**Project #1 Incident Response Report –**

**Part B: Summary After Action Report**

**By: Reece Zunino**

**CSIA 310 (6380) 6/13/2023**

**INTRODUCTION**

Sifers-Greyson is a well-known and established organization headquartered in Grayson County, Kentucky, USA. The president of the company is Ira John Sifers, III. He is the great-grandson of one of the company’s founders and the head of the engineering department. For Sifers-Grayson to compete with other organizations, they must be able to uphold compliance with NIST 800-171 and Federal Acquisition Regulations (DFARS including section 252-204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. Because of the recent acquisition of government contracts, the organization needs to bolster its security posture and comply with the recently stated regulations.

The recent penetration test conducted by the cybersecurity consulting firm Red Team showed that the organization is severely lacking in many aspects of information security, physical security, and incident response by the previously cited government regulations. The company has many departments but needs a centralized IT or incident response team. Each department is responsible for its infrastructure updating and monitoring, some of which are contracted out to third parties without direct oversight by the organization’s security department to ensure these standards are met.

The organization’s IT department, infrastructure, network, protocols, and incident response needs to be reviewed and severely improved to comply with government regulations. The organization may have full knowledge of its weaknesses and security shortfalls, but there needs to be more emphasis on fixing them before the contracts start. The penetration test was conducted so that the organization can meet its goals to become in compliance and be more in line with the NIST and DFARS standards.

“Pen tests are more comprehensive than vulnerability assessments alone. Penetration tests and vulnerability assessments both help security teams identify weaknesses in apps, devices, and networks. However, these methods serve slightly different purposes, so many organizations use both instead of relying on one or the other” (IBM, 2023). After the penetration test, the assessment revealed many vulnerabilities within the organization’s network, including physical and information security. The incident response from the security department was also lacking due to shortfalls in automated detection software and the IT department being understaffed. To have an effective security response team and IT department, more experienced staff must be on hand to see these shortfalls so that they can be rectified promptly and brought up to management.

**PENETRATION TEST RESULTS/INCIDENT ANALYSIS**

The results from the penetration test from the 24-hour attack period showed many vulnerabilities within the organization. Many failures of established policies were evident due to the different types of successful breaches that the Red Team could conduct. The attack was so successful that the Red Team obtained the new proprietary source code for the AX10 Drone system.

The rules of engagement (ROE) for the penetration test were against three different sites. The R&D Center 10.10.135.0/24, the Test Range 10.10.145.0/24, and the corporate headquarters 10.10.100.0/24. The Red Team was able to use both physical and technical means to penetrate the organization’s infrastructure to see how deep they could get and what information they could extract.

The Red Team first attacked the company’s engineering center’s R&D servers by hacking into the enterprise network through an unprotected network connection. There was no firewall to protect the server, nor did the network have an automated detection system that would have deterred or alerted the incident response team (IRT) so that they could enact countermeasures to thwart the attack. From that point, the Red Team could exfiltrate files from those servers and managed to steal 100% of the design documents and source code for the AX10 Drone System.

The Red Team also obtained around 20% of the company’s employees’ login credentials by leaving unattended USB drives in the corporate lounge, where employees eat lunch and take breaks. These USB drives had keylogging software loaded onto them, allowing the Red Team to obtain their login credentials for later use in a different attack. However, what was also found out during this physical security breach was that Sifers-Grayson employees were exceptionally friendly and talkative as they opened the RFID-controlled doors for the “new folks” on the engineering staff (who were Red Team members).

In another attack, the Red Team used the stolen login credentials to install malware over the network onto a workstation connected to a PROM burner in the R&D DevOps lab. The malware was then installed onto a test vehicle, which conducted flight tests at the testing grounds. The malware was activated during the flight test, making the drone return home and land in the Sifers-Grayson headquarters parking lot. These combined attacks proved that one of the weakest links within Sifers-Grayson is its employee’s lack of training in social engineering attacks and the ability to follow proper procedures with unattended or unmarked removable media devices.

The Red Team’s final attack against Sifers-Greyson was using several stolen credentials to send phishing emails from within the company’s email system. This was also a test against the already failing human factor of Sifers-Grayson’s IT infrastructure because security is everyone’s responsibility. “Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it is from a company you know or trust, like a bank or a credit card or utility company” (Federal Trade Commission, 2022). The Red Team reported that over 80% of the recipients clicked on the video link for cute kittens or cute cats. Twenty percent (20%) of the recipients clicked on the video link for a business news story. A video link to a sports event wrap-up for the Kentucky Volunteers basketball team had over 95% click-through rate.

**RECOMMENDATIONS FOR IMPROVEMENTS**

**Employees:** The employees at Sifers-Grayson need to have regular training in physical and information security. Regular training should also be on removable media devices and social engineering attacks and how to prevent them. This training should be conducted at a minimum annually so that if there is new information that is out, it can be passed down to the lowest level of an employee because everyone is responsible for security. Having the employees conduct this training will help bolster the company’s security posture and assure your customers that you take their information security seriously. “More than one-third of reported data breaches involve phishing emails. When building your cybersecurity layers, training on cybersecurity basics and best practices is essential to help end-users identify phishing emails and other common cyber scams that threaten your network’s security. This training can be reinforced through periodic phishing simulations, which test users’ vigilance in recognizing suspicious emails, further strengthening your defenses” (Mersch, 2021).

**Technology:** Most enterprise systems rely on other technology to keep them safe. This also includes the proper governance of such technologies. This would consist of proactively identifying vulnerabilities within the network, asset and risk management, and risk mitigation. “As part of continuous vulnerability management, an organization should run automated vulnerability scanning tools against all systems on the network frequently. Multiple dynamics can determine this frequency and could occur as broadly as annually, or as narrowly as weekly, depending on the asset classification” (Tripwire Researcher, 2022). Sifers-Greyson needs to consider coming into compliance with government regulations and standards that they must invest in a multi-layered security infrastructure. This type of security infrastructure allows itself to be semi-autonomous when defending itself. “Layered security is a network security approach that deploys multiple security controls to protect the most vulnerable areas of your technology environment where a breach or cyberattack could occur. The purpose of a multi-layered security approach is to ensure that each individual component of your cybersecurity plan has a backup to counter any flaws or gaps. These layers work together to bolster your defenses and build a solid foundation for your cybersecurity program” (Mersch, 2021). Investing in an automated detection system such as Intrusion Detection and Prevention System (IDS, IPS) allows the system to detect an intrusion faster than analysts may be able to spot it monitoring the network.

**Processes/Procedures:** The processes and procedures at Sifers-Grayson did not hold up to an attack by the Red Team. No redundancy was in place to help mitigate or even prevent a physical or cyber-related attack on the company. There must be policies in place and enforced in order to combat cybersecurity both at the workstation and around the building. Guidelines posted in common areas allow employees to keep the company’s security needs in mind. Having these policies also shows employees that they can be terminated or disciplined if they are found violating them and may incentivize them to enforce them more. Also, having some hierarchy within the IT department will allow for more efficient handling of security threats and separate individual roles within the organization. Ensuring that physical security is enforced is a first line of defense from threats. The Red Team being able to enter the building without badges should not have happened, and it needs to be expressed to all employees that this is unacceptable practice at Sifers-Grayson. Additionally, there needs to be processes and procedures developed and implemented for Incident Handling and First Response so that there is a faster response time when an incident occurs.

**LESSON LEARNED**

The penetration test conducted at Sifers-Grayson was an alert to the faltering systems in place for the company’s physical and information security systems, including their incident response. The recommendations will allow the company to improve, learn and grow its security posture and needs in the future. Cybercrime is an ever-evolving beast that comes up with new tactics, techniques, and technologies to exploit an organization's vulnerabilities for many different reasons. Some of the musts that need to happen at Sifers-Grayson are:

* Dedicated security and incident response team.
* Invest in more security professionals to become more effective.
* Strictly enforce physical security policies within the organization.
* Implement regular vulnerability monitoring and auditing of infrastructure.
* Invest in a more robust Cybersecurity training program for all employees.
* Conduct regular penetration tests to ensure that standards are being met.
* Invest in an incorporated Red Team into the organization and conduct in-house capture-the-flag events to keep skills sharp.

**References**

Federal Trade Commission. (2022, October 25). How to recognize and avoid phishing scams. Consumer Advice. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

IBM. (2023). What is penetration testing? IBM - United States. https://www.ibm.com/topics/penetration-testing

Mersch, A. (2021, October 4). What is layered security & how does it defend your network? Prosource | Business Technology Blog. https://blog.totalprosource.com/what-is-layered-security-how-does-it-defend-your-network#:~:text=Layered%20security%20is%20a%20network,breach%20or%20cyberattack%20could%20occur

NIST. (2012, August). Computer Security Incident Handling Guide. NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Tripwire Researcher. (2022, July 18). 4 stages of vulnerability management program best practices. Tripwire | Security and Integrity Management Solutions. https://www.tripwire.com/state-of-security/vulnerability-management-best-practice