Cyber Resiliency:

Practical Measures to Safeguarding Your Business

Toh Wang Hin

Head of Information Security & Digital Risk, Bank of Singapore

Agenda

1. Understanding Cyber Threats
2. What are the practical measures to safeguard your business
3. Key Takeaways

Understanding Cyber Threats

Cyber Threat Statistics

Ransomware
72.7%
Global organisations fell prey to ransomware attack

277 days
Time taken to identify and contain a data breach

Phishing
41%
Cyber attacks start with Phishing Email

USD $4.45M
Global average cost of a data breach

Data Breach
USD $5.90M
Average cost of a data breach in Financial Industry

88%
Global malware attacks occurred via email

Credentials
30%
Cyber attacks were from compromised login credentials

Third Parties
45%
Businesses experienced third-party related business interruption

Source: [Statista, IBM, Gartner]

Practical Measures to Safeguard Your Business

Privileged Access Management

Privileged access management is a security mechanism that safeguards user identities with elevated access or privileged capabilities beyond regular users.

Cybercriminals target privileged accounts so that they can compromise the entire organisation.

Recommended Measures

- Adopt the principle of "Least Privilege", allowing users to receive the minimum level of access required by them to perform their job functions.
- Keep track of all privileged accounts. Continuously monitor, log and audit privileged account activities to identify potential risks within the environment.

Multi-Factor Authentication (MFA)

MFA is an additional login security layer to verify a user's identity when requesting access to a system. MFA requires the user to provide 2 or more information for authentication:

"Something you know" password or PIN
"Something you have" such as token
"Something you are" such as biometric

Recommended Measures

- Enforce the use of MFA for critical systems and privileged accounts to enhance security by adding layers of protection.
- Strengthen users' credentials by requiring users to provide multiple forms of verification for access.

Cybersecurity Training and Awareness Program

Cybersecurity awareness training helps to educate employees on cyber risks and threats. Many regulators require organisations and their employees to undergo regular security awareness training.

Business is about people, process and technology. The human aspect should not be ignored.

Recommended Measures

- Conduct regular cybersecurity awareness training sessions for all employees to educate them on cybersecurity best practices.
- Promote a culture of employee vigilance and responsiveness to cyber threats.
- Encourage reporting of suspicious cyber threats, such as phishing emails.

Vulnerability Management and Patch Management

Vulnerability management is a capability that identifies vulnerabilities on systems. Patch management is the process of applying updates to systems and software to close the vulnerabilities.

Vulnerabilities can be exploited by cyber attackers to access and infiltrate to critical systems and data.

Recommended Measures

- Conduct regular vulnerability assessments and penetration testing to identify and address weaknesses in your systems.
- Define a process for remediation actions to close the vulnerabilities and limit their exposure to your organisation.

Third Parties Cyber Risk Management

In digital world today, Third Party vendors provides services to businesses in many forms, such as outsourced services, packaged software to software-as-a-service products.

Cybercriminals could exploit the digital supply chain as a mechanism for cyberattacks.

Recommended Measures

- Conduct due diligence of the vendor's cybersecurity practices prior to engaging the Third Party.
- Implement vendor contracts and service agreements and to include specific cybersecurity requirements and incident reporting protocols.

Incident Response Plans

An Incident Response Plan is a set of procedures that helps the organisation to detect and respond to cyber-attack. If used effectively together with Disaster Recovery Plan, the Incident Response Plan will help to mitigate the impact of a cyber event on the business operations and reputation.

Recommended Measures

- Establish a robust Incident Response Plan for your organisation,
- Develop clear protocols for responding to cyber incidents, including incident response team's roles and responsibilities.
- The Incident Response Plan must be tested regularly. This is to ensure the organisation's incident preparedness.

Key Takeaways

Key Takeaways

Practical Measures for Your Business

Develop actionable steps towards strengthening your organisation’s cyber resilience.

Call to Action

Adopt a proactive strategy to mitigate risks and ensure that you’re well-equipped to navigate cyber threats successfully.