THE SHIFTING TIDE IN CYBERSECURITY RESPONSIBILITY IN SOFTWARE PRODUCTS AND SERVICES

Category: Privacy Law, Infosec, and POPIA,Technology Law
written by Tshepiso Hadebe | July 25, 2023



On 2 March 2023 the White House announced the publication of the US National Cybersecurity Strategy ("**Strategy**"). 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 the 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.

Strategic objective 3.3 of the Strategy suggests shifting liability for insecure software products and services. It recognises that entities introduce vulnerable and insecure products or services into the US digital ecosystem. This is because many vendors ignore best practices for secure development, ship products with insecure default configurations, or known vulnerabilities and integrate third party software of unvetted or unknown origin. Entities evade responsibility by leveraging their market position to fully disclaim any liability by way of contracts.

Cognisant of that fact that even the most advanced software security program cannot prevent all vulnerabilities, the objective is to shift liability onto these entities that fail to take **reasonable precautions** to secure their software. The end goal is that the responsibility is placed on the stakeholders that are most capable of taking action to prevent bad outcomes and not the end users who bear the brunt of insecure software or the open-source developer component that is integrated into a commercial product. This results in a market that is driven to produce safer products and services and preserves innovation and the ability of small businesses to compete against market

leaders. To this end the Biden-Harris Administration is set to work with Congress and the private sector to develop legislation that will establish liability for software products and services.

Furthermore, 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 organisations. 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 should take ownership of the security outcomes of their customer's purchase 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 into each stage of software development lifecycle. 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.[1]

On the 15 September 2022 the European Commission published the European Union Cyber Resilience Act ("**CRA**") This is a proposal for regulation on cybersecurity requirements for products with digital elements in order to bolster cybersecurity rules to ensure more secure hardware and software. Chapter two, article 10 of the CRA sets out the obligations of manufacturers who seek to introduce or place products with digital elements onto the EU market.

In terms of article 10(2) manufacturers are obligated 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, including 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 the service providers now bear, might translate into additional costs for customers. For instance, the assessments that are required by the European Union CRA might result in additional costs which might lead to a rise in costs of the products.

These efforts are a commendable in their recognition and emphasis of the need for collaboration in building a secure cyberspace. However, only time will tell if it will all come to fruition.

Contact us for more good, clear and precise advice!

---

[1] This refers to a set of high-level secure software development practices that can be integrated into each stage of the software development lifecycle.