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 can be just as important and just as in-depth as 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 [6]. 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" [9].

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" [5], 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 [10]. 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) [4].

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 [4].

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 [4].

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 [4].

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 [5, 7].

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" [1]. 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" [1].

5 METHOD OF ATTACK

It is believed that the attacker was able to remotely access the system 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.

6 NOW YOU SEE ME 2

While not a real-life example, the movie Now You See Me 2 [8] presents a potential example of a physical security breach. In the movie, the main characters are able to breach a company's phone presentation by disguising as server maintenance, quickly convincing security that the original server maintainer was crazy, and installing a device that would allow them to control the presentation.

6.1 Attack

While very entertaining, the attack in the movie is not entirely realistic. Quick uniform changes and pretending that you belong was presented to seem entirely plausible. Regardless, the important parts of the attack were that the server room was easily accessible by all staff with only one layer of security. The single layer was a wired door that was left open by the original server maintainer.

Once the main character was in the server room disguised, he took a portable camera that could immediately print out a picture and pretended that it was "picture day" for the maintainer. The maintainer was not fooled by the lies, however, he was too confused and insisted that the character should not be there. Regardless, The main character printed out the picture and placed it on a badge for a mental facility.

Upon calling for security, the main character was able to convince the security that the maintainer was crazy and that he was the real maintainer. The main character was then able to install a device that would allow him to control the presentation.

6.2 Analysis

This attack was successful because of a lack of physical security. The server room was easily accessible by all staff and only had a single layer of security. The maintainer also left the door open, allowing the main character to easily enter the room. With no physical keycard, identification, or other security, the main character was able to easily enter the room.

6.3 Mitigation

Ideally, the server room would have had a physical keycard, identification, or other security that would have prevented the main character from entering the room. The maintainer should have also locked the door behind him, preventing the main character from entering the room. Lastly, ideally the security guards would have been trained to be aware of social engineering and to not be easily convinced by lies.

7 MISSION IMPOSSIBLE [2]

A more realistic example of a physical security breach is in the movie Mission Impossible. In the movie, Ethan Hunt (played by Tom Cruise) is tasked with stealing the NOC list from a CIA building. The NOC list is a list of all CIA agents that are currently undercover. The CIA building is heavily guarded and has many layers of security.

7.1 Attack

The move shows the many physical layers of security that the CIA building has. The building has a security guard, a security camera, a keycard reader, and a physical key. Access to the NOC list is also restricted to only the physical computer that the NOC list is on. The server room employs many measures and monitors to prevent unauthorized access.

Specifically, the server room has pressure-sensitive floors, a temperature monitor, sound sensor, and lasers above the ventilation system. All of these measures are disabled while an authorized person is in the room, and re-enabled when they leave.

Ethan Hunt goes through the ventilation system, uses a mirror to reflect the lasers, and is slowly lowered to the floor by a wire. He then hacks into the computer and steals the NOC list.

7.2 Analysis

Here we can see that the CIA building has many layers of physical security. Despite all of these layers, Ethan Hunt was still able to breach the security. Unfortunately, the CIA building failed to account for plot armor, which is a classic mistake in the field of cybersecurity.

7.3 Mitigation

Realistically, the CIA building should have had a more secure ventilation system; we see that the team was able to get into the ventilation system (and the building itself) by disguising as firefighers. The CIA did not have proper protocols or procedures for fire alarms or drills, which allowed the team to easily enter the building.

Additionally, requiring an authorized person to be in the room to access the computer would be a good requirement.

8 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 similarly has a "Red Team" that is tasked with trying to hack GitLab [3].

ACKNOWLEDGMENTS

I would like to thank Google for their Plasma Globe attack, and the creators of Mission Impossible for their interesting portrayal of physical security.

REFERENCES

[1] Eric Levenson Alex Marquardt and Amir Tal. 2021. Florida water treatment facility hack used a dormant remote access software, sheriff says. *CNN* 2021, 20210210 (2021).
[2] Tom Cruise. 1996. Mission: Impossible. https://www.imdb.com/title/tt0117060/
[3] GitLab. 2023. *Red Team Rules of Engagement.* https://handbook.gitlab.com/handbook/security/threat-management/red-team/
[4] Google. 2022. *EP003: Red Team | Hacking Google.* YouTube. Retrieved Jan 28, 2024 from https://youtu.be/TusQWn2TQxQ
[5] Google. 2022. *Meet the team responsible for hacking Google.* Google. Retrieved Feb 11, 2024 from https://blog.google/technology/safety-security/meet-the-team-responsible-for-hacking-google/
[6] Google. 2023. *Data and Security - Data Centers - Google.* Google Cloud. Retrieved Feb 11, 2024 from https://www.google.com/about/datacenters/data-security/
[7] Google. 2023. *USB Keystroke Injection Protection.* GitHub. Retrieved Jan 28, 2024 from https://github.com/google/ukip
[8] Louis Leterrier. 2016. Now You See Me 2. https://www.imdb.com/title/tt3110958/
[9] Google Cloud Tech. 2023. *Google Data Center Security: 6 Layers Deep.* Google. Retrieved Feb 11, 2024 from https://youtu.be/kd33UVZhnAA
[10] Michal Zalewski. 2012. The Google plasma globe affair of 2012. *Coredumb.cx* plasma_globe (2012).