Navigating The Cyber Threat Landscape

Data Protection And Cybersecurity For Tax Professionals

2 April 2025, Wednesday

Facilitated by:
Mr Kendrick Choo & Ms Sheryl Chung

KEY TAKEAWAYS

- In 2024, scam victims in Singapore suffered astonishing losses of S$1.1 billion, marking a staggering 70% increase from the previous year.
- By bridging the cybersecurity knowledge gap among their employees, organisations can drastically reduce the risk of falling victim to phishing attempts or other malicious activities that exploit human vulnerabilities.
- CISO-as-a-Service enables SMEs with limited IT and cybersecurity expertise/resources to gain direct access to a pool of experienced professional cybersecurity consultants for expert guidance tailored to their specific cybersecurity risk profile.

In 2024, scam victims in Singapore suffered astonishing losses of S$1.1 billion, marking a staggering 70% increase from the previous year, according to the Singapore Police Force's Annual Scams and Cybercrime Brief 2024.

Despite the alarming statistics, many victims of cybercrimes mistakenly believe that they are immune to scams and cyberattacks. However, cyber criminals can target anyone and any organisation. This misguided sense of security, coupled with poor cyber resilience, makes them an easy target for cyber criminals and scammers.

"While there is no foolproof method to prevent cyberattacks, organisations can enhance their cyber resilience to stand a better chance against cyber threats," shared Kendrick Choo, GRC Consultant, and Sheryl Chung, Manager, RSM Singapore, during a recent webinar organised by the Singapore Chartered Tax Professionals. The webinar aimed to guide tax professionals on the best cybersecurity practices to adopt.

Understanding Cyberattacks

A cyberattack is an intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorised access to a network, computer system or digital device. Common types of cyberattacks include malware attacks, social engineering scams, and ransomware.

Cyberattacks can target anyone, but certain organisations may face a heightened risk. For example, a professional accounting and tax firm may be an attractive target for cyber criminals as it handles highly sensitive information on a daily basis. Moreover, financial information is often transmitted and processed digitally, increasing its exposure to data breaches, ransomware, and other forms of cyber threats.

Bridging the Cybersecurity Knowledge Gap

The lack of cybersecurity knowledge was cited by the Cyber Security Agency of Singapore (CSA) as the top challenge faced by organisations for the non-adoption of cybersecurity measures, while a joint study by Stanford University and security firm Tessian revealed that nine in 10 data breach incidents are caused by employees' mistakes.

A case in point is a Singapore commodities company that lost S$57.2 million after an employee responded to a phishing email, believing it to be from a vendor informing the company of a change in bank account details for payment. The company made the payment to the "updated" bank account, only to discover it was a scam when it received a late payment notice from the actual vendor. This incident underscores the severe consequences of employees not being attuned to cybersecurity.

By bridging the cybersecurity knowledge gap among their employees, organisations can drastically reduce the risk of falling victim to phishing attempts or other malicious activities that exploit human vulnerabilities.

Maintaining Cyber Hygiene

Maintaining good cyber hygiene practices is crucial for protecting organisations against cyber threats. Simple yet effective practices – such as implementing multi-factor authentication on critical systems, setting strong passwords and enforcing regular password changes, practising proper identity and access management, setting up malware protection and firewalls, or even updating software on a regular basis – can significantly enhance protection.

Establishing an Incident Response Plan

While bridging the cybersecurity knowledge gap and maintaining good cyber hygiene can reduce cyber risks, these are not foolproof methods to prevent cyberattacks. "When it comes to cybersecurity incidents, it is not a matter of if, but when," cautioned Mr Choo.

Evidently, cyberattacks are happening to a significant majority of firms. It is critical for Singapore organisations to stay vigilant in their approach to cybersecurity, particularly in how they prepare for and respond in the event of a cyberattack. In this regard, organisations should establish an incident response plan to outline how the organisation will detect, contain, and recover from cybersecurity incidents.

Detection involves identifying and understanding the nature of the cyber threat as quickly as possible. Once a cybersecurity incident is identified, the next step is to limit the scope of the incident by isolating affected systems, blocking malicious traffic, and/ or implementing temporary fixes to prevent further damage.

After the cybersecurity incident has been contained, the next phase aims to restore normal operations and services. This typically includes restoring data from backups, repairing systems, and ensuring all vulnerabilities have been addressed.

As the organisation goes about detecting, containing and recovering from the incident, it should also be keeping all relevant stakeholders informed throughout the entire process. Effective communication can help maintain trust despite the unfortunate incident.

Government Schemes Available

If you are thinking about enhancing your organisation's cybersecurity readiness but are not sure where to start, below are a couple of government schemes available to help you on your cybersecurity journey.

Chief Technology Officer-as-a-Service (CTO-as-a-Service)

Developed by the Infocomm Media Development Authority (IMDA), CTO-as-a-Service enables small and medium-sized enterprises (SMEs) in Singapore to tap on professional consultants, at no cost, to simplify cybersecurity and data protection.

This programme is designed to enable local SMEs to self-assess their digital readiness and needs, access market-proven and cost-effective digital solutions, as well as engage digital consultants for in-depth digital transformation strategy advisory and project management services under the SMEs Go Digital Programme.

Essentially, any SME that wants to know how to get started in going digital, understand what types of solution to adopt for its specific business challenge, or select the solution that best meets its needs, can consider tapping on CTO-as-a-Service.

Note: The deadline for sign-up of the complimentary CTO-as-a-Service Digital Consultancy is **30 September 2025**. Eligible SMEs may continue to sign up for the service till then.

Chief Information Service Officer-as-a-Service (CISO-as-a-Service)

Developed by CSA, CISO-as-a-Service is an initiative to help organisations starting on their cybersecurity journey, especially SMEs with limited IT and cybersecurity expertise/resources, establish cybersecurity baselines.

Under this initiative, cybersecurity consultants take on the role of CISO at participating organisations and focus on implementing foundational cyber hygiene practices within these organisations. Specifically, the cybersecurity consultant may perform a comprehensive cyber health checkup on the organisation, develop a cybersecurity health plan tailored for the organisation, or help close the cyber hygiene gaps identified. The emphasis to start with foundational practices ensures that basic vulnerabilities are addressed before more advanced cybersecurity strategies are considered.

CISO-as-a-Service enables SMEs with limited IT and cybersecurity expertise/resources gain direct access to a pool of experienced professional cybersecurity consultants for expert guidance tailored to their specific cybersecurity risk profile. Eligible SMEs can enjoy up to 70% co-funding support when they sign up for CISO-as-a-Service.

Conclusion

In conclusion, the rise in cyberattacks highlights the urgent need for organisations, especially those in the accounting and tax sectors, to strengthen their cybersecurity measures. By bridging the cybersecurity knowledge gap, maintaining good cyber hygiene, and establishing a robust incident response plan, organisations can better protect themselves against cyber threats. Leveraging government schemes such as CTO-as-a-Service and CISO-as-a-Service can provide valuable support in this journey. Ultimately, a proactive approach to cybersecurity not only safeguards sensitive information, it enhances the organisation's reputation as a trusted and responsible entity.

Please click here to rate this article.

Facilitators

Mr Kendrick Choo
GRC Consultant
RSM Singapore

Email: kendrickchooxh@rsmsingapore.sg

Ms Sheryl Chung
Manager, Business Development
RSM Singapore

Email: sherylchungsp@rsmsingapore.sg

This technical event commentary is written by SCTP's Tax Head, Accredited Tax Advisor (Income Tax) Felix Wong and Senior Tax Manager, Accredited Tax Practitioner (Income Tax & GST) Joseph Tan. For more insights, please visit https://sctp.org.sg/Tax-Articles.