Security Strategies

WHAT IS A SECURITY STRATEGY

Security Strategy

- A Security Strategy is a document created frequently which helps outline the main security concerns of an organisation and forms a plan on how to deal with them.

- In the United Kingdom we have The National Security Strategy which specifies the risks that UK faces and how the government will address these risks.

Security Strategy

- Without an in place security strategy it is often not very clear how security functions support to the overall aims of the organisation.
- Having a good security strategy will help any organisation to have good security management and indeed good corporate governance of the organisation.
- A strategic plan should note the "*current state*" of security practices and describe initial points to be addressed in the next 12 months, goals that need to be achieved in the next 18-24 months and longer term goals that will be met over the next 36 months period. This plan is usually developed by the CISO and is designed to be a living document.
- The vision, goals, and objectives of this plan should be reviewed at least annually.

Who is the CISO?
What do they do?

A **Chief Information Security Officer** (**CISO**) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

The CISO directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and information technology (IT) risks.

They respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures.

Who is the CISO? What do they do?

- The CISO must have knowledge the current working security state of the company/organisation.
- To-do this, the CISO will continuously review in place assets such as hardware, software, network configurations, policies, security controls, prior audit results, etc.
- There main goal is to gather information on the current technology/application portfolio, the already existing business plans, while also trying to gain an understanding of the types of critical data required by the business stakeholders.

Who is the CISO? What do they do?

Typically, the CISO's influence reaches the entire organization. Responsibilities may include, but not be limited to:

- Computer emergency response team/computer security incident response team
- Cybersecurity
- Disaster recovery and business continuity management
- Identity and access management
- Information privacy
- Information regulatory compliance (e.g., US PCI DSS, FISMA, GLBA, HIPAA; UK Data Protection Act 1998; Canada PIPEDA, Europe GDPR)
- Risk management
- Security and information assurance
- Information security operations center (ISOC)
- Information technology controls for financial and other systems
- IT investigations, digital forensics, eDiscovery

Research Task

- Use the Worldwide Web to research, Risk Management, Disaster Recovery Plans & Business continuity Management.
- What are they and what is their purpose?

How do you plan your Security Strategy?

Before you can create your Security strategy plan you must consider

- Compliance/Audit Function (Legislation i.e GDPR)
- Client requirements
- Utilise existing frameworks (US – NIST, UK – Cyber Security Essentials Frameworks, ISO 27001)

Approach to Strategy Plan

You should approach your security strategy using the
CIA triad (Confidentiality, Integrity, Availability)

Examples

- If you are an online retail company you would base your security plan around availability of data, due to the customers needs to have constant availability to the data (Amazon lose £1 million every minute there website is down).
- Law firms may approach there plan focusing on confidentiality, with the need to keep clients records confidential due the sensitive data they may hold on clients(GDPR).
- A medical Organisation may use a Hybrid model as patients need there data to be confidential, Integrity to make sure the patient receives the correct medical procedure and the need to have patients records available at all time.