Are You Prepared?

Singaporean Industries at High Risk for Cybersecurity Threats in 2024: Communications Considerations

Cyber crime across the globe is on the rise, and a combination of artificial intelligence (“AI”), digitalisation of emerging economies, and the increased connectivity of organisations across geographies with varying cybersecurity standards and regulations, means 2024 is set to be the most active year for cybersecurity to date. Importantly for organisations tracking this trend and preparing potential responses, cyber crime is also getting more expensive for those who find themselves unfortunate victims, both in monetary value and reputational harm. According to IBM,[1] the average cost of a cyber breach in 2023 was $4.45 million USD, and for organisations with high levels of security skills shortages that number ballooned to $5.26 million USD.

Looking at the Asia Pacific (“APAC”) region as a whole, the World Economic Forum (“WEF”) has taken notice of the confluence of an emerging digital economy alongside a sharp increase in cybersecurity vulnerabilities, and has declared the region as “the new ’ground zero’ for cyber crime incidents.”[2] While countries such as Singapore and Australia are touted as positive examples of improved national regulations, establishing national task forces and fostering greater awareness and education,[3] the reality is the interconnectivity of APAC economies, through both public and private enterprises, means each entity is only as strong as its weakest connected link. Particularly given the acceleration of the digital economy in a post-Covid era, the APAC region is more vulnerable than ever to a variety of cyber attacks.

Per IBM’s Security X-Force Threat Intelligence Index,[4] APAC was the most attacked region in 2022, accounting for 31% of attacks globally. Check Point Research[5] found that APAC witnessed the highest year-over-year increase in weekly cyber attacks during the first quarter of 2023, averaging 1,835 attacks per organisation compared to the global average of 1,248 attacks per week. Given the state of the cybersecurity industry across the APAC region, the impacts of these cyber attacks can often be larger than in other regions. For example, according to a Positive Technologies report,[6] as many as 49% of successful attacks on organisations resulted in the compromise of sensitive information, while in 27% of successful attacks organisations’ core operations were disrupted. Despite the large number of cyber incidents, only 38% of APAC business consider themselves highly prepared to respond according to Cloudflare’s Asia Pacific Cybersecurity Readiness Survey.[7]

Zooming in on Singapore, a new research report[8] from Rubrik Zero Labs found that 62% of organisations in the country suffered sensitive data loss from November 2022 - November 2023, with 23% of respondents reporting multiple losses over the same time period. In the same study, 86% of IT and security leaders responded that their organisation’s current data growth is outpacing their ability to secure their data and manage risk, and less than half of respondents said there was a single senior executive who is responsible for data and its security.

Excluding government agencies, which accounted for 22% of attacks from 2022 through HQ 2023 according to Positive Technologies,[9] the Singaporean industries most at risk were financial services, shipping/logistics, and healthcare.

Financial Services

Singapore serves as a financial hub for the APAC region, with dozens of financial services organisations headquartered in the country alongside the internationally connected Singapore Exchange ("SGX"). The country is consistently at the forefront of financial technologies, from the prevalence of QR codes at local markets to the widespread investment of cross-border payment connectivity through APIs and blockchain technologies. Financial service institutions across Singapore contain significant amounts of user data, much of which could be considered confidential or Personally Identifiable Information ("PII"). Threat actors with malicious intent understand the prevalence of financial data held in the area and interconnectivity of many financial services systems, making these financial service institutions a prime target.

Shipping/Logistics

Singapore sits at the center of the world's shipping and logistics economies, with connections to more than 600 ports worldwide. More than 80% of the world's cargo can be connected back to Singapore according to the Ministry of Education.[10] As the shipping and logistics industry continues to digitalise, there are increased demands for IT and IoT technology connectivity to support efficiencies and optimisations across fleets. However, this digitalisation also brings ever-growing cyber risk, threatening the operational disruptions of global supply chains. Operational disruptions at a much smaller scale, such as the Colonial Pipeline cyber incident in 2021, which was one of the most significant critical infrastructure ransomware[11] attacks in the United States, disrupting a crude oil pipeline that transported gasoline up and down the east coast, or the cargo ship stuck[12] in the Suez Canal in 2021, which held up over $60 billion in trade, had far-reaching effects up and down their respective supply chains. The potential impacts of a cybersecurity incident in Singapore's shipping industry could be catastrophic beyond operational disruptions, including significant data theft, personnel industry, cargo or ship damage, and more.

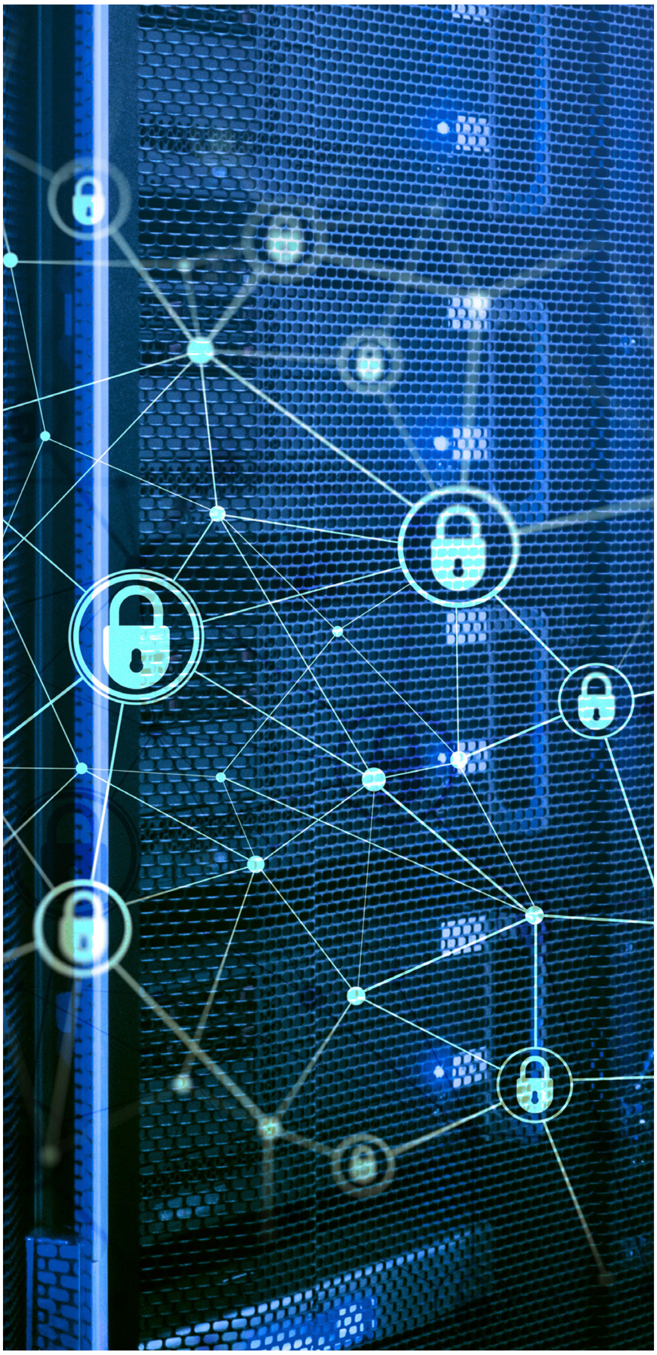
Healthcare

Whether it is hospital and healthcare networks or advanced technology medical devices, Singapore is not immune to the cybersecurity risks faced by the worldwide healthcare community. Singapore has been attempting to position itself as a global leader in health cybersecurity and AI for healthcare for several years now, and there have been significant investments[13] to support these efforts. Government entities have recognised these risks as the Ministry of Health plans to introduce a Health Information Bill to better govern the sharing of healthcare information across networks. As organisations operating in this industry are keenly aware, the possession of Personal Health Information ("PHI") and the inherent risk of any compromise in integrity of electronic medical devices make these companies prime targets for threat actors.

Conclusion

While organisations across every industry are subject to potential cyber attacks, certain industries are higher value targets for criminals, depending on the information they hold, where they operate, and the potential for overall disruption a cyber attack may cause them. As part of preparing for the inevitable, organisations should work to understand the unique risks associated with their industry and location. Singapore's economy is driven by specific industries that must take special consideration when preparing for data or operational impacts caused by cyber attacks. Organisations operating in these industries would be wise to invest in cybersecurity crisis communications plans and table-top exercises that aim to protect their license to operate and financial welfare.

Cybersecurity crisis communication plans help organisations efficiently and effectively navigate and respond to crises and, in the process, protect stakeholder relationships, mitigate legal risk, and reduce short- and long-term business impact. These plans usually include formalised crisis management teams, roles, and responsibilities, incident decision-making authority, escalation and declaration protocols and more. Putting these plans to practice through table-top exercises and simulations provides low-pressure opportunities to ensure that everyone knows their roles and responsibilities, and to identify any additional gaps needed to protect an organisation.



ELI SEROTA
Director, Cybersecurity & Data Privacy Communications
+65-6831-7800
eli.serota@fticonsulting.com

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. **fticonsulting.com**

Endnotes

[1] Ang, A. 2024, January 16. $15M Singapore-London partnership to help stem APAC's growing. Healthcare IT News.

[2] Check Point Research. 2023, April 27. Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most. Check Point.

[3] Ibid.

[4] Christian, A. 2021, June 22. The untold story of the big boat that broke the world. WIRED UK.

[5] Cloudflare. 2023. Securing the Future: Asia Pacific Cybersecurity Readiness Survey.

[6] Easterly, J., & Fanning, T. 2023, May 7. The attack on Colonial Pipeline: what we've learned what we've done over the past two years. Cybersecurity and Infrastructure Security Agency (CISA).

[7] IBM. 2023. Cost of a data breach 2023.

[8] IBM. 2024. IBM X-Force Threat Intelligence Index 2023.

[9] Ibid.

[10] Ministry of Education Singapore. n.d. Maritime Industry

[11] Online Bureau. 2023, November 21. 62% of organisations in Singapore suffered loss of sensitive data in the last year: Report. Economic Times CIO Southeast Asia.

[12] Positive Technologies. 2023, September 12. Cybersecurity threatscape of Asia: 2022–2023.

[13] World Economic Forum. 2024, January 2. Why is the Asia Pacific region a target for cybercrime - and what can be done about it?