KPMG 30+ YEARS IN VIETNAM & CAMBODIA

Technical Update

March 2024

IMPLICATIONS OF CYBER ATTACKS ON PRIVACY COMPLIANCE IN VIETNAM

In Vietnam, approximately 13,900 cyberattacks were reported targeting systems nationwide. Over the past five years, more than 83,000 computers and servers fell victim to attacks involving encryption ransomware in 2023. [1] Most cyberattacks targeted businesses operating in the digital environment or offering online services, such as those in finance, e-commerce, telecommunications, and technology, such as securities firms, banks, and IT companies.

Cyberattacks pose a threat to both individuals and organizations. They jeopardize individuals by, potentially, compromising their banking and investment accounts and misusing their personal information for unlawful activities. Meanwhile, business operations may be disrupted, reputation damaged, and legal repercussions may occur if inadequate cybersecurity measures are not implemented. Furthermore, cyberattacked organizations are likely to be evaluated by competent authorities for compliance with (personal) data protection laws.

To mitigate the risk of non-compliance, organizations must become familiar with and adhere to existing regulations.

1. How Vietnam's privacy laws address cyberattacks

a. *Personal data protection (PDP) Decree*

Decree No. 13/2023/ND-CP (or "Decree 13"), which focuses on personal data protection, does not specify measures for safeguarding personal data. According to Article 26 of Decree 13, entities processing personal data must implement two primary protective measures: managerial and technical. Further, Article 23 mandates that organizations in control of personal data must report any violations of personal data protection laws, such as breaches or cyberattacks, within 72 hours.

A decree is being drafted to establish administrative penalties for data breaches, in order to hold organizations accountable for disregarding their responsibilities as outlined below. The lack of explicit regulatory protective measures necessitates companies to consult additional industry-specific regulations and network security regulations to safeguard themselves.

b. *Network Information Security regulations*

In 2015, Vietnam enacted a comprehensive law on network information security to safeguard against cyber threats. In the Law on Network Information Security, the principles of securing information systems within the country, including networks and servers, are outlined. For information systems that support online services or government functions, Decree No. 85/2016/ND-CP and Circular No. 12/2022/NHNN provide detailed security standards and practices.

From managerial to technical aspects of security, these documents emphasize creating and updating information security policies, forming specialized security teams, and securing human resources.

On the technical side, the guidelines require the implementation of secure network zones, remote management practices, access control, intrusion prevention, and malware defenses. In addition, they call for more rigorous security protocols, including improved network architecture, data protection, and emergency recovery plans to ensure operational continuity.

[1] According to the Vietnam Cyber Security Summary Report in 2023 conducted by Vietnam National Cyber Security Technology Joint Stock Company (NCS) [https://ncsgroup.vn/tong-ket-an-ninh-mang-viet-nam-nam-2023-va-du-bao-2024/]

For general noncompliance, fines range from VND 10 million to VND 30 million, and for not responding promptly to security incidents, fines range from VND 30 million to VND 70 million.

With the Vietnamese government committed to protecting personal information, enforcing Decree 13 will result in severe penalties if data breaches occur.

c. Sectoral regulations

There are specific industry-specific regulations tailored to ensure network information security, which address the unique needs of each industry.

For instance, article 20 of Circular 121/2020/TT-BTC stipulates strict regulations for the securities sector. Securities firms that offer online trading services must ensure uninterrupted and efficient transactions while ensuring the security, integrity, and confidentiality of their systems. They must set up robust operating, managing, and usage procedures for their online trading systems and maintain backups and contingency plans. The provisions highlight the importance of network information security within the securities industry, with noncompliance attracting fines between VND 100 million and VND 150 million.

In the banking sector, Circular 09/2020/TT-NHNN details a thorough management framework and technical measures for safeguarding IT assets, including information, physical, and software assets. As part of management measures, all IT assets associated with information systems must be catalogued, updated annually, and appropriate security measures must be applied based on the system classification. A technical strategy includes data encryption, loss prevention strategies, mobile device and removable media policies (such as disabling devices, remotely wiping data), managing software assets, and updating security patches regularly.

To prevent conflicts of interest and ensure effective oversight, legal representatives must also be directly involved in information security, incident response, and staff role segregation.

2. What companies need to do:

Although Decree 13 does not provide specific mandates on the actions companies must take for personal data protection and cyberattack prevention, the legal framework comprising the Network Information Security Law, Decree 85, and Circular 12, coupled with penalties under Decree 15, will continue to ensure compliance with information security practices among companies managing information systems.

As a result, in order to reduce the company's legal risk in the event of a data breach, it is essential that the company adhere to established technical standards for network information security, along with fulfilling its obligations under the Network Information Security Law and regulations applicable to its industry.

How KPMG can help

Our assistance in meeting general regulatory requirements encompasses a wide range of areas. We assist organizations in understanding and complying with regulatory obligations, such as data protection laws, cybersecurity frameworks, and industry-specific regulations. Our team stays up-to-date with the latest legal requirements, ensuring that our clients are well-informed and prepared to meet compliance obligations.

Our support includes developing compliance programs, conducting risk assessments, and providing training on compliance best practices. We also offer advice on data privacy regulations, such as the General Data Protection Regulation (GDPR) and Decree 13, and assist businesses in developing and implementing appropriate policies and procedures to protect customer data.

Together with our IT Advisory experts, we offer a one-stop solution to help businesses navigate the ever-changing legal landscape.

Explore more about:

- Personal data protection (PDP) Regulation - Legal Services

Contact us

Hanoi

46th Floor, Keangnam Landmark 72,
E6 Pham Hung, Me Tri, Nam Tu Liem

T +84 (24) 3946 1600

Ho Chi Minh City

10th Floor, Sun Wah Tower,
115 Nguyen Hue, Ben Nghe, District 1

T +84 (28) 3821 9266

Da Nang

Unit D3, 5th Floor, Indochina Riverside Towers,
74 Bach Dang, Hai Chau I, Hai Chau

T +84 (236) 351 9051

Scan to visit our website: kpmg.com.vn

Email: info@kpmg.com.vn