CYBERSECURITY COMPLIANCE IN LIGHT OF THE WEF'S CYBERSECURITY OUTLOOK

Category: IT Law,Technology Law,Uncategorized
written by Khomotso Maake | April 5, 2024

In January 2024, the World Economic Forum published its Global Cybersecurity Outlook for 2024 ("**Report**"). The purpose of the Global Cybersecurity Outlook Report is to provide insight into global cybersecurity challenges facing organisations by distilling cyber-risk issues. Major findings from the Report include the widening cyber inequality and cyber challenges as a result of emerging technologies.

The first key insight highlighted in the Global Cybersecurity Outlook Report is the growing cyber inequality between organisations that are cyber resilient and those that are not. The Report found that organisations that maintain a minimum level of cyber resilience is disappearing. Small and medium enterprises ("**SMEs**") are disproportionately affected by this disparity. According to the Report, a significant number of SMEs in comparison to the large organisations lack cyber resilience to fulfil their critical operational requirements.

Other key insights relate to longstanding challenges relating to cyber resilience challenges due to emerging technologies. According to the Report, the most concerning impact of Generative Artificial Intelligence ("**Generative AI**") lies in adversarial capabilities (phishing, malware and deep fakes) which pose a significant threat to cyber resilience within organisations. Generative AI is a type of Artificial Intelligence that is capable of creating new content such as code, text, image, videos through the use of generative models, by learning patterns from existing data and generating new data with similar characteristics. This highlights the importance for organisations, in the pursuit of

adopting new technologies, to recognise the critical importance of understanding the immediate, mid-term, and long-term implications of these innovations on their cyber resilience.

The Global Cybersecurity Outlook Report also highlights how effective cyber and privacy regulation effectively reduces cyber risk in organisations. For example, an organisation can mitigate cyber risks by implementing a security incident management policy that aligns with privacy laws. Such a policy provides guidance on handling cyber threats and incidents effectively. Furthermore, implementing technical measures such as passwords and access controls can reduce cyber risks. However, although regulations reduce cyber risk, the Report acknowledges that there are too many conflicting regulations across different countries. The Report recognises that improved alignment across different industries and countries would render cyber and privacy regulation even more beneficial.

The US National Cybersecurity Strategy ("**Strategy**") was published in March 2023. The purpose of the Strategy is to create a safe and secure digital space for American citizens. In order to fulfil this purpose, the Strategy recognises the need to rebalance the responsibility to defend cyberspace. It aims to do so by shifting the responsibility for cybersecurity away from individuals, small businesses, local governments and placing it on organisations that have the capacity and are in the best position to reduce cybersecurity risk.

Pillar five of the Strategy recognises the importance of forging international partnerships to pursue shared goals. To this end, the US Cybersecurity and Infrastructure Security Agency, National Security Agency and the Federal Bureau of Investigations partnered with Australia, Canada, the United Kingdom, Germany, Netherlands, and New Zealand to publish guidance on balancing cybersecurity risk. Published on the 13 April 2023, the Guide on Shifting the Balance of Cybersecurity Risk: Security by Design and Default Principles ("**Guide**"), is meant to serve as a cybersecurity map for manufacturers of technology and associated products. The first of its kind, the Guide is meant to represent an international effort to reduce exploitable vulnerabilities in technology used by governments and the private sector. It provides guidance and recommendations for software manufacturers on software product security principles, secure by design tactics and secure by default tactics.

The Guide recommends that software manufacturers take ownership of the security outcomes of their customers purchases and evolve their products accordingly. This is to ensure that the burden of security will not fall solely on the customer. As part of the secure by design tactics, the Guide recommends the integration of the Secure Software Development Framework SP 800-218 ("**the Framework**") into each stage of software development lifecycle. The Framework seeks to mitigate security risks, vulnerabilities and prevent hostile interventions, by requiring that providers adhere to secure software development practices when creating software. Adopting such practices can assist software producers become more effective at detecting, mitigating and removing vulnerabilities. In addition, it encourages software manufacturers to prioritise secure by default configurations in their products.

It can be argued that the US National Cybersecurity Strategy and the EU Cybersecurity Resilience Act ("**CRA**") can provide global guidance and alignment on some aspects of cybersecurity regulation. The CRA was published in September 2022 and was approved by the European Union on 12 March 2024. The CRA seeks to protect consumers when purchasing or using digital components, by ensuring that these products are safe, secure and resilient against cyber threats. It achieves this by imposing obligations on manufacturers intending to introduce or place products with digital elements into the EU market. The CRA aims to guarantee high cybersecurity for products with digital elements and their integrated remote data processing solutions.

In terms of article 10(2), manufacturers are required to assess the cybersecurity risks associated with

a product containing a digital element. The outcomes of the assessments must be taken into account during the planning, design, development, production, delivery and maintenance phases of the product. This must be done with the view of minimising cybersecurity risks, preventing security incidents and minimising the impact of such incidents, in relation to the health and safety of users.

The potential implications of these developments for service providers includes their inability to contractually exclude liability for cybersecurity risks that are a result of their failure to take reasonable precautions to make sure that their software is secure. However, the additional responsibility that service providers now bear, might translate into additional costs for customers. For instance, the assessments that are required by the European Union, the CRA might result in additional costs which are then passed on to the consumer.

Developing cyber resilience remains an ongoing undertaking for organisations, regardless of their size, it necessitates continuous effort and attention. Due to the increased pace of the adoption of new technologies, it is imperative that organisations invest in cyber resilience strategies.

Contact us for more good, clear and precise advice!