Security

Cybersecurity laws keep HK companies on their toes

by Gigi Onag | Dec 21, 2018 12:00pm

Hong Kong companies are still grappling with the impact of new cybersecurity laws, particularly the China Cyber Security Law and the General Data Protection Regulation (GDPR), which took effect on June 1, 2017 and May 25, 2018 respectively.

Lost in interpretation

Dominic Wai, partner, ONC Lawyers

"Many of the bigger companies and those with business in the EU or Mainland China have taken extensive steps and made investment in enhancing their cybersecurity systems and staff training to cope with the requirements of GDPR and the China Cyber Security Law," says Dominic Wai, partner at ONC Lawyers.

However, he notes that many small- and middle-sized enterprises are still adopting a wait-and-see approach to see whether the regulatory authorities will really take enforcement actions against overseas enterprises on any violations of the cybersecurity regulations.

"These enterprises may not be properly prepared to cope with the requirements or the investigations that would ensue if there was a breach of GDPR or the China Cyber Security Law," Wai says.

Daniel Kwong, chief technology and innovation officer, CITIC Telecom says.

Furthermore, he points out that many companies have limited understanding of the compliance process because the laws are new to them.

"And because they do not get enough advice on the issues, they may not get a full picture on what these issues are. Hence, they are not likely to form a solid interpretation of the laws," Kwong says.

But this dilemma is understandable given the current situation.

Wai says: "One of the many challenges is that the scope, interpretations and applications are still not clear, which makes it difficult for enterprises to know or understand how they could comply with the law, or whether what they have been doing might or might not be violating the laws."

He adds that one common mistake of many companies is assuming the laws do not apply to them because they have no operations or business in the EU or Mainland China.

"The best thing to do if their business operations involve the processing of personal data—whether by the enterprise itself or via a third party processor— is for the company to review their processes for handling personal data carefully and thoroughly. This is to ensure that the relevant requirements under the law, such as cybersecurity standards and notification requirements are met," Wai says.

The silver lining

Amid uncertainties around the new laws, the current reality of tighter control over data privacy is leading companies to shape up and conduct their cybersecurity hygiene.

"The concept of a good privacy practice is not new to many of the Hong Kong enterprises given that Hong Kong has the Personal Data (Privacy) Ordinance in place years ago. However, the requirements [of the new cybersecurity laws] still have slight differences in areas such as data breach notifications and explicit consent among others," says Keith Yuen, cybersecurity leader, EY Greater China Advisory.


Keith Yuen, cybersecurity leader, EY Greater China Advisory.

"In order to fully comply with the regulation—even though these relevant regulations have been enforced for some time now—enterprises are still working on this in terms of cybersecurity posture and there is far more work that needs to be done," Yuen says.

Yuen observes that organizations with outbound business and operations are facing the pressure of complying with multiple regulatory requirements as they crop up around the world.

And with the China Cyber Security Law, the scope covers much boarder areas than just privacy. It includes multi-level protection system, real-name registration, and critical information infrastructure to name a few.

Since it took effect, Chinese regulators have conducted selected investigation on enterprises across various industries based on the new established law and regulations.

There are reported cases for different non-compliances which resulted in monetary penalties or warnings and these affected enterprises are required to remediate those violations within a given time.

As a result, a majority of organizations in China have started to initiate different programs to assess their current position against the law, and to identify gaps and corresponding remediation action plan to fix the issue, according to Yuen.

"These enterprises would either allocate additional resources or outsource third party consultants to go through their business processes and business models again to take stock of how information especially personal information is collected, processed and stored," Yuen says. "They will also invest further in strengthening their security governance to ensure that proper controls are in place for the collection, use and storage of personal information."

He adds that some companies also budget extra spending in their annual IT plan for the purchase of data protection tools or incident monitoring system to enhance the incidence reporting mechanisms. In terms of security management, a privacy officer position is created in some enterprises to solely handle this matter and more regular assessments and/or audits are conducted as a governance control within the enterprises.

"Therefore, although the implementation of the regulations forces the enterprises to spend extra investment, it does bring a positive impact to their security posture," Yuen says.

Adopt a security framework

With new cybersecurity laws expected to be enforced in other countries, Yuen says an ad hoc approach in handling compliance to data protection/cybersecurity regulations is not effective.

Alan Lee, executive director of Advisory Services, EY, also says: “A sustainable cybersecurity framework is necessary for an organization to ensure that cyber risk is managed.”

By implementing a cybersecurity framework and executing its activities, top management can measure and supervise cyber risks and threats continuously.

“An organization should implement the three lines of defense concept to appropriately manage cyber risk. The first line of defense is responsible for day-today activities—monitoring and protecting information assets. The second line of defense is responsible for governing those tasks and ensuring that information assets have applicable monitoring, reporting and tracking; and the third line of defense is responsible for ensuring compliance,” Lee says.

“In addition, companies can also consider adopting some international best practices such as ISO 27001 and NIST:CSF. By adopting these frameworks, companies do not only provide guidelines for implementation based on international best practices, but also demonstrate to their key stakeholders about their commitment in fighting cyberattacks,” says Lee.

Compliance is a long-term journey

EY executives say that compliance to new cybersecurity laws is a long-term journey and not a one-off project.

“Organizations often implement various technologies without addressing the people and process aspects. In fact, these should not be considered as an IT project and the requirements could not be addressed purely by technology tools,” Lee says.

They should be addressed by an enterprise-wide risk management program involving all business units, he adds.

“Data mapping is critical to these compliance projects as organizations are required to understand the current state of personal data processing activities and such activities could not be completed by the IT team alone. Without understanding the data flows relevant to the organizations including the transferees, the organizations would not be able to determine effective data protection measures,” Lee says.

SIDEBAR

Daniel Kwong, chief technology and innovation officer, CITIC Telecom CPC

Challenges to understanding cybersecurity laws

• Identification of personal information from different systems—different systems have their own rules and the interpretation of personal information may vary. Without accurate identification of personal information based on each law, companies may be at risk of violating the regulations.

• Some laws have special requirements for CIIO (Critical Information

Infrastructure Operators)—companies need to see whether they have fall into those categories.

• Data location and cross-border process—Some laws may have special requirements on the location for data storage and data cross boarder process. For example, under GDPR, personal data that is associated with EU citizens should be processed and stored within EU borders. Any transfer of personal data to a third country can take place only if certain conditions are met by the data exporter and the data importer.

• Penalties and legal liability—As the laws are relatively new and it’s hard to get concrete explanations on every rule, enterprises are at risk of violating the laws and get penalized or bear legal liabilities.

Daniel Kwong, chief technology and innovation officer, CITIC Telecom CPC

Read More On

cyber law Cybersecurity China Hong Kong GDPR Ernst & Young Akamai CITIC Telecom CPC