

Media title: Organisations are not doing enough to protect data privacy: PwC

Author: Nguyen Huong

Source: Vietnam Investment Review on 14 March 2018

Online link: <http://www.vir.com.vn/organisations-are-not-doing-enough-to-protect-data-privacy-pwc-57108.html>

Organisations are not doing enough to protect data privacy: PwC

22:48 | 12/03/2018

Like 0 Share 0 Tweet Share Print Email

In today's data-driven society, privacy, security and trust are more vital and intertwined than ever before. But many organisations are not doing all they can to protect data privacy, according to new findings released today from PwC's 2018 Global State of Information Security Survey (GSISS).



PwC forecasts investments in advanced authentication and encryption rising in 2018

Less than half of respondents (49 per cent) say their organisation limits collection, retention, and access of personal information to the minimum necessary to accomplish the legitimate purpose for which it is collected.

Only 51 per cent of respondents have an accurate inventory of where personal data for employees and customers are collected, transmitted, and stored. And only 53 per cent require employees to complete training on privacy policy and practices.

Media title: Organisations are not doing enough to protect data privacy: PwC

Author: Nguyen Huong

Source: Vietnam Investment Review on 14 March 2018

Online link: <http://www.vir.com.vn/organisations-are-not-doing-enough-to-protect-data-privacy-pwc-57108.html>

When it comes to third parties who handle personal data of customers and employees, less than half (46 per cent) conduct compliance audits to ensure they have the capacity to protect such information. And a similar number (46 per cent) say their organisation requires third parties to comply with their privacy policies. The survey draws on responses of 9,500 senior business and technology executives from 122 countries.

Sean Joyce, PwC's US cybersecurity and privacy leader said: "Using data in more innovative ways opens the door to both more opportunities and more risks. There are very few companies that are building cyber and privacy risk management into their digital transformation. Understanding the most common risks, including lack of awareness about data collection and retention activities, is a starting point for developing a data-use governance framework."

Businesses in Europe and the Middle East generally lag behind those in Asia, North America, and South America in developing an overall information security strategy and implementing data-use governance practices, according to 2018 GSISS findings.

	Overall information security strategy	Requires employee training on privacy	Accurate inventory of personal data	Limits data collection, retention, and access	Audits compliance by third parties	Requires compliance by third parties
North America	59%	58%	53%	53%	47%	47%
Asia	59%	57%	55%	53%	49%	47%
South America	54%	50%	52%	47%	50%	50%
Europe	52%	47%	47%	44%	42%	44%
Middle East	31%	29%	20%	19%	26%	26%

Media title: Organisations are not doing enough to protect data privacy: PwC

Author: Nguyen Huong

Source: Vietnam Investment Review on 14 March 2018

Online link: <http://www.vir.com.vn/organisations-are-not-doing-enough-to-protect-data-privacy-pwc-57108.html>

PwC expects emerging improvements in authentication technology, including biometrics and encryption, to increasingly help business leaders build trusted networks.

The stakes are high – and there is room for improvement

Senior executives recognise the rising stakes of cyber insecurity. In PwC 21st Global CEO Survey, cyber threats entered the top 5 threats to growth for the third time, with 40 per cent of CEOs saying they were extremely concerned about this, up from 25 per cent last year.

There is some cause for optimism. 87 per cent of global CEOs say they are investing in cybersecurity to build trust with customers.

Nearly as many (81 per cent) say they are creating transparency in the usage and storage of data. But

less than half say they are taking these actions “to a large extent.” And more worrying is that less than a third of African CEOs and nearly a quarter of North American CEOs (22 per cent) say they are “not at all” creating transparency in the usage and storage of data.

The importance of building trust

Consumers have relatively low confidence that companies will use personal data in a responsible way. In the US, for example, only 25 per cent of consumers say they believe most companies handle sensitive personal data responsibly (PwC’s 2017 US Consumer Intelligence Series survey).

PwC expects emerging improvements in authentication technology, including biometrics and encryption, to increasingly help business leaders build trusted networks.

Half of respondents say the use of advanced authentication has improved customer and business partner confidence in the organisation’s information security and privacy capabilities. Also, 48 per cent say advanced authentication has helped reduce fraud and 41 per cent say it has improved the customer experience. In addition, 46 per cent say they plan to boost investment in biometrics and advanced authentication this year.

Media title: Organisations are not doing enough to protect data privacy: PwC

Author: Nguyen Huong

Source: Vietnam Investment Review on 14 March 2018

Online link: <http://www.vir.com.vn/organisations-are-not-doing-enough-to-protect-data-privacy-pwc-57108.html>

Using biometrics, however, creates its own exposure to privacy regulation and public concern as it relates to companies needing to track biometric information. And relying on knowledge-based authentication—when users provide a mother’s maiden name, for instance—potentially leaves an organisation vulnerable to attack if the knowledge is stolen in a separate breach.

PwC also expects increased pressure on industry to encrypt data for protection, which will drive related investments. Among financial sector respondents, 46 per cent say they plan to increase investment in encryption this year.

Data privacy: a matter for the corporate board

Less than a third (31 per cent) of 2018 GSISS respondents say their corporate board directly participates in a review of current security and privacy risks. For organisations worth more than \$25 billion the figure is only a bit higher (36 per cent).

Paul O'Rourke, PwC's Asia Pacific cybersecurity and privacy leader said: “Organisations of all sizes should boost the engagement of corporate boards in the oversight of cyber and privacy risk management. Without a solid understanding of the risks, boards are not well positioned to exercise their oversight responsibilities for data protection and privacy matters.”

Viewing GDPR and NIS as an opportunity

The EU’s General Data Protection Regulation (GDPR), which applies to any organisation that does business in the EU, will go into effect in May 2018. Some 2018 GSISS respondents worldwide say they were already making some preparations for GDPR in the first half of 2017—a year before the compliance deadline. About a third of respondents (32 per cent) had started a GDPR assessment, for example, and this figure was a bit higher in Asia (37 per cent) than elsewhere.

Media title: Organisations are not doing enough to protect data privacy: PwC

Author: Nguyen Huong

Source: Vietnam Investment Review on 14 March 2018

Online link: <http://www.vir.com.vn/organisations-are-not-doing-enough-to-protect-data-privacy-pwc-57108.html>

The EU's Directive on Security of Network and Information Systems (NIS directive), which aims to boost cyber resilience, also goes into effect in May 2018. Businesses identified by member states as operators of essential services (critical infrastructure), as well as digital service providers (search engines, cloud computing services and online marketplaces), face new requirements under the directive for security and for reporting incidents to national authorities. As with GDPR, companies could face serious consequences for noncompliance.

Grant Waterfall, PwC's Europe, Middle East and Africa cybersecurity and privacy leader said: "CEOs should see GDPR and the NIS directive not as compliance drills but rather as strategic opportunities to align their business for success in a data-driven world. In addition, companies should be reaching out to regulators to build relationships and lines of communication before compliance deadlines arrive."

CEOs should see GDPR and the NIS directive not as compliance drills but rather as strategic opportunities to align their business for success in a data-driven world. In addition, companies should be reaching out to regulators to build relationships and lines of communication before compliance deadlines arrive.



PwC leads professional services sector in Global Brand Index

PwC increases its position amongst the world's strongest and most valuable brands.



PwC Vietnam and VNCERT form strategic partnership for cyber security incident response

In order to promote the development of national cyber security emergency response networks, PwC Vietnam is collaborating with the Vietnam Computer Emergency Response Teams to strengthen training activities ...



PwC beefs up security for rising threat of cybercrime

According to PricewaterhouseCoopers' 2016 report, around 45 per cent of boards now have a cybersecurity strategy.

By Nguyen Huong