servicenow

Point of View

The Global CISO Study

How Leading Organizations Respond to Security Threats and Keep Data Safe in Asia

Global Issues, Regional Focus

Businesses in Australia and Singapore, the two countries we surveyed in Asia, are coming under increasing scrutiny as cybercrime evolves and laws change to keep pace. Asian countries are seen as the most likely targets of cyber-attacks in the world, with Australia and Singapore considered top-ten targets in the region.[1] In Australia, the number of detected security incidents more than doubled last year from the previous year.[2] Last year also saw Australia's largest data breach in history. Unsurprisingly, then, Singapore will now hold companies responsible for using stolen data, even if they do not know its origin, and the Australian government recently passed legislation that will require organizations to disclose any serious data breaches.

In this tumultuous environment, CISOs are coming under pressure to position their companies as information security leaders—and most are worried that the job is not getting done. It takes just one breach to not only threaten their reputation, but a business's bottom line. The survey results show that that a more robust threat response strategy is the answer, and Australian CISOs are more confident in their ability to protect critical data.

Our survey showed that respondents from Australia and Singapore, like their peers around the world, are worried about their ability to protect data and respond to threats. They say they must do more to improve organizational skills and increase the automation of security tasks. Yet compared to CISOs around the world, Australian CISOs rate themselves highly at preventing a range of security attacks.

Our key findings for the region include:

- 75% of CISOs in Asia are highly concerned that breaches are going unaddressed, and 71% are worried about their ability to detect the breach in the first place. (CISOs in other parts of the world are even more concerned.) Just 20% of Asian executives say their company is highly effective at preventing security breaches.
- Most security organizations fail to prioritize alerts based on the threatened data's importance—66% of respondents in Singapore and 72% in Australia say they have difficulty doing so, vs. 70% globally.
- CISOs in Singapore and Australia are more likely to say a lack of resources is a significant barrier to the success of their security function.
- CISOs in Australia and Singapore are betting on automation, and the pace of automation is quickening: just over one-third of respondents in Asia (38%) automate more than 40% of their security processes today, while two-thirds (66%) plan to automate that amount in three years—numbers roughly on par with global averages.

75%

of CISOs in Asia are highly concerned that security breaches are going unaddressed.

66%

of respondents in Singapore and

72%

in Australia say it is difficult to prioritize security alerts based on business criticality.

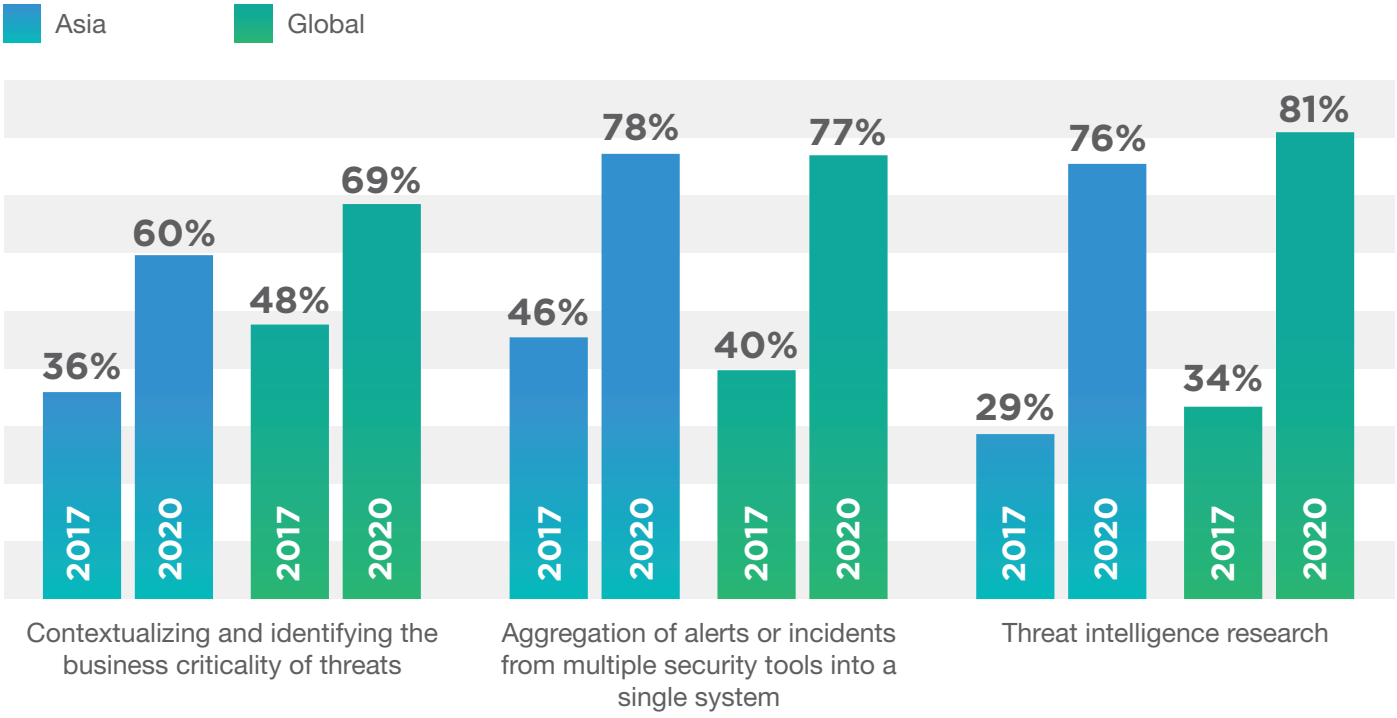
The Automation Advantage

Advances in automation hold great promise—but organizations in the region have much work left to do. Only 36% in both Singapore and Australia have automated the prioritization of alerts based on mission-relevant data today, which trails the global total of 48%. And while they lead their global peers in automating the aggregation of relevant information from business units, less than half (48% in Singapore and 44% in Australia) say they are doing this today.

Over the next three years, security functions will begin automating more strategic tasks. Threat intelligence research, aggregation of alerts from multiple security tools, and contextualizing alerts based on business criticality will see the fastest growth.

Automated tasks are growing more sophisticated

Q: Which tasks are you automating today? Which do you plan to automate by 2020?



People still matter in the age of automation. Attracting skilled talent and upskilling and retaining existing talent are rated as the most important elements to the success of security functions. Singapore is even more focused than Australia on these goals (94% cite attracting and upskilling talent, compared with 80% in Australia; 92% cite retaining talent, compared with 76% in Australia).

Meet the "Security Response Leaders" from Around the World

We filtered the global survey data to identify respondents who stand out for their security capabilities. The resulting leader group makes up 11% of the overall sample; 21% of that group comes from Australia and 15% comes from Singapore. Of all the CISOs surveyed from Australia, 14% qualified for this leader group, equaling France for the highest proportion of leaders in any participating country. In Singapore, 10% of respondents are Security Response Leaders.

To qualify as Security Response Leaders, respondents must assess themselves as highly effective at protecting against the following types of attacks:

- Breach of personal information about customers (e.g., their preferences, passwords)
- Threats from insiders within the company
- Breach of personal information about employees
- Distributed Denial of Service (DDoS) by criminals, governments, or "hacktivists"
- Breach of customer credit-card or financial information
- Watch and wait attacks (monitoring of data and activity over time to identify vulnerabilities)

As we analyzed the performance of these Security Response Leaders, we found that they tend to demonstrate more maturity than other respondents across a variety of areas.

Security Response Leaders display certain characteristics that set them apart from other organizations. Among other things, they:

- Are more focused on increasing automation to make the security function successful, and are automating more strategic tasks.
- Report tight integration with other functions across the enterprise.
- Say strong relationships between IT and security are important to the success of their success of their security function.
- Rate the prioritization of security alerts in the larger context of the business as critical to the success of their security function.
- See security as a core strategic goal for their company.

Conclusion

Keeping data safe is a global challenge, and CISOs in Asia are feeling the pressure. Data breaches may be inevitable, but organizations in Australia and Singapore must still address and respond to the same security risks. CISOs across the region must focus on automation and use technology to maximize the value of human capital in order to protect their organizations from the growing threat of security breaches.

About the research

ServiceNow and Oxford Economics surveyed 300 chief information security officers (CISOs)—including 50 from Singapore and 50 from Australia—about their strategies for navigating this challenging environment. This report covers the findings from our analysis of survey results from Singapore and Australia. Numbers for Asia represent the average results from these two countries. See our full report (https://www.servicenow.com/c-suite/ciso.html) for in-depth, global analysis from the survey, as well as real-world commentary from CISOs.

Footnotes

1. Cyber Exposures and Solutions in Asia: How risk management and insurance protect your financial statements, Aon Risk Solutions, 2014.

2. The Global State of Information Security Survey 2016, PwC.