Achieving digital resilience:

Security automation in Korea

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.

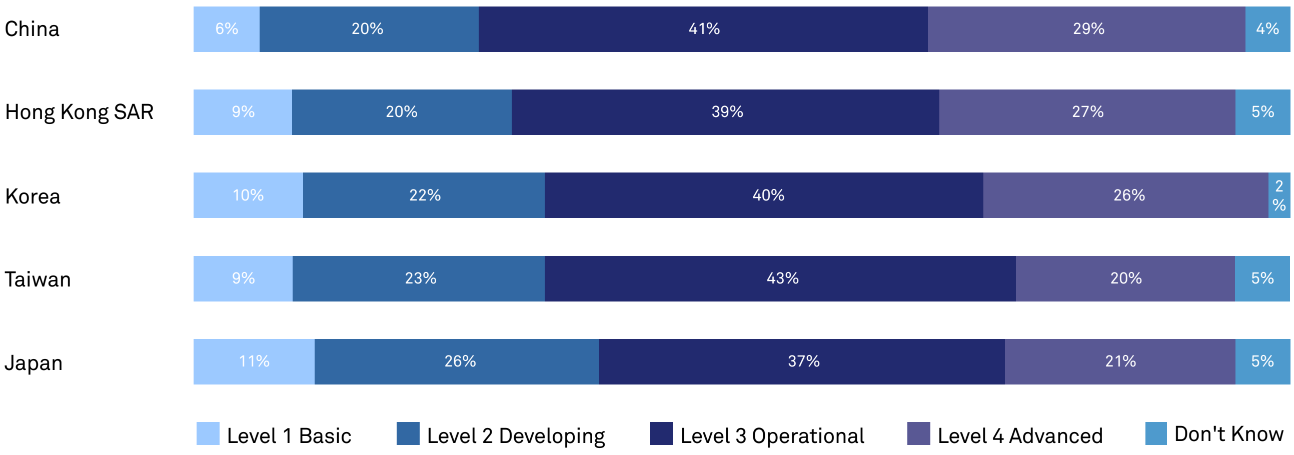
While there are common challenges, different regions and some markets show interesting distinctions. Here are some key barriers and enablers for the security automation landscape in Korea.

The state of security automation in Korea (Maturity)

Korea has the second highest levels of security automation maturity across North Asia (behind mainland China), equal to Hong Kong. Sixty-six percent of organisations in Korea report maturity levels of three (operational) or four (advanced), compared to an average of 64% for all markets in our research.

However, Korea is also tied for 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)?

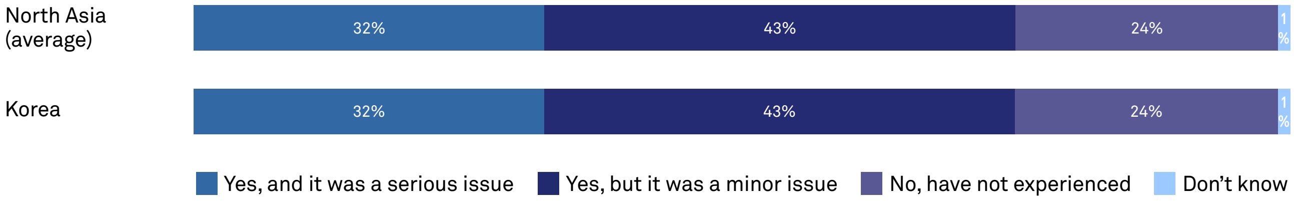


Across the five industries targeted, transport and logistics organisations reported the highest levels of security automation maturity in Korea, while retail and wholesale organisations reported the lowest.

Prevalence of security issues

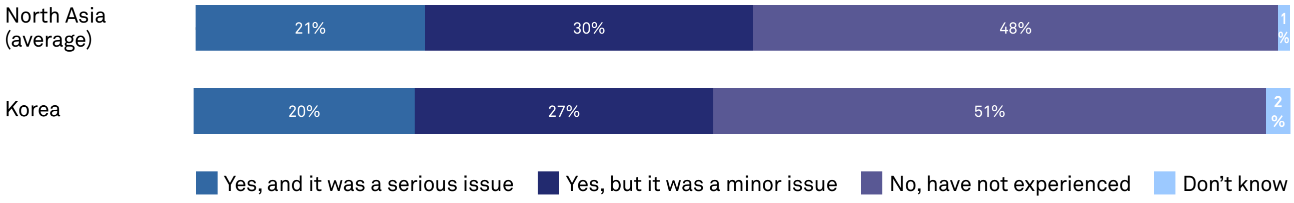
Organisations throughout all regions continue to grapple with challenges around rising security incidents. That's reflected amongst Korean respondents, with 43% of firms seeing an increase in 'minor' attacks over the past 12 months, which is on par with the average across all countries in the region. Thirty-two per cent of Korean firms saw a rise in 'serious' security incidents, while just 24% 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?



Korea fares slightly better when it comes to actual breaches, with 51% having not experienced a significant increase in breaches over the last 12 months. That still leaves 27% of firms which recorded an increase in minor breaches, and 20% reporting an increase in major issues.

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

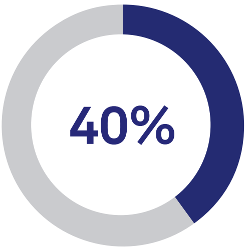


Impact of damage

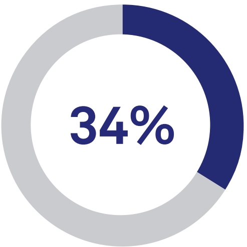
Korean firms reported a range of significant impacts from security incidents. Along with China, the country was tied for the highest percentage of legal and regulatory impacts – including lawsuits and regulatory penalties – with 18% of respondents citing this as an issue.

The country also recorded the highest proportion (28%) of companies that lost customers as a result of an incident or breach. 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.

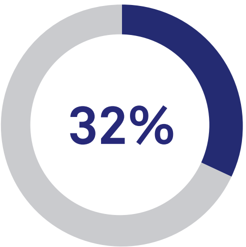
Overall, the top three impacts across organisations in Korea were:



Reputational damage

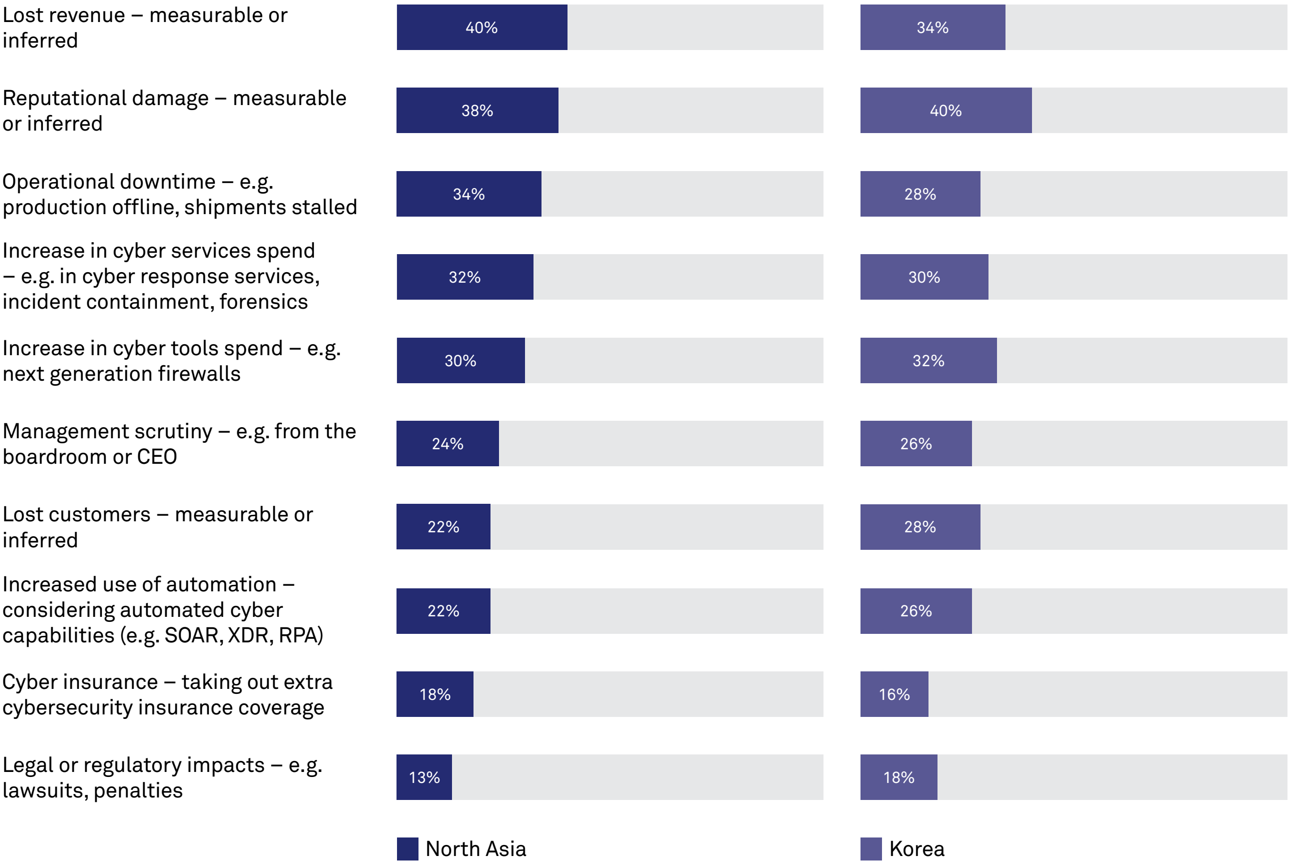


Lost revenue



Increase in cyber tools spend

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

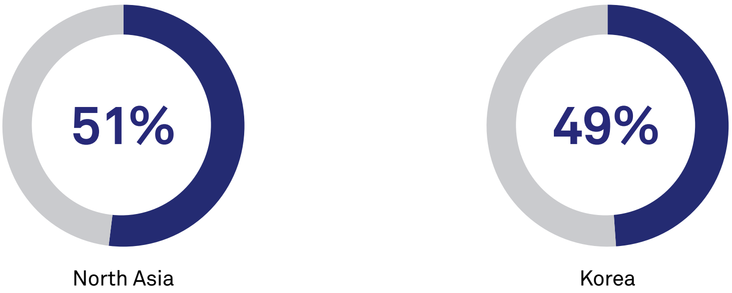


Benefits of automation

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 for automation to cut through this 'noise' in Korea, which experiences a large percentage (41%) of false positive alerts.

Well-architected and implemented security automation can help dramatically reduce the likelihood and impact of a severe breach. Executives in Korea believe that effective security automation could have helped reduce 49% 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 Korea 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**