Triad Security

Triad has a dedicated network system used to access internet services. All staff have been given access to training for using internet services though the Triad dedicated network.

Triad has around 40 staff members who use the network regularly.

Hackers have attacked Triad’s network servers and personal and business data was affected. Triad was able to recover the data and business activities have been restored to normal.

Before the attack some cybersecurity policies existed at Triad:

* Always connect using secure Wi-Fi
* Protect sensitive data
* Talk to the IT department if you notice anything unusual
* Avoid opening emails from an unauthorised address

Triad is now aware that a cyber attack can happen in multiple ways. The most commonly faced cybersecurity risks at Triad are:

* Phishing attacks
* Hacking
* Ransomware

Triad is wanting to implement cybersecurity measures to prevent future attacks by:

Training staff to avoid unsolicited emails that request a response

Installing a comprehensive anti-virus system

Installing spam filters for all messages and emails

Installing a network firewall

Implementing policies to ensure that data is accessed securely.

Triad needs to develop cybersecurity policies and procedures to address the threat of the most commonly faced cybersecurity risks.

You have joined the staff as an IT expert and policy developer. You need to review the existing Triad cybersecurity policies and complete the activities below.

**Activity 1. Report on organisation threats and trends associated with cyber security.**

Your report needs to include:

* Introduction
* Current cybersecurity threats
* Ways to deal with phishing attacks, ransomware, and hacking
* Cybersecurity trends
* Existing cybersecurity practices at Triad
* Recommendations for Triad.

Your report should be between 200-500 words

|  |  |
| --- | --- |
| Cybersecurity threats and trends | |
| **Introduction:**  Cybersecurity has become a critical concern for organizations across all sectors as the digital landscape continues to evolve. With the increasing sophistication of cyber threats, and the increase of employees working from home, there has been an increase of challenges for organisations to protect their assets, data, and systems from malicious actors.   This report aims to provide a clear indication of cyber security trends, review and assess the current security measures here at Triad Security, and propose strategic recommendations to update our policies to reflect the emerging challenges faced in modern cyber security. | |
| **Current cybersecurity threats:**  The most common cyber security threats identified previously at Triad Security are:   * Phishing * Ransomware * Hacking | |
| **Techniques to resolve phishing attacks** | * Training staff to avoid unsolicited emails that request a response. * Installing spam filters for all messages and emails |
| **Techniques to resolve hacking** | * Installing a network firewall * Implementing policies to ensure that data is accessed securely. |
| **Techniques to resolve ransomware** | * Installing a comprehensive anti-virus system * Implementing policies to ensure that data is accessed securely. |
| **Current trends in cyber security:**   1. **Remote working cyber security risks. *–*** *Working remotely from home has become more common post Covid-19. As a result, employees are more at risk. Home offices tend to have less secure firewalls as well as employees using personal devices whilst at home, which has not been set up to organisational policy. Malicious attackers are adapting their techniques to take advantage of this.* 2. **The evolving trend of IoT devices. *–*** *As the world increases its reliance on digital technologies, the amount of IoT devices per organisation increases, too. As IoT devices are usually contained in a system of devices that connect via the Internet, it creates a larger number of attack surfaces. This increases the risk of being attacked by hybrid ransomware attacks, where a hacker gains remote access to one or more devices in an IoT network whilst demanding a ransom.* 3. **Cloud services & cloud security threats. *–*** *Cloud vulnerability continues to be a serious threat in organisations. Cloud services has developed into a more common practice for organisations, as people work from home post Covid-19. Whilst cloud services offer a range of benefits, they pose a real risk in the case of:*  * ***Misconfigured cloud settings –*** *This is a significant cause of data breaches & unauthorised access, insecure interfaces and account hijacking. According to a report by IBM, the* [*global average cost of a data breach*](https://www.ibm.com/reports/data-breach) *is at $4.88 Million USD in 2024.* * ***Cloud migration –*** *Cloud migration is the process of moving data, applications and other business elements across a cloud service. During cloud migration sensitive data may be exposed if not handled correctly and securely, which can lead to data breaches.* * ***Increase in entry points –*** *With developing and expanding cloud services, there will be an increase in entry points. Each entry point represents a potential attack vector; therefore, the increase of entry points will overall create vulnerabilities & weaknesses making it easier for attackers to gain access.* | |
| **Existing cyber security practices at Triad Security:**  Policies indicating that employees:   * Always connect using secure Wi-Fi * Protect sensitive data * Talk to the IT department if they notice anything unusual * Avoid opening emails from unauthorised addresses | |
| **Conclusion:**  In this report, we identified several vulnerabilities, threats and trends that are increasingly challenging for organisations like Triad Security. The shift towards remote working, the growing reliance on IoT devices, and the widespread adoption of cloud services have expanded the attack surface, making it more difficult to protect critical assets, data, and systems from malicious actors. These trends highlight the need to develop robust cybersecurity measures tailored to the evolving threat landscape.  Phishing, ransomware, and hacking continue to be the most common threats faced by Triad Security. While our current security practices provide a solid foundation, they must be updated to address emerging risks more effectively. Implementing comprehensive training for staff, enhancing network security through firewalls as well as developing a BYOD Policy along with ensuring that people working from home have access to company devices, and adopting advanced antivirus solutions are critical steps in mitigating these threats. Additionally, the growing use of IoT devices and cloud services requires updating our security policies, particularly in ensuring secure configurations and managing the increase in entry points that could be exploited by attackers.  Given the findings of this report, Triad Security must continue to evolve its cybersecurity strategies. By adopting the recommended measures, such as refining our remote working policies, securing IoT devices, and managing cloud configurations, we can significantly reduce our risk exposure. It is crucial that we implement ongoing staff training and regular security audits as this is essential in maintaining a strong security stance in an effective security environment. | |

**Activity 2. Develop cybersecurity policies and procedures for Triad cybersecurity**.

Based on the information you have compiled in your report, develop a password protection policy and a data protection policy using the following templates:

|  |  |
| --- | --- |
| Password Protection Policy | |
| **Purpose** | The purpose of this policy is to strengthen the protection of systems at Triad Cybersecurity by establishing a policy that governs how employees create, store and sign into company computer systems. |
| **Resources** | Multi-factor authentication, training <https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2> Passkey (FIDO2),  Password Managers |
| **Relevant personnel** | All Triad Security Employees |
| **Relevant legislation** |  |
| **Password Protection Policy (50-100 words)**  **(standaardise the company wide process for updating passwords at a periodic cycle.) (require specific complexity & uniqueness)** | |

|  |  |
| --- | --- |
| Data Protection Policy | |
| Purpose |  |
| Resources |  |
| Relevant personnel |  |
| Relevant legislation |  |
| Password Protection Policy (50-100 words) | |

**Activity 3. Conduct a meeting with your manager to discuss your report (Activity1) and the new policies you have developed (Activity2).**

You will need to highlight any legislation that applies to each policy and how the policy meets the organisational requirements. You also need to highlight cyber security threats which may impact organisational operations and provide solutions to resolve those threats.

In the meeting you need to discuss the following points:

Discuss policies and procedures developed in Question 2

Discuss the report prepared in Question 1

Review current cybersecurity threats facing Triad

Discuss improvements needed in policies and procedures

You will conduct the meeting with a classmate, who will play the role of your manager. Meeting time approx. 7-10 minutes.

Complete the following meeting template and write the information related to the meeting discussion

|  |  |  |  |
| --- | --- | --- | --- |
| Meeting of Triad and Policy Developer | | | |
| Meeting Objective: | | | |
| Attendees: | | | |
| Venue: | | | |
| Date: | | | |
| Minutes of Meeting: | | | |
|  | Matters Discussed | Actions Suggested | Target data and personnel involved |
| Discuss policies and procedures |  |  |  |
| Discuss report |  |  |  |
| Review current cybersecurity threats |  |  |  |
| Discuss improvements needed in policies and procedures |  |  |  |

Your lecturer/assessor will observe your performance and complete the following performance checklist.

**Performance criteria checklist for Meeting:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lecturer/ Assessor to complete** | | | |
| **Does the candidate meet the following criteria** | **YES** | **NO** | **Lecturer/Assessor comments** |
| Discussed policies and procedures developed in activity 2 (eg purpose, scope and relevant legislation of policies) |  |  |  |
| Discussed the report prepared in activity 1 (eg highlighted policies which help in improving cyber security) |  |  |  |
| Reviewed the cybersecurity threats |  |  |  |
| Discussed ways to resolve cybersecurity threats |  |  |  |
| Discussed improvements needed in policies and procedures |  |  |  |
| Completed the meeting minutes using template |  |  |  |
| Completed the meeting in the given timeframe |  |  |  |
| Used active listening to understand the manager’s point of view |  |  |  |
| Allowed other people to discuss the issues |  |  |  |

**Activity 4. Prepare and deliver a PowerPoint presentation to create awareness about cybersecurity**.

Based on your report, policies, and meetings with your Triad manager, prepare and deliver a PowerPoint presentation (approx. 10 minutes). Present your powerpoint to a classmate who will play the role of manager/colleague.

Your PowerPoint is to be designed for the staff at Triad Security. You must include the following in your presentation:

Prepare at least 10 slides

* Introduction
* Deliver cybersecurity policies and procedures
* Importance of cybersecurity
* Ways to improve cybersecurity at Triad
* How to avoid common cybersecurity risks
* Conclusion
* Allow others (lecturer or fellow students) to question and answer the questions.

Your PowerPoint MUST provide training for at least 2 cybersecurity threats, and MUST define steps to protect the information system at Triad Security.

Your lecturer/assessor will observe your performance and complete the following performance checklist.

**Performance criteria checklist for Presentation:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lecturer/ Assessor to complete** | | | |
| **Does the candidate meet the following criteria** | **YES** | **NO** | **Lecturer/Assessor comments** |
| Communicated purpose clearly |  |  |  |
| Organised and easy to follow |  |  |  |
| Presenter exhibited a good understanding of the topic |  |  |  |
| Presenter spoke clearly |  |  |  |
| Time for presentation was used effectively |  |  |  |
| Slides enhanced presentation |  |  |  |
| The presenter responded effectively to audience questions and comments |  |  |  |