# Achieving digital resilience:

## Security automation in Japan

Cybersecurity leaders throughout the world face a range of challenges every day. Amid an increasingly sophisticated threat landscape, complex IT infrastructure environments and widening security perimeters, they hold a vitally important role in keeping our data safe.

Given skills are in high demand, automated security tools are becoming critical for supporting the everyday activities of security professionals. To help executives understand how to take advantage of this opportunity, Omdia – in partnership with Telstra – surveyed 250 senior technology decision-makers to assess the maturity of security automation strategies across North Asia. With insights from a range of business sizes and sectors, the research arms executives with valuable new tools to bolster their cyber resilience.

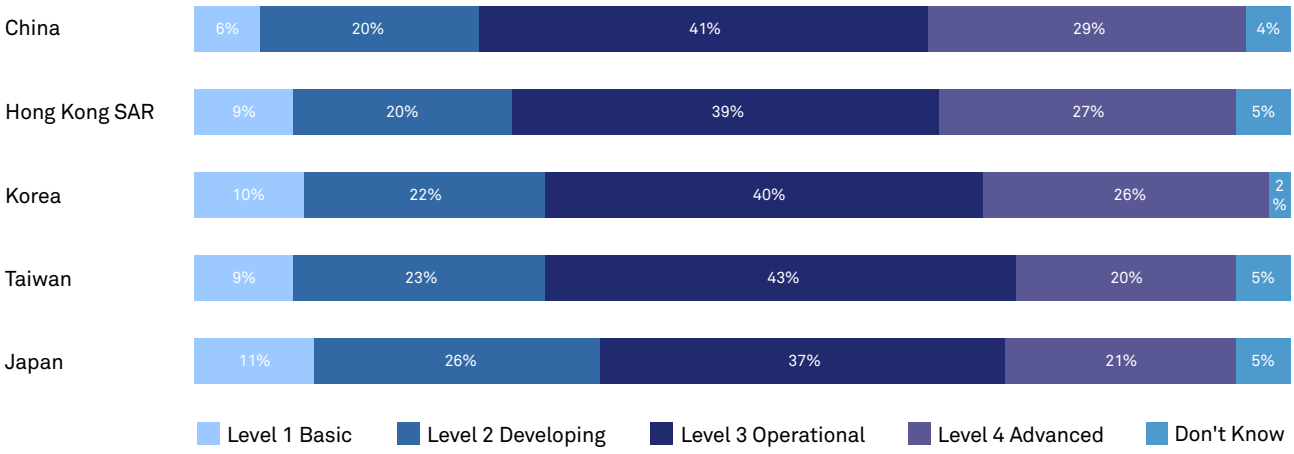
While there are common challenges, different regions and some markets show interesting distinctions. Here are some key barriers and enablers for the security automation landscape in Japan.

## The state of security automation in Japan (Maturity)

Japan has the lowest levels of security automation maturity compared to its North Asia counterparts. Fifty-eight per cent of organisations in Japan report maturity levels of three (operational) or four (advanced), compared to an average of 64% for all markets in our research.

Japan also has the highest percentage (37%) of organisations reporting levels one (basic) and two (developing) maturity levels.

**How mature is your organisation in using security automation across the cybersecurity attack framework on a scale of 1 (basic) to 4 (advanced)?**



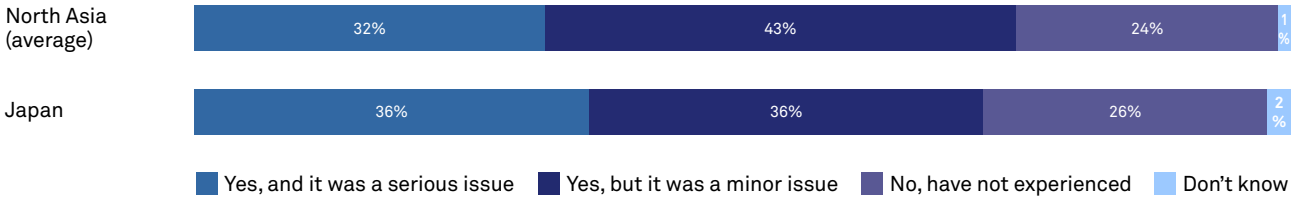

Across the five industries targeted, banking and financial services organisations reported the highest levels of security automation maturity in Japan, while transport and logistics organisations reported the lowest.

# Prevalence of security issues

Organisations throughout all regions continue to grapple with challenges around rising security incidents. That's most severe amongst Japanese respondents, who have experienced the highest proportion of 'serious' security incidents and breaches.

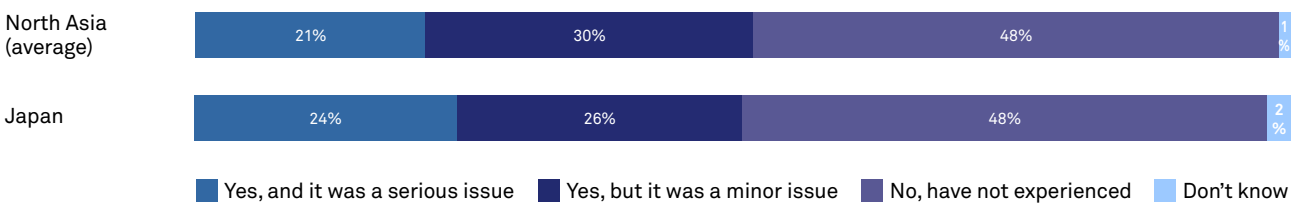
Thirty-six per cent of firms in Japan saw an increase in 'serious' attacks over the past 12 months, compared to 32% across North Asia. On the other hand, Japan recorded the lowest percentage (36%) of firms that have experienced a rise in 'minor' incidents, while 26% haven't experienced a rise at all.

**Has your organisation experienced a significant increase in overall security incidents attacking key business resources in the last 12 months?**




Japan doesn't fare much better when it comes to actual breaches, with 24% of firms having experienced a significant increase in serious breaches over the last 12 months. Again, Japan had the lowest percentage (26%) of firms reporting an increase in minor breaches, while 48% say they haven't experienced a rise.

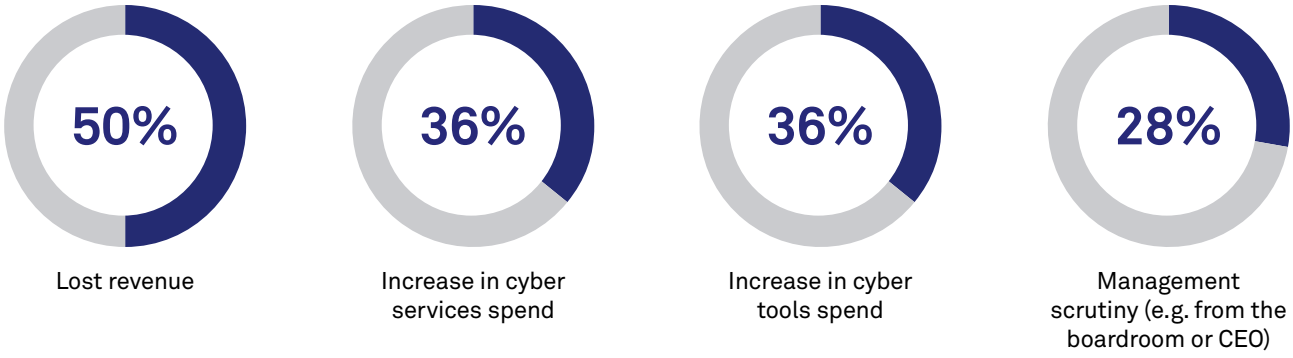
**Has your organisation experienced a significant increase in security breaches in the last 12 months?**



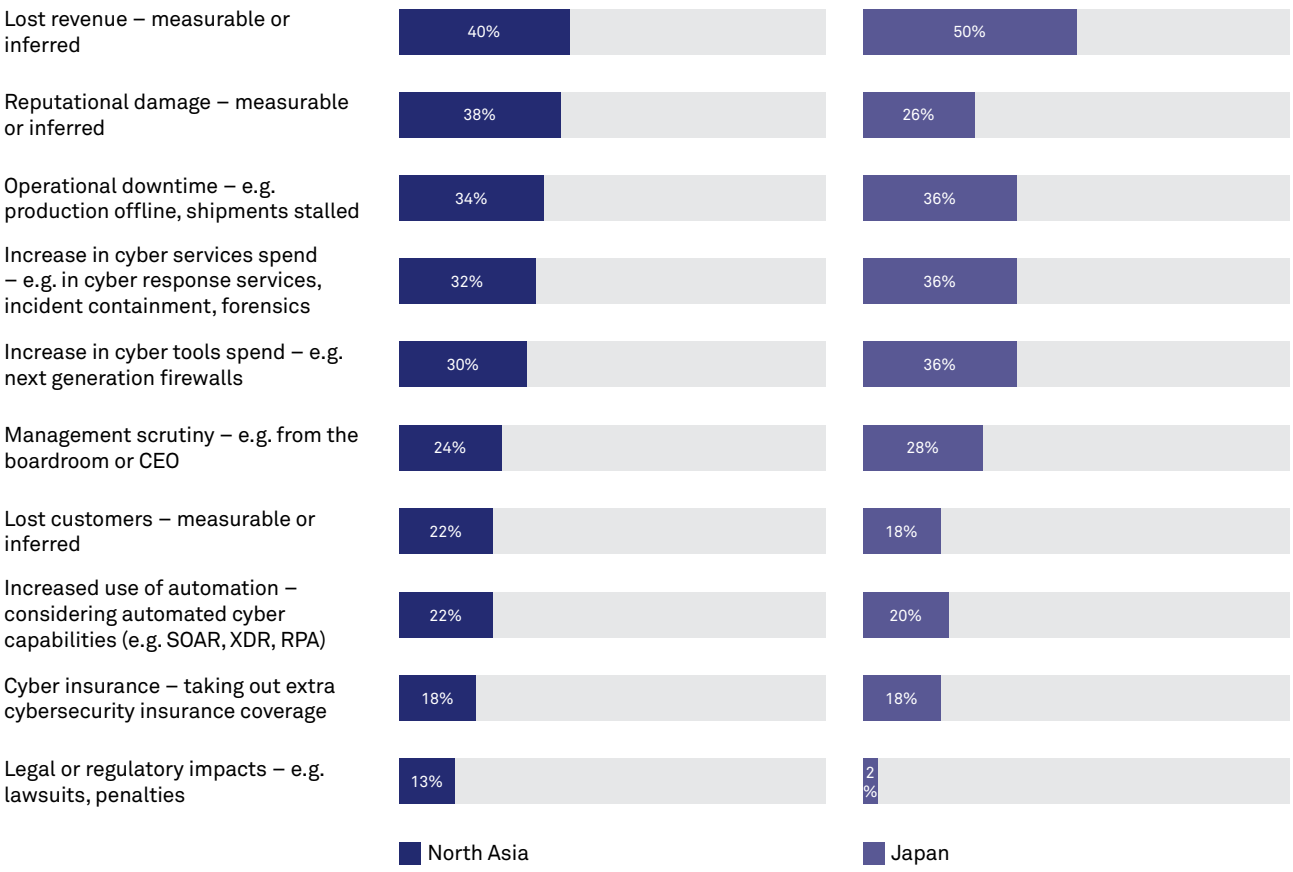
# Impact of damage

Japanese firms are the most impacted by security incidents according to our research. The country experienced the highest proportion of negative impacts, with 50% having lost revenue from incidents or breaches, compared to an average of 40% across the region.

**Japanese firms were more heavily impacted than any other country in the region in four areas:**




**In the last 12-18 months, what was the impact of the most significant cybersecurity incident or breach on your organisation?**

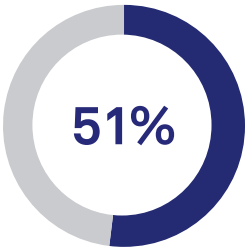


# Benefits of automation

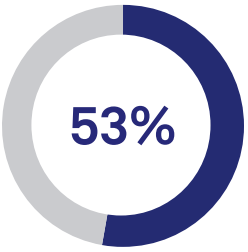
Security automation has potential to help drive a range of benefits for all organisations, particularly when it comes to reducing the time spent on repetitive, lower-value tasks and addressing false positive alerts. There is a significant opportunity for automation to help cut through this ‘noise’ in Japan, which experiences the second largest percentage (42%) of false positive alerts.

Well-architected and implemented security automation can help dramatically reduce the likelihood and impact of a severe breach. Executives in Japan believe that effective security automation could have helped reduce 53% of the serious impacts caused by incidents and breaches, which is the most optimistic in the region.

**Of the 'serious' cybersecurity incidents or breaches that impacted your organisation in the past 12 months, what percentage could have been reduced with optimised security automation?**




North Asia




Japan

Security automation is a vital tool for helping organisations improve cybersecurity resilience and fight back against the increasingly sophisticated threat landscape in Japan and around the world. It’s imperative that firms in the region identify their maturity level and put a strategy in place to build world-class automation capabilities throughout their business.

Contact your Telstra account representative for more details.

**telstra.com.hk** **telstraenquiry@team.telstra.com**