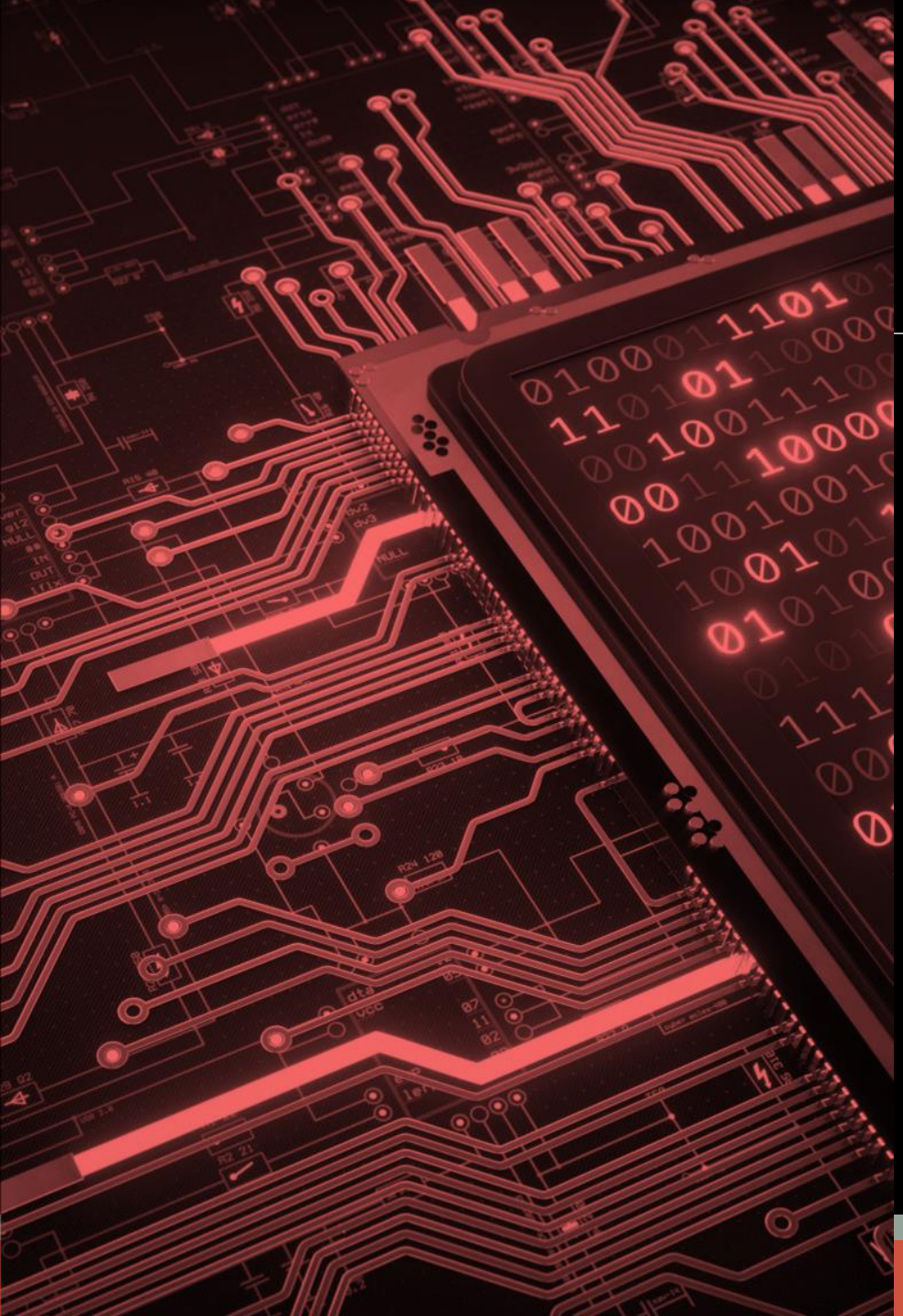
Cognicions

...Technology enablers & facilitators

Securing Tomorrow, Today:

"Navigating Cyber Security Risks with Strategic Precision"

RONALD KOHLMAN



Principles

- It's important for organisations to have a well-defined incident response plan in place to effectively detect, respond to, and mitigate the impact of cyber security incidents
- Organisations must allocate resources to bolster cyber security measures and establish robust incident response strategies to mitigate these risks and reduce the potential harm resulting from cybercrimes
- Even highly skilled technology firms can fall victim to Cyber-attacks
- Organisations bear a responsibility to ensure the highest level of cyber security for their systems and data, as well as to demonstrate their commitment to these efforts
- Cyber security governance, risk management, and strategy are integral components of a comprehensive approach to safeguarding digital assets in the face of evolving cyber threats

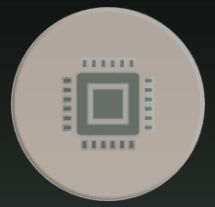
Cyber Risk and Strategy

- With the increasing frequency and sophistication of cyber threats, it is essential for businesses to develop robust and comprehensive strategies to mitigate risks and safeguard sensitive information and maintain the integrity of digital systems.
- Cyber security risk refers to the potential harm or adverse impact that may arise from vulnerabilities and threats in the digital realm. It encompasses the likelihood of exploitation of weaknesses in information systems, networks, applications, or processes, leading to unauthorised access, data breaches, disruptions, or damage to digital assets. Cyber security risk involves the intersection of three key elements: vulnerabilities, threats, and consequences.
- Cyber security strategy is a comprehensive and proactive plan that outlines an organisation's approach to managing and mitigating cyber threats, protecting digital assets, and ensuring the confidentiality, integrity, and availability of information systems. It involves strategic planning, resource allocation, and the implementation of measures to safeguard against cyber-attacks, data breaches, and other security risks in the digital environment.

Challenges

Securing the cyberspace, we use every day presents unique challenges due to several factors

Complexities
these challenges encompass the ability of malicious actors to operate globally, the interconnectedness between cyberspace and physical systems, and the complexities involved in mitigating vulnerabilities and their potential impacts within intricate cyber networks



Adoption
the adoption of sound cyber security practices is of utmost importance for both individuals and organisations, regardless of their size

Cyber hygiene
practicing good "cyber hygiene," which includes using strong passwords, keeping software up to date, exercising caution when encountering suspicious links, and enabling multi-factor authentication, is fundamental and significantly enhances online safety

Principles
cyber security principles are equally applicable to individuals and entities

Applicability
for both governmental and private organisations, the development and implementation of customised cyber security strategies and procedures are crucial for safeguarding and sustaining business operations

Increasing risk
with information technology's increasing integration into all aspects of our society, the risk of widespread or high-impact incidents that could disrupt essential services vital to the well-being and livelihoods of millions of people across the globe is on the rise

Rising attacks
these attacks on our technology are happening with greater sophistication, frequency, and tenacity

Challenges

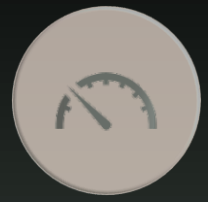
Securing the cyberspace, we use every day presents unique challenges due to several factors

Supply chain disruption
attacks on an organisation's suppliers or service providers can disrupt the supply chain and impact an organisation's ability to deliver products or services

Loss of customer trust
customers may lose trust in an organisation that fails to protect their data. This can result in decreased customer loyalty and revenue

Liability
organisations may be liable for the damages caused by a cyber-attack, particularly if negligence is proven

Regulatory fines
organisations may face fines and penalties for failing to comply with cyber security and data protection regulations



Business disruption
cyber-attacks can disrupt day-to-day business operations, leading to downtime, lost productivity, and potential damage to customer relationships

Fraud
cybercriminals can engage in financial fraud, including embezzlement and fraudulent wire transfers, causing financial harm to organisations

Environmental damage
for some cases, cyber-attacks can result in environmental damage, especially when critical infrastructure or industrial control systems are targeted

Downside of cyber-crime

Financial Loss

Cyber-attacks can lead to direct financial losses through theft, fraud, or ransom payments. Organisations may also incur costs associated with incident response, recovery, and legal actions.

Data Breaches

Breaches result in the exposure of sensitive and confidential data, leading to financial, reputational, and legal consequences. Organisations may face fines and legal action for failing to protect data. Identity theft from the data breach.

Reputational Damage

A data breach or cyber incident can erode trust and damage an organisation's reputation. This can lead to customer loss, decreased revenue, and challenges in regaining trust.

Legal and Regulatory Consequences

Non-compliance with data protection and privacy regulations, like GDPR or HIPAA, can result in significant fines and legal actions.

Operational Disruption

Cyber-attacks can disrupt day-to-day operations, causing downtime and lost productivity. Ransomware attacks, for example, can lock systems until a ransom is paid.

Intellectual Property Theft

Cybercriminals may target intellectual property, trade secrets, or proprietary information, resulting in the loss of competitive advantage and business secrets.

Extortion

Ransomware attacks and other extortion schemes can force organisations to pay ransoms to regain control of their systems and data. Common method here is to “crypto lock” the organisation's systems and data.

Some common cyber security threats that organisations and individuals often face

Unauthorised Access	Insider Threats	Data Breach	Security Policy Violations	System and Network Intrusions
Lost or Stolen Devices	Identity Theft	Cyber Espionage	Phishing	Ransomware
Malware	Distributed Denial of Service (DDoS) Attacks	Man-in-the-Middle (MitM) Attacks	Software Vulnerabilities	SQL Injection
Cross-Site Scripting (XSS)	Zero-Day Exploits	Password Attacks	Social Engineering	IoT Vulnerabilities
Credential Stuffing	Insider Threat	Supply Chain Attacks	Cryptojacking	Advanced Persistent Threats (APTs)

Key components of managing cyber risk

Risk assessment

evaluating the organisation's assets, identifying vulnerabilities and threats, and assessing the potential impact of successful cyber-attacks

Risk mitigation

implementing security controls and measures to reduce the likelihood of successful attacks and minimise the impact if they occur. This may include the implementation of firewalls, antivirus software, encryption, access controls, and employee training

Incident response

developing and practicing plans for responding to and recovering from cyber security incidents. This involves having procedures in place to detect, contain, eradicate, and recover from security breaches

Continuous monitoring

regularly monitoring and assessing the organisation's digital environment for changes in the threat landscape, emerging vulnerabilities, and the effectiveness of existing security measures

Compliance

ensuring compliance with relevant cyber security regulations, industry standards, and best practices to meet legal requirements and industry expectations

Key components of a cyber security strategy

Risk Assessment

Identify and assess potential cyber risks by evaluating vulnerabilities, threats, and the potential impact of security incidents on the organisation's digital assets

Governance and Leadership

Establish a clear governance structure with designated leaders and responsibilities for cyber security.

Ensure that cyber security is integrated into the organisation's overall governance framework

Policy Development

Formulate and enforce cyber security policies that define acceptable practices, guidelines, and standards for employees, contractors, and third-party partners.

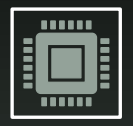
These policies cover areas such as access controls, data protection, and incident response

Incident Response Planning

Develop and maintain incident response plans to guide the organisation's actions in the event of a cyber security incident. This includes procedures for detecting, responding to, and recovering from security breaches

Security Awareness and Training

Implement ongoing cyber security awareness programs to educate employees about potential risks, best practices, and their role in maintaining a secure digital environment



Technology Investment

Invest in and regularly update cyber security technologies such as firewalls, antivirus software, intrusion detection/prevention systems, and security information and event management (SIEM) solutions

Defence-in-Depth Strategy

Implement a defence-in-depth strategy that involves layering multiple security controls and measures to provide comprehensive protection against a variety of cyber threats

A robust cyber security strategy is essential for individuals, businesses, and governments alike to safeguard sensitive data and maintain the integrity of digital systems

Summary

- Navigating cyber security risks and developing effective strategies to deal with cyber-crime is essential for all organisations
- Crucial steps for organisations to mitigate existing cyber risks and provide a strategy to enhance future cyber security measures
- Cyber security risk is the potential harm from vulnerabilities and threats
- Cyber security incidents are malicious acts compromising confidentiality, integrity, or availability of information assets, impacting systems, networks, and data
- Essential nature of a robust cyber security strategy for individuals, businesses, and governments is to safeguard sensitive data and maintain digital system integrity
- Cyber security risk assessment is a critical component of an effective risk management program, involving systematic identification and evaluation of potential risks
- Cyber security strategy as a comprehensive and proactive plan outlining an organisation's approach to managing and mitigating cyber threats and risks

About Ronald

Ronald is a highly experienced and knowledgeable IT professional in the field of program and test management.

He has had many roles working across transformational initiatives and complex enterprise technology solutions.

- Leadership in Transformational Programs
- Global Experience and Cross-Continental Team Leadership
- Governance Frameworks and Tools
- Delivery of Complex Technology Solutions
- Executive-Level Engagement and Consulting

He has been writing and publishing technology industry specific documents for several years. Imparting his practical working experience within these documents.

You can purchase his technology & project books on Amazon:

You've had a Cyber Attack - Now what?
Securing Tomorrow, Today: Navigating Cyber Security Risks with Strategic Precision
How to Create a Cyber Security Roadmap: A necessity for your organisation
Program Management Plan: A usable Template for you
Business Case Template: An approach to documenting your next IT business case
Successfully Delivering User Acceptance Testing for your project
IT Deployment Management Framework
Steering Committee Terms of Reference and Charter
UAT Planning Guide
Defect Management Plan

Cognicions

...Technology enablers & facilitators

Thank You

COGNICIONS.COM

COGNICIONS PTY LTD

ABN 83 611 219 642

MELBOURNE

PO BOX 125, OLINDA,
VICTORIA 3788

+61 (0) 402 448 050

INFO@COGNICIONS.COM