CSL3350 – Enterprise Security and Governance

Assignment 2: Case Study: Analysis of Contemporary Computer Security Issues

Glen TEAKLE 10532981

Joondalup Campus/Online

Dr Mohi Ahmed

Contents

[Executive Summary 3](#_Toc136332727)

[Analysis and Explanation of Incidents 4](#_Toc136332728)

[Incident 1. 4](#_Toc136332729)

[Incident 2. 4](#_Toc136332730)

[Incident 3. 4](#_Toc136332731)

[Assumptions and Root Causes of Incidents 4](#_Toc136332732)

[Recommendations 4](#_Toc136332733)

[Technical 4](#_Toc136332734)

[Non-Technical 5](#_Toc136332735)

[Plan to Defend 6](#_Toc136332736)

[Cyber Safety Education and Training. 6](#_Toc136332737)

[Policy Creation and Adoption. 6](#_Toc136332738)

[Multi Factor Authentication. 6](#_Toc136332739)

[Adopting a Zero Trust Mindset. 7](#_Toc136332740)

[Implementing Next Generation Firewalls. 7](#_Toc136332741)

[Subnetting/Network Segmentation. 7](#_Toc136332742)

[Intrusion Detection System (IDS). 7](#_Toc136332743)

[Incident Detection and Prevention System (IDPS). 7](#_Toc136332744)

[Purchase of Personal Devices. 7](#_Toc136332745)

[References 8](#_Toc136332746)

# Executive Summary

A mining organisation in Perth with more than 20,000 employees (many of them with an aboriginal background) over various sites has recently been affected by several incidents in relation to cyber security. This report aims to analyse and explain the incidents in detail. The reported incidents involve areas such as: passwords, availability of computers, cyber awareness and best practices relating to cyber security.

The main focus of this report is mitigation; however it will also cover how and why the incidents occurred, the root cause(s) of such incidents and recommendations to help prevent any similar incidents occurring in the future. Lastly, a short-term and long-term plan with strategies to defend against cyber-attacks has been outlined. Assumptions have been made where appropriate.

# Analysis and Explanation of Incidents

Incident 1. An employee’s private email address has been logged into using one of the publicly accessible computers. This has resulted in phishing emails sent to many of the company’s executives requesting payments which led to donations being made by them.

**How it Occurred.**

The employee likely didn’t log out of his account when finished on the computer, so anyone else can access their email in the browser. Recent files could have been remotely accessed by an attacker to find the notepad file containing the user credentials (see incident 2). An attacker could remotely access the email, and this is likely the case as demonstrated by the emails sent requesting help for aboriginal communities, and the denial from the employee that they are the one who sent them. The email address has likely been hacked. The “human factor” in information security is one of the biggest risks as identified by Kaspersky (2017), where it was reported that 45% of cyber incidents were caused by uneducated staff and simple mistakes. As demonstrated in this incident, social engineering can then be used to attack vulnerable humans. A common result of this type of attack is ransomware, which has occurred within this mining organisation (see incident 3).

Incident 2. An attacker has likely discovered the notepad file with the saved login credentials and used them to login to the employee’s email account. Unsolicited emails were sent from this account resulting in phishing and a ransomware attack.

**How it Occurred.**

Saving login credentials on a computer in an easily accessible notepad file which is likely not itself, password protected or saved in a secure location ie not on the desktop. As mentioned in incident 1, an attacker could remotely gain access to the computer and notepad file containing the password. This incident could also have been caused by another employee, perhaps disgruntled, who has access to this particular login as many of the employees share passwords for ease of access, due to the lack of available computers. The computers also do not have any password protection so anyone that is not an employee of the site (visitors, unauthorised parties) could also potentially gain access. Furthermore, no multi-factor authentication (MFA) is in place to properly authenticate an employee logging in.

Incident 3. A successful ransomware attack has occurred after an attacker has gained initial access to an employee email account and has impersonated the employee by sending emails from it. The receiver has opened a PDF file attachment contained in the email, as it was seemingly from another legitimate employee of the mine site. However, this file contained malware and once opened it locked all the user’s files/folders contained on the computer and demanded a payment to unlock everything.

**How it Occurred.**

The email access was likely gained through one of the following methods:

* The employee not logging out of his email account.
* Sharing of login credentials with other employees.
* Saving login credentials to a notepad file that was easily accessible by other users.
* No education regarding opening of email attachments.

# Assumptions and Root Causes of Incidents

The following is a list of all likely causes of the above incidents. This list includes assumptions made based on the scenario.

* Employees sharing ID cards and login credentials (username, password) for easier access of the limited computers.
* Employees do not log out of accounts when finished (ie email).
* Employees do not use complicated passwords or change them regularly.
* There is no education regarding the dangers of opening email attachments.
* There is no education relating to social engineering.
* There is no cyber awareness or training (specifically on phishing).
* No antivirus software is installed on the computers.
* Router settings may be set as default.
* Employees plug in personal devices (phones, USB’s) to the computers.
* Software on the computers is not regularly updated or patched with security updates.

# Recommendations

There are numerous ways to employ countermeasure methods within this organisation that would help mitigate further potential threats and cyber-attacks, while also increasing employee awareness. These can be categorised as either Technical or Non-technical and are summarised below.

## Technical

* Email scanning/filters to detect malware attachments. Coupled with employee awareness of opening attachments, scanning software would help by identifying potentially damaging emails containing malware (Barracuda Networks, 2022).
* Implementation of multi-factor authentication (MFA) for all employees to verify their identity whenever they login to a computer. Using the supplied RFID cards together with some form of biometric authentication would be an ideal solution. MFA is a proven method to prevent password-related attacks (ACSC, n.d). If an employee does not log out of a system after use, the system should timeout after a short time and require the MFA authorisation again for access.
* Access management/Principle of least privilege (Ahmed, n.d.). Employees should only be able to access what they need to on the computers relative to their specific roles and should not have access to anything else (ie no private email or social media on computers).
* Prohibiting any saving/uploading of personal data onto the computers. This includes the use of personal devices (eg mobile phones, USB’s) being plugged in.
* No saving passwords on computers in any form. The use of a password manager such as Nordpass (Nord Security, 2023) would make remembering passwords unnecessary for employees. The only requirement is remembering the master password for the password manager.

## Non-Technical

* Regular cyber-awareness education and training for all employees and executives. Including but not limited to:
* Password creation and use.
* Phishing.
* Clicking on attachments.
* Ransomware education.
* Account use.
* Antivirus.
* Firewalls.
* Dangers of password sharing.
* Knowing who to report an incident to, and how.

Cyber training should be conducted in short sessions and kept as non-technical as possible. (ie one session dedicated to passwords). This will ensure not to overload employees with too much information at once, thereby increasing the risk of them becoming careless if they feel too much responsibility (Ahmed, n.d). Another option would be to employ the use of a program such as Security Education Training and Awareness (SETA https://livlab.org/seta/) which is a program aimed at helping organisations to mitigate security issues caused by human error (SETA, 2023). Training should include information on the latest security issues/breaches. Employees should be made aware of the latest changes/updates to existing policies and any new policies in place. (Ahmed, n.d).

* Education on data in its various stages (in storage, in use and in transit) and the dangers of not securing it (Ahmed, n.d.)
* Implementing security policies for all employees to comply with and abide by.
* Forbidding any sharing of RFID cards, passwords/login credentials. Implementing biometrics as part of MFA would help mitigate this issue completely. This would also help prevent a remote attack as the attacker likely does not have access to an employee’s biometrics (unless the attacker is themself an employee).
* Enforcing regular password changes (for example every 2 months) and denying the user of any access until this has been completed.
* Personal devices locked away onsite to prevent theft/misuse.

# Plan to Defend

Further to the above recommendations, what follows is a plan to defend, mitigate and protect against any potential cyber threats against the mining organisation. This plan should be implemented as soon as possible, and is in recommended order of implementation, based on the reported security incidents.

## Cyber Safety Education and Training.

This should be made a regular, mandatory part of work life for all relevant staff on the mine site to attend. It should include the following topics:

* Password creation and management. Dangers of password sharing.
* Data in storage, use and transit.
* Policies in place and compliance requirements.
* Email phishing/clicking on potentially dangerous attachments.
* Ransomware.
* Account use/privileges.
* Antivirus and Firewalls.

Policy Creation and Adoption. The Australian Cyber Security Centre (ACSC) along with the Australian Signals Directorate (ASD) both have published guidelines to aid in the creation of policies that align with Australian standards. These can be found [here](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines) and [here](https://www.asd.gov.au/cyber-security).

[This](https://specopssoft.com/blog/password-policy/) link may also prove helpful in the creation of specific password policies.

Relevant policies that need to be implemented into this organisation, with regular revision and updates where necessary include:

* Password Management.
* Email.
* Use of Personal Devices.
* Incident Reporting.
* Disaster Recovery Plan.
* Lessons Learned.

All policies should be given to new employees, as well as current employees being made aware of their existence and implementation. Compliance of each relevant policy should be a necessity for any employee who works at this organisation.

## Multi Factor Authentication.

The previously reported incidents could all have been prevented, or at least mitigated with the use of MFA. Introducing MFA to the employees will educate them as to the effectiveness of the “something you have, something you are and something you know” strategy. The employees already possess one of these (RFID cards) so implementing the other two would be simple and immediately effective if used correctly.

## Adopting a Zero Trust Mindset.

Employees and executives should acknowledge that threats can exist both in and outside their organisation (NSA, 2021). A Zero Trust model assumes that certain things will occur or have already occurred. For example: malware being downloaded or an attacker gaining initial access to a system. This model constantly questions whether users, devices and network components should be trusted, and monitors their subsequent actions under the assumption that they cannot be (NSA, 2021).

## Implementing Next Generation Firewalls.

These contain more security layers and capabilities for protection compared to traditional firewalls (Cisco, 2023 & New Era Technology, 2022). Additional capabilities include application awareness and control, integrated intrusion prevention and threat intelligence delivered from the cloud (Cisco,2023).

## Subnetting/Network Segmentation.

The ransomware attack could easily spread to other computers on the organisation’s network if it was programmed to do so. If the network was segregated however, the spread of this virus could be contained until it was removed. Splitting the network into smaller subnets would also be beneficial if one of the subnets was kept for Admin/IT purposes only. This would help prevent things such as an employee accidentally deleting sensitive files/folders, or even accessing data they should not have access to by restricting content (NSA, 2018). Subnetting combined with the use of firewalls is a strong method of incident prevention (Pott, 2018).

## Intrusion Detection System (IDS).

The use of an application-aware IDS would add another layer of defence to the organisation by ensuring any malicious activity would not go unnoticed (NSA, 2018). An IDS would identify any activity on the network that is not regular and could be configured so that Admin get notified directly (Shanley, n.d). False alarms and “noise” are an unfortunate complication in IDS use that could become more of a problem if the IDS is not configured properly, but this could be regularly attended to.

## Incident Detection and Prevention System (IDPS).

The use of an IDS should be upgraded if plausible, to an IDPS which not only detects intrusions, but also acts to mitigate a threat and contain it as quickly as possible (Shanley, n.d). There are different types of IDPS and they can be installed at specific points in the network to monitor and prevent malicious activity. Some types are also not vulnerable to direct attacks and may go unnoticed by an attacker (Shanley, n.d). IDPS’ can also collect data which allows for analysis of an attack (how and why it occurred). This information would be helpful to use in the disaster recovery plan policy.

## Purchase of Personal Devices.

A long-term goal of this organisation, depending on budget and necessity, could be the purchase of tablets and laptops for those employees that don’t specifically need a computer for their role. This would help with control access and maintaining access for other employees using the limited number of available computers.

# References

Ahmed, M. (n.d), CSL3350 *Introduction to hacking: Module 2* [Lecture notes]. Canvas. <https://courses.ecu.edu.au/>

Ahmed, M. (n.d), CSL3350 *Data: Module 5* [Lecture notes]. Canvas. https://courses.ecu.edu.au/

Ahmed, M. (n.d), CSL3350 *Authentication: Module 9* [Lecture notes]. Canvas. <https://courses.ecu.edu.au/>

Australian Cyber Security Centre. (2022). PROTECT YOURSELF:

MULTI-FACTOR AUTHENTICATION. <https://www.cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides/protect-yourself-multi-factor-authentication>

Barracuda Networks. (2022). *Barracuda's free Microsoft 365 Email Threat Scan*.https://www.barracuda.com/products/email-scan?&utm\_source=google&utm\_medium=search\_cpc&utm\_campaign=1817237198&utm\_adgroup=66930289422&utm\_term=email%20malware%20scanner&utm\_position=&utm\_matchtype=e&utm\_device=c&utm\_content=344983308363&\_bn=g&gclid=Cj0KCQjw98ujBhCgARIsAD7QeAgK9asU1QzCFtnEd3DCTFgV3YJeb2Mt5auT9XKV8oesiD2z1GnR8uYaAiuMEALw\_wcB

Cisco. (2023). *What Is a Next-Generation Firewall?* <https://www.cisco.com/c/en_au/products/security/firewalls/what-is-a-next-generation-firewall.html>

IT Living Labs. (2023). *Security Education Training and Awareness (SETA)*. <https://livlab.org/seta/>

Kaspersky. (2023). *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

National Security Agency. (2018). *NSA’s Top Ten Cybersecurity Mitigation Strategies*. https://media.defense.gov/2019/Jul/16/2002158046/-1/-1/0/DDD-190716-666-071.PDF

National Security Agency. (2021). *Embracing a Zero Trust Security Model*. <https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF>

New Era Technology. (2022*). Cybercrime Is On The Rise – What That Means For Australian Businesses*. <https://www.neweratech.com/au/blog/cybercrime-is-on-the-rise-what-does-that-mean-for-australian-businesses/>

Nord Security. (2023). *Secure and intuitive password manager*. https://nordpass.com/password-managers/?gad=1&gclid=Cj0KCQjw98ujBhCgARIsAD7QeAiWgJsChqJKB\_ZfvddRDfTHyazEmOUAJ9oBZpUfDgw5Q494k2VQ9ZoaAhjzEALw\_wcB

Pott, T. (2018). *The Gorilla Guide to Enterprise Security Fundamentals*. Actualtech Media.

Shanley, L. (n.d), CSG3309 *Protection mechanisms: Module 8* [Lecture notes]. Canvas. https://courses.ecu.edu.au/