

Cybersecurity program

An introduction



March 22, 2023

Name: Gihan shamike liyanage

INFO 6027 W2023 Assignment 3

Cybersecurity Program Development for Business

Creating a cybersecurity program for a business is critical to protecting the organization's sensitive information and assets from potential cyber threats.

Understanding Risk

Risk is the possibility of harm or loss as a result of unforeseeable events or circumstances. Risk can refer to a variety of risks in business, including financial risk, operational risk, reputational risk, regulatory risk, and cybersecurity risk.

Understanding risk entails determining the likelihood of an event occurring as well as the potential consequences of that event. A risk assessment entails identifying the risks that a company faces, analyzing the likelihood and potential impact of each risk, and then ranking them in order of likelihood and severity.

[What is it worth to the business?](#_Toc99708071)

Understanding and managing risk is critical for any business's success because it can help protect against financial losses, reputational damage, and other negative consequences. While the cost of implementing effective risk management strategies may appear to be prohibitively expensive, the potential benefits to the business can far outweigh the costs. Effective risk management can assist in ensuring business continuity by reducing the impact of unexpected events and ensuring that the business can continue to operate in the face of disruption.

What is a Digital Ecosystem?

A digital ecosystem is a network of digital devices, services, and platforms that collaborate to create value for businesses and users. It consists of numerous components such as hardware, software, data, people, and processes.

Open and interconnected architectures of digital ecosystems, allowing different components to work together seamlessly. They frequently involve a number of partners, including software vendors, hardware manufacturers, service providers, and content creators, who work together to create a cohesive and integrated ecosystem.

Mobile app ecosystems, social media platforms, cloud computing platforms, and the Internet of Things (IoT) are all examples of digital ecosystems. These ecosystems typically offer a variety of benefits to businesses and users, including increased efficiency, increased productivity, improved connectivity, and access to a broader range of services and products.

Effective digital ecosystem management entails creating an environment that encourages collaboration and innovation, as well as implementing appropriate security and privacy safeguards to protect against cyber threats. It is also necessary to monitor and evaluate the ecosystem on an ongoing basis to ensure that it remains relevant and effective in meeting the needs of businesses and users.

[Cybersecurity can be defined as…](#_Toc99708073)

Cybersecurity is the set of practises, technologies, and policies that are designed to protect computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It entails safeguarding digital data and assets against a wide range of cyber threats, such as malware, ransomware, phishing attacks, social engineering, and other types of cyber attacks. To minimize the impact of cyber attacks, effective cybersecurity necessitates a comprehensive approach that includes ongoing risk assessments, employee training and awareness programes, secure network architecture and design, regular software updates and patching, and incident response plans.

Cybersecurity is a constantly changing field, with new technologies and threat vectors appearing on a regular basis. To effectively protect against cyber threats and safeguard sensitive data and assets, organizations and individuals must stay current on the latest cybersecurity trends and best practices.

[How to measure Cybersecurity success?](#_Toc99708074)

The reduction of risk to the organization is one of the most important indicators of cybersecurity success. Regular risk assessments, vulnerability scans, and penetration testing can be used to identify potential weaknesses and evaluate the effectiveness of security controls. Another measure of cybersecurity success is the effectiveness of incident response efforts. Other than that the effectiveness of employee training and awareness programs is another important measure of cybersecurity success. The final outcome of the cybersecurity should be business contiuety and it can be measured by the organization's ability to maintain business continuity in the face of a cyber attack. This includes assessing the effectiveness of disaster recovery plans as well as the organization's ability to recover from an attack.

[Why should we consider a framework?](#_Toc99708075)

A cybersecurity framework should be considered by organisations because it provides a more structured and comprehensive approach to managing cybersecurity risks. A framework is a set of guidelines, best practices, and industrial standards established by cybersecurity experts. A framework can ensure that all aspects of cybersecurity are covered, from identifying risks to implementing security controls and monitoring for threats and provides a structured process for assessing cybersecurity risks, implementing controls, and monitoring for threats to aid in continuous improvement.

[Defense in Depth.](#_Toc99708076)

Defense in depth is a cybersecurity strategy that entails implementing multiple layers of security controls to safeguard the assets of a company and place redundant security controls to ensure that if one fails, there are others in place to protect. Defense in depth engages implementing security controls at multiple levels, such as the network, application, and user levels, to provide comprehensive protection.

[What are controls and why we need them as part of a cybersecurity strategy?](#_Toc99708077)

In cybersecurity, controls refer to security counter measures that are implemented to reduce or mitigate risks to information systems and data. There are three major controls in cybersecurity and those are

* Management controls.
* Operational controls.
* Technical controls.

Management controls refer to issues that management needs to be addressed and operational controls address correct implementation and use of security policies. Controls can help to protect against insider and outsider threats and finally technical controls Involve the correct use of hardware and software security capabilities in systems.

[Threat Agents](#_Toc99708078)

Individuals, groups, or organizations that have the capability and intent to exploit vulnerabilities and cause harm to a system or organization are referred to as threat agents. They are classified into various categories based on their motivation, expertise, and goals. Cybercriminals, Insiders, Compititors and Terrorists are some of the examples for treat agents.

[Current trends influencing Threat Agents](#_Toc99708079)

Because of the COVID-19 pandemic, most of the organizations have implemented remote work policies, which has increased the use of cloud-based tools and services. This has also broadened the attack surface for threat agents, who can now target employees working from home or exploit vulnerabilities in remote access tools. IOTs are another trend in today’s world that causes influencing treat agents. The spread of IoT devices has created new opportunities for threat agents to exploit vulnerabilities in connected devices and gain access to sensitive data or control systems. Other than that threat agents are using AI and machine learning algorithms to develop more sophisticated attacks that can evade traditional security measures as AI becomes more prevalent in cybersecurity.

[The nature of present-day hackers?](#_Toc99708080)

Today’s world hackers are highly skilled, persistent, and frequently work with other hackers to gain access to sensitive data. They are motivated by monetary gain or political objectives, and they use more sophisticated techniques to carry out their attacks.

[Attack examples](#_Toc99708081)

There are many different types of cyber attacks that can be carried out against organizations and individuals. Phishing attacks, Ransomware, Distributed Denial of Service (DDoS), Man-in-the-middle, Insider threats and Zero-day attacks are some examples for different types of cyber attacks.

[Governance, and why it matters in a cybersecurity program](#_Toc99708082)

Governance refers to the process of establishing policies, procedures, and controls to guide decision-making and ensure accountability within an organization. Governance ensures that the cybersecurity program of the organization is in line with the overall business objectives and strategies. This contributes to ensuring that cybersecurity risks are managed in a way that promotes the achievement of the organization's objectives. Other than that governance ensures that the cybersecurity program complies with all relevant regulations and standards, such as GDPR, HIPAA, and ISO 27001 and defines clear roles and responsibilities for cybersecurity management, ensuring that everyone understands what is expected of them and who is responsible for various aspects of the cybersecurity program.

[Overview of a basic Cybersecurity Program:](#_Toc99708083)

* Vision and Mission Statement - The vision statement expresses succinctly what the organisation wishes to become. Vision statements should be ambitious.
* [What is at Risk? -](#_Toc99708085) There are various assets that are at risk of being compromised or lost due to a cyber attack such as confidential data, Operational systems, Reputation, Business continuity and Availability of services.
* [Asset Valuations](#_Toc99708086) - Asset valuation is the process of determining the monetary value of an organization's assets, which can include physical assets and intangible assets.
* [Business Impact Analysis](#_Toc99708087) - Process that helps organizations identify and prioritize critical business functions and processes, and assess the potential impact of disruptions to these functions and processes.
* [Mitigating Risk](#_Toc99708088) - Taking actions to reduce the impact of potential risks.
* Incident‐Response Planning - The process of creating a set of procedures to follow in the event of a security breach. The goal of incident response planning is to reduce the impact of a security incident by detecting it as soon as possible, containing it to prevent further damage, and restoring normal operations as soon as possible.

[People are the most effective controls in cybersecurity](#_Toc99708090)

This is due to the fact that people can make mistakes, be manipulated or deceived, or have limited knowledge and expertise in specific areas of cybersecurity. Employee education and training can help them understand the risks associated with cybersecurity as well as how to identify and respond to potential threats. Creating clear policies and procedures for handling sensitive information and responding to security incidents can help employees understand their roles and reduce the likelihood of human error.

[Senior management approval for the cybersecurity program is paramount](#_Toc99708091)

Senior management approval is essential for the success of a cybersecurity program because a cybersecurity program requires resources, including financial, human, and technical resources. Senior management approval is necessary to allocate the necessary resources to implement the program effectively. Other than that management support can help ensure that the cybersecurity program is integrated into the culture of the organization and that all employees understand its importance. Furthermore, senior management approval is necessary to ensure that the cybersecurity program aligns with the organization's risk management strategy.

[We need the right message to motivate the company](#_Toc99708092)

Motivating employees to take cybersecurity seriously can be difficult, but it is critical for the cybersecurity program's success. One way of archiving it is ensuring the employees of the organization make understand the importance of cybersecurity and how it relates to the organization's success. Assist them in comprehending the consequences of a cybersecurity breach, including financial losses, reputational damage, and potential legal ramifications. Help employees understand that cybersecurity is about more than just protecting the company's data; it is also about protecting their personal information. In order to protect their personal information as well as the company's data, emphasise that cybersecurity is everyone's responsibility. To help employees understand the impact of a cybersecurity breach, we can use real-world examples. Other than that communicate regularly and provide training and resources wiil be useful to mortivate the employees in cybersecurity and highlight that cybersecurity is not only management’s responsibility, it must be a collective effort and each and every employee must be responsible for it.

[The need for a Cybersecurity‐Awareness Training program](#_Toc99708093)

Any organization that wants to protect itself from cyber threats must invest in cybersecurity awareness training. The primary goal of such a program is to educate employees and other stakeholders about cybersecurity risks and to provide them with the knowledge and skills they need to help prevent cyber-attacks. Cybersecurity-awareness training can help employees understand the importance of protecting sensitive information and create a security-focused culture within an organization. Moreover cybersecurity-awareness training can be benefit to employees to understand their role in responding to security events, which can help reduce the impact of such incidents and minimize downtime.

[How to live cybersecure](#_Toc99708094)

To live cybersecure, employees can take various precautions like keep software and hardware devices up to date, use strong and unique passwords, use antivirus and anti-malware softwares, backup important data and maintain DR sites up to date and use intrusion detection and prevention systems.

# References

Brown, W. S. (n.d.). In W. S. Brown, *Computer Security Principles and Practice.* Pearson.

*Cyber Security*. (n.d.). Retrieved from Synopsys: https://www.synopsys.com/glossary/what-is-cyber-security.html

Groot, J. D. (2022). *What is Cyber Security? Definition, Best Practices & Examples*. Retrieved from DigitalGuardian: https://www.digitalguardian.com/blog/what-cyber-security

Meeuwisse, R. (2017). *Cybersecurity for Beginners.* Cyber Simplicity Limited.

Shinde, A. (2021). *Introduction to Cyber Security.* HARPERCOLLINS 360.

Steinberg, J. (2019). *Cybersecurity For Dummies.* Wiley.

Tunggal, A. T. (2023). *Why is Cybersecurity Important?* Retrieved from Upguard: https://www.upguard.com/blog/cybersecurity-important