CHRISTIAN SAJERE, *Founder, Christian Sajere Cybersecurity and IT Infrastructure (Christian Sajere Pty. Ltd) (Cybersecurity and Technology Expert, Entrepreneur)*
Company Website: https://christiansajere.com/
Personal Linkedin: https://www.linkedin.com/in/christiansajere

Christian Sajere is a Cybersecurity Practitioner, with significant expertise in the realm of cybersecurity. He formerly held the esteemed position of a University Associate at Curtin University in Bentley until February 2024. Currently, he spearheads Christian Sajere Cybersecurity and IT Infrastructure, a startup dedicated to crafting bespoke strategies for fostering cyber resilience in enterprises. These strategies are intricately woven with a profound comprehension of a business's core objectives, thus aiding in safeguarding corporate data.
Christian holds industry accreditations including the distinguished CompTIA Secure Infrastructure Expert (CSIE) and CompTIA Security Analytics Expert (CSAE). He is also a member of the Australia Institute of Company Directors (AICD), Australia Information Security Association (AISA), and the Australian Computer Society (ACS).

TIP 1: CONDUCT A COMPREHENSIVE RISK ANALYSIS

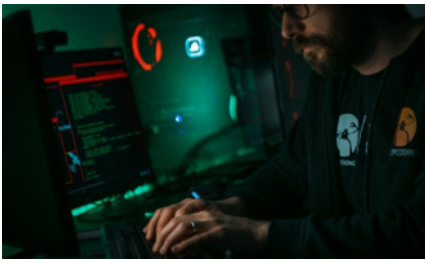
Begin with a holistic risk analysis across all domains, including compliance, cybersecurity, technology, and business risk. Identify potential threats and vulnerabilities, and develop quick and efficient remediation strategies. This proactive approach lays the foundation for robust cybersecurity.

TIP 2: ALIGN WITH INDUSTRY BEST PRACTICES AND STANDARDS

Organisations should align their IT systems with industry best practices and standards, such as the NIST Cybersecurity Framework, Essential 8, and ISO 27001. This ensures continual improvement and readiness to adapt to the evolving cybersecurity landscape.

TIP 3: DETERMINE IT AND INFRASTRUCTURE MATURITY LEVELS

Assess your organisation's IT and infrastructure maturity levels. Evaluate your security implementations and identify areas for improvement based on your business operations. This step helps in understanding your current security posture and planning enhancements.



TIP 4: IMPLEMENT SECURITY POSTURE MANAGEMENT

Regularly perform security posture management to gauge your organisation's ability to withstand cyberattacks. This involves continuous monitoring, assessment, and improvement of your security measures to stay ahead of potential threats.

TIP 5: ENFORCE REGULATORY COMPLIANCE

Ensure adherence to governmental regulations and industry-specific requirements. This includes implementing necessary IT risk factors during the cybersecurity framework rollout to maintain compliance and protect your organisation from legal and financial repercussions.

TIP 6: CUSTOMISE RISK MANAGEMENT APPROACHES

Tailor your risk identification and remediation strategies based on the size and nature of your organisation. A one-size-fits-all approach doesn't work; customise your cybersecurity measures to address specific risks effectively.

TIP 7: FOSTER A SECURITY-FIRST CULTURE

Promote a culture of cybersecurity awareness and best practices among employees. Regular training and awareness programs can help employees recognize and respond to potential threats, making them an integral part of your cybersecurity defense.

TIP 8: PRIORITISE DATA PROTECTION

Implement robust data protection measures, including encryption for data at rest and in transit. Protecting your data ensures that, even if it is accessed, it remains unusable to unauthorised parties, thereby minimising the impact of potential breaches.

TIP 9: PARTNER WITH RELIABLE SECURITY PROVIDERS

Choose security partners, not just products, for long-term cybersecurity solutions. A reliable partner will continuously support your security needs and help you adapt to new threats, ensuring sustained protection.

TIP 10. REGULARLY UPDATE AND PATCH SYSTEMS

Ensure that all software and systems are regularly updated and patched. Cyber attackers often exploit known vulnerabilities in outdated software. By keeping your systems up to date, you reduce the risk of being targeted by these attacks. Automate this process where possible to ensure no critical updates are missed.