Achieving digital resilience:

Security automation in Taiwan

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.

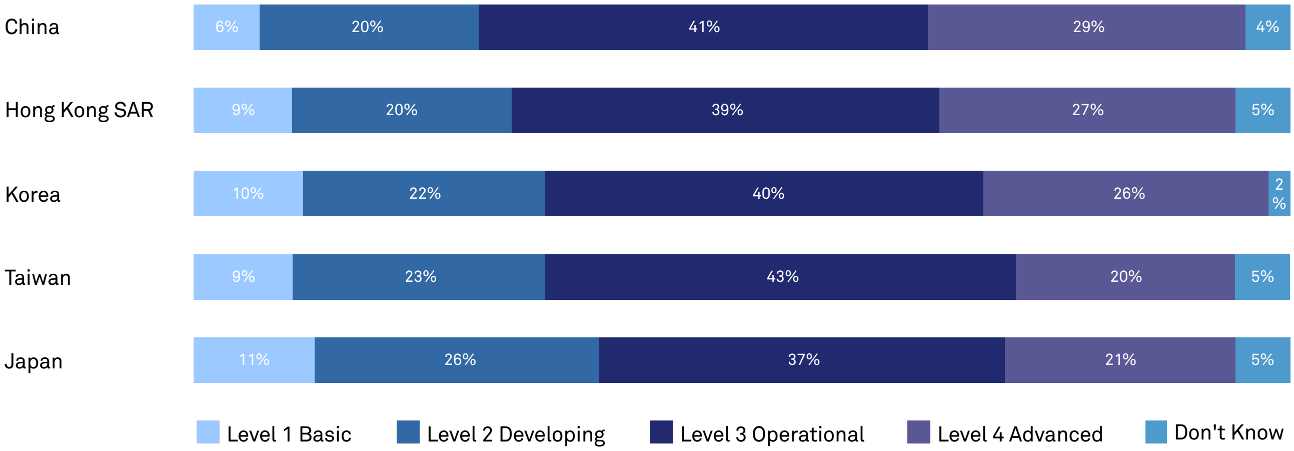
While there are common challenges, different regions and some markets show interesting distinctions. Here are some key barriers and enablers for the security automation landscape in Taiwan.

The state of security automation in Taiwan (Maturity)

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

Taiwan also has the second highest percentage (32%) 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)?

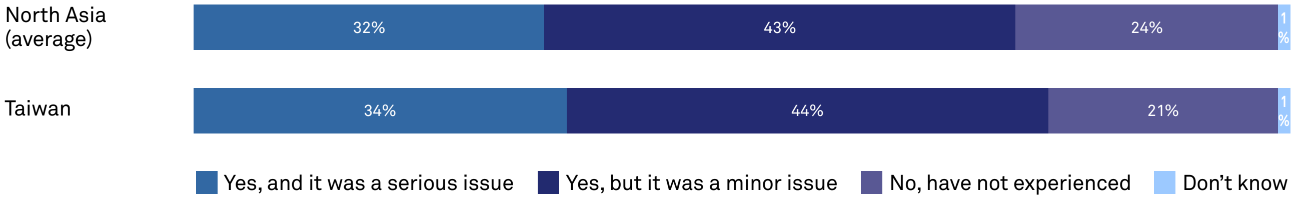


Across the five industries targeted, healthcare organisations reported the highest levels of security automation maturity in Taiwan, while transport and logistics organisations reported the lowest.

Prevalence of security issues

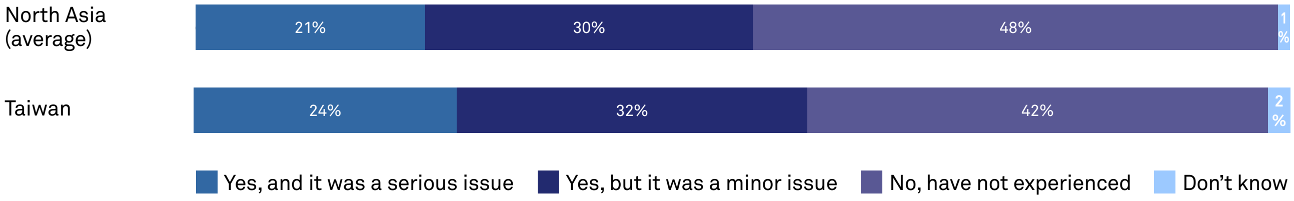
Organisations throughout the region continue to grapple with challenges around rising security incidents. That's reflected amongst Taiwanese respondents, with 34% of firms seeing an increase in 'serious' attacks over the past 12 months, the second highest across North Asia. Forty-four per cent of organisations in Taiwan also reported an increase in 'minor' incidents, with 21% reporting no increase.

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



When it comes to actual breaches, 24% of Taiwanese respondents report having experienced a significant increase in serious breaches over the last 12 months. A further 32% of firms also reported an increase in minor breaches, while 42% say they haven't experienced a rise.

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

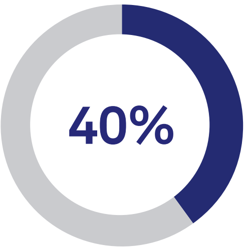


Impact of damage

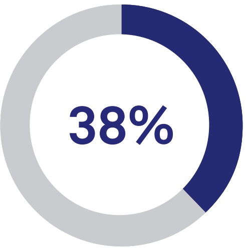
Taiwanese firms reported a range of significant impacts from security incidents. The country suffered the highest percentage of operational downtime – with 40% of respondents citing this as an issue.

Encouragingly, 26% of organisations responded to their most significant cyberattack by implementing more automated security services, which is equal to the highest in North Asia. Taiwan also tied for the highest increase in cyber services spend (36%).

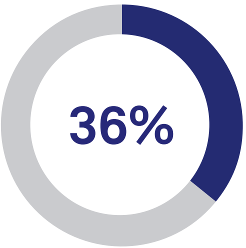
Overall, the top three impacts across organisations in Taiwan were:



Operational downtime

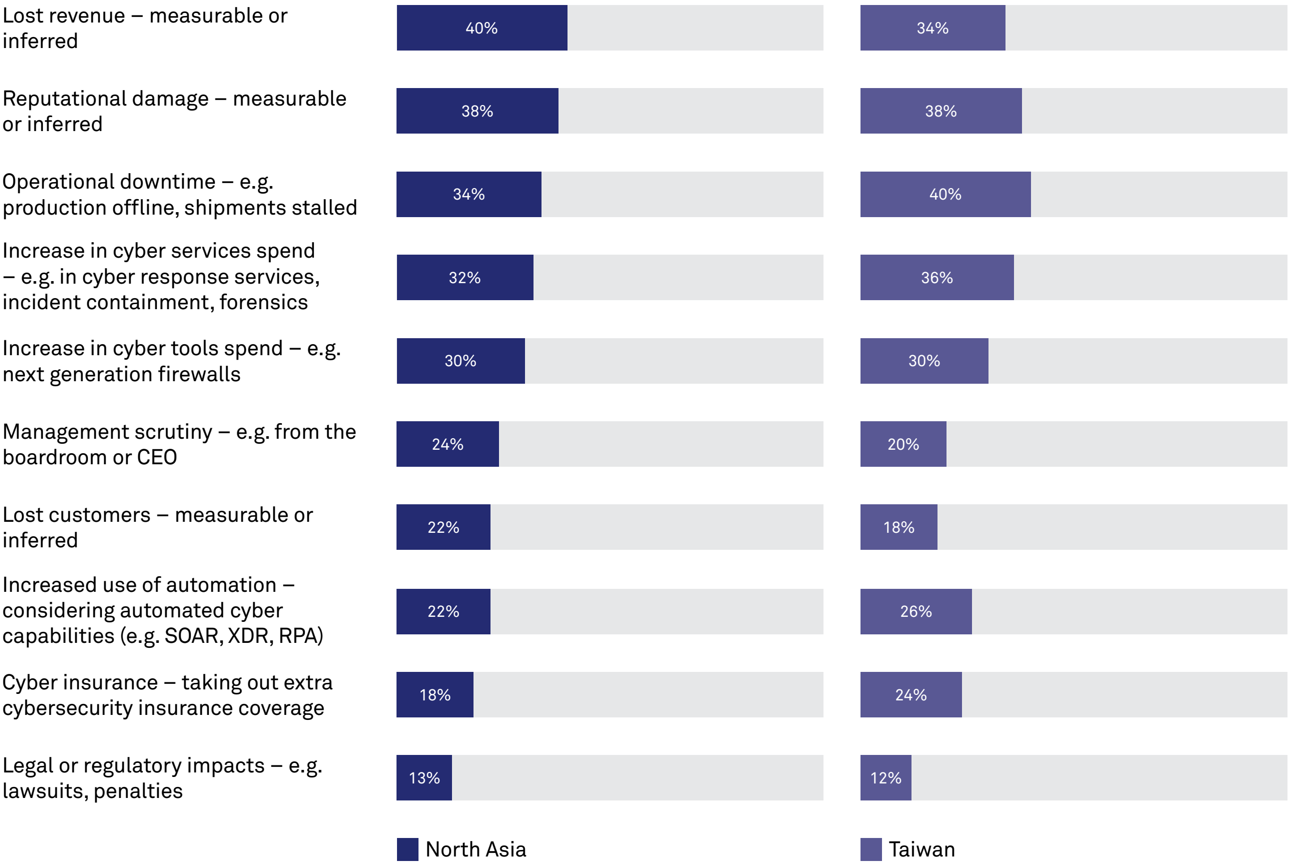


Reputational damage



Increase in cyber services spend

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

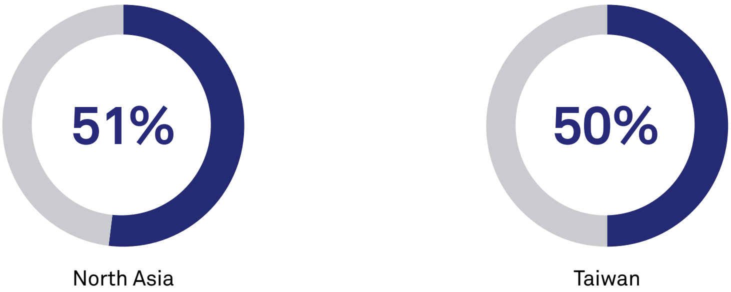


Benefits of automation

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. While Taiwan is tied for the lowest percentage of false positive alerts (41%), there remains a significant opportunity for automation to help cut through this ‘noise’.

Well-architected and implemented security automation can help dramatically reduce the likelihood and impact of a severe breach. Executives in Taiwan believe that effective security automation could have helped to reduce 50% of the serious impacts caused by incidents and breaches.

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



Security automation is a vital tool for helping organisations improve cybersecurity resilience and fight back against the increasingly sophisticated threat landscape in Taiwan 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**