Achieving digital resilience:

Security automation in Hong Kong

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.

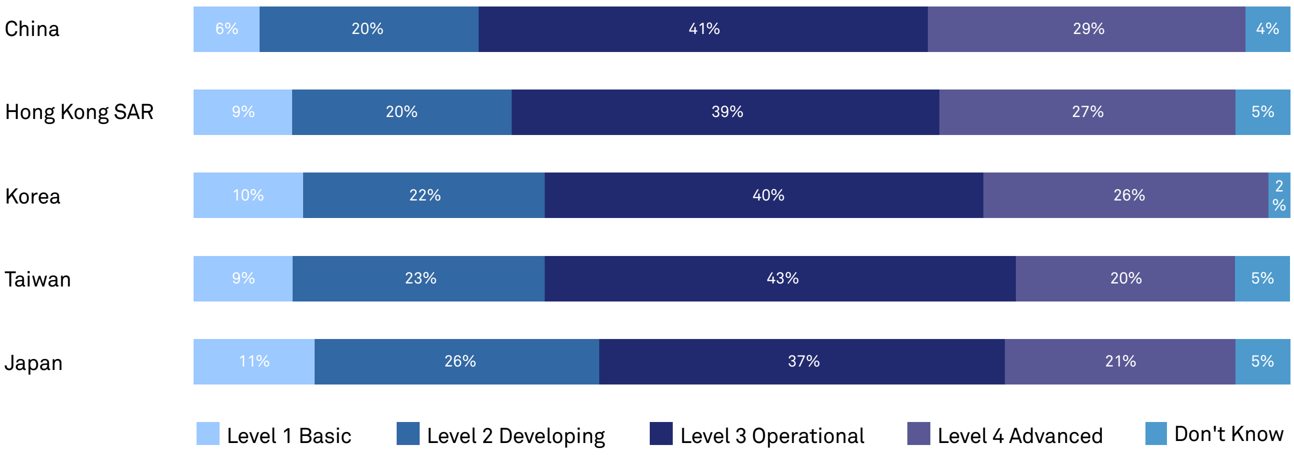
While there are common challenges, different regions and some markets show interesting distinctions. Here are some key barriers and enablers for the security automation landscape in Hong Kong.

The state of security automation in Hong Kong (Maturity)

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

Hong Kong also has the second lowest representation 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) ?

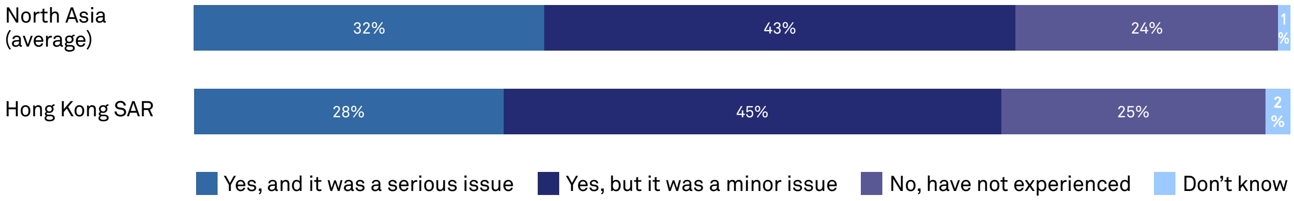


Across the five industries targeted, retail and wholesale organisations reported the highest levels of security automation maturity in Hong Hong, while healthcare organisations reported the lowest.

Prevalence of security issues

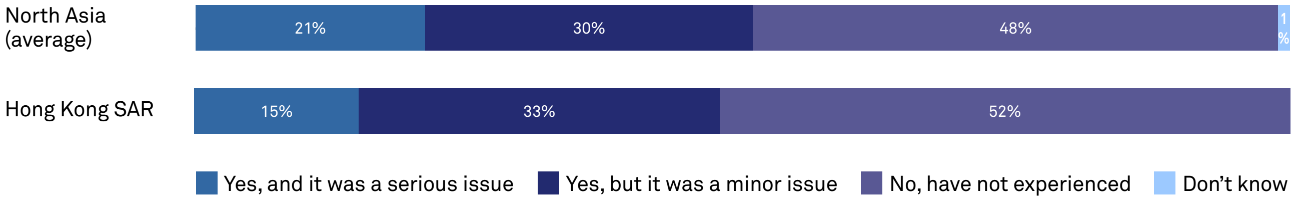
While organisations throughout North Asia continue to grapple with challenges around rising security incidents, Hong Kong had the lowest prevalence of ‘serious’ security incidents in the region. Twenty-eight per cent of firms in Hong Kong saw a significant increase in ‘serious’ security incidents, compared to an average of 32% across the region. However, 45% percent of firms saw an increase in 'minor' issues, which is only 1% behind the highest response from Chinese organisations.

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



Just 15% of Hong Kong organisations have experienced a significant increase in serious breaches over the last 12 months across their entire IT stack, which is also the lowest in the region, although 33% of firms reported an increase in minor breaches, which is the highest in the region.

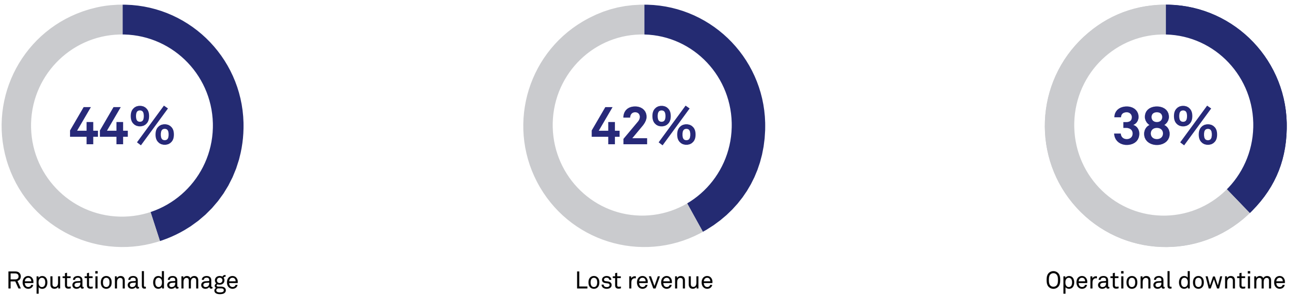
Has your organisation experienced a significant increase in security breaches in the last 12 months?



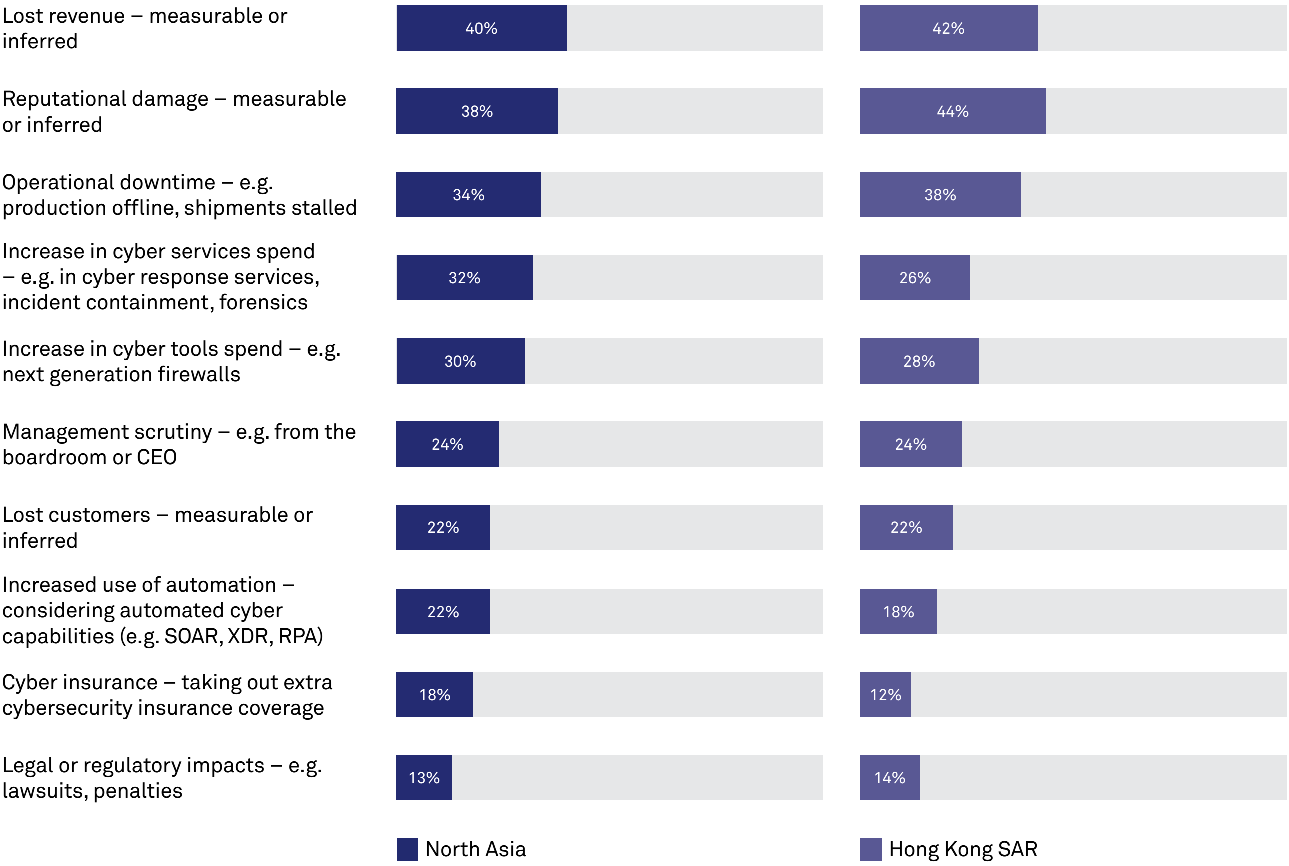
Impact of damage

Hong Kong organisations experienced the highest proportion of reputational damage from breaches across the region. Forty-four per cent of firms in Hong Kong suffered reputational damage over the last 12 months, compared to 38% across North Asia. It also had the second highest percentage of firms reporting impacts due to operational downtime, with 38% recognising this as an issue.

Overall, the top three impacts of security incidents and breaches in Hong Kong were:



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

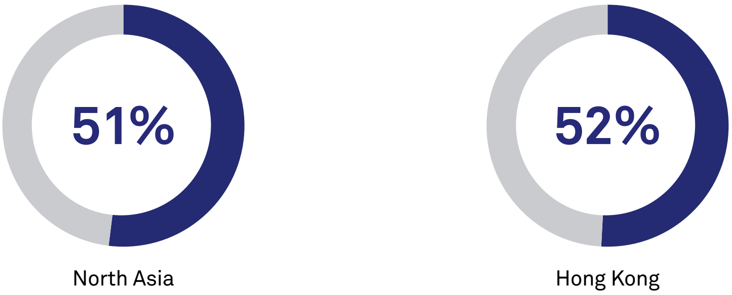


Benefits of automation

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 Hong Kong firms reported the lowest percentage (41%) of false positive alerts, there remains a significant opportunity for automation to cut through this ‘noise’.

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



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