Webinar on 5 Ways to Assess Your Cyber-Readiness and Compliance
30 November 2022

Speakers:
Alex Duperouzel, Managing Director of ComplianceAsia
Andrew Silberstein, Managing Principle of the Tech Par Group

Cybersecurity risks are widespread and growing globally, impacting companies of all sizes and across industries in a variety of ways: from increasing frequency to the sophistication of cyber-attacks - all of which significantly impact the financial, reputational and regulatory requirements of companies, both private and public.

Financial institutions must continuously look to strengthen their cyber security position and ensure they have robust cyber hygiene practices in place for future disruptions. It is critical to understand cyber threats and identify the cyber risk gap as a way of measuring your cyber readiness.

Cybersecurity from a regulatory perspective

- Singapore position is based around the Technology Risk Management Guidelines which were last updated in 2021
- Singapore also has strict data privacy requirements
- Older cyber related rules that are soon to be updated with new legislation for Hong Kong
- The new laws in Hong Kong criminalising a variety of cyber related actions will come into effect soon

2022 Key threat statistics in APAC

45%
Of APAC respondents reported an increase in the number of attacks

50%
Breaches Reported by APAC Organisations.

47%
Of respondents say they have a formal ransomware response plan

62%
Of respondents that were breached were unable to obtain safe harbor, the legal remedy that provides a defence to liability caused by data breaches if they maintain a cybersecurity program that meets an industry-recognized standard that can show compliance at the time of attack.

80%
Of respondents were either “very concerned” or “somewhat concerned”

Countering The 5 Biggest Cyber Threats

Biggest Cyber Security Threats are:

1. Social Engineering/ Phishing Attacks
2. Malware & Ransomware Attacks
3. Inadequate Authentication and Authorisation
4. Configuration Mistakes
5. Third Party Exposure

Cyber Readiness = Cyber Defense

1. Organisational Behavior/ Email Defenses
2. Endpoint Detection, Backup and Recovery Capability
3. Security Controls
4. Vulnerability Management
5. Risk Management, Governance

CHALLENGE:

Protecting your Business

- Managing cyber risk has become an essential part of the daily life of a company.
- Addressing the complexity of a rapidly evolving IT environment, the transition to the cloud, and a remote and/or hybrid workforce.
- Navigating the increased frequency and sophistication of cyber-attacks, including ransomware, which significantly impact the financial, reputational and regulatory requirements of companies, both private and public.

SOLUTION:

Cyber Readiness Assessment

- Cost-effectively addressing the mitigation of the threat of ransomware and other cyber attacks
- Delivering a cybersecurity solution through a cloud-based platform using industry-proven and accepted testing tools
- Proving board-ready reports executives can understand, and your technical team can act upon.
- Performed without disrupting your operation and nominal involvement of your IT team.
- Completed within one month, start-to-finish, ROI achieved within one year or less.

ComplianceAsia Consulting Ltd. Suite 1102, ChinaChem Tower, 34-37 Connaught Road, Central, Hong Kong
Tel: (852) 2868 9070 www.complianceasia.com