Insurance Authority Guideline on Cybersecurity — Are you ready?

Highlights

What are the key requirements of the Guideline on Cybersecurity?

How PwC can help?

Background

- Draft Guideline on Cybersecurity (the "Guideline") was issued in Nov 2018 to the Hong Kong Federation of Insurers for industry consultation.
- The Guideline is likely to be finalized in Q1 2019. Authorised Insurers are expected to comply from 1 July 2019.
- The Guideline is to be issued under s.133 of the Insurance Ordinance, which sets out the minimum standard of cybersecurity that is expected of an Authorised Insurer to put in place.

Governance

- Cybersecurity strategy and framework should be established and endorsed by the Board.
- Framework should include defined cybersecurity objectives, requirements for competency of people, well-defined processes and technology for managing cyber risk and timely communication of the strategy with all data users.
- While the Guideline sets out some high-level principles, it's not a standard. In fact, as required by the Guideline, Authorised Insurers should make reference to internationally recognised standards, such as ISO27001 and NIST.
- An appropriately skilled management team should be defined, including clear responsibilities, reporting lines and risk tolerance levels.

Identification, Risk Assessment & Control

- A process should be in place to identify cyber threats and conduct assessment on the effectiveness of mitigating measures and manage cyber risks within the tolerance levels.
- A self-assessment tool (as part of the ERM program) should be put in place to identify and map its information assets or critical functions, evaluate inherent cyber risks, and assess business impact.

Continuous Monitoring

- A systematic monitoring process for detection of cyber incidents should be maintained including network monitoring, security testing, internal and external audits of cybersecurity framework, policy, standard, procedures, and systems.
- All elements of the cybersecurity framework should be tested at least annually using different techniques and latest methodologies such as vulnerability assessment, penetration testing, and scenario-based testing.

Response & Recovery

- Incident response plan should be developed covering different scenarios of cyber incidents.
- Incident response drills should be conducted at least annually.
- Incident should be reported to the Insurance Authority no later than 72 hours after detection.

Information Sharing & Training

- Authorised Insurers should gather and analyse relevant cyber risk information and participate in cyber threat information sharing groups.
- Cybersecurity awareness training should be provided to all system users, taking into account the type and level of cyber risk the Authorised Insurer faces and the latest cyber threats.

pwc

PwC was recognized as a leader in Cybersecurity Consulting for 2 consecutive years in 2017 and 2018 by ALM consulting.

The ALM Vanguard: Cybersecurity Consulting, ALM Intelligence

PwC is a recognised leader in Digital Forensics and Incident Response Services. Amongst the 14 evaluated vendors, PwC had the highest score in the Current Offering category.

The Forrester Wave™: Digital Forensics And Incident Response Service Providers, Q3 2017

How PwC can help?

- Our team is comprised of professionals with expertise spanning multiple disciplines bringing substantial knowledge and experience from across the entire cybersecurity lifecycle – from assessment, strategy, design, implementation, operations and incident response, including data privacy, outsourcing and offshoring, regulatory compliance, technology and operations, risks and controls. **Our team can help you expedite the preparation process to meet the new cybersecurity guideline requirements.**
- We have developed a mature cybersecurity advisory and independent assessment approach which meets the regulator's expectations.
- You may choose **any combination of our service components** to meet your specific requirements.
- We will ensure **knowledge transfer** so that your team can build and operate a sustainable process going forward.
- An effective approach to **help you throughout the preparation process to get ready for the new cybersecurity guideline.**

About PwC's Cybersecurity and Regulatory Advisory Services

Providing a blend of assurance and advisory skills, our Cybersecurity and Regulatory Advisory Services practice is able to leverage deep experience from PwC's strong footprint in Hong Kong, Mainland China and Asia. We have the largest dedicated team in Asia to provide local knowledge and experience. Our partners and staff are dedicated to providing objective and tailored business insights and solutions to turn regulations into opportunities and growth.

For more information, please contact:

Kenneth Wong
Partner
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

Gary Ng
Partner
+852 2289 2967
gary.kh.ng@hk.pwc.com

Lars Nielsen
Partner
+852 2289 2722
lars.c.nielsen@hk.pwc.com