www.pwc.com/id

Key Findings from the Global State of Information Security Survey™ 2017

Indonesian Insights

pwc

Key Findings from the Global State of Information Security Survey™ 2017

Indonesian Insights

By now, the numbers have become numbing. Cybersecurity incidents are daily news, with ongoing reports of escalating impacts and costs. Beyond the headlines, however, you'll find new reasons for optimism.

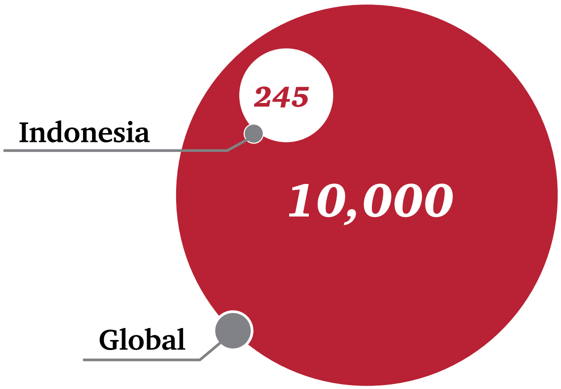
There is a distinct shift in how organisations are now viewing cybersecurity, with forward-thinking organisations understanding that an investment in cybersecurity and privacy solutions can facilitate business growth and foster innovation.

We take a closer look at how innovative businesses are responding and how Indonesian organisations are doing compared to their global peers.

Table of Contents

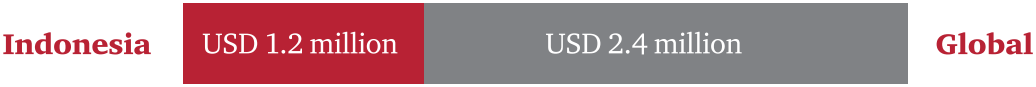
The state of cybersecurity in Indonesia

Number of survey respondents
Indonesia vs Global



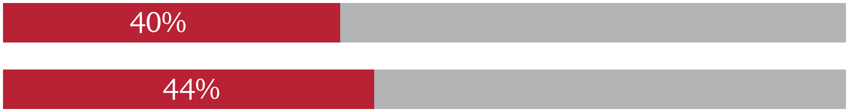
Current and former employees are still the primary source of attacks

Average financial losses in information security

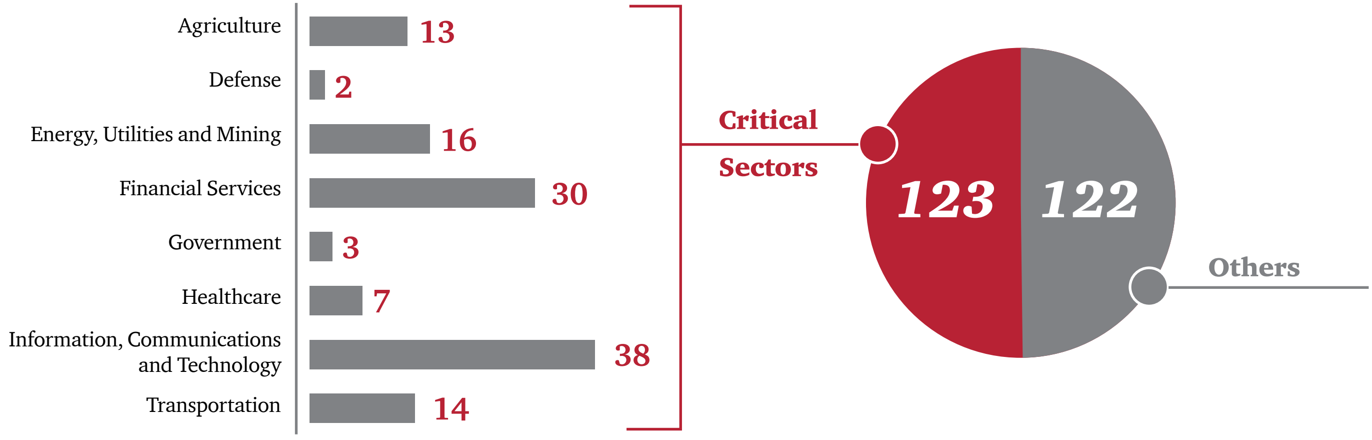


Chief Information Security Officer ("CISO"), Chief Security Officer ("CSO") or equivalent senior information security executive reports to

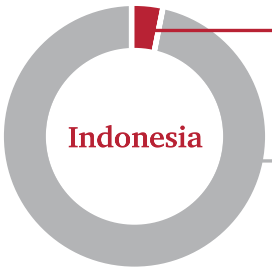
- **Board of Directors**
- **Chief Executive Officers**



Half of the respondents come from critical sectors



Average IT security budget compared to overall IT budget

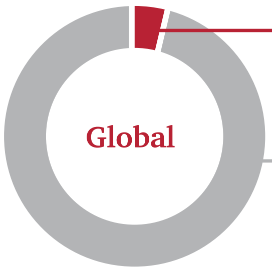


Average IT security budget

USD 1.4 million (3.2%)

Average overall IT budget

USD 44.2 million



Average IT security budget

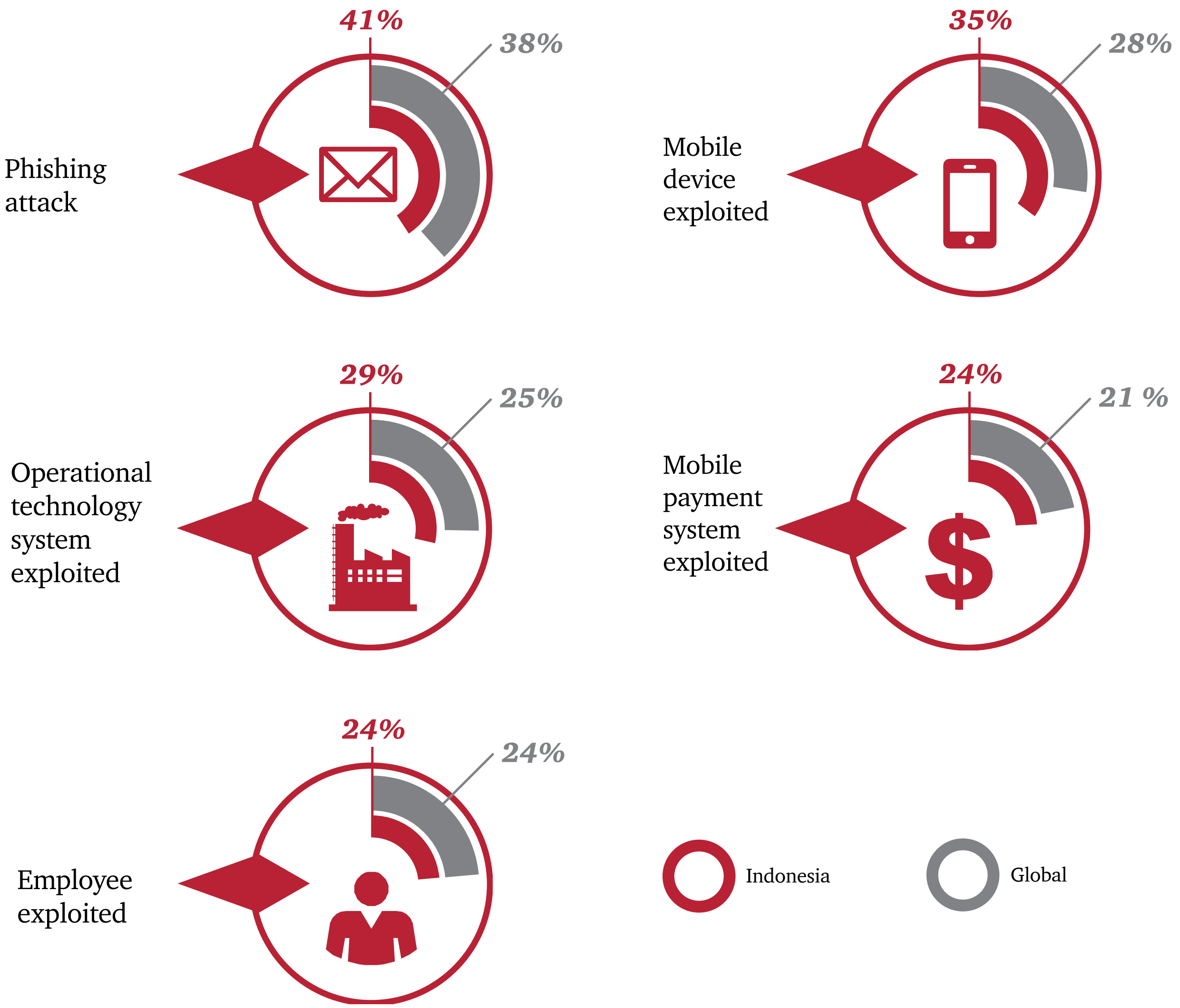
USD 5.1 million (3.7%)

Average overall IT budget

USD 138 million

Top vectors of cybersecurity incidents

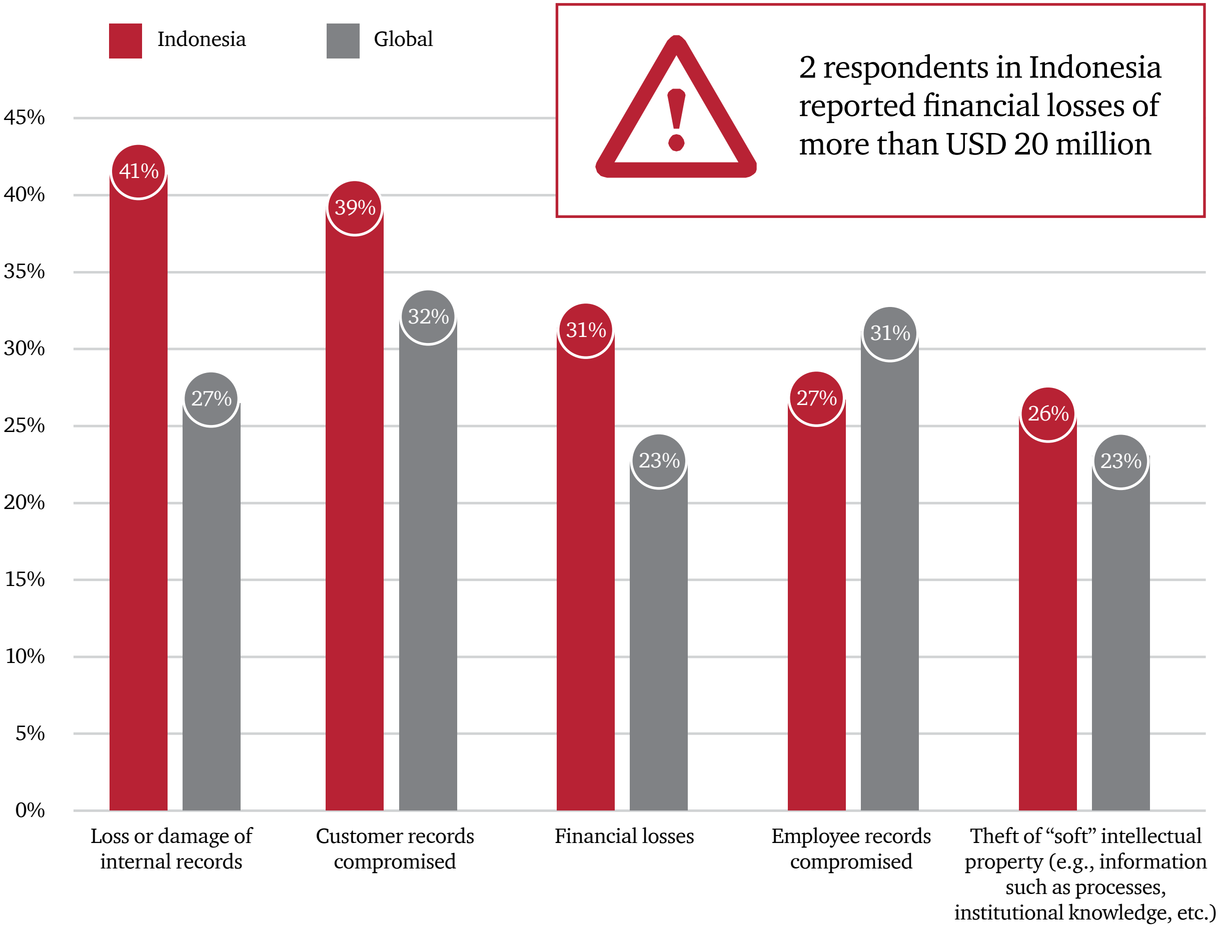
Phishing attack was cited as the top source of incidents by both Indonesian and global respondents in 2016. Increased use of mobile devices and implementation of mobile payments were also heavily exploited by attackers. Strengthening security awareness and mobile security has become more critical for businesses.



3

What are the impacts of the cyber incidents?

Most cyber incidents reported by the Indonesian respondents are related to the loss or compromise of business information such as internal records, customer, employee and intellectual information. This indicates the needs to strengthen the protection of information asset and privacy.

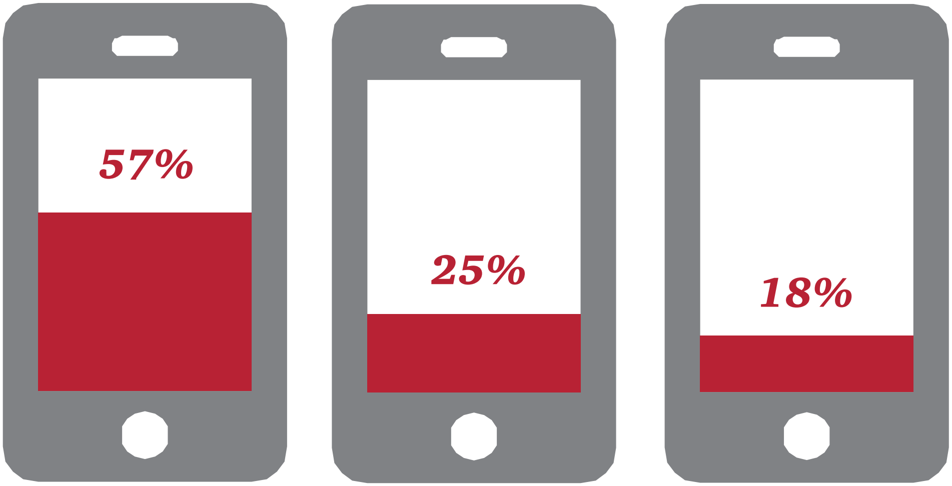


⚠ 2 respondents in Indonesia reported financial losses of more than USD 20 million

Impact of digitisation to security spending

The world's shift towards digitisation has driven companies to implement innovative products, enabling new optimisation in business processes. Many organisations now no longer see cyber security as a barrier or an IT cost, but rather a solution to facilitate business growth, create market advantages and build brand trust.

With this shift, many companies in Indonesia have decided to invest more in security as an impact of implementing digitised solutions.



Organisations investing more in security

No changes in security spending

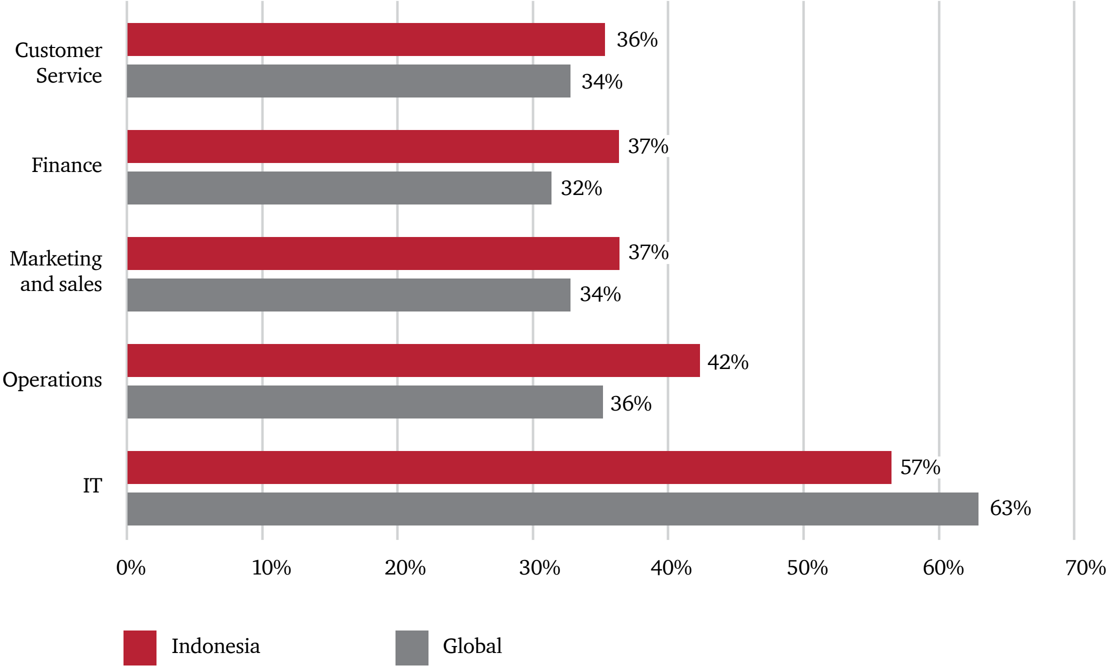
Investing less or don't know

5

As trust in cloud models deepens, organisations are running more sensitive business functions on the cloud

By now, it’s become clear that off-premises cloud-based storage of applications and data can be more secure than on-premise corporate systems. No wonder, then, that more businesses are entrusting more sensitive data and workloads to cloud providers.

Compared to the global statistics, many of the Indonesian respondents have been running their key processes on the cloud. Companies should follow this by putting proper cloud computing security practice in place.



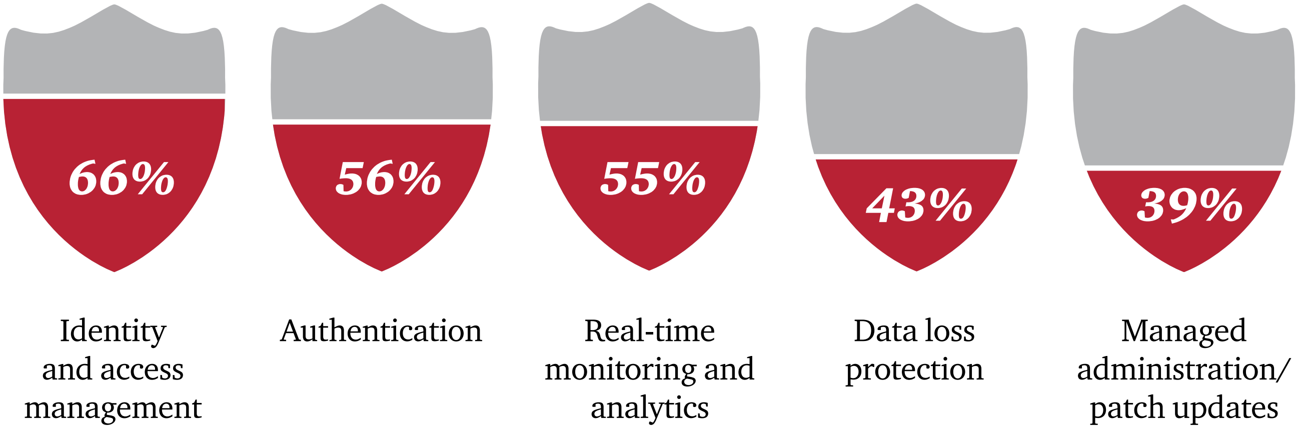
6

Respondents are embracing managed security services to extend and enhance their cyber security capabilities

Once a cyber security program is in place, disparate components must be thoroughly integrated, professionally managed and continuously improved. That's a tall order for resource-constrained organisations, and many are addressing this challenge by adopting managed security services.

54% of the Indonesian respondents have used managed security services to address their challenges in resources and costs to implement sound cybersecurity practices. This number may increase in the future as compared to the global response of 62%.

Managed security services used by Indonesian respondents in 2016

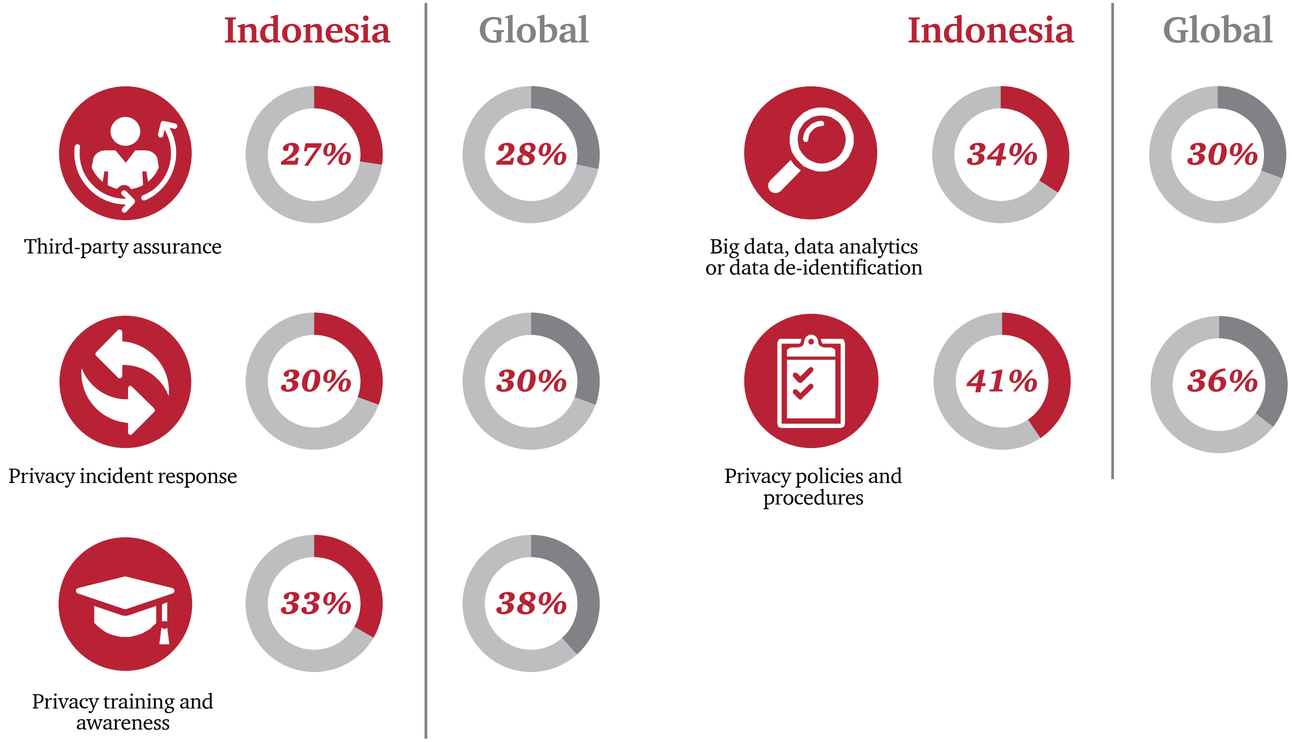


7 As data privacy becomes an increasingly critical business requirement, employee training is a top priority

Just late last year, the Ministry of Communications and Information Technology released the regulation no. 20/2016 concerning privacy protection in electronic systems.

Many Indonesian companies are starting to update their privacy policies, procedures and conduct privacy assessments.

Top privacy initiatives for 2016

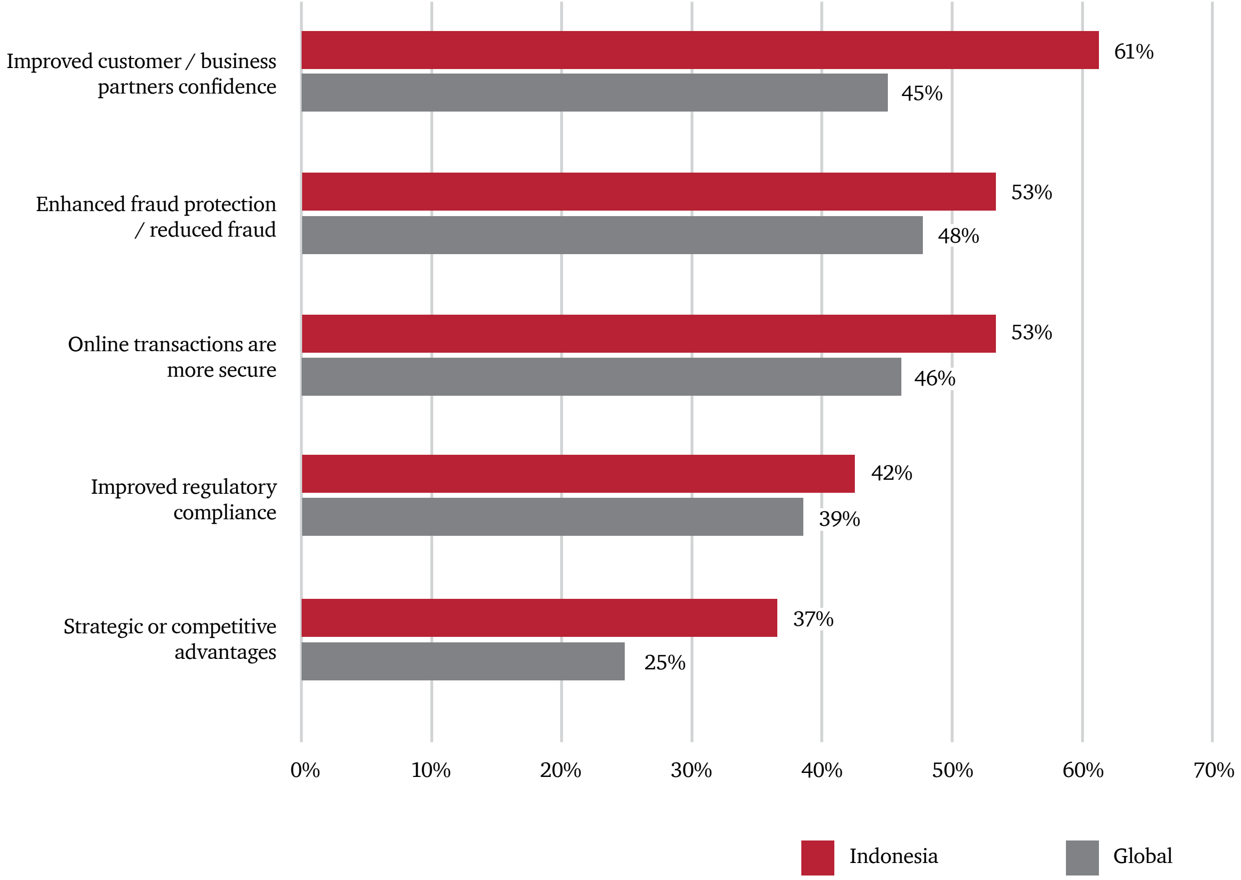


8

Benefits of implementing advanced authentication

Strong password practices are often disregarded by users and this is causing many organisations to start looking for more advanced authentication. In the past, advanced authentication was only applicable to government systems and large financial institutions. Now social media, e-commerce and email providers have introduced multifactor authentication across a range of transactions.

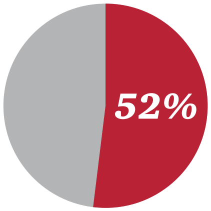
With advanced authentications, businesses are looking to add an extra layer of security and improve trust among customers and business partners.



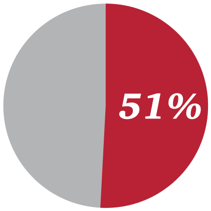
9 Collaboration to combat cyber attacks

Combatting cyber attacks is no longer a task for the individual. It requires collaborative actions at both a sector and national level. 52% of our Indonesian respondents said that a collaboration in the industry, including between competitors, have been formally undertaken to improve security and reduce the potential for future risk.

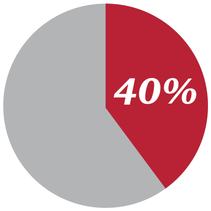
Organisations expect that through this collaboration, sharing and receiving more actionable information from industry peers will stay at the top with 51% responses, followed by sharing and receiving more actionable information with government entities (40%). Improving threat and intelligence awareness comes next with 38% responses.



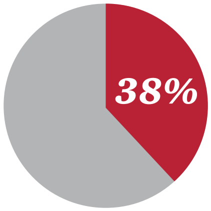
Collaboration in the industry have been done formally



Sharing and receiving more actionable information from industry peers



Sharing and receiving more actionable information with government entities



Improving threat and intelligence awareness

10 Focus of security spending in the next 12 months

Through the survey result, we’ve seen that most Indonesian organisations are going to focus their security spending to improve mostly in the capabilities, both in human resources and processes in place on top of their technology spending.

Some of the main focus on human resource / people include training on privacy policy and practices and hiring CISOs and CSOs in charge of security programmes. In the process area, developing security strategies, establishing standards for external parties and vulnerability assessment remain top priority. In the technology area, implementation of mobile device malware protection, tools to discover unauthorised devices and malicious code detection tools are at the forefront.

This is in quite a contrast to where the global result shows a relatively balanced focus between people, process and technology development in the information security focus.

Visit www.pwc.com/gsiss2017 to explore the data further

Our Team

Subianto
Partner
subianto.subianto@id.pwc.com
+62 21 5212901 ext. 90501

Chairil Tarunajaya
Partner
chairil.tarunajaya@id.pwc.com
+62 21 5212901 ext. 71315

Handikin Setiawan
Director
handikin.setiawan@id.pwc.com
+62 21 5212901 ext. 71003

Paul van der Aa
Advisor
paul.vanderaa@id.pwc.com
+62 21 5212901 ext. 71806

Jeffry Kusnadi
Senior Manager
jeffry.kusnadi@id.pwc.com
+62 21 5212901 ext. 71003

Pandu Aryanto
Director
pandu.aryanto@id.pwc.com
+62 21 5212901 ext. 71170

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

At PwC, our purpose is to build trust in society and solve important problems. We are 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.

PwC shall not be liable to any user of this report or to any other person or entity for any inaccuracy of this information or any errors or omissions in its content, regardless of the cause of such inaccuracy, error or omission. Furthermore, in no event shall PwC be liable for consequential, incidental or punitive damages to any person or entity for any matter relating to this information.

PwC will not disclose the name of any respondent without their prior approval and under no circumstances will PwC disclose individual entity data.