging to Oldsmar surfaced days before the breach occurred".

With a lack of proper financial resoruces, it is difficult to ensure that the water treatment system is up-to-date and secure.

Another interesting perspective of cyber security culture is how it relates to federal and public policy. The Biden Administration is slowly making progress to have cyber-security requirements, and the Environmental Protection Agency released a mandate for public water systems to "evaluate the adequacy" of any digital defenses through sanitation surveys [10].

5 CREDIT CARD SKIMMERS

An interesting example of a physical security breach is the use of credit card skimmers. Credit card skimmers are devices that are placed on top of a credit card reader that are able to read and store the information of a credit card. The skimmer is then retrieved by the attacker and the information is used to make unauthorized purchases [11].

While not be a direct physical security breach, the use of credit card skimmers is directly related to cyber security, as credit card information can be viewed as a form of digital information.

Though the mindset and knowledge of card skimming may not wholly be a part of a cyber secure culture, being aware of the current dangers and threats is important to a cyber secure culture. Customers, credit card companies, and businesses all need to be aware of the dangers of credit card skimmers.

In one instance, six people were arrested and charged with using credit card skimmers to steal over $5 million dollars from credit unions and banks [11]. This provides a critical reminder for the importance of physical security when it comes to cybersecurity. No matter how secure the software of an ATM is, a credit card skimmer can still be placed on top of it.

5.1 The Culture of Credit Card Skimming

While the typical scope of a security culture may be based off of a company's policies, executives, and employees, cultures are not limited to just companies. The cyber-secure culture of a city, state, or country can also be evaluated, analyzed, and improved. The Federal Bureau of Investigation (FBI) has a page dedicated to credit card skimming, and the FBI is working to educate the public about the dangers of credit card skimming [11].

6 CONCLUSION

Being aware of all potential entrypoints and the human element of security is important to keep in mind when designing a secure system. Security exploits could stem from the design of a building (such as a server room being too accessible) to the training of its employees.

Ensuring that all employees are trained to be aware of physical security and the dangers of social engineering is important. Additionally, ensuring that all employees are trained to be aware of the dangers of plugging in unauthorized devices is important. Having properly defined protocols and procedures for unlikely events is also important. Companies should internally test their security-GitLab for example (similar to Google) has a "Red Team" that is tasked with trying to hack GitLab [12].

Lastly, a culture is not limited to just a company. A city, state, or country can also have a culture of security. Informing family, friends, and the public about the dangers of social engineering, phishing, and plugging in unauthorized devices is important.

REFERENCES

[1] Google. Data and security - data centers - google, January 2023. URL https://www.google.com/about/datacenters/data-security/.

[2] Google Cloud Tech. Google data center security: 6 layers deep, January 2023. URL https://youtu.be/kd33UVZhnAA.

[3] Google. Meet the team responsible for hacking google, August 2022. URL https://blog.google/technology/safety-security/meet-the-team-responsible-for-hacking-google/.

[4] Michal Zalewski. The google plasma globe affair of 2012, October 2012. URL https://lcamtuf.coredump.cx/plasma_globe/.

[5] Google. Ep003: Red team | hacking google, October 2022. URL https://youtu.be/TusQWn2TQxQ.

[6] Google. Usb keystroke injection protection, July 2023. URL https://github.com/google/ukip.

[7] Eric Levenson Alex Marquardt and Amir Tal. Florida water treatment facility hack used a dormant remote access software, sheriff says, February 2021. URL https://www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html.

[8] Christopher Krebs. How to stop handing our cybersecurity keys to hackers, February 2021. URL https://thehill.com/opinion/cybersecurity/538237-how-to-stop-handing-our-cybersecurity-keys-to-hackers/.

[9] Christian Vasquez. Did someone really hack into the oldsmar, florida, water treatment plant? new details suggest maybe not., April 2023. URL https://cyberscoop.com/water-oldsmar-incident-cyberattack/.

[10] Christian Vasquez. Epa issues water cybersecurity mandates, concerning industry and experts, March 2023. URL https://cyberscoop.com/epa-water-cyber-regulations/.

[11] The Federal Bureau of Investigation. Skimming | federal bureau of investigation, January 2023. URL https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/skimming.

[12] GitLab. Red team rules of engagement, 2023. URL https://handbook.gitlab.com/handbook/security/threat-management/red-team/.