**Logo, company name

Description automatically generated**

**Security Assessment Exercise Report**

Version N.3

August 1, 2023

Table of Contents

[1. Summary 3](#_Toc141734798)

[1. Assessment Scope 3](#_Toc141734799)

[2. Summary of Findings 3](#_Toc141734800)

[3. Summary of Recommendations 7](#_Toc141734801)

[2. Goals, Findings, and Recommendations 8](#_Toc141734802)

[1. Assessment Goals 8](#_Toc141734803)

[2. Detailed Findings 8](#_Toc141734804)

[3. Recommendations 10](#_Toc141734805)

[3. Methodology for the Security Control Assessment 13](#_Toc141734806)

[3.1.1 Risk Level Assessment 13](#_Toc141734807)

[3.1.2 Tests and Analyses 14](#_Toc141734808)

[3.1.4 Tools 14](#_Toc141734809)

[3.1.5 Risk Assessment 15](#_Toc141734810)

[4. Figures and Code 16](#_Toc141734811)

[4.1.1 Risk Assessment & Checklist 16](#_Toc141734812)

[4.1.2 Process or Data flow of System, use-cases, security checklist, graphs, etc. 17](#_Toc141734813)

# Summary

Goal:

The goal of the assessment is to secure the office from physical intrusions and breaching, secure the computer and network from any malware possibly implemented or installed by the terminated employee, to ensure that confidential information is protected, and to report and deter the terminated employee of attempting any malicious actions against the business.

It is to be noted that this assessment exercise is performed for research and educational purposes. A notable purpose is to see how passive reconnaissance can help blue team or the defending party from security weaknesses and threat actors. Only malicious activities against the business will be reported, the rest of the findings on social media will be found inconsequential or inconclusive, for the privacy of the individual.

Methods:

The methods used to solve the vulnerabilities were installing and changing additional security measures and policies. Additionally, logging any downloads, emails ingoing and outgoing, installs, and accounting possible social media accounts to report any possible defamation against the business.

## Assessment Scope

The terminated employee had access to the office suite, all the unlocked office spaces, and a workstation computer with access to the business’s cloud server. He had been employed for less than one year, most of the information he acquired or projects he participated in are non-confidential, but it is unknown whether he has confidential information. It has been noted that he was using social media during work hours.

## Summary of Findings

Physical Security & Policies:

* The front office door is always left unlocked. **Moderate risk.**
* Only one person sees the door most days. **Low risk.**
* No cameras inside the office or entrance. **Moderate risk.**
* Double doors in Storage room can be breached via slipping a card through door crack and knob. **High risk.**
* Monitors in three offices and the flat screen in the conference room are viewable from outside the window. **Observational Low Risk.**

Computer Security:

* Did not wipe the storage of the workstation computer system on termination. **Moderate risk.**
* Did not check any logs of what was downloaded on to the computer on termination. **Low risk.**

Network Security:

* Did not check any logs of what was uploaded on to the server before termination. **Moderate risk.**
* The business has updated their servers to a new firewall. **Observational-Low risk.**
* The files and folders on the server can be modified, deleted, and added by anyone with access to the server. **Observational-Moderate Risk**.
* Phishing emails being sent to employees’ company email accounts. **Observational-Moderate Risk**

Social Media:

* Social-media accounts were found, specifically a LinkedIn and a Facebook account. All posts are inconsequential or inconclusive so far. **Observational-Low risk.**

Of the findings discovered during our assessment, 1 was considered **High risks**, 4 **Moderate risks (2 Observational)**, 7 **Low (3 Observational)**, 0 **Informational risks**. The SWOT used for planning the assessment are broken down as shown in Figure 2.

Figure 1. Findings by Risk Level

There are a total of 12 issues that were found and amended, there were less serious vulnerabilities because the business had already had some policies for security. The business already outsourced most of the responsibilities to 3rd party services such as the office building owner and the IT/network security company maintaining their network. See Figure 2.

A diagram of a company's strength

Description automatically generated

Figure 2. SWOT

All weaknesses were fixed or reported, no results of malicious actions found. The measures taken place have reduced the amount of threat actors and the chance of an attack on the business.

There are only a couple of top-level threats because the business already had most of the proper physical security and policies in place but never employed or enforced those until the threats were made apparent. The threat actor could have exploited the known holes of the security or expected the security of the business lax. The computer and network security are being handled by a 3rd party company that is approved by the government so they can handle projects from the government or any business needing that level of security. On top of that, the network security was updated and maintained at the time of the employee’s termination. However, it was imperative to do a checkup on security and download/upload logs because the threat actor had direct access to the workstation and could have planned on being terminated and installed a malware capable of activating remotely or on a timer. So far, no sensitive information or defamation has been spread by threat actors on social media.

## Summary of Recommendations

* Update the office policy to keep the door locked by default and give the employees keys to the office. **Easy fix.**
* Install a doorbell with a camera on the office entrance. **Moderately Difficult fix.**
* Routinely check the logs that account for downloads to the workstations. **Easy routine.**
* Wipe workstation computer prior to the day of termination for employees. **Moderately fix.**
* Review logs from CMIT that account for uploads to the server. **Easy routine.**
* Inform the building owner of the terminated employee and notify security or contact the police if seen on the premises of the property. **Easy fix.**
* Routinely review social media to scan for defamation or spread of any damaging information related to the company. **Easy routine.**
* Hire another secretary or admin. **Moderately Difficult fix.**
* Change the access control to the server so that certain folders can be locked with a password. **Moderately/Very Difficult Fix.**
* Change the access control to the server so that a password is needed to modify or delete files or folders. **Moderately Difficult fix**
* Employ a policy for the employees to use the Keeper Password Management Application. **Moderately Difficult fix**.
* Install a cover plate knob for the double doors in the storage room. **Easy fix.**
* Replace the doorknob for the double doors in the storage room. **Easy fix**.
* Use window blinds frequently or turn monitor away from the window. **Easy fix.**

# Goals, Findings, and Recommendations

## Assessment Goals

The purpose of this assessment was to do the following:

* To secure the office from physical intrusions and breaching.
* Secure the computer and network from any malware possibly implemented or installed by the terminated employee.
* To ensure that confidential information is protected.
* To report and deter the terminated employee from attempting any malicious actions against the business.
* It is to be noted that this assessment exercise is performed for research and educational purposes.
  + One notable purpose is to see how effective passive recon is for the defending party to defend against threat actors.
  + Another notable purpose is to practice the use of passive recon tools and CADD to map out the physical vulnerabilities of the office.
  + Only malicious activities against the business will be reported, the rest of the findings on social media will be found inconsequential or inconclusive, for the privacy of the individual.

## Detailed Findings

Physical Security & Policies:

* The front office door is always left unlocked. **Moderate risk.** The door to the office space was constantly left unlocked because the location of the office had been relocated to a safer area of the city, which led the employees and management to feel comfortable leaving the doors unlocked. This can lead to significant consequences due to internal threat actors taking advantage of the vulnerability.
* Only one person sees the door most days. **Low risk.** Although the office doesn’t get frequent visitors, the risk of piggybacking or sneaking into the office is still a possibility. To mitigate that, the secretary is stationed by the front door, but she doesn’t attend work the whole work week which leads to the front door being unmonitored. This discounts the mitigation significantly because if the secretary is not monitoring the door, then no one is.
* No cameras inside the office or entrance. **Moderate risk.** Having cameras in the office can be seen as a risk to privacy or intrusion if the cameras are vulnerable to being accessed by unauthorized individuals. However, the risk of not being able to spot or identify intruders, and not being able to record workplace incidents is a larger risk than the risk of intrusion. This could also be slightly mitigated if the presence by the front door is covered more frequently, but it won’t solve unseen intruders or unrecorded workplace incidents.
* Double doors in Storage room can be breached via slipping a card through door crack and knob. **High risk.** Someone can easily access the storage room and the rest of the office space through this method which can lead to theft, unauthorized access to confidential information, unauthorized access to equipment and technology, and vandalism. The method can be done with other tools or equipment since the gap between the two doors has no cover protecting the latch.
* Monitors in three offices and the flat screen in the conference room are viewable from outside the window. **Observational Low Risk.** This is a risk that has to be monitored depending on the scale and confidentiality of certain projects being worked on. Having information viewable from outside of the office can lead to weakness to the access control for confidential information. Threat actors can easily take photos of unattended monitors that are facing the window.

Computer Security:

* Did not wipe the storage of the workstation computer system on termination. **Moderate risk.** It is true that the terminated employee did not look competent enough to install any malicious program undetected. It doesn’t mean that he could not get help in doing so or accidentally do it himself.
* Did not check any logs of what was downloaded on to the computer on termination. **Low risk.** If the terminated employee was aware that his termination was soon, he could have prepared or taken measures to get retribution once being let go. After all, he was let go because of his unethical behavior.

Network Security:

* Did not check any logs of what was uploaded on to the server before termination. **Moderate risk.** Although CMIT solutions are the only ones to check those logs, asking for those logs from them would have been no trouble. If the terminated employee managed to upload a virus, the firewall and detection system may send out an alert, but methods could have been used to avoid detection, so checking the logs is important.
* The business has updated their servers to a new firewall. **Observational-Low risk.** Although the firewall update is necessary, it can still disrupt business activity. One way it affected the business is by disrupting employees connecting to the company’s network and their workstation from home. During these updates, the internal network and some systems may act unpredictably. It’s best to observe any changes going on when the firewall is being updated.
* The files and folders on the server can be modified, deleted, and added by anyone with access to the server. **Observational-Moderate Risk**. There are countermeasures already in place to mitigate the high risk such as back up servers that frequently update, alerts, and a 30-day recycle bin storage, but being able to modify files to such a degree without access control can lead to some major disruption.
* Phishing emails being sent to employees’ company email accounts. **Observational-Moderate Risk.** Policies, tools, and CMIT are used as countermeasures to mitigate the risk. However, phishing attempts still occur infrequently. So far, the only solicitation was for phone numbers. The attempts must be monitored through documentation or by further utilizing or contacting CMIT solutions. Monitor the attempts in case they become frequent, or the solicitations escalate.

Social Media:

* Social-media accounts were found, specifically a LinkedIn and a Facebook account. All posts are inconsequential or inconclusive so far. **Observational-Low risk.** It is not expected that any defamation or malicious posts will be made against the business by this individual. However, to ensure that no defamation or damaging information is being spread, monitor social media tags that involve the business such as #AES or #AtlanticEngineeringServices. This risk is easy to track and the accounts belonging to the individual have been recorded, the accounts found may not be definitive.

## Recommendations

Disclaimer: Some of these recommendations may address the same found weaknesses with different methods, please carefully review the policies, systems, and data affected when considering these recommendations.

* Update the office policy to keep the door locked by default and give the employees keys to the office. **Easy fix.** Keeping the door locked and giving employees keys to the office space is a simple fix to prevent intruders from entering the office. The policy may be inconvenient to employees and hard to get used. This policy can be temporary, but only if there are other countermeasures in place to mitigate the risk of undetected intrusion.
* Install a doorbell with a camera on the office entrance. **Moderate fix.** Reinstalling a new doorbell for a new one is not entirely necessary if the policy to keep the door locked stays. If the fix is performed, keep in mind that the footage needs to be stored somewhere, maintained, and would need to be occasionally monitored.
* Review logs that account for downloads to the workstations. **Easy routine.** Utilizing CMIT solutions, occasionally checking download history on file explorer, or using Webroot malware scan to check if there are any malware downloaded on to the computer.
* Wipe workstation computer prior to the day of termination for employees. **Moderately Difficult fix.** Although it was locked prior to the day of termination for the employee, its best to organize the downloads and documents into respective folders then wiping the workstation’s storage to ensure that no malware is on the computer or be potentially uploaded to the server. This will ensure that no project data or drawings are lost in the process. This can be a tedious process if there are many files in storage.
* Review logs from CMIT that account for uploads to the server. **Easy routine.** This can be done by simply contacting CMIT to have them review the uploads to the server and sending a document of it being checked, this is a fast and great process to ensure no malware was uploaded to the server.
* Inform the building owner of the terminated employee and notify security or contact the police if seen on the premises of the property. **Easy fix.** Contacting the owner of the building by email with a description of the employee and letting them know of the situation will include more people looking out for the terminated employee. However, this should be done with heavy consideration as it may not be necessary.
* Routinely review social media to scan for defamation or spread of any damaging information related to the company. **Easy routine.** This routine does not need to be frequent. The accounts recorded may not be definitive as the individual could use aliases. However, through searching social media tags related to the company such as #AES can be another way of finding malicious posts made. So far, no malicious post has been found.
* Hire another secretary or admin. **Moderately Difficult fix.** The time and cost of hiring and training a new secretary or administrator would be great. Considering the probability of the risk happening, it is not likely enough for this option to be worth the trouble unless there is another reason beyond security. This option could be used on the approach of not wanting to employ a policy to keep the door locked. This would be a great way to ensure that there are always eyes on the door. The new hire would further ensure security by being another person monitoring systems and the internal network.
* Change the access control to the server so that certain folders can be locked with a password. **Moderately/ Very Difficult Fix.** To perform this recommendation option, contact CMIT solutions, they are the ones able to walk through the process to enable the feature. This fix could be extremely tedious depending on the approach of locking the folders. Either it would have to be done manually or it could be automatically done, depending on the limitations of the server and the method of locking folders. One limitation for the automatic method is the fact that it may not be desired to have all folders locked. The password for each folder can be unique depending on the method being used to lock the folder. The benefit from this fix is that old project folders cannot be modified or deleted unintentionally.
* Change the access control to the server so that a password is needed to modify or delete files or folders. **Moderately Difficult Fix.** Using CMIT solutions to enable this option is the only method available since they have the privilege to do so. Once the feature is implemented, all folders will need a password to be modified, moved, or deleted. Given the level of professionalism of the employees, the password can be short and generic so it would be easy to input, but it would act as a warning for a user if they performed an unintended action. If an employee gets terminated, the password can be changed to avoid data breaches.
* Employ a policy for the employees to use the Keeper Password Management Application. **Moderately/ Very Difficult fix**. Depending on the approach, this option could a tedious process. Ensuring that all employees are on and have their information stored would be time-consuming. Then ensuring all the passwords are safe can take plenty of time depending on how many unsafe passwords are found. The fix is a great way to track account breaches and know if an employee’s data has been recorded to a database. The password management system also has a feature for password generation.
* Install a cover plate knob for the double doors in the storage room. **Easy fix.** Doing this would prevent the double doors from being unlock with small objects.
* Replace the doorknob for the double doors in the storage room. **Easy fix**. Replacing the latch with one that can make it impossible for the latch to be interacted with in such a way that it would be unlocked would ensure that the door would be secure from that method.
* Use window blinds frequently or turn monitor away from the window. **Easy fix.** Either way could be done but consider doing so when working on confidential projects. Performing this fix would prevent threat actors from stealing information by taking pictures inside the office and display screens.

# Methodology for the Security Control Assessment

### Risk Level Assessment

Table - Risk Values

| Rating | Definition of Risk Rating |
| --- | --- |
| High Risk | Exploitation of the technical or procedural vulnerability will cause substantial harm to the business processes. Significant political, financial, and legal damage is likely to result |
| Moderate Risk | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to organization. |
| Low Risk | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment |
| Informational | An “Informational” finding, is a risk that has been identified during this assessment which is reassigned to another Major Application (MA) or General Support System (GSS). As these already exist or are handled by a different department, the informational finding will simply be noted as it is not the responsibility of this group to create a Corrective Action Plan. |
| Observations | An observation risk will need to be “watched” as it may arise as a result of various changes raising it to a higher risk category. However, until and unless the change happens it remains a low risk. |
| Non-Risk | A note or findings of a search or process that state that there is no risk or an improbable chance of it becoming a low risk due to error or unexpected various changes. However, it should not be expected to change or needed to be “watched.” Once expected to be changed, it should immediately be re-labeled as an observational risk. |

Table - Ease of Fix Definitions

| Rating | Definition of Risk Rating |
| --- | --- |
| Easy | The corrective action(s) can be completed quickly with minimal resources, and without causing disruption to the system or data |
| Moderately Difficult | Remediation efforts will likely cause a noticeable service disruption   * A vendor patch or major configuration change may be required to close the vulnerability * An upgrade to a different version of the software may be required to address the impact severity * The system may require a reconfiguration to mitigate the threat exposure * Corrective action may require construction or significant alterations to the manner in which business is undertaken |
| Very Difficult | The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling   * An obscure, hard-to-find vendor patch may be required to close the vulnerability * Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity * Corrective action requires major construction or redesign of an entire business process |
| No Known Fix | No known solution to the problem currently exists. The Risk may require the Business Owner to:   * Discontinue use of the software or protocol * Isolate the information system within the enterprise, thereby eliminating reliance on the system   In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the Business Owner, and reviewed by IS Management, to validate that security incidents have not occurred |

### 3.1.2 Tests and Analyses

Physical Security:

* Observing the entrances and office layout and documenting any weakness found.
* Using Revit to make a layout of the office to map out weakness found.
* Pen tested the double door to test weakness to breaching.

Computer Security:

* Using Webroot malware scan to analyze the terminated employee’s workstation computer’s security.
* Utilizing CMIT to test whether malware was stored on any workstations.

Network Security:

* Utilizing CMIT to test whether malware was uploaded to the server.
* Observing phishing email attempts on work email accounts.

Social Media:

* Passive reconnaissance observations with social media, search engines, and conversational AI.
* Scanning posts on found social media accounts for any defamation, damaging information, or other malicious statements based on date of employment and date of termination.

### 3.1.4 Tools

This assessment was completed using the network security tools, physical security policies, and computer security tools employed by the business.

Physical Security:

* CADD and Revit were used to design the layout of the office.
* The doorbell was implemented as a solution to let the whole office know of a visitor or someone at the door.
* A card was used to perform a penetration test on the storage room double door.

Computer Security:

* Windows file explorer
* Windows 11 Defender
* Webroot malware scan
* CMIT solutions support

Network Security:

* CMIT solutions support was utilized in reviewing and testing network security vulnerabilities, especially internal security.

Social Media/ Passive Recon:

* Fake accounts were made to keep anonymity and a wordlist with relevant information of the terminated employee to perform a passive reconnaissance on the potential threat actor on social media.
* Google and Bing were utilized for passive recon to ensure any information was found to aid in the search of any defamation or damaging information being spread.
* Bing AI, and Chat GPT were utilized for further passive recon to ensure that all social media accounts were found by optimizing queries, prompts, and information.

Documentation:

* Excel, notepad, and screen shots were used to document any findings.

### 3.1.5 Risk Assessment

[See in 4.1.1](#_Risk_Assessment_&)

# Figures and Code

### Risk Assessment & Checklist



Figure 7. Risk Assessment Check list with Access and Network Controls.



Figure 8. Overall Risk Assessment Table.

### Process or Data flow of System, use-cases, security checklist, graphs, etc.

A drawing of a house

Description automatically generated

Figure 9. 2D Top-Down Layout of the Jacksonville Office with Sketches Mapping out Vulnerabilities.

A drawing of a house

Description automatically generated

Figure 10. 3D Top Corner View of Office Layout of the Jacksonville Office.

A grey building with many windows

Description automatically generated

Figure 11. 3D Window View of Office Layout of the Jacksonville Office.

A screen shot of a computer

Description automatically generated

Figure 12. Malware Scan of the Terminated Employee’s Workstation Computer.

A computer screen with a list of text

Description automatically generated

Figure 13. Desktop Folder of the Terminated Employee’s Workstation Computer.

A screenshot of a computer

Description automatically generated

Figure 14. Downloads Folder of the Terminated Employee’s Workstation Computer.

A screenshot of a computer

Description automatically generated

Figure 15. Desktop Folder of the Terminated Employee’s Workstation Computer.

A screenshot of a computer

Description automatically generated

Figure 16. Spreadsheets Folder of the Terminated Employee’s Workstation Computer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Table of Social Media Accounts and Scan of Malicious Posts of Terminated Employee | | | | |
| Social Media | Social Media Account | Malicious Posts | Mentions or tags to business | Link to page |
| LinkedIn | Found | None | None | <https://www.linkedin.com/in/nabeel-anwar-e-i-4023a284/> |
| Facebook | Found | None | None | https://www.facebook.com/nabeel.anwar.357 |
| TicTok | Not Found | N/A | N/A | N/A |
| Instragram | Not Found | N/A | N/A | N/A |

Figure 17. Table of Social Media Accounts and Scan of Malicious Posts of Terminated Employee.