AVA GROUP
SECURITY RISK MANAGEMENT

Cybersecurity Centre of Excellence

Cybersecurity Matters

Validating and ensuring the security of an organisation's data systems is no longer a luxury. Attacks against connected systems and devices are on the rise and continuing to grow at an alarming rate. Between 2016 and 2017 alone there was a 600% increase in internet-connected device (IoT) attacks*

Threat of attack should be a concern for organisations as they are not only disruptive but can often be incredibly costly. In 2018, the average expected total financial cost of a cybersecurity incident to an organisation is over US$ 800k**. With predictions that a business somewhere will fall victim to attack every 14 seconds by 2019, worldwide damages associated with cybercrime are estimated to cost over US$ 6 trillion by 2021***.

Given these startling statistics, adequate steps must be taken for an organisation to ensure the products and manufacturers accessing their data networks are secure. The significant increase in cyber threats has left organisations scrambling for methods to test and verify that systems are compliant and safe. Despite this, no single adopted global standard exists for cybersecurity testing, often leaving organisations with the challenge of deciphering third-party test results without a meaningful baseline.

Standards & Methodology

Ava Group demonstrates a strong commitment to data security by establishing the Cybersecurity Centre of Excellence (CCoE). The CCoE's mission is to ensure a high standard of cybersecurity and that all Ava Group products are subjected to rigorous and continuous testing during development and their entire lifespan to ensure there are no weaknesses in the product that could compromise an organisation's security credentials.

Ava Group has developed a market-leading testing, verification and lifecycle program based upon the National Institute of Standards & Technology (NIST) Cybersecurity Framework combined with the 2900 cybersecurity Standards of the globally-recognised independent testing organisation Underwriter Laboratories (UL). The implementation of these well-known and verifiable standards ensures that customers can trust and have confidence in the cybersecurity profile of Ava Group's tested products.

Robust cybersecurity hardening is not a one-time test or event. Patches, updates, and the ever-changing threat environment require ongoing testing and validation. Our products are continually tested throughout the development lifecycle and in response to emerging threats and security patches to ensure up-to-date resilience. The CCoE also offers customers access to market-leading security configuration information, product-specific hardening guides and validated testing reports, as well as offering greater value with expert advice regarding overall enhancements for the protection of the data network infrastructure as a whole.

Leading the Way

No longer can physical or logical security systems be considered adequately protected by isolating them to their own network. Such systems are becoming part of the overall data ecosystem and must be treated with the same cybersecurity standards as other data network devices. Establishing the CCoE underscores our commitment to providing robust cybersecurity across our technology portfolio. With a long standing and proven pedigree in data network infrastructure protection through its Future Fibre Technologies (FFT) Data Network Infrastructure Physical Security (DNIPS), the addition of the CCoE, Ava Group reinforces an industry-leading attitude to the importance of cybersecurity.

* Source: Symantec 2018 Internet Threat Report
** Source: PwC Global State of Information Security Survey
*** Source: Herjavec Group 2017 Cyber Crime Report