**Project #1 Incident Response Report –**

**Part A: Incident Response Report Form**

**By: Reece Zunino**

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

**SIFERS-GRAYSON CYBERSECURITY INCIDENT REPORT FORM**

1. Contact Information for the Incident Reporter and Handler

– Name: Reece Zunino

– Role: Cybersecurity consultant with

– Organizational unit: Nofsinger Consulting, LLC, Assistant to Sifers-Greyson Blue Team Analysts.

– Email address: reece.zunino@NofsingerConsulting.com

– Phone number: +1(485) 651-7889

– Location: 1555 Pine Knob Trail, Pine Knob, KY 42721.

1. Incident Details

– Status change date/timestamps (including time zone): when the incident started when the incident was discovered/detected, when the incident was reported, when the incident was resolved/ended, etc.

* On June 11, 2023, a penetration test was carried out by a red team of a cybersecurity consulting firm that Sifers-Grayson hired. This penetration test assessed the organization’s network security and overall cybersecurity posture. The attack by the consulting firm Red Team went undetected by Sifers-Greyson’s security teams, and the breach was unknown until the next day.

– Physical location of the incident (e.g., city, state)

* 1555 Pine Knob Trail, Pine Knob, KY 42721.

– Current status of the incident (e.g., ongoing attack)

* The attack is no longer ongoing and has been resolved.

– Source/cause of the incident (if known), including hostnames and IP addresses

* R&D Center 10.10.135.0/24
* Test Range 10.10.145.0/24
* Corporate HQ 10.10.100.0/24.

– Description of the incident (e.g., how it was detected, what occurred)

* The red team of a cybersecurity consulting firm that Sifers-Grayson hired conducted a penetration test at Sifers-Greyson. The red team first gained access to the organization’s R&D servers by hacking an unprotected connection on the enterprise network. The Red Team proceeded to exfiltrate files from those servers and managed to steal 100% of the design documents and source code for the AX10 Drone System. The consulting firm’s Red Team could then steal passwords for 20% of the employee logins using keylogging software installed on USB keys left on the lunch table in the headquarters building employee lounge. The team gained access to the employee lounge due to the lack of concern from other employees, and they let the Red Team members in without company credentials or asking them basic questions about where their badges were. The Red Team continued its efforts to penetrate the organization. They used the stolen login to install malware over the network onto a workstation connected to a PROM burner in the R&D DevOps lab. Using the installed malware, the Red Team took control of one of the drones and landed it in the company parking lot, proving the link was not secure. Using the employee login credentials, the Red Team sent phishing emails to other employees using videos and links to emails and where they were forwarded. Due to the lack of enterprise monitoring and automated detection capabilities, the attack went undetected for the 24hr penetration test period.

– Description of affected resources (e.g., networks, hosts, applications, data), including systems’ hostnames, IP addresses, and function

* The incident affected many different resources within the Sifers-Grayson network. The R&D department at R&D Center 10.10.135.0/24 had malware installed onto their systems and compromised a critical asset. The Test Range at Test Rang 10.10.145.0/24 had an aerial test vehicle hijacked and sent back to the company. This could have happened during a high-visibility event and shown the organization's severe lack of security resources. The Corporate HQ at 10.10.100.0/24 was also affected by employees having their credentials stolen and their accounts used to send phishing emails to other employees on the network and beyond.

– If known, incident category, vectors of attack associated with the incident, and indicators related to the incident (traffic patterns, registry keys, etc.)

* The attack vectors used by the Penetration test team were USB Keyloggers, internet phishing emails, weak encryption, impersonating employees (insider threat), and malware.

– Prioritization factors (functional impact, information impact, recoverability, etc.)

* Functional Impact- **IP addresses, source code, and email accounts.**
* Informational Impact- **PII, Secret and proprietary information, employee credentials.**
* Recoverability- **The actions presented during the penetration test would have been unrecoverable. The amount of information stolen and the ability to steal proprietary equipment would have been a significant loss to the company. It would have had a detrimental impact on the trust of our customers.**

– Mitigating factors (e.g., a stolen laptop containing sensitive data was using full disk encryption)

* None

– Response actions performed (e.g., shut off host, disconnected host from the network)

* None

– Other organizations contacted (e.g., software vendor)

* None

1. Cause of the Incident (e.g., misconfigured application, unpatched host)

* There is a lack of proper security procedures in essential information assurance and security procedures regarding physical security. This would include training on adequately handling unknown removable media devices in the workplace. There is also a lack of automated detection software that would have mitigated some of the attack vectors that the Team used to gain access to the organization’s network.

1. Cost of the Incident

* The cost of this incident could be detrimental if it had been an actual attack. The cost estimate could have been anywhere from $500K to over $1M due to the stolen drone and much more losses in contract revenue and customer trust.

1. Business Impact of the Incident

* Due to this being a test, the business has no real impact. However, if this had been a real attack, the impact could have been unrecoverable, leading to the organization’s collapse.

1. General Comments

* There must be a bigger emphasis on the security posture of the network. Workstations need to have better security in place to hinder unwanted access to the network such as dual authentication. All employees need to undergo retraining in physical and information security so that they know the risk it can pose to the organization. New policies need to be written to be able to handle an incident like this so that there is a response to an incident. More security response employees should be hired to have the ability to respond to an incident of this size. New automated software needs to be installed so that the network can detect an attack before it escalates out of control and has a detrimental impact.