

The logo for Hogan Lovells, consisting of the name "Hogan Lovells" in a black serif font, positioned within a solid lime green square.

Hogan
Lovells

Cyber-Security Webinar: Risks & Regulation for Multi-National Financial Institutions with Operations in Europe and Asia





Monday 27th June 2016

Agenda

- Introduction
- Cybersecurity Standards
- Information Sharing
- Data Breach Notification

Introduction: Reasons to Focus on Cybersecurity

Evolving threat landscape.

<u>Threat Type</u>		<u>Who and What</u>	<u>Examples</u>
Advanced Persistent Threat (APT)		Organized state-funded groups methodically infiltrating enterprises on a persistent basis with sophisticated tools	<ul style="list-style-type: none">• JP Morgan, NYT, unpublicized Wall Street firms, USG
Industrial Control System Attacks		Targeted attacks to control or disrupt activities of power plants and other large-scale industrial control systems	<ul style="list-style-type: none">• Stuxnet• Probe attacks on utilities/
Cybercrime		Organized crime rings targeting corporate and personal data for primarily for financial gain	<ul style="list-style-type: none">• Target• Neiman Marcus
Hactivism/ Reputational		High visibility attacks to advance “movements,” political/policy views, produce reputational impact	<ul style="list-style-type: none">• French TV5• Sony
Insider		Employee or contractor using access to information for personal, competitive, policy or financial goals	<ul style="list-style-type: none">• Snowden• AT&T

Introduction: Traditional Vectors of Attack

- Malware
- Phishing
- Social engineering
- Other browser-based attacks
- Network/security vulnerabilities
- SSL Attacks

Introduction: Trends and Future Fears

- **The Cyber Crimes become more common events similar to common Crime.**
 - Cyber Extortion
 - Cyber Abductions
 - Cyber Lock outs
 - Cyber Vandalism

Introduction: The U.S. Cyber Compliance Landscape: (Relatively) Mature

- Gramm Leach Bliley Act: Interagency Guidelines on Security Standards: - applies to Nonpublic Personal Information
- 47 State Data Breach Notification Laws (some state insurance commissioners)
- Key financial services regulators have stated an expectation that regulated entities have a written incident response program.
- State Regulator Focus (including NAIC and Insurance Commissioners)
- Information Sharing (FS-ISAC and CISA)
- FFIEC Guidance
- NIST Cybersecurity Framework broadly embraced

Cyber Security Standards in Asia

- No regional policy framework and limited inter-governmental co-operation to date.
- China's regulatory developments are important to watch:
- emerging standards for “secure and controllable” technology
- preference for indigenous technologies
- disclosure of source codes and technology transfer
- Monetary Authority of Singapore (“MAS”) has detailed TRM requirements that address cyber issues from a technology perspective
- Hong Kong's Monetary Authority (“HKMA”) has put Cyber Fortification Initiative out for consultation. CFI will introduce benchmarks for threat identification and incident management
- Reference to international examples (such as NIST) are often made
- SWIFT incidents have highlighted need to develop clear standards to avoid “weakest links” in the region

Cyber Security Standards in Europe

- Network and Information Security Directive (the "Cybersecurity Directive")
- General Data Protection Regulation ("GDPR")
- Second Payment Services Directive ("PDS2")

Information Sharing in Asia

- Practices differ significantly by jurisdiction:
 - some regulators expect prompt reporting and will share information with other institutions
 - SWIFT incidents illustrate that many jurisdictions are lacking on this front
- HKMA's Cyber Fortification Initiative makes improved information sharing a key component of the new regime

Information Sharing in Europe

- **Cybersecurity Directive**
 - National Computer Security Incident Response Teams (CSIRTs)
 - National reporting to CSIRTs or other competent authorities
 - Information exchange via European level Co-operation Group or at CSIRT level

Incident Response and Breach Notification in Asia

- Financial Institutions in the region often now face two aspects of notification:
- industry regulator(s)
- data protection authorities and data subjects
- Increasingly demanding requirements raise challenges
- Cross-border aspects are often encountered given regional hubbing of data and patchwork of regulatory requirements

Incident Response and Breach Notification in Asia

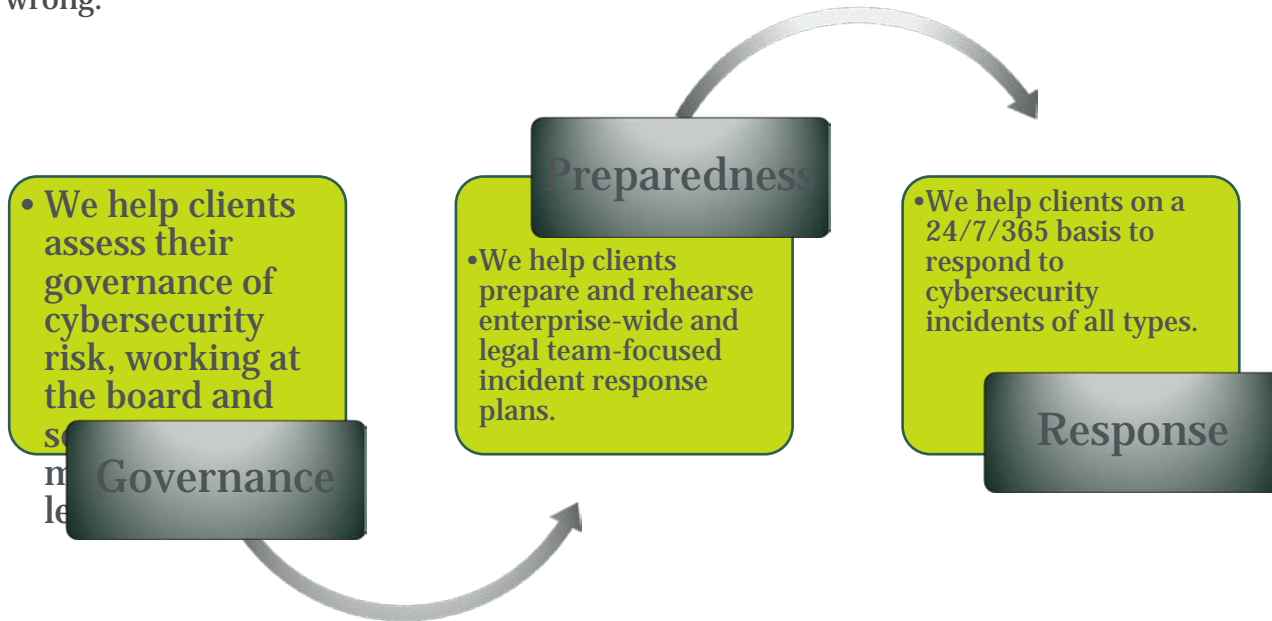
Jurisdiction		Data Breach Obligation?
China	Yellow	Some sector-specific requirements
Hong Kong	Yellow	Recommended
Singapore	Yellow	Recommended
South Korea	Red	Yes
Malaysia	Green	No
Taiwan	Red	Yes
India	Red	Yes
Indonesia	Green	No, but new law in force in 2017
Japan	Yellow	Some sector-specific requirements
Philippines	Red	Yes
Thailand	Green	No, but new law will introduce controls
Australia	Green	No, but evaluating new law

Incident Response and Breach Notification in Europe

- New reporting obligations
 - on operators of essential services and digital service providers under Cybersecurity Directive
 - for personal data breaches under GDPR
 - on payment service providers under PSD2

Hogan Lovells' comprehensive approach

- Our cybersecurity and incident response capabilities are one part of our comprehensive approach to cybersecurity, with preparedness of utmost importance. Because we understand what goes into incident preparedness and associated efforts to strengthen your technical, compliance and governance systems, we are well positioned to assist when, despite best efforts, things go wrong.



Questions & Answers

The logo for Hogan Lovells, consisting of the name "Hogan Lovells" in a black serif font, positioned within a solid lime green square.

Hogan
Lovells

Cyber-Security Webinar: Risks & Regulation for Multi-National Financial Institutions with Operations in Europe and Asia

Monday 27th June 2016