Telstra

Achieving digital resilience:

Security automation in China

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.

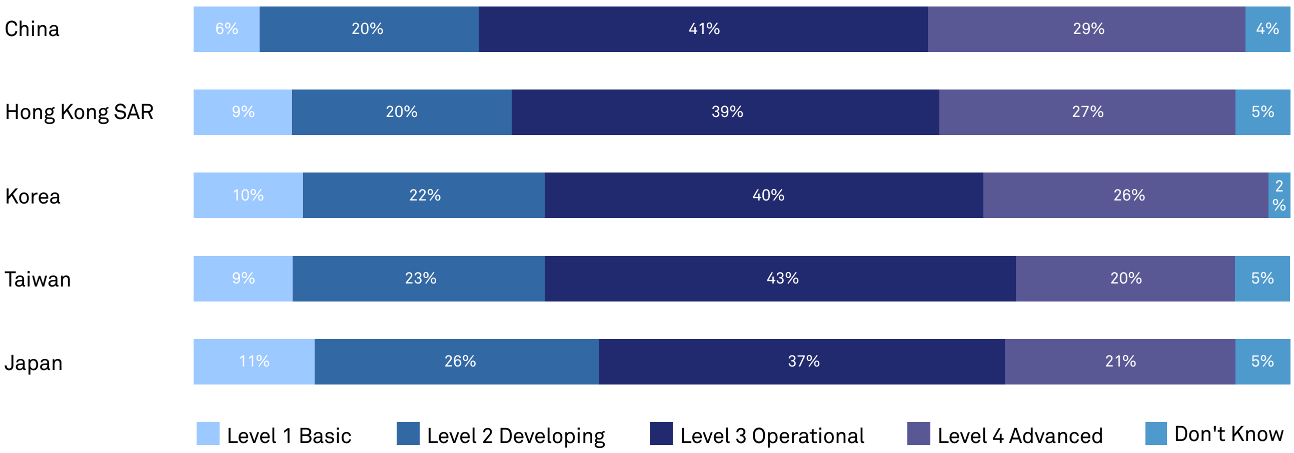
While there are common challenges, different regions and some markets show interesting distinctions. Here are some key barriers and enablers for the security automation landscape in China.

The state of security automation in China (Maturity)

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

China also has the lowest percentage (26%) 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)?

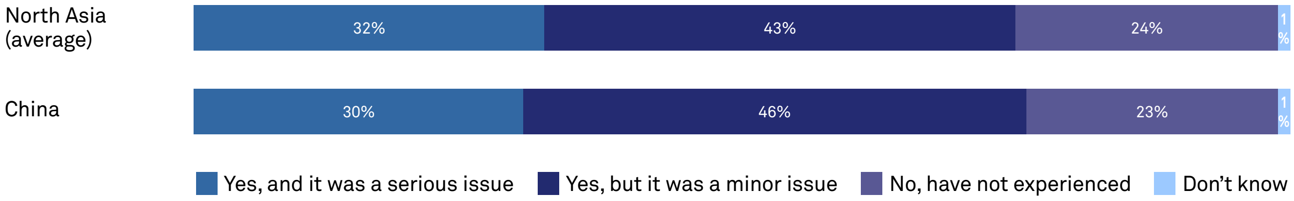


Across the five industries targeted, retail and wholesale organisations reported the highest levels of security automation maturity in China, while banking and financial services organisations reported the lowest.

Prevalence of security issues

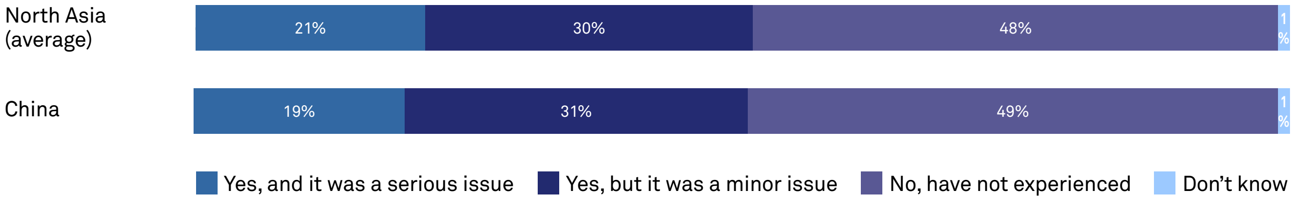
Organisations throughout all regions continue to grapple with challenges around rising security incidents. That's reflected amongst Chinese respondents, with 46% of Chinese firms seeing an increase in 'minor' attacks over the past 12 months, which is the highest of any in the region. Additionally, 30% of Chinese firms saw a rise in 'serious' security incidents, while 23% did not notice any increase at all.

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



China fares slightly better than the average across North Asia when it comes to actual breaches, with 49% having not experienced a significant increase in breaches over the last 12 months. That still leaves 31% of firms which recorded an increase in 'minor' breaches, and 19% reporting an increase in major issues.

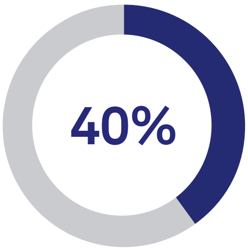
Has your organisation experienced a significant increase in security breaches in the last 12 months?



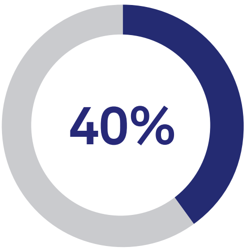
Impact of damage

Chinese firms reported a range of significant impacts from security incidents. The country suffered the equal highest percentage of legal and regulatory impacts – including lawsuits and regulatory penalties – with 18% of respondents citing this as an issue. It also has the second highest proportion (26%) of companies that lost customers due to an incident or breach.

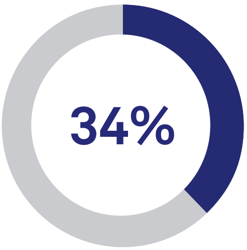
Overall, the top three impacts across organisations in China were:



Lost revenue

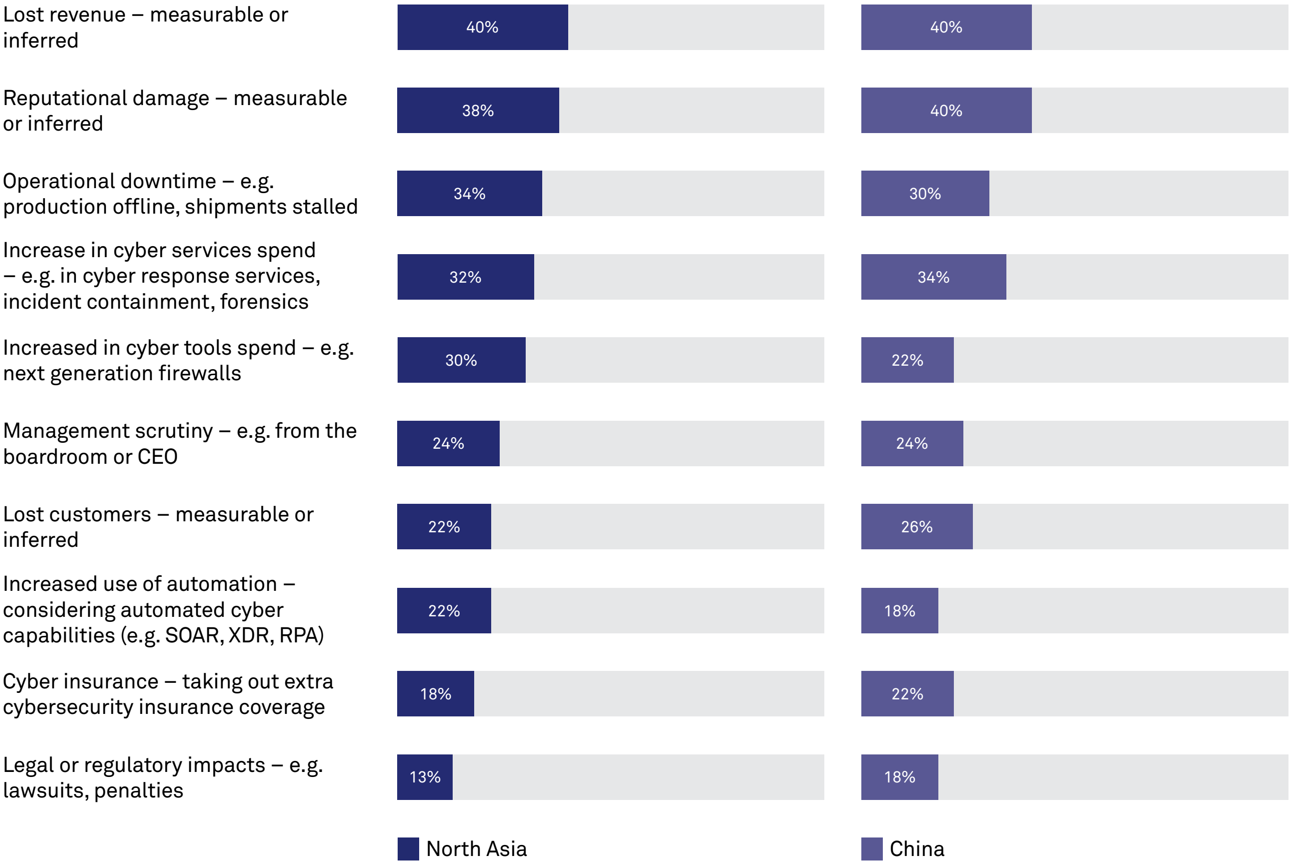


(Tied) Reputational damage



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?

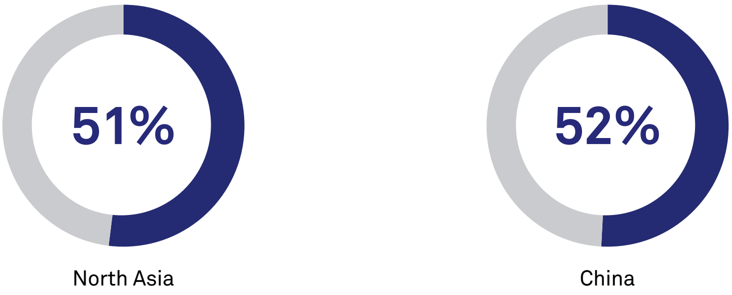


Benefits of automation

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. There is a significant opportunity with automation to help cut through this ‘noise’ in China, which experiences the largest percentage (44%) of false positive alerts.

Well-architected and implemented security automation can help dramatically reduce the likelihood and impact of a severe breach. Executives in China believe that effective security automation could have helped reduce 52% of the serious impacts caused by incidents and breaches.

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?



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