www.pwc.com/sg

Reclaiming cybersecurity

The Global State of Information Security® Survey 2016 – Singapore highlights

pwc

Cyber-threats intensified in the past year

Many executives are declaring cyber as the risk that will define our generation. This publication highlights some of the key findings from our global report, a joint effort with *CIO* and *CSO*, *The Global State of Information Security® Survey 2016*. It includes local figures based on responses by participants in Singapore, and some food for thought for management to strengthen their organisations' cyber resilience.

The numbers have become numbing. Year after year, cyber-attacks continue to escalate in frequency, severity and impact. The total number of security incidents detected by respondents globally saw an increase of 38% this year. Here are some facts and figures, revealed by our survey findings, on security incidents over the past year.

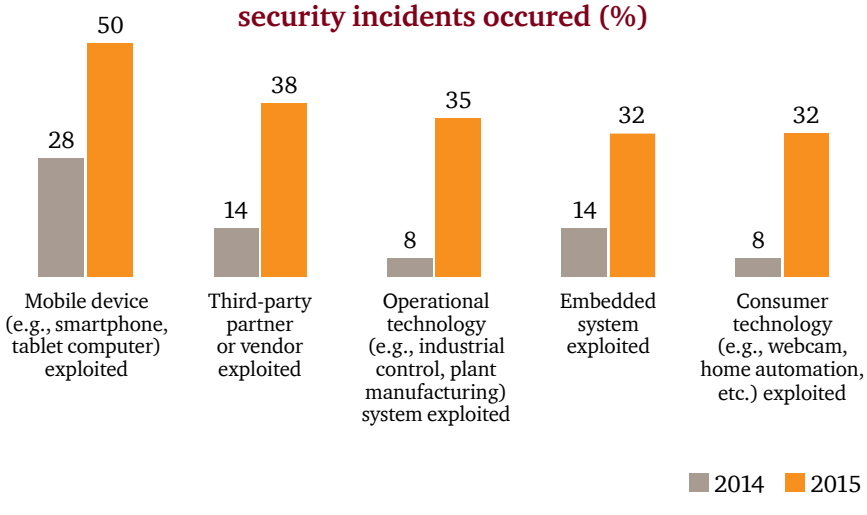
Security incidents in 2015

Global average

38% More security incidents were detected in 2015 than in 2014

56% Increase in theft of "hard" intellectual property (e.g., strategic business plans, etc.) in 2015

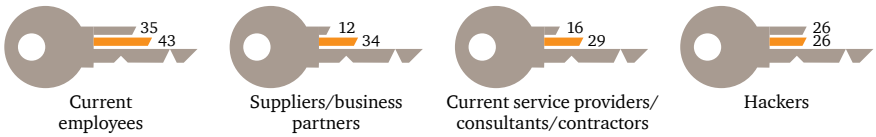
*Most common areas where security incidents occured (%)



"Some of today's most significant business trends – the explosion of data analytics, the digitisation of business functions, and the increasingly borderless and interconnected digital platforms, to name a few – have expanded the usage of technologies and data, and are creating more risk than ever before."

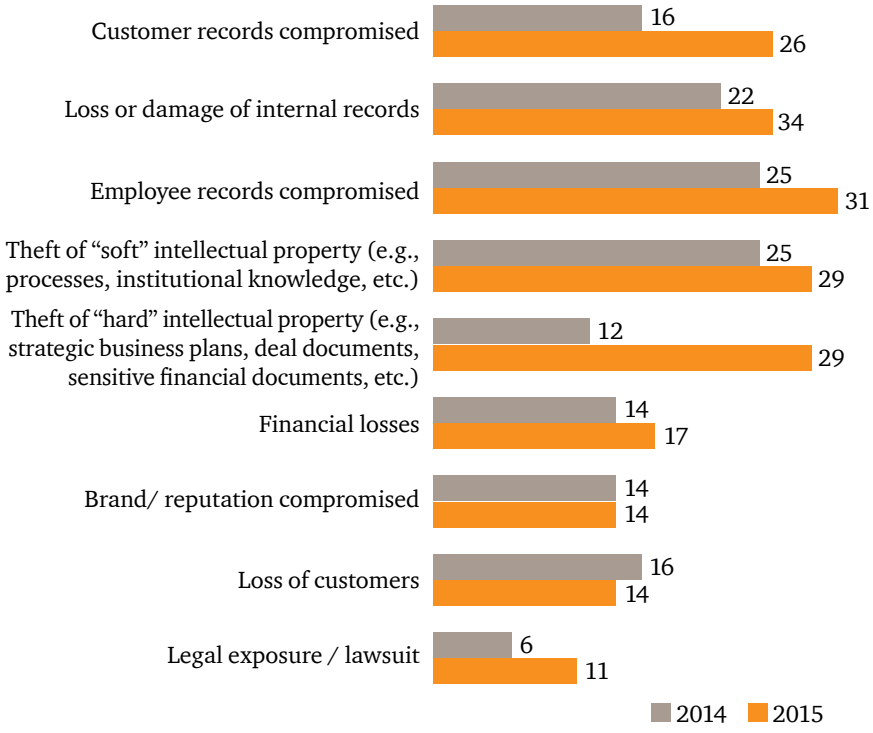
– Vincent Loy
Financial Crime and Cyber Leader
PwC Singapore

*Likely sources of security incidents (%)

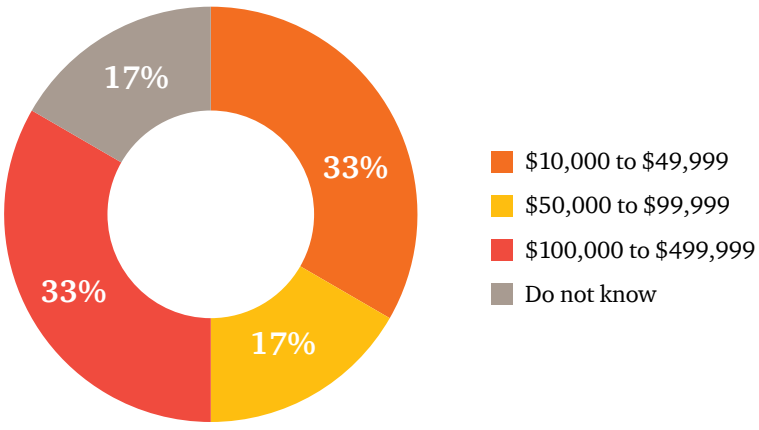


22% Global average while employees remain the most cited source of compromise, incidents attributed to business partners percentage has climbed.

*Areas where businesses have been compromised (%)



*2015 Estimated total financial losses as a result of all security incidents



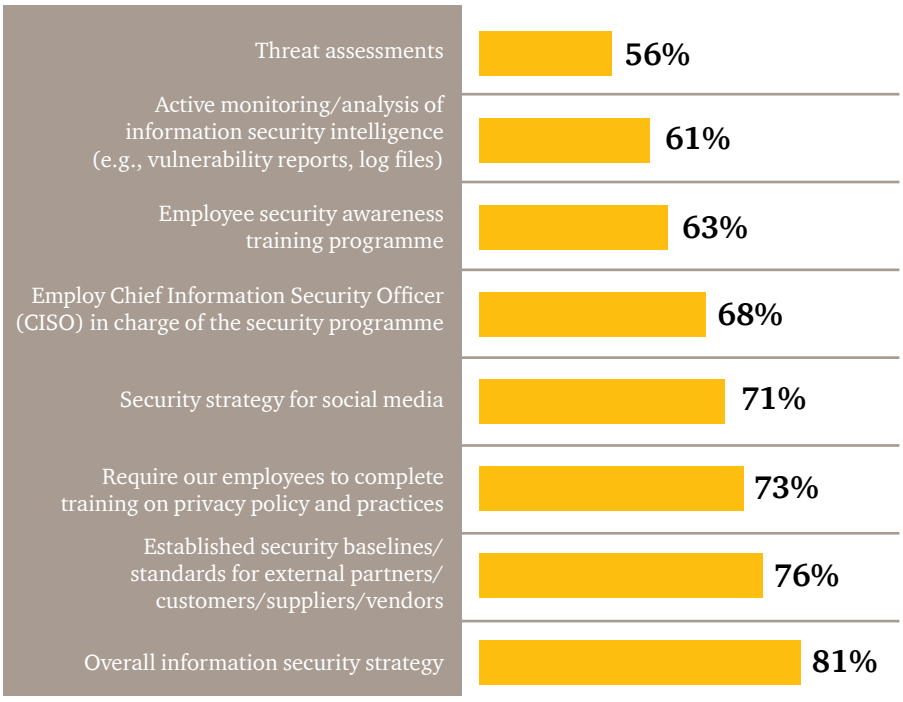
*Singapore average

Turnaround and transformation in cybersecurity

As threats continue to mount, understanding and managing cybersecurity risks have become top of mind for leaders in business and government. Increasingly, they are adopting innovative technologies like cloud-enabled cybersecurity, big data analytics and advanced authentication to reduce cyber-risks and improve cybersecurity programmes.

Businesses are also embracing a more collaborative approach to cybersecurity, one in which intelligence on threats and response techniques is shared with external partners. Internally, organisations are rethinking the roles of key executives and the Board of Directors to help create more resilient and proactive security capabilities. Here's a snapshot of how businesses are investing in cybersecurity and taking measures to manage cyber-risks.

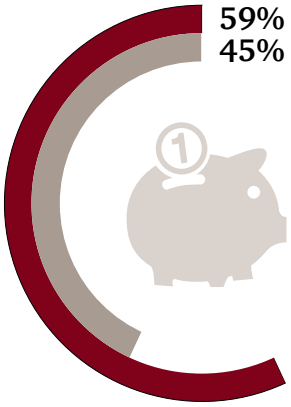
***Security safeguards businesses are investing in to defend against evolving cyber-risks**



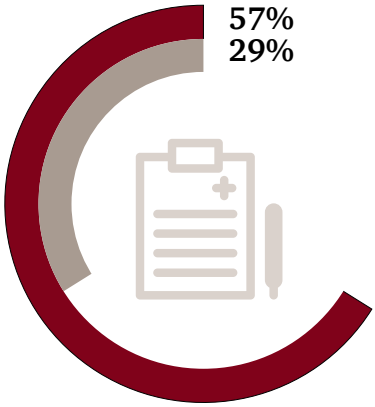
"The 'bare minimum' is ineffective against increasingly adept assaults. Businesses need to rethink their cybersecurity practices and focus on innovative technologies that can help reduce risks. The advantage will go to companies who have the right data, understand data and know how to take active steps in putting the information into good use"

– Tan Shong Ye
IT & Data Risk Leader
PwC Singapore

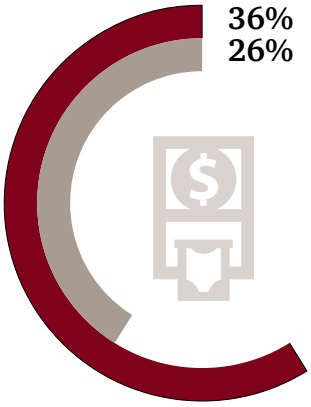
*Greater Board participation in information security



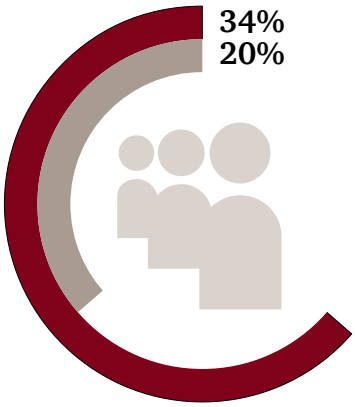
Security budget



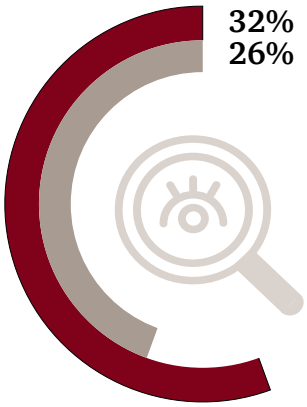
Security policies



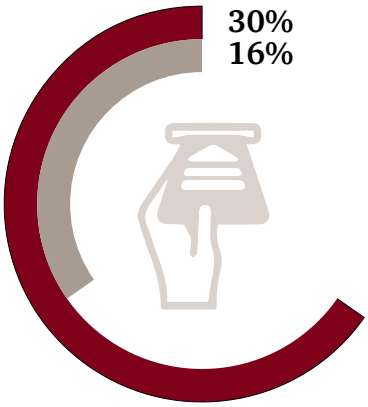
Security technologies



Review roles and responsibilities of security organisation



Review of current security and privacy risks



Review of security and privacy testing

*Singapore average 2014 2015

Leadership in achieving cyber resilience: Setting the proper tone and structure

Cybersecurity needs to be an intrinsic part of any organisation. To protect their organisations' bottom line, reputation, brand and intellectual property, the executive team needs to take ownership of cyber risk. Market leaders are transforming their organisations from ones that are centered on security and technology to ones that combine these with business management, risk disciplines and cyber threat expertise. We recommend executive management take the following steps to build cyber resilience within their organisation:

1. Establish cyber risk governance
The foundation of a strong cyber resilient organisation is a governance framework for managing cyber risks. This is established by deciding who will be on each of the teams, and setting up operating processes and a reporting structure. Connections should also be made to other risk programmes such as disaster recovery, business continuity, and crisis management.

2. Understand your cyber organisational boundary
An organisation's cyber vulnerabilities extend to all locations where its data is stored, transmitted, and accessed – by employees themselves, its trusted partners, and its customers. Organisations should also consider new areas such as big data, analytics, and social media.

3. Identify your critical business processes and assets
Organisations should determine what comprises their most valuable revenue streams, business processes, assets, and facilities. We refer to these collectively as "crown jewels." After these are identified, understand where they are located and who has access to them.

4. Identify cyber threats
Effective cyber risk monitoring focuses on building a sustainable and resilient approach to putting intelligence inputs from various teams under a common lens to quickly correlate threats in real time. Organisations should establish a robust threat-analysis capability built on shared intelligence, data, and research from internal and external sources.

5. Improve your collection, analysis, and reporting of information
Organisations should ensure their cyber risk operations team supports three primary functions to build robust cyber and technical threat intelligence capabilities. These are: collection and management, processing and analyzing, and reporting and action.

6. Plan and respond
The development of prepared responses – playbooks – is a necessary step in adequately planning and preparing responses to cyber events. Using the intelligence gathered throughout the playbook development process, each playbook says who should take action, what their responsibilities are, and exactly what they should do. Executive management should also frequently revisit cyber intelligence gathering techniques, leverage and update cyber insurance options, and upgrade cyber security technologies.

> ***"The 'cyber' challenge for companies over the next 12 months is two-fold: (1) How to prioritise investments allocated to cybersecurity (2) Finding the right balance between technologies, process and people."***

– Jimmy Sng
Partner
PwC South East Asia Consulting

Beyond the basics - Reclaiming cybersecurity through innovation

As technologies evolve and adversaries sharpen their skills, how can businesses anticipate the risks of tomorrow? Here are some innovative approaches that organisations can consider:

Leverage on Big Data analytics

A data-driven approach can shift security away from perimeter-based defenses and enable organisations to put real-time information to use in ways that can help predict security incidents. It enables companies to better understand anomalous network activity, and to quickly identify and respond to security incidents.

Harness the power of cloud-enabled cybersecurity

Cloud computing has emerged as a sophisticated tool as cloud providers steadily invested in advanced technologies for data protection, privacy, network security and identity and access management. Many also have added capabilities that enable them to improve intelligence gathering and threat modeling, better block attacks, enhance collective learning and accelerate incident response.

Partnering up to sharpen cybersecurity intelligence

As businesses share more data with an expanding roster of partners and customers, it makes sense that they also would swap intelligence on cybersecurity threats and responses. External collaboration allows organisations to share and receive more actionable information from industry peers, as well as Information Sharing and Analysis Centers (ISACs).

Insure what which cannot be protected

By now, it seems clear that technically adept adversaries will always find new ways to circumvent cybersecurity safeguards. Today, first-party insurance products cover data destruction, denial of service attacks, theft and extortion; they also may include incident response and remediation, investigation and cybersecurity audit expenses. Other key areas of coverage include privacy notifications, crisis management, forensic investigations, data restoration and business interruption.

Our Cyber-risk team

Vincent Loy
Financial Crime and Cyber Leader
+65 6236 7498
vincent.loy@sg.pwc.com

Kyra Mattar
Director
+65 6236 3850
kyra.mattar@sg.pwc.com

Tan Shong Ye
IT & Data Risk Leader
+65 6236 3262
shong.ye.tan@sg.pwc.com

Bahgya Perera
Director
+65 6236 7270
bhagya.g.perera@sg.pwc.com

Jimmy Sng
Partner
+65 6236 3808
jimmy.sng@sg.pwc.com

Maggie Leong
Senior Manager
+65 6236 3765
maggie.leong@sg.pwc.com

PwC insights on cybersecurity

As the number and sophistication of cyber-attacks increases, prevention, detection methods and cybersecurity innovation are on the rise as forward-leaning business leaders focus on solutions that reduce cybersecurity risks and improve performance. In this report, we'll show you how innovative businesses are going about this challenge, and how these efforts connect and intersect in ways that enable them to implement an integrated approach to protecting assets, reputation as well as competitive advantages.

The Global State of Information Security® Survey 2016 is a worldwide study by PwC, CIO, and CSO. The results discussed in this report are based on responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices from 127 countries.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at ***www.pwc.com/sg***.

Scan the QR code below to read the full report

pwc