**Cyber security**

1. Cyber security principles

The cyber security principles allow businesses to protect their information technology and operation technology systems, applications and data from cyber threats in a strategic manner. The cyber security principles consist of 5 principles which are – 1. Govern, 2. Identify, 3. Protect, 4. Detect, 5. Response (Cyber Security Principles | Cyber.gov.au, 2024).

**GOVERN**

Governing includes developing a strong cyber security culture. A Chief Information Security Officer provides leadership and oversight of cyber security (*Cyber Security Principles | Cyber.gov.au*, 2024). Security risk management activities for systems and applications are already integrated into organisational risk management frameworks. Security risks for systems, applications and data are accepted before being authorised for use and continuously throughout their operational life (*Cyber Security Principles | Cyber.gov.au*, 2024).

**IDENTIFY**

The function of identifying involves identifying assets and security risks. The business importance of systems, applications and data is determined and documented (*Cyber Security Principles | Cyber.gov.au*, 2024). The confidentiality and integrity requirements for applications and data are determined and documented. Security risks for applications, systems and data are identified and documented.

**PROTECT**

The function of protecting involves implementation of controls to manage security risks. Systems and applications are designed and maintained according to their business importance and their confidentiality, integrity and availability requirements. Systems and applications are designed to reduce their attack surface (*Cyber Security Principles | Cyber.gov.au*, 2024). Vulnerabilities in systems and applications are identified and nullified in a timely manner. Applications, settings and data are backed up in a secure and proven manner on a regular basis. Robust and secure identity and access management is used to control access to systems, applications and data. Physical access to systems, supporting infrastructure is made unavailable to authorised personnel (*Cyber Security Principles | Cyber.gov.au*, 2024).

**DETECT**

The function of detecting involves detecting and analysing cyber security events to identify cyber security incidents (*Cyber Security Principles | Cyber.gov.au*, 2024). Event logs are documented and analysed in a timely manner to detect cyber security events. Cyber security events are analysed in a timely manner to identify cyber security incidents (*Cyber Security Principles | Cyber.gov.au*, 2024).

**RESPOND**

The function of responding involves responding to and recovering from cyber security incidents. Cyber security threats are analysed, contained and recovered from in a timely manner (*Cyber Security Principles | Cyber.gov.au*, 2024).

1. **Applications**

Applications that could be used include software security, network surveillance and Identification and Access Control (IAM).

**Software Security**

Software security contains controls like code signing and may assist security rules like file-sharing rights and multi-factor authentication (Sharma, 2024).

**Network Surveillance**

Network surveillance is the continuous monitoring of harmful behaviour towards a system. Network surveillance is similar to other tools like firewalls and anti-viruses, monitoring for cyber security threats can be done manually or by a security software.

**Identification and Access Control (IAM)**

Identification and Access Control is when management regulates who has access to data, network and systems. Cyber security is practiced when management identifies users and executes an access control (Sharma, 2024).

**Benefits of Cyber Security**

The benefits of cyber security are that it protects an organisation’s sensitive information, builds customer trust, reduces company costs from cyber security threats, reduces vulnerability, and protects the business’ reputation. Having good cyber security as a business also helps the business gain a competitive advantage, and the business avoids legal fines and penalties which saves costs.

**Objectives of Cyber Security**

The objectives of cyber security aim to protect an organization’s digital assets and keep a secure environment. The main objectives of cyber security are to prevent unauthorized access, reduce risks and threats, enhance security awareness, ensure compliance, protect critical infrastructure, and foster a secure culture (Khan, 2024).

**Actionable Solutions for Addressing Cyber Security Threats**

There are many actionable solutions for addressing cyber security threats to protect the organization’s digital assets. Keeping software and systems updated is a good solution to address cyber-attacks and to prevent them. An organization should install a firewall to prevent cyber security threats as it blocks any cyber-attacks from infiltrating the system. Using strong passwords to protect all systems is a viable solution for addressing cyber security threats. Access management is also a good way to address cyber security threats as it blocks staff from downloading certain software that could harm the organization’s system.

<https://www.youtube.com/watch?v=awhqnSskWjU>



**References:**

*Cyber Security Principles | Cyber.gov.au*. (2024). Cyber.gov.au. <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles#:~:text=Purpose%20of%20the%20cyber%20security%20principles&text=IDENTIFY%3A%20Identify%20assets%20and%20associated>

Khan, Z. (2024, July 15). *Aims and Objectives of Cyber Security: Complete Guide*. Digitalregenesys.com; Digital Regenesys Blogs. <https://www.digitalregenesys.com/blog/aims-and-objectives-of-cyber-security>

Sharma, V. (2024, June 20). *Top 15 Important Applications of Cybersecurity - 2022*. Www.knowledgehut.com. <https://www.knowledgehut.com/blog/security/applications-of-cyber-security>