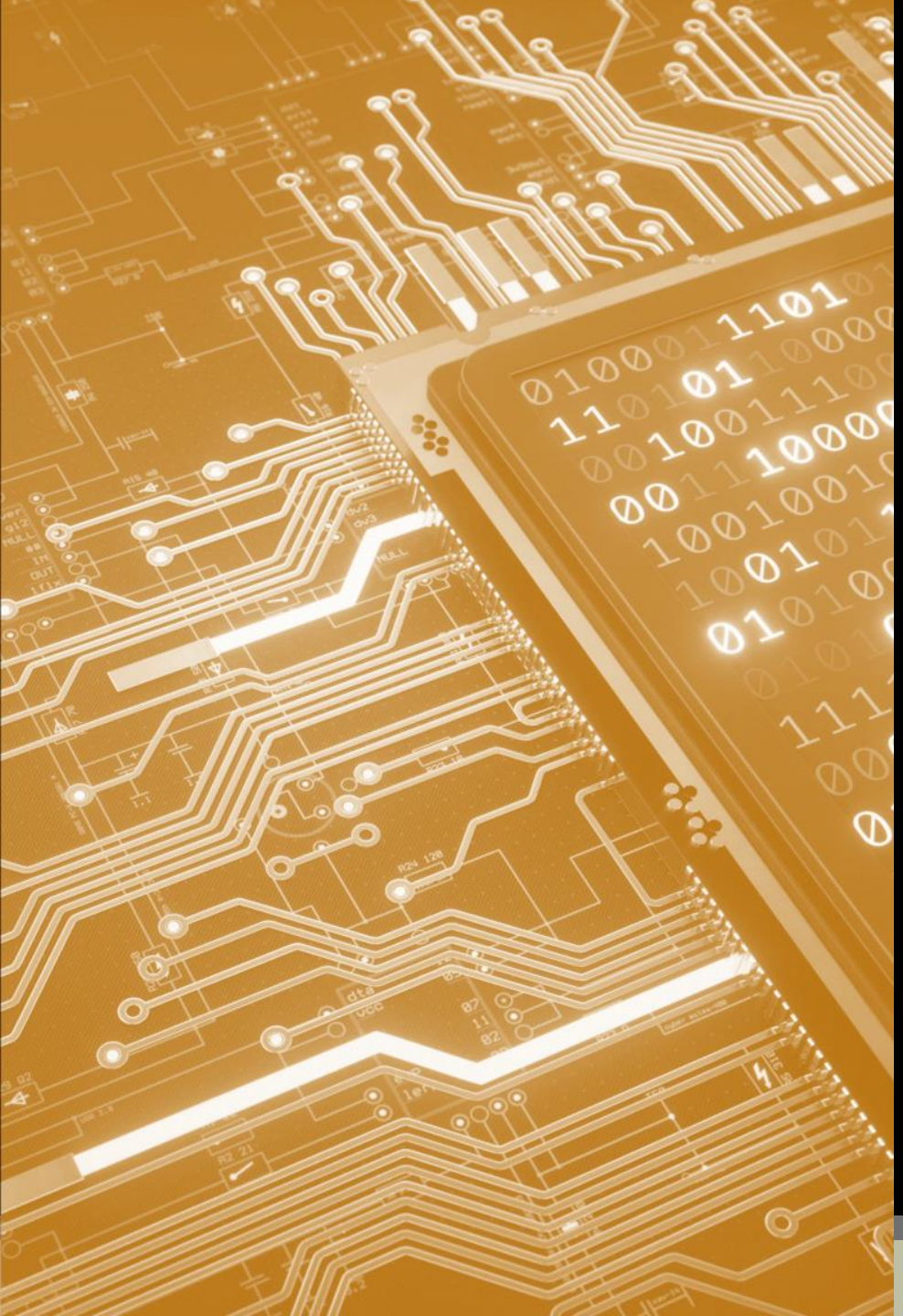
Cognicions

...Technology enablers & facilitators

YOU'VE HAD A CYBER ATTACK NOW WHAT?

"TURNING THE TIDE: NAVIGATING THE AFTERMATH OF A CYBER SECURITY ATTACK WITH RESILIENCE AND RESPONSE"

RONALD KOHLMAN



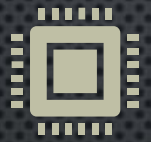
PRINCIPLES

- Organisations must allocate resources for robust cyber security measures and incident response to mitigate risks. Cyber-crime poses ongoing threats to individuals, businesses, and governments, requiring a multi-pronged approach:
  1. Implement strong security controls, including firewalls and access controls.
  2. Educate employees on cybersecurity, identifying and avoiding threats.
  3. Develop a response plan for investigating, containing, and restoring systems after an attack.
- A cyber security incident disrupts or breaches information systems, affecting businesses of all sizes. Organisations need well-defined incident response plans to minimise damage, protect assets, and restore normal operations promptly.

COMMON CYBER ATTACKS

A cyber security incident disrupts or breaches information systems, affecting businesses of all sizes. Organisations need well-defined incident response plans to minimise damage, protect assets, and restore normal operations promptly.

Malware: Damages or gains unauthorized access to computer systems.



Phishing: Deceptive attempts to trick individuals into revealing sensitive information.

Ransomware: Encrypts files, demanding payment for release.

Denial of Service (DoS) and Distributed Denial of Service (DDoS): Overloads systems to disrupt functioning.

SQL Injection: Exploits database vulnerabilities for unauthorized access.

Man-in-the-Middle (MitM) Attacks: Intercepting and altering communication between two parties.

A cyber-attack is a malicious and deliberate attempt by individuals or organisations to exploit vulnerabilities in computer systems, networks, or digital devices. The motives behind cyber-attacks can vary and may include theft of sensitive information, disruption of operations, financial gain, or political motives. The cost impact can be enormous.

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)

CAUSES OF CYBER-ATTACKS

There are many different causes of cyber-attacks, but some of the most common include:

1. Financial gain: Cyber-criminals may launch cyber-attacks to steal money, credit card information, or other valuable data.
2. Espionage: Governments and corporations may launch cyber-attacks to steal sensitive information from their rivals.
3. Vandalism: Cyber-criminals may launch cyber-attacks to damage or disrupt computer systems or networks.
4. Activism: Hacktivists may launch cyber-attacks to protest government policies or corporate practices.

DOWNSIDE IMPACT 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

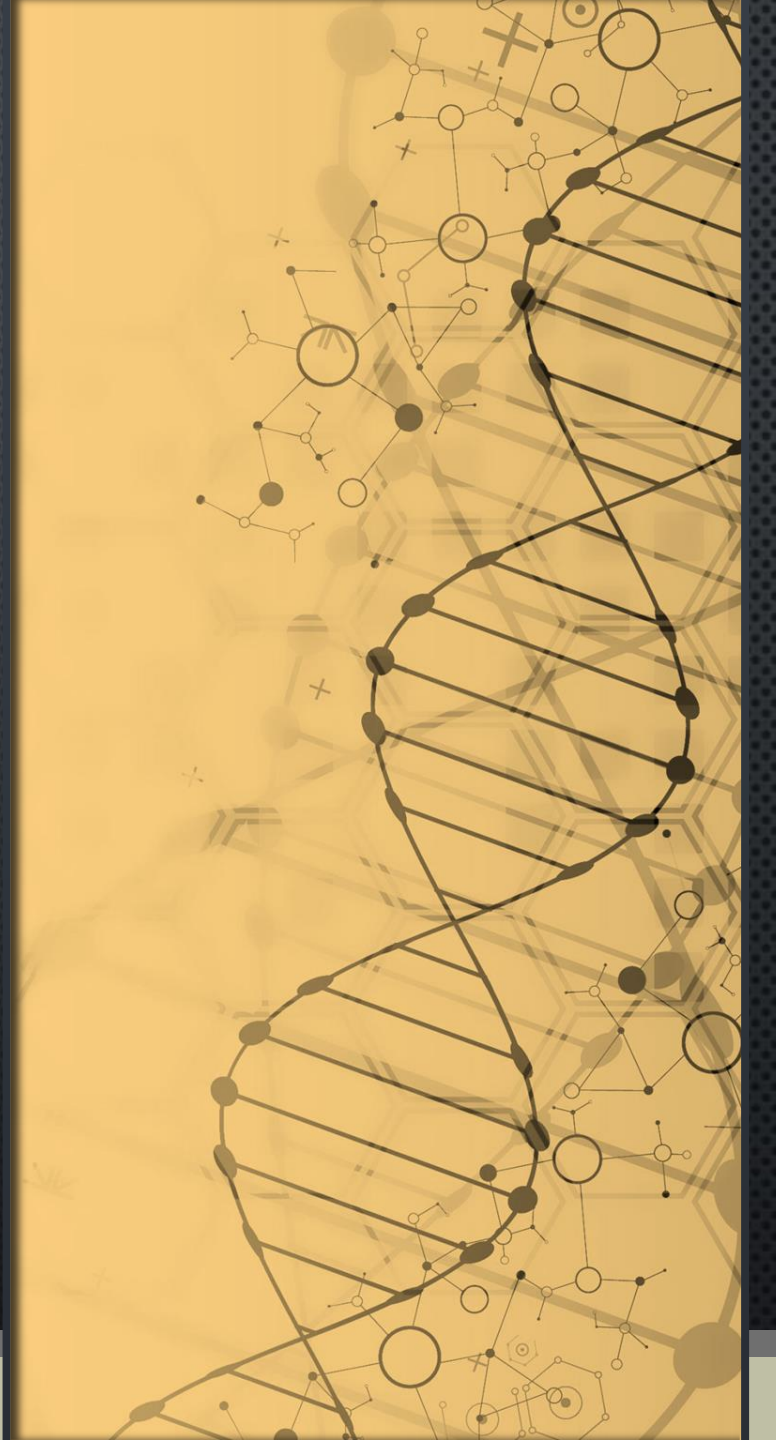
Ransomware attacks and other extortion schemes can force organisations to pay ransoms to regain control of their systems and data. Common method here is to “crypto lock” the organisation's systems and data.

IMMEDIATE ACTIONS TO TAKE WHEN A CYBER-ATTACK OCCURS

IF YOU SUSPECT OR CONFIRM THAT A CYBER-ATTACK HAS OCCURRED, IT'S IMPORTANT TO RESPOND PROMPTLY AND EFFECTIVELY TO MINIMISE DAMAGE AND PROTECT YOUR SYSTEMS AND ORGANISATION AND RESTORE NORMAL OPERATIONS. CYBER-ATTACKS CAN BE DEVASTATING FOR BUSINESSES AND ORGANISATIONS, CAUSING FINANCIAL LOSSES, REPUTATIONAL DAMAGE, AND DATA BREACHES.

Remedy for Cyber Attacks

- **Incident Response Plan:**
  Execute a well-defined incident response plan to contain, eradicate, and recover from the attack
- **Forensic Analysis:**
  Conduct a thorough forensic analysis to understand the scope and impact of the attack
- **Data Recovery:**
  Restore data from backups to minimise data loss
- **Legal Action:**
  Pursue legal action against attackers if identifiable and applicable



YOUR CLOUD SERVICE PROVIDER HAS HAD A CYBER SECURITY INCIDENT

EXPERIENCING A CYBER SECURITY INCIDENT WITH YOUR CLOUD SERVICE PROVIDER CAN BE DISRUPTIVE, BUT HAVING A WELL-PREPARED RESPONSE PLAN IS CRUCIAL

Remedy: Restoring Access and Data Recovery

- Communication
- Data Recovery
- Collaboration
- Alternate Access

Prevention: Strengthening Security Measures

- Incident Response Plan
- Security Audits
- Redundancy
- Encryption
- Access Controls
- Continuous Monitoring
- Vendor Security Assessments

Actions to Take: Post-Incident Recovery and Strengthening

- Post-Incident Analysis
- Regulatory Compliance
- Communication Strategy
- Legal Review
- Cyber Insurance
- Future Preparedness

Continuous Improvement:

- Lessons Learned
- Security Awareness
- Redundancy Planning
- Third-Party Relationships

Cloud Service Provider – Preparation

Preparation is key in handling a cyber security incident involving your Cloud Service Provider (CSP). Cloud service providers can be attacked and there have been some notable cyber-attacks against cloud service providers in recent times. They are not infallible.

Develop an Incident Response Plan (IRP)

- Create a Cross-Functional Team
- Define Incident Categories
- Establish Communication Protocols
- Conduct Regular Training and Drills

Know Your Cloud Environment

- Inventory of Cloud Assets
- Cloud Service Provider Liaison
- Cloud Security Best Practices

Data Protection and Backup

- Data Encryption
- Regular Backups
- Redundancy Planning

Continuous Monitoring and Threat Intelligence

- Implement Continuous Monitoring
- Threat Intelligence Integration

Legal and Compliance Considerations

- Understand Legal Obligations
- Cyber Insurance

Communication and Public Relations

- Develop Communication Plans
- Media Relations

Post-Incident Analysis and Improvement

- Conduct Post-Incident Analysis
- Update Incident Response Plan
- Continuous Improvement

Regulatory Compliance

- Stay Informed About Regulations
- Regular Audits

Third-Party Relationships

- Vendor Risk Management
- Collaborative Security Initiatives

Employee Training and Awareness

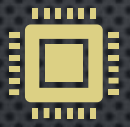
- Security Training Programs
- Incident Reporting Procedures

CYBER SECURITY A DYNAMIC AND EVOLVING FIELD

CYBER SECURITY IS A DYNAMIC AND EVOLVING FIELD, AND WHILE IT CANNOT GUARANTEE ABSOLUTE PROTECTION AGAINST ALL THREATS, IMPLEMENTING EFFECTIVE CYBER SECURITY MEASURES CAN SIGNIFICANTLY REDUCE THE RISK OF SECURITY BREACHES AND THEIR IMPACT.

PREVENTION STRATEGIES

Employee Training: Educate employees on cyber security best practices and how to recognise and avoid potential threats



Patch Management: Regularly apply security patches and updates to address vulnerabilities

Network Security Measures: Implement firewalls, intrusion detection/prevention systems, and secure network configurations

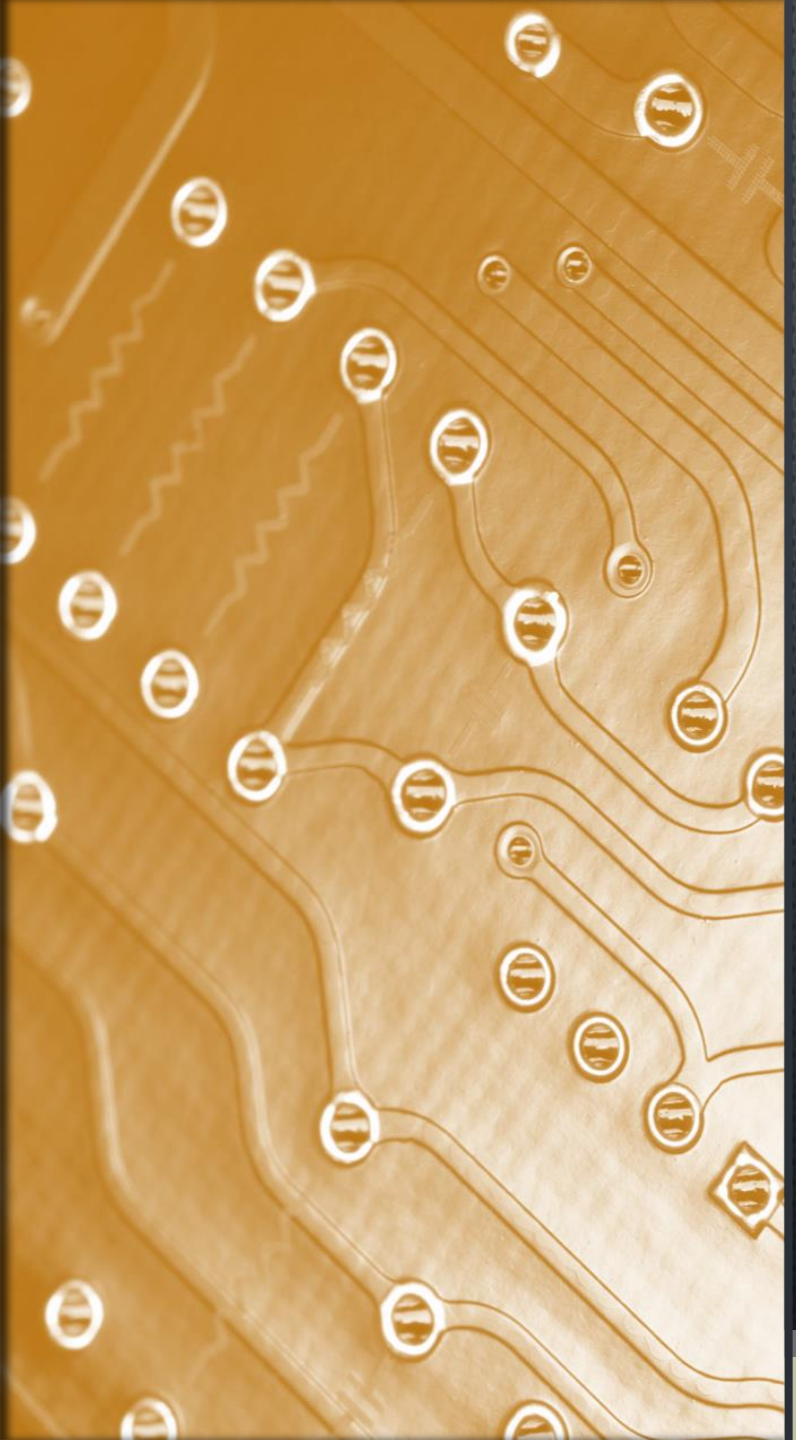
Multi-Factor Authentication: Enhance access controls with multi-factor authentication for critical systems

Regular Audits and Assessments: Conduct cyber security audits to identify and rectify weaknesses

Security Policies and Procedures: Develop and enforce comprehensive security policies and procedures

Collaboration with Security Experts: Engage with cyber security experts to assess and improve overall security posture

- Cyber-attacks pose serious threats to individuals and organisations
- A holistic approach to cyber security involves not only responding effectively to incidents but also implementing preventive measures and continuously adapting to the evolving threat landscape
- Combining technical defences with user education and a robust incident response strategy is essential for a resilient cyber security posture



IMPORTANT CONSIDERATIONS

CYBER SECURITY IS AN ONGOING CHALLENGE, BUT ORGANISATIONS CAN TAKE STEPS TO PROTECT THEMSELVES FROM CYBER-ATTACKS AND MINIMISE THE DAMAGE IF THEY ARE ATTACKED.

WHEN ADDRESSING CYBER-ATTACKS, SEVERAL IMPORTANT CONSIDERATIONS SHOULD BE PLANNED FOR TO ENHANCE CYBER SECURITY AND MINIMISE POTENTIAL RISKS. TO ADDRESS THESE CHALLENGES, ORGANISATIONS NEED TO TAKE A MULTI-PRONGED APPROACH TO CYBER SECURITY:

- **IMPLEMENT STRONG SECURITY CONTROLS:**
  THIS INCLUDES USING FIREWALLS, INTRUSION DETECTION SYSTEMS, AND ACCESS CONTROLS TO PROTECT SYSTEMS FROM UNAUTHORISED ACCESS.
- **EDUCATE EMPLOYEES ABOUT CYBER SECURITY:**
  THIS INCLUDES TEACHING THEM HOW TO IDENTIFY AND AVOID PHISHING ATTACKS, MALWARE, AND OTHER THREATS.
- **HAVE A PLAN FOR RESPONDING TO CYBER-ATTACKS:**
  THIS INCLUDES HAVING A TEAM IN PLACE TO INVESTIGATE ATTACKS, CONTAIN DAMAGE, AND RESTORE SYSTEMS.

ADDITIONAL CONSIDERATIONS

1. Multi-Layered defence:	2. Regular Security Audits:	3. Employee Training and Awareness:	4. Patch Management:	5. Access Controls and Least Privilege:
6. Incident Response Plan:	7. Data Encryption:	8. Continuous Monitoring:	9. Backup and Disaster Recovery:	10. Vendor Security Assessments:
11. Regulatory Compliance:	12. Network Segmentation:	13. Threat Intelligence Integration:	14. Endpoint Security:	15. Cloud Security Best Practices:
16. Legal and Privacy Considerations:	17. Collaborative Security Initiatives:	18. End-of-Life Systems:	19. Insider Threat Mitigation:	20. Cybersecurity Insurance:

By addressing these considerations, organisations can build a resilient cyber security posture and be better prepared to defend against a wide range of cyber threats.

Regularly reassess and update security measures to stay ahead of evolving risks in the dynamic landscape of cyber security.

POLICIES TO CONSIDER

A well-structured set of security policies not only helps prevent incidents but also guides the organisation in responding effectively when incidents occur.

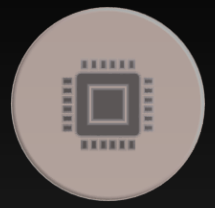
Regular training, communication, and updates are essential to ensure that employees are aware of and adhere to these policies.

- Security
- Password Management
- Identity Management
- Access Management
- Systems Monitoring
- Email Usage
- User Account Management
- Data Protection
- Audit
- Change Management
- Security Review
- External Access Management
- Cloud Solutions Incident Response
- Zero Trust Framework
- Vulnerability Management

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



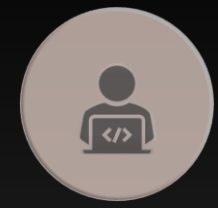
Adoption
the adoption of sound cyber security practices is of utmost importance for both individuals and organisations, regardless of their size

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

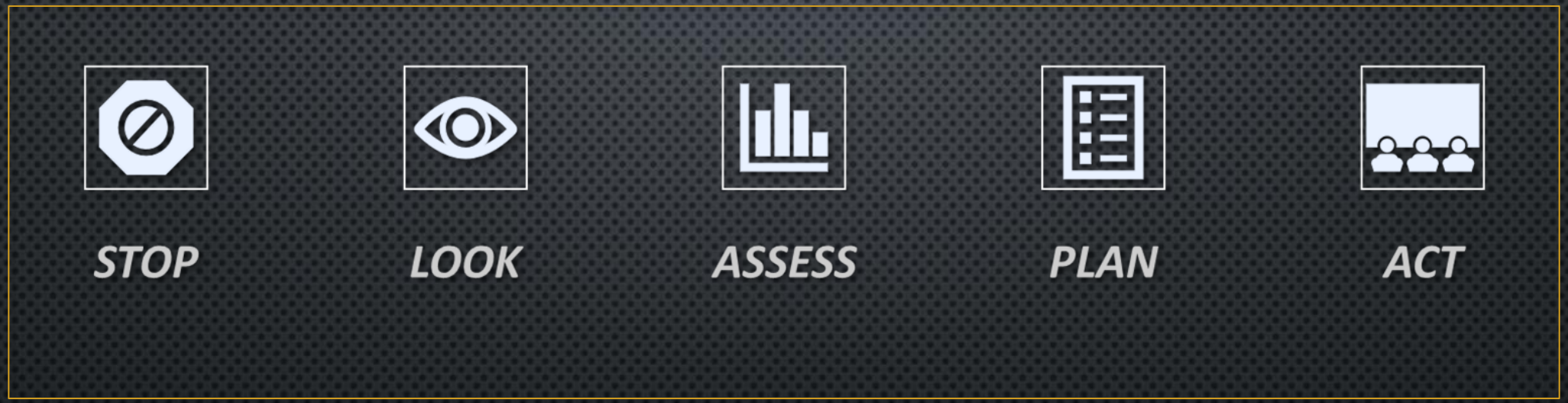
Business disruption
cyber-attacks can disrupt day-to-day business operations, leading to downtime, lost productivity, and potential damage to customer relationships

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

NOTABLE ADVICE

- When you have a problem, e.g. a cyber event (attack), do the following:



- Don't immediately jump straight in and attempt to fix the problem with the first thing that comes to mind. Understand your problem first.

SUMMARY

- Cyber security Attack has the potential to do harm from vulnerabilities and threats
- Cyber security attacks are malicious acts compromising confidentiality, integrity, or availability of information assets, impacting systems, networks, and data
    1. Understand the shared responsibility model of cloud security
    2. Implement strong access controls and data encryption
    3. Establish a regular vulnerability management process
    4. Provide regular security awareness training to employees
    5. Have a plan for responding to cyberattacks
    6. Regularly test, train, and update incident response plans
- Organisations must allocate resources for robust cyber security measures and incident response to mitigate risks. Cyber-crime poses ongoing threats to individuals, businesses, and governments, requiring a multi-pronged approach:
    1. Implement strong security controls, including firewalls and access controls
    2. Educate employees on cybersecurity, identifying and avoiding threats
    3. Develop a response plan for investigating, containing, and restoring systems after an attack
- Organisations need well-defined incident response plans to minimise damage, protect assets, and restore normal operations promptly

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