ANTHONY BABAJIDE BALOGUN
ID No: UB73361SIN82521

COURSE TOPIC:

CYBER SECURITY AND RISK MANAGEMENT

ATLANTIC INTERNATIONAL UNIVERSITY

MARCH 2022

TABLE OF CONTENT

1.0 INTRODUCTION

The process of protecting any internet based connected systems such as hardware, software and data from cyber threats and attacks is known as Cybersecurity. A good and well-planned cybersecurity strategy should provide a strong security posture against malicious attacks designed to access, alter, delete, destroy an organization's or user's sensitive data or information. It is also an effective way in preventing or mitigating attacks that is aimed to destroy system's or device's operations.

A good and strong cybersecurity strategy provides layers of protection to protect against cyber threat and crime such as gaining access to sensitive information with the aim of altering or destroying data, extorting money from users or organizations and an attempt to disrupt business operations.

Despite all the efforts of cybersecurity professionals to close security gaps, attackers are always looking for new ways to exploit emerging vulnerabilities and weaknesses. Cybersecurity best practices and technologies can assist an organization to implement strong cyber security measures that will reduces weaknesses and vulnerabilities to cyber-attacks in order to protect critical and sensitive information systems without affecting the users and customers

2.0 CYBER SECURITY AND RISK MANAGEMENT

2.1 Definitions

(i) Cybersecurity

According to IBM, “Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.” (IBM, n.d.)

The process of protecting any internet based connected systems such as hardware, software and data from cyber threats and attacks is known as Cybersecurity. A good and well-planned cybersecurity strategy should provide a strong security posture against malicious attacks designed to access, alter, delete, destroy an organization's or user's sensitive data or information. It is also an effective way in preventing or mitigating attacks that is aimed to destroy system's or device's operations.

(ii) Risk Management

According to Association for Project Management (APM), “Risk analysis and risk management is a process that allows individual risk events and overall risk to be understood and managed proactively, optimising success by minimising threats and maximising opportunities and outcomes.” (APM, n.d.)

3.0 CYBER SECURITY DOMAINS

A good and strong cybersecurity strategy provides layers of protection to protect against cyber threat and crime such as gaining access to sensitive information with the aim of altering or destroying data, extorting money from users or organizations and an attempt to disrupt business operations.

3.1 Layers of protections

3.1.1 Critical infrastructure security

This countermeasure is aimed at protecting the computer systems, networks, and other assets that people and society depends upon for national security, economic health and public safety.

3.1.2 Network security

Network security is a measure put in place or protecting a computer network from attackers or hackers, such include wired and wireless (Wi-Fi) connections.

3.1.3 Application security

This countermeasure assists in helping to protect applications running on-premises and also in the cloud. Security should be enforced into applications at the initial stage otherwise known as the design stage with considerations for how data is handled and even the user's authentication into accessing resources on the network

3.1.4 Cloud security

This enables the encryption of both data at rest (in storage) as well as data in motion (as it moves from the on-premise to the cloud). Cloud security also encrypt data in use (during processing) to support customer privacy, business requirements and regulatory compliance.

3.1.5 Information security

Information security is a countermeasure for data protection in other to secure sensitive data from unauthorized access, exposure and theft.

3.1.6 End-user education

This security domain help to create security awareness across the organization and to strengthen endpoint security. A good example will be a security training organized for users on how to delete suspicious and malicious email attachments and to avoid using or plugging in an unknown USB device found somewhere into a system.

3.1.7 Disaster recovery / business continuity planning

This is a countermeasure put in place to respond to an unplanned or unexpected event such as natural disasters, power outages and cybersecurity incidents with the aim to minimize a disruption to key operations.

4.0 COMMON CYBER THREATS

Despite all the efforts of cybersecurity professionals to close security gaps, attackers are always looking for new ways to exploit emerging vulnerabilities and weaknesses. Those emerging and evolving threats include:

4.1 Malware

Malware refers to malicious software such as worms, viruses, Trojans and spyware which allows unauthorized access with the aim of causing damages to a computer. They are designed by attackers to avoid familiar detection methods such as antivirus tools which can scan malicious file attachments.

4.2 Ransomware

This type of malware is designed by attackers to lock down files, data or systems in order to threatens the owner or an organization of deleting their sensitive data if certain conditions are not met. Mostly, attackers use ransomware to demand money from their victims.

4.3 Phishing

Phishing is an attack in the form of a social engineering which tricks users into making available their sensitive information. In this type of attack or scam, emails or text messages which appears to originate from a genuine company asking for sensitive information such as credit card details or login information.

4.4 Insider threats

Either current or old employees, business partners, contractors or anyone who has at one time or another had an access to a system or networks in the past can be considered as an insider threat if they abuse their access rights or permissions.

4.5 Distributed denial-of-service (DDoS) attacks

The main aim of a Distributed denial-of-service (DDoS) attack is to make an attempt to crash a server, website or network by flooding it with traffic which usually comes from multiple and coordinated systems. DDoS attacks floods enterprise networks through a protocol known as the simple network management protocol (SNMP) which is used for such devices like modems, printers, switches, routers and servers.

4.6 Advanced persistent threats (APTs)

In an Advanced persistent threat, an intruder or group of attackers penetrate a system and remain undetected for a long period of time. The primary aim is to spy on business activities and to steal sensitive data while avoiding a pre-defined defensive countermeasure.

4.7 Man-in-the-middle attacks

This is an eavesdropping attack whereby a cyber-criminal highjack messages between two parties in order to steal data. For example, an attacker can intercept unencrypted data on an unsecure Wi-Fi network which is being transmitted between guest's device and the network.

5.0 CYBER SECURITY TECHNOLOGIES AND BEST PRACTICES

Cybersecurity best practices and technologies can assist an organization to implement strong cyber security measures that will reduces weaknesses and vulnerabilities to cyber-attacks in order to protect critical and sensitive information systems without affecting the users and customers. The following are the notable and recommended best practices:

5.1 Identity and access management (IAM)

Popularly known by its acronym **IAM**, it defines the roles and access permissions and privileges for each user as well as the conditions under which they are granted access or denied their privileges. Its methodologies include single sign-on which allows a user to log in to a network once without submitting their credentials during the same session.

It also enables multifactor authentication thereby requiring two or more access credentials from a use before an access is being given. IAM tools also have the ability to give cybersecurity professionals deeper visibility into suspicious activities on end-user devices which helps to speed up an investigation and response times to identify and contain the damage of a breach or attack.

5.2 A comprehensive data security platform

This protects sensitive information within various environments which include the hybrid multi-cloud environments. An efficient data security platform provides automated and real-time visibility into data weaknesses as well as monitoring the alerts to data vulnerabilities and risks involved before they actually become a data breach.

5.3 Security information and event management (SIEM)

This practice analyze data from security events to automatically detect suspicious user activities and provides an immediate preventative or remedial response. The solutions include advanced detection methods such as user behavior 'analytics' and 'artificial intelligence (AI)'. Security information and event management (SIEM)can automatically respond to cyber threat in line with the organization's risk management plans and objectives.

6.0 BENEFITS OF CYBER SECURITY

- Business protection against cyberattacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.

- Regulatory compliance.
- Business continuity.
- Improved confidence in the company's reputation and trust for developers, partners, customers, stakeholders and employees.

7.0 CYBER SECURITY VENDORS AND TOOLS

Well notable known security tools and systems are listed below:

- Identity and access management (IAM)
- Firewalls
- Endpoint protection
- Antimalware
- Intrusion prevention/detection systems (IPS/IDS)
- Data loss prevention (DLP)
- Endpoint detection and response
- Security information and event management (SIEM)
- Encryption tools
- Vulnerability scanners
- Virtual private networks (VPNs)
- Cloud workload protection platform (CWPP)
- Cloud access security broker (CASB)

8.0 CYBER SECURITY AND CLOUD-BASED NETWORKING

8.1 Definition

Cloud Computing

According to Microsoft, “Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale.” (Microsoft, n.d.)

8.2 Types of cloud computing

There are three main types of cloud computing, namely;

(i) Public clouds

This is the type of cloud computing systems owned and operated by a third-party service provider(s).

(ii) Private cloud

This another type of cloud computing where IT infrastructure resources are used and shared by a business or organization.

(iii) Hybrid cloud

This is a type of cloud computing that combines the functions of both public and private clouds.

8.3 Types of cloud services

The followings are the known services that cloud has to offer its subscribers:

(i) Infrastructure as a service (IaaS)

(ii) Serverless computing

(iii) Platform as a service (PaaS)

(iv) Software as a service (SaaS)

(v) NaaS Network as a service Network

(vi) STaaS Storage as a service Storage

(vii) DaaS Data as a service Data

(viii) DBaaS Database as a service

(ix) IPaaS – Integration platform as a service

8.4 Mobile Cloud Computing

According to IBM, “Mobile cloud computing uses cloud computing to deliver applications to mobile devices. These mobile apps can be deployed remotely using speed and flexibility and development tools. Mobile cloud applications can be built or revised quickly using cloud services. They can be delivered to many different devices with different operating systems, computing tasks, and data storage. Thus, users can access applications that could not otherwise be supported.” (IBM, What is mobile cloud computing?, n.d.)

9.0 CLOUD COMPUTING OVERVIEW

The possibility and probability of any internet user(s) right now using cloud computing is obvious even if the person did not realize it. Cloud computing may actually be behind the use of an online service to send email, edit documents, watch movies or TV, listen to music, play games or even store pictures and so many more.

9.1 Benefits of cloud services

(i) Create cloud-native applications

It allows to quickly build and deploy scale web applications, mobile and API. It also takes advantage of cloud-native technologies and approaches such as 'containers', 'Kubernetes', 'API-driven communication and DevOps'.

(ii) Test and build applications

Cloud services decreases application development cost and time by using the readily available cloud infrastructures that can conveniently be scaled up or down.

(iii) Store, back up and recover data

Cloud services safe guard your data more efficiently whilst transferring your data over the Internet to an offsite cloud storage system that is accessible from anywhere and on any device.

(iv) Analyze data

Cloud services unifies data across teams, divisions and locations in the cloud. The availability of machine learning and artificial intelligence makes it easy to uncover insights for more informed decisions.

(v) Stream audio and video

You can use cloud services to get connected with your audience anywhere and at any time on any device with the facility of high-definition video and audio with global distribution.

(vi) Embed intelligence

Cloud services can use intelligent models to assist customers to provide valuable insights from the data captured.

(vii) Deliver software on demand

This service is also known as software as a service (SaaS) which is an on-demand software that lets you offer the latest software versions and updates available to customers at any time it is needed and wherever they are located.

10.0 CYBER SECURITY RISK MANAGEMENT

10.1 Definition

According to itgovernance.co.uk, “Cyber risk management is the process of identifying, analysing, evaluating and addressing your organisation’s cyber security threats.” (itgovernance.co.uk, n.d.)

No matter what the cyber criminal’s plan is, your business will at one point face some type of financial problems as a result of any successful cyber-attack. That is the main reason why having a plan on how your company prevents and reacts to cyber-crime is absolutely necessary.

Adequate cybersecurity risk management begins at the top of an organization. Business leaders must work towards establishing a culture of cybersecurity awareness in order to have a successful risk management plan.

Without human resources participation in the process and without the whole organization buying into the goal and objectives of keeping a business safe from cyber-attack, there is no way to develop a risk management strategy that would work. That is why businesses must start creating and imbibing a culture in which employee accountability and involvement is encouraged.

By arranging together an effective cybersecurity risk management plan for your business, you are helping to put your company in an advantageous position to do the following:

- Properly identify cybersecurity risks
- Understand where your company is most vulnerable
- Understand the potential damage of these risks
- Define a strategy for protecting your company
- Understand how to minimize the impact of cyberattacks
- Mitigate some of the risks via risk transfer

10.2 Cyber Risk Management Process

A risk management plans and strategy usually follow these steps:

- Identify the risks that might compromise your cyber security.
- Analyze the gravity of each risk by assessing its likelihood of occurring
- Evaluate how each risk fits within your risk level acceptability
- Prioritize the risks
- Determined how to respond to each risk.

  Four options are available to choose from under this strategy:

  Treat: Updating the impact of the risk by implementing security controls

Tolerate: Decide on whether to retain the risk or not

Terminate: Avoiding the entire risk by ending or changing the process or activity causing the risk

Transfer: You can decide to share the risk with another party by taking out insurance

- Reviewing of controls to make sure they are still fit for the purpose designed it for.

11.0 CYBER SECURITY RISK MANAGEMENT AWARENESS

11.1 Awareness Training

'Hackers' perpetrate their cyber-attack by first by tricking 'less-knowledgeable' members of an organization into providing or revealing some sensitive information such as a 'login name' and 'password' or some form of access control combination 'coordinates' to them in order to have an access to the organization’s systems and networks. This type of cyberattack is known as "phishing” or “social engineering.”

A typical social engineering trick will probably send an email to employees that is made to look as if the CEO or any other line manager boss sent it by asking them to click on a link or install something on their computer.

The best way to avoid these types of attacks is by educating employees about cybersecurity and create an awareness so that when they see these types of emails, they are able to recognize them as potential security threats.

Putting together an effective cybersecurity awareness and training will make sure that all employees get training related to cyber threats, this process should be the basis of every organization’s cybersecurity risk management plan.

Employees should not only be educated on what to look for but also be equipped with the knowledge of what to do and who they should contact if they see something suspicious.

12.0 ASSESSING CYBER SECURITY RISKS

The procedure of assessing an organization's cybersecurity risks is similar to the process of assessing any other business risks it may face. The two main factors to be considered when it comes to assessing risks are; determining the probability of the risk and the impact of the event should it occur.

Once these factors have been considered then you will be able to focus the necessary things to be done to reduce the probability or gravity of each potential risk. This process should serve to give a better understanding of the potential risks in order to take the proper steps towards controlling, avoiding and mitigating them. A cybersecurity risk assessment is all about understanding and mitigating cyber risk within the entire organization.

12.1 Performing a Data Audit

An organization's business’s data is obviously one of its most valuable assets and Data breaches are the costliest types of cyberattacks. That is the main reason why performing a data audit is the most important step in assessing cybersecurity risks.

Below are a few questions to be asked and answered in the process of performing a data audit:

- What type of data do you collect?
- Where and how do you store it?
- How well is it protected?
- Who has access to this data?
- What are the potential consequences of this 'data' being compromised?

However, third-party vendors and other partners also have access to your data, make sure that you are aware of their risk management procedures they are taking in order to reduce cyber-attacks that could affect your organization.

13.0 THE RESPONSE PLAN

Irrespective of how good a cybersecurity risk management plan may be, attacks are bound to happen. That is the main reason why having a response plan is as important as having a security plan itself. A response plan is a set of instructions and procedures an organization has put in place should a cyberattack occur.

An effective and well-planned response plan allows you to act quickly and reduce the time and potential impact of any attack.

These are the common response plan for a cyber-attack:

- **Containment:**

Take possession of the systems and networks that was attacked in order to identify the attack and prevent the threat from escalating.

- **Data Audit:**

Data audit is needed to be performed on sensitive data in order verify if any of the data has been breached, corrupted or stolen to better understand the potential risks.

- **Eradication:**

Delete or discard every file that have been infected and replace damaged or non-functional hardware or software if need be.

- **Log Events in Detail:**

Event logs are very important, a log of the incident and response must be documented accordingly. Important information such as the exact time and location of the attack, the person who discovered it, how it was reported, the specific data that was compromised, the extent of the damage and the response to the breach must be logged as soon as possible.

- **Public Acknowledgement:**

When a cyber-attack occurred and has affected customer's data, a public statement must be made as soon as possible.

- **Consult Legal Team:**

A legal team must be briefed as soon as possible in order to determine whether compliance risks are available and if the cyber-attack has had an impact on any regulations.

- **Contact Police:**

The law enforcement agents must be notified of the attack in the possible event that your business was not the only business targeted in the attack.

- **Recovery:**

The systems administrator for the organization must restore the system and network to its working state bearing in mind the system’s integrity, security and level of data loss.

- **Follow-up:**

Continuous gathering of logs, performing audits and testing of the system even after the cyber-attack must be carried out. Discuss the attack with the organization's team in order to understand what could have been better done, what errors were made and what could be done to avoid similar attacks should it occur again.

- **Other response plans:**
    - Continue to 'monitor' the results of your response plan.
    - Be sure to review and test the incident response plan and update it when appropriately.
    - Remember to keep all stakeholders informed regarding the state of the cybersecurity
    - risk management plan.

14.0 CONCLUSION

Putting in place and establishing an efficient and proper cybersecurity risk management plan for your business is arguably very important in order to properly identify risks and responding to them as quickly and efficiently as possible when they occur.

Irrespective of how good a cybersecurity risk management plan may be, attacks are bound to happen. That is the main reason why having a response plan is as important as having a security plan itself. A response plan is a set of instructions and procedures an organization has put in place should a cyberattack occur.

An effective and well-planned response plan allows you to act quickly and reduce the time and potential impact of any attack.

It also gives you the opportunity to reduce the negative effect and impact which a cyberattack can have on your customer's and general public reputation. However, not all risks especially in the world of cybersecurity can be avoided or reduced. That is why it is always a good idea to transfer as much of the risk as possible to a third party by taking out or purchasing business insurance.

15.0 BIBLIOGRAPHY

APM. (n.d.). *What is risk management?* Retrieved from Definition: https://www.apm.org.uk/resources/what-is-project-management/what-is-risk-management/

IBM. (n.d.). *What is cybersecurity?* Retrieved from What is cybersecurity?: https://www.ibm.com/topics/cybersecurity

IBM. (n.d.). *What is mobile cloud computing?* Retrieved from What is mobile cloud computing?: https://www.ibm.com/cloud/learn/what-is-mobile-cloud-computing

iosafe. (n.d.). What is a NAS device and how does it work? Retrieved from What is a NAS device and how does it work?: https://iosafe.com/data-protection-topics/what-is-a-nas-device/

itgovernance.co.uk. (n.d.). *Cyber Risk Management Service*. Retrieved from What is cyber risk management?: https://www.itgovernance.co.uk/cyber-security-risk-management

Microsoft. (n.d.). *What is cloud computing?* Retrieved from What is cloud computing?: https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/