



26 October 2017

Global State of Information Security[®] Survey 2018

At a glance...

PwC recently launched the Global State of Information Security[®] Survey 2018, based on responses of more than 9,500 senior business and technology executives from 122 countries. Themed “Strengthening digital society against cyber shocks”, the survey is focused on why businesses are vulnerable to cyber disruptions and what they can do about it.

Lack of effective preparations for cyber attacks

PwC's **Global State of Information Security® Survey 2018** shows that executives worldwide acknowledge the increasingly high stakes of cyber insecurity. 40% of survey respondents cite the disruption of operations as the biggest consequence of a cyberattack, 39% cite the compromise of sensitive data, 32% cite harm to product quality, and 22% cite harm to human life.

Yet many companies at risk of cyberattacks remain **unprepared** to deal with them: 44% percent say they do not have an overall information security strategy. 48% percent say they do not have an employee security awareness training programme, and 54% say they do not have an incident-response process.

Only **48%**
have adapted key
processes for
uncovering cyber
risks

While **44%**
say they do not
have an overall
information
security strategy

Next steps for business leaders

1 C-suite must lead the change

Senior leaders driving the business must take ownership of building cyber resilience. Setting a top-down strategy to manage cyber and privacy risks across the enterprise is essential.

2 Risk resilience as a path to rewards — not merely to avoid risk

Achieving greater risk resilience is a pathway to stronger, long-term economic performance.

3 Purposefully collaborate and leverage lessons learned

Industry and government leaders must work across organisational, sectoral and national borders to identify, map, and test cyber-dependency and interconnectivity risks as well as surge resilience and risk-management.

Key survey findings

Business leaders understand new risks tied to emerging technologies



Disruption of operations or manufacturing



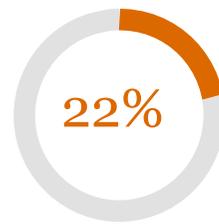
The loss or compromise of sensitive data



Harm to the quality of products produced



Damage to physical property



Harm to human life



28%

Cite mobile device exploitation as the cause of the security incident, overtaking phishing attacks as the top threat vector

59%

Say digital transformation has increased information security spending

Survey respondents report adoption of many cybersecurity and privacy leading practices:



Overall information security strategy



Employee security awareness training program



Security standards for external partners/customers/suppliers/vendors



Teams regularly meet to coordinate/communicate information security issues

www.pwc.com/gsis
Cybersecurity and Privacy

Strengthening digital society against cyber shocks

Key findings from The Global State of Information Security* Survey 2018



Read more on how businesses can build the resilience needed to withstand disruptive cyberattacks in our [report](#).

Contact us

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. For further information, please reach out to us.



Robert Trong Tran

Director, Cyber Security and Privacy Services

Tel: +84 28 3823 0796 Ext. 1007

Mobile: +84 (0) 932 756 125

Email: robert.trong.tran@pwc.com

www.pwc.com/vn



facebook.com/pwcvietnam



youtube.com/pwcvietnam



linked.com/company/pwc-vietnam

At PwC Vietnam, our purpose is to build trust in society and solve important problems. We're a member of the PwC network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory, tax and legal services. Find out more and tell us what matters to you by visiting us at www.pwc.com/vn.

©2017 PwC (Vietnam) Ltd. All rights reserved. PwC refers to the Vietnam member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.