

Information Security Risk Management & Audit Report for BCAS Campus

2024

Student ID: MS23487284 | Student Name: M.A.K.Tharika | Student Mail: [MS23487284@my.sliit.lk](mailto:MS23487284@my.sliit.lk)

Table of Contents

[Table of Figures 2](#_Toc164781186)

[Table of Tables 3](#_Toc164781187)

[1. Executive Summary 4](#_Toc164781188)

[2. Introduction 5](#_Toc164781189)

[3. Asset Identfication 6](#_Toc164781190)

[4. Risk Identification 7](#_Toc164781191)

[5. Allegro Worksheet 10 for the above-mentioned Risks, 8](#_Toc164781192)

[5.1. OCTAVE Allegro 10 worksheet for Network attack, 8](#_Toc164781193)

[5.1.1. Justifications 11](#_Toc164781194)

[5.2. Octave Allegro 10 Social Engineering Attack, 12](#_Toc164781195)

[5.2.1. Justifications, 14](#_Toc164781196)

[5.3. Octave Allegro 10 worksheets for Ransomware Attacks, 15](#_Toc164781197)

[5.3.1. Justifications, 17](#_Toc164781198)

[5.4. OCTAVE Allegro 10 worksheet for Virus Attack, 18](#_Toc164781199)

[5.4.1. Justifications, 20](#_Toc164781200)

[5.5. Octave Allegro 10 Social for Tailgating, 21](#_Toc164781201)

[5.4.2. Justifications, 23](#_Toc164781202)

[6. Conclusion, 24](#_Toc164781203)

[7. References 25](#_Toc164781204)

# Table of Figures

[Figure 1: How the attacks against org. affects on company reputation. [2] 10](#_Toc164780758)

[Figure 2: Cost of Phishing attacks. [4] 13](#_Toc164780759)

# Table of Tables

[Table 1: OCTAVE Allegro 10 worksheet for Network attack. 9](#_Toc164781172)

[Table 2: Octave Allegro 10 Social Engineering Attack. 12](#_Toc164781173)

[Table 3: Octave Allegro 10 worksheets for Ransomware Attacks. 15](#_Toc164781174)

[Table 4: OCTAVE Allegro 10 worksheet for Virus Attack. 18](#_Toc164781175)

[Table 5: OCTAVE Allegro 10 worksheet for Tailgaiting. 21](#_Toc164781176)

# Executive Summary

BCAS Campus is a leading educational institution committed to providing industry-relevant skills through higher-level education. With a student population of more than 3500 across five campuses, including the main campus in Colombo and branches in Kandy, Jaffna, Galle, and Kalmunai, BCAS ensures students are trained to make a positive impact in their chosen fields.

The institution has achieved recognition through various awards, including Sri Lanka’s Most Successful Employer Award, Outstanding Contribution to the Cause of Education Award, and Asia’s Best Employer Brand Awards from renowned international award ceremonies. BCAS has a rich history going back to 1999, focusing initially on providing necessary computing education and English language skills to school leavers. Over the years, it has evolved to offer diverse programs, including the flagship "Access Programme," which prepares students for employment and higher education opportunities both locally and internationally.

BCAS has made significant strides in preparing students for the Middle Eastern job market, with over 10,000 alumni employed in West Asia. Additionally, a substantial number of alumni have found employment in countries like Great Britain, Canada, Australia, and the United States of America.

The institution’s vision is to become the premier private university in the South Asian region, while its mission revolves around producing market-relevant quality human resources with ethics and social responsibility through innovation, research, and skills development.

BCAS is dedicated to revolutionizing education by offering engaging and accessible programs designed to provide to learners of all ages and backgrounds. Through cutting-edge technology and creative teaching methods, BCAS aims to bring subjects to life and facilitate effective learning experiences.

# Introduction

This document is focused on risk management of the BCAS campus using the OCTAVE framework. The OCTAVE framework offers a systematic approach to identifying, analyzing, and mitigating information security risks specific to the organization's operational context. By employing OCTAVE, BCAS aims to comprehensively assess the threats, vulnerabilities, and potential impacts on its information assets, thereby enhancing its resilience to cyber threats and disruptions.

Nowadays rapidly evolving technological landscape, ensuring the security and integrity of educational institutions' information systems is critical. BCAS Campus, as a leading educational institution, recognizes the critical importance of effective risk management in safeguarding its information assets and ensuring business continuity. To address this need, BCAS has undertaken the task of conducting an Information Security Risk Management and Audit utilizing the **Operationally Critical Threat, Asset, and Vulnerability Evaluation** (OCTAVE) framework.

Further in this document risks of BCAS assets related to those risks and how to control/manage them will be included.

# Asset Identfication

BCAS contains the following assets,

|  |  |
| --- | --- |
| **Hardware Assets** | * PC * Monitors * Projectors * Fingerprint Machines * Digital Boards * Key Boards * Access points * Servers * Cables * Printers |
| **Software Assets** | * Operating Systems * Firewalls * Application software * VLE |
| **People Assets** | * Employees * Students |
| **Physical Assets** | * Buildings * Class Rooms * Tables * Chairs * Labs |

# Risk Identification

In BCAS following security risks exist,

1. **Network attack:** In the BCAS networks are not hidden the SSIDs are visible to everyone and this increases the risk of network attack. Also, the passwords are not that much advanced.

|  |  |
| --- | --- |
| **Assets Affecting** | Information, Mail Server |
| **Threat Scenario** | An attacker conducting a Man In The Middle(MITM) attack on the company server. The attacker will eavesdrop and take a copy of the email conversations between the campus and students. |

1. **Social Engineering Attack:** On the campus, other than computing school many schools and departments exist, these departments have people with less security awareness, therefore there is a risk of facing a Social Engineering phishing attack.

|  |  |
| --- | --- |
| **Assets Affecting** | VLE, Employee Credentials, Information such as courseworks/course materials |
| **Threat Scenario** | An attacker conducting a phishing attack targeting BCAS employees to gain their VLE credentials. |

1. **Ransomware Attack:** A few software are not up to date, they contain vulnerabilities that can be exploited and install malware as ransomware.

|  |  |
| --- | --- |
| **Assets Affecting** | System Data such as Office Account details, Payments slips, SLAs, etc… |
| **Threat Scenario** | A ransomware attack installed in a Marketing employee's PC encrypts all the data and demands a ransom from the organization. |

1. **Virus Attack:** In some PCs of computer labs on the campus the admin approval request for installing software has been removed, therefore students can download and install software as they wish, which can lead to virus attacks.

|  |  |
| --- | --- |
| **Assets Affecting** | Lab PC, OS(windows 11) , applications on the PC, Information of the PCs |
| **Threat Scenario** | The student has downloaded a virus accidentally and ran it, this makes the computer slow, data theft. This might lead to a hardware crash because the virus might run some processes behind the users. |

1. **Tailgaiting:** Employees can insert into the premises as a student/ employee by the main gate by following an employee/ student to the premises.

|  |  |
| --- | --- |
| **Assets Affecting** | Hardware devices and physical assets |
| **Threat Scenario** | An intruder from the outside tailgates an employee secretly goes to a lab premises and installs a keylogger device on one of the PCs of IT administrators, this might lead to data theft and data Disclosure. |

# Allegro Worksheet 10 for the above-mentioned Risks,

## OCTAVE Allegro 10 worksheet for Network attack,

Table 1: OCTAVE Allegro 10 worksheet for Network attack.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | Mail Server and its information. | | | | | |
| Area of Concern | *Data breach using MITM.* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | An Attacker | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | The attacker will place himself in between the communications of the mail server and the client, and because of the weak security of WIFI, he can gain access to the network and eavesdrop on the packets using a tool such as Wireshark and go through the network packets/content. | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Personal Gain | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | By eavesdropping the network and taking a copy of the data. (Data Breach) | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High**   **90%** | * **Medium**   **45%** | | * **Low**   **15%** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value(10)** | **Score** |
| Confidential information such as student VLE credentials, course materials, and organizational agendas can be disclosed. This will damage the student's trust towards the organization (BCAS Campus) and lead to reputational damage and customer confidence damage. | | | | Reputation & Customer  Confidence | | 6 | 5.4 |
| Financial | | 4 | 3.6 |
| This also can lead employees to resign because of the reputational damage therefore productivity can be harmed. | | | | Productivity | | 2 | 1.8 |
| Safety & Health | | - | - |
| Leakage of Confidential information may lead to Fines and legal penalties. | | | | Fines & Legal Penalties | | 4 | 3.6 |
| User Defined Impact Area | | - | - |
| **Relative Risk Score** | | | | | | | | **14.4** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Hardware | Place the access points in a safer place where intruders can’t access.  Install a firewall device with proper configurations such ASA firewall of CISCO. | | | |
| Application | Change router credentials and hide router SSID.  Encrypt the connection using encryption technology.  Change the router password into an unpredictable password. | | | |
| User | Aware users to follow the below rules when sending emails,   * Always send screenshots of credentials when sharing. * Monitor the users/devices who log into your wifi network. * Always follow the password policy when updating passwords. | | | |
|  |  | | | |
|  |  | | | |
|  |  | | | |

### Justifications

In this chapter, you can find a justification for selecting the above impact and probability levels,

#### Probability level,

For this threat scenario, the chosen probability level is High which is 90%, This level was predicted after going through several resources, in Figure 1 below one of the research approach results has been shown.

According to previous attempts towards the campus and research conducted by Nile [1] earlier for other campuses, we can say that the probability rate of MITM occurring can be stated as medium.

#### Impact level,

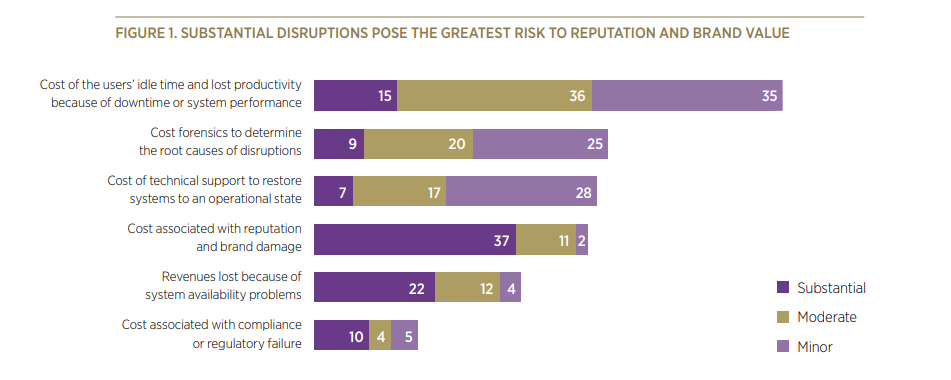
In the MITM passive attacks, there can be data disclosure and data theft which is a confidentiality violation which harms the organizational reputation. 

Figure 1: How the attacks against org. affects on company reputation. [2]

Using the help of the above research as well the value of Reputation & Customer Confidence has been selected as 6/10 and Financial is 4/10.

If the attackers get user credentials and log into user accounts they can change those passwords as legitimate users can't use them. This will affect productivity slightly as well and there can be scenarios where the reputational damage causes the productivity loss. The chance of these is low therefore the value has been chosen as 2/10.

These mentioned issues won't affect the Safety & Health of a person therefore that has been kept blank.

If a data disclosure occurs there can be fines and penalties involved because customers/ employees have the right to sue an organization if their data got breached. [3] Therefore the value of Fines and penalties has been chosen as 4/10.

## Octave Allegro 10 Social Engineering Attack,

Table 2: Octave Allegro 10 Social Engineering Attack.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | | | | **Information Asset Risk Worksheet** | | | | | | | |
| **Information Asset Risk** | | **Threat** | Information Asset | | | VLE, Employee Credentials, Information such as course works/course materials | | | | | | | |
| Area of Concern | | | *An attacker conducting a phishing attack targeting BCAS employees to gain their VLE credentials.* | | | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | | | An attacker | | | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | | | Send a phishing mail with a link similar to the BCAS VLE password resetting portal and pretend to be a BCAS employee who asked to reset your password. | | | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | | | Personal Gain | | | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | | | * **Disclosure** * **Modification** | | | * **Destruction** * **Interruption** | | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | | | Data Breach by phishing scam | | | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | | | * **High**   **(90%)** | | * **Medium**   **(45%)** | | | * **Low**   **(15%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | | |
| **Impact Area** | | | **Value** | **Score** |
| Data Disclosure such as,   * Leakage of course materials. * Leakage of Assessments. * Leakage of Assessment Marks.   Which harms the Reputation & Customer Confidence and leads to Financial Damage. | | | | | | | Reputation & Customer  Confidence | | | 7 | 6.3 |
| Financial | | | 5 | 4.5 |
|  | | | | | | | Productivity | | | - | - |
| Safety & Health | | | - | - |
| The company can get sued because of the data disclosure. | | | | | | | Fines & Legal Penalties | | | 5 | 4.5 |
| User Defined Impact Area | | | - | - |
| **Relative Risk Score** | | | | | | | | | | | | | **15.3** |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | | | | | | | | | | |
| * **Accept** | | | | * **Defer** | | | * **Mitigate** | | | * **Transfer** | | | |
| **For the risks that you decide to mitigate, perform the following:** | | | | | | | | | | | | | |
| *On what container would you apply controls?* | | | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | | | | | | | | |
| Technical | | | * Apply spam filters to emails. * Scan malicious links in suspicious emails. | | | | | | | | | | |
| Employee wise | | | * Conduct awareness Sessions. * Conduct training sessions. * Conduct phishing campaings. | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |

### Justifications,

In this chapter, you can find a justification for selecting the above impact and probability levels,

#### 5.1.1.1. Probability level,

The reason to choose probability high for the phishing attack is it is the most common type of attack that exists According to a study [4].

#### 5.1.1.2. Impact Level,

According to a study, the cost of phishing in some organizations can be shown below,

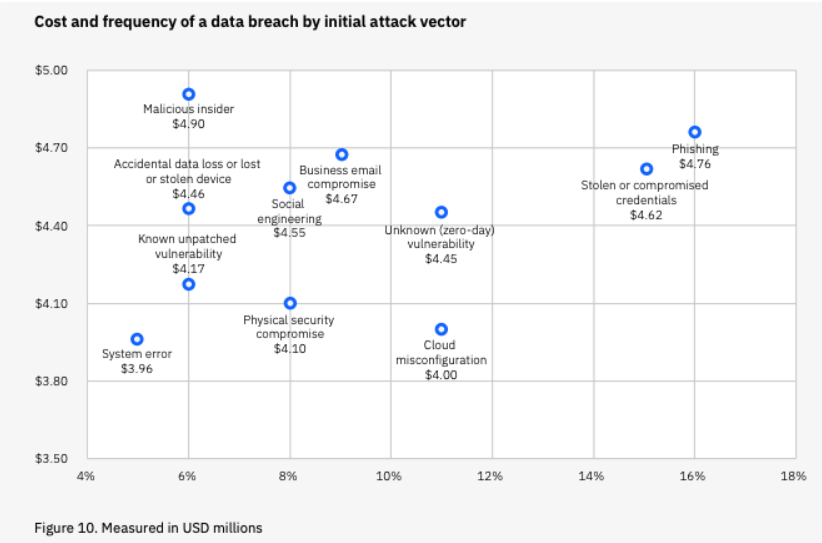


Figure 2: Cost of Phishing attacks. [4]

## Octave Allegro 10 worksheets for Ransomware Attacks,

Table 3: Octave Allegro 10 worksheets for Ransomware Attacks.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | | | | **Information Asset Risk Worksheet** | | | | | | | |
| **Information Asset Risk** | | **Threat** | Information Asset | | | System Data such as Office Account details, Payments slips, SLAs, etc… | | | | | | | |
| Area of Concern | | | A few pieces of software are not up to date, they contain vulnerabilities that can be exploited and install malware as ransomware. | | | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | | | An attacker | | | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | | | Exploiting a software vulnerability such as CVE-2013-4341CVE-97355. | | | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | | | To gain course materials/assignments for personal gain. | | | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | | | * **Disclosure** * **Modification** | | | * **Destruction** * **Interruption** | | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | | | Data Breach. | | | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | | | * **High**   **(90%)** | | * **Medium**   **(45%)** | | | * **Low**   **(15%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | | |
| **Impact Area** | | | **Value** | **Score** |
| Disclosure of information such as,   * Account Details. * Trade secrets. * Student Marks. * SLA.   Which harms the Reputation & Customer Confidence and leads to Financial Damage. | | | | | | | Reputation & Customer  Confidence | | | 8 | 3.6 |
| Financial | | | 9 | 4.05 |
| Destruction of information can lead to less productivity. | | | | | | | Productivity | | | 9 | 4.05 |
| Safety & Health | | | - | - |
| Also, information disclosure might lead to Fines & Legal Penalties. | | | | | | | Fines & Legal Penalties | | | 9 | 4.05 |
| User Defined Impact Area | | | - | - |
| **Relative Risk Score** | | | | | | | | | | | | | **15.75** |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | | | | | | | | | | |
| * **Accept** | | | | * **Defer** | | | * **Mitigate** | | | * **Transfer** | | | |
| **For the risks that you decide to mitigate, perform the following:** | | | | | | | | | | | | | |
| *On what container would you apply controls?* | | | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | | | | | | | | |
| Administrative | | | Implement a strict patch management policy to ensure timely updates for all software.  Conduct regular security awareness training for employees to identify and avoid phishing attempts.  Implement strong password policies and enforce multi-factor authentication. | | | | | | | | | | |
| Technical | | | Patch the identified vulnerabilities (eg:CVE-2013-4341 and CVE-97355) immediately.  Implement network segmentation to restrict access to sensitive data.  Deploy intrusion detection/prevention systems (IDS/IPS) to monitor for suspicious activity.  Regularly back up critical data and implement disaster recovery procedures. | | | | | | | | | | |
| Physical | | | Secure access to server rooms with physical controls like keycard access. | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |

### Justifications,

Here are the reasons to choose the above probability and impact levels,

#### Probability level:

The chosen probability level is 90% which is high. Attackers actively exploit known vulnerabilities, making the likelihood of a successful attack high. According to a study done under Verizon highlights that 80% of breaches involved vulnerabilities that had patches available. [5]

#### Impact Levels:

Disclosure of Information which is chosen as High Impact - Score: 8, because of Leakage of sensitive data like account details, SLAs, or student marks can damage reputation, erode trust, and potentially lead to legal issues. The Ponemon Institute's "Cost of a Data Breach Report 2023" indicates the average cost per lost record due to a data breach is $245. This cost reflects the financial impact of recovery, legal fees, and reputational harm. [6]

Very high financial impact -Score 9, because Data breaches can incur significant financial costs for recovery, potential regulatory fines, and lost revenue due to downtime or reputational damage. The same Ponemon Institute report states the global average total cost of a data breach in 2023 was $4.35 million. [6]

Destruction of Information impact which is the same level as Financial impact given because of, Losing access to critical data like course materials, assignments, payment records, or SLAs disrupts operations, hinders productivity, and can potentially lead to financial losses.

Fines and Legal penalties have high score for impact because Depending on the data types involved, regulations like GDPR might impose significant fines for data breaches.

## OCTAVE Allegro 10 worksheet for Virus Attack,

Table 4: OCTAVE Allegro 10 worksheet for Virus Attack.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | | | | **Information Asset Risk Worksheet** | | | | | | | |
| **Information Asset Risk** | | **Threat** | Information Asset | | | Lab PC, OS(windows 11) , applications on the PC, Information of the PCs | | | | | | | |
| Area of Concern | | | *System exploiting usning a virus.* | | | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | | | Malicious actors/ Unintentional actors | | | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | | | In some PCs of computer labs on the campus the admin approval request for installing software has been removed, therefore students can download and install software as they wish, which can lead to virus attacks. | | | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | | | Malicious actors: Motive could include stealing data (e.g., student information), disrupting operations, or installing ransomware.  Unintentional actors: Lack of awareness or understanding of security risks. | | | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | | | * **Disclosure** * **Modification** | | | * **Destruction** * **Interruption** | | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | | | Data Breach. | | | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | | | * **High**   **(90%)** | | * **Medium**   **(45%)** | | | * **Low**   **(15%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | | |
| **Impact Area** | | | **Value** | **Score** |
| Reputation & Customer Confidence: Virus outbreaks can damage the institution's reputation for IT security, impacting student and faculty trust. (Assign a value based on your organization's priorities)  Financial: Costs associated with virus removal, data recovery, and potential hardware damage. (Assign a value) | | | | | | | Reputation & Customer  Confidence | | | 7 | 6.3 |
| Financial | | | 5 | 4.5 |
| Productivity: Disruption of lab activities due to infected systems. (Assign a value). | | | | | | | Productivity | | | 6 | 5.4 |
| Safety & Health | | | - | - |
|  | | | | | | | Fines & Legal Penalties | | | - | - |
| User Defined Impact Area | | | - | - |
| **Relative Risk Score** | | | | | | | | | | | | | **16.2** |
|  | | | | | | | | | | | | |  |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | | | | | | | | | | |
| * **Accept** | | | | * **Defer** | | | * **Mitigate** | | | * **Transfer** | | | |
| **For the risks that you decide to mitigate, perform the following:** | | | | | | | | | | | | | |
| *On what container would you apply controls?* | | | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | | | | | | | | |
| Administrative Controls | | | Re-implement the admin approval process for software installation.  Implement a policy for allowed software in the labs.  Conduct security awareness training for students about safe software practices. | | | | | | | | | | |
| Technical Controls | | | Install and maintain antivirus software with real-time scanning on all Lab PCs.  Implement application whitelisting to restrict software execution only to approved programs.  Utilize network segmentation to isolate lab traffic from other critical systems. | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |

### Justifications,

The following are why I have chosen the above Probability and Impact levels,

#### Probability level:

This threat occurs because of the absence of an admin approval process for software installation on Lab PCs. This allows students to download and install any software, significantly increasing the likelihood of encountering malware. That is why the probability level is chosen as high.

#### Impact levels:

Reputation & Customer Confidence (High Impact), A virus outbreak in Lab PCs can significantly damage the institution's reputation for IT security. This can lead to a loss of trust from students, faculty, and potential partners. The IBM Security X-Force Threat Intelligence Index 2023 shows that highlights reputational damage as a major consequence of cyberattacks. [7]

Financial (Medium Impact), Financial impacts associated with virus outbreaks include costs for, Removing the virus and restoring affected systems, Recovering any lost or damaged data, In severe cases, malware can damage hardware components. While these costs can be significant, in the case of Lab PCs, they might be less impactful compared to a broader system outage.

Productivity (Medium Impact) chosen because, Infected Lab PCs disrupt planned lab activities, impacting student and faculty productivity. This can lead to delays in coursework, research, and overall learning outcomes.

## Octave Allegro 10 Social for Tailgating,

Table 5: OCTAVE Allegro 10 worksheet for Tailgaiting.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | | | | **Information Asset Risk Worksheet** | | | | | | | |
| **Information Asset Risk** | | **Threat** | Information Asset | | | Hardware devices and physical assets | | | | | | | |
| Area of Concern | | | *Employees can insert into the premises as a student/ employee by the main gate by following an employee/ student to the premises.* | | | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | | | Malicious actors | | | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | | | Attackers seeking to steal equipment or data, or disgruntled individuals wanting to cause damage. | | | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | | | Theft of hardware (e.g., laptops, servers), data stored on devices, or vandalism of equipment. | | | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | | | * **Disclosure** * **Modification** | | | * **Destruction** * **Interruption** | | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | | | Data Breach. | | | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | | | * **High**   **(90%)** | | * **Medium**   **(45%)** | | | * **Low**   **(15%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | | |
| **Impact Area** | | | **Value** | **Score** |
| Security breaches can damage the organization's reputation, impacting trust from stakeholders. Costs associated with replacing stolen equipment, repairing damaged assets, and potential data recovery. | | | | | | | Reputation & Customer  Confidence | | | 5 | 2.25 |
| Financial | | | 6 | 2.7 |
| In extreme cases, unauthorized individuals could pose a physical threat to employees or cause safety hazards. Which causes issues in Safety & Health. | | | | | | | Productivity | | | - | - |
| Safety & Health | | | 5 | 2.25 |
| In extreme cases, unauthorized individuals could pose a physical threat to employees or cause safety hazards. Which leads to Fines & Legal Penalties. | | | | | | | Fines & Legal Penalties | | | 7 | 3.15 |
| User Defined Impact Area | | | - | - |
| **Relative Risk Score** | | | | | | | | | | | | | **10.35** |
|  | | | | | | | | | | | | |  |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | | | | | | | | | | |
| * **Accept** | | | | * **Defer** | | | * **Mitigate** | | | * **Transfer** | | | |
| **For the risks that you decide to mitigate, perform the following:** | | | | | | | | | | | | | |
| *On what container would you apply controls?* | | | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | | | | | | | | |
| Administrative Controls | | | Implement a security awareness program to educate employees about tailgating risks and proper access procedures.  Consider issuing temporary badges to visitors to distinguish them from authorized personnel. | | | | | | | | | | |
| Physical Controls | | | Install a physical barrier system (e.g., mantrap) at the main entrance to prevent unauthorized access after someone enters.  Increase security personnel presence at entry points, especially during high-traffic times.  Utilize security cameras to monitor entry points and deter suspicious activity. | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |
|  | | |  | | | | | | | | | | |

### 5.4.2. Justifications,

Justifications for the above probability and impact levels lie below,

#### 5.4.1.1. Probability levels

Reputation & Customer Confidence (Value: 5, Score: 2.25), A security breach due to tailgating can damage the organization's reputation for physical security. This can erode trust from customers, partners, and employees about data and equipment safety.

Financial (Value: 6, Score: 2.7), Financial impacts associated with tailgating can include, Replacing stolen hardware like laptops or servers, Repairing damaged equipment, and Recovering data if lost due to stolen devices.

Safety & Health (Value: 5, Score: 2.25), In extreme cases, unauthorized individuals gaining access through tailgating could pose a physical threat to employees or cause safety hazards.

ines & Legal Penalties (Value: 7, Score: 3.15), Data breaches or security incidents resulting from tailgating can lead to fines or legal penalties depending on the regulations (e.g., HIPAA, GDPR) and the type of data exposed.

[5]

# Conclusion,

BCAS Campus, a leading educational institution, has identified critical security risks through the OCTAVE framework analysis. These risks threaten valuable information assets like student data, course materials, and employee credentials. The identified risks include Network Attacks, Social Engineering, Ransomware, Virus Attacks, and Tailgating.

These risks can have severe consequences for BCAS, including Data Breaches, Disruptions, Reputational Damage, and Financial Loss. BCAS must prioritize risk mitigation strategies including Implementing strong network security measures like hidden SSIDs and robust password policies, Conducting security awareness training to educate staff about social engineering tactics, Patching outdated software and implementing application whitelisting to restrict unauthorized software installation, Strengthening physical access control through measures like security cameras and mantrap systems at building entrances.

By proactively managing these risks, BCAS can safeguard its information assets, ensure business continuity, and maintain its reputation as a trusted educational institution.

# References

|  |  |
| --- | --- |
| [1] | Nile , "Man-In-The-Middle (MitM) Attack: Definition & Defenses," Nile , 01 04 2024. [Online]. Available: https://nilesecure.com/network-security/man-in-the-middle-mitm-attack-definition-defenses/. [Accessed 18 04 2024]. |
| [2] | IBM, "Forbs Insight," Forbs, 2014. |
| [3] | EUR-lex, "GDPR Documentation," EUR-lex, 01 01 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed 18 04 2024]. |
| [4] | J. Rushton, "Techopedia," 50+ Phishing Statistics You Need to Know – Where, Who & What is Targeted, 01 03 2024. [Online]. Available: https://www.techopedia.com/phishing-statistics. [Accessed 21 24 2024]. |
| [5] | VErizon , "VErizon," VErizon , 1 3 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/. [Accessed 23 04 2024]. |
| [6] | Ponemon Institute's, "Cost of a Data Breach Report 2023," *Cost of a Data Breach Report 2023,* p. 13, 01 01 2023. |
| [7] | IBM, "IBM X-Force Threat Intelligence Index 2024," *IBM,* p. 65, 01 01 2024. |