Cyber security is everyone’s responsibility

Submitted by: PR Artistry Limited
Wednesday, 21 October 2020

SMEs are a critical component of supply chains but can be the weakest link, Guy Lloyd at CySure explains why SMEs need to step up their cyber resilience

Organisations at the top of the supply chain rely on a nimble network of SMEs to provide niche products. This unique status provides SMEs with disproportionate access to important information. So, while it might be the big-name brands that generate attention grabbing headlines about data breaches, it can be the weak security credentials of smaller organisation’s that expose the entire chain.

The weakest link
Cyber criminals target SMEs as many don’t have robust security measures in place and lack the technical know-how to carry out a cyber security audit to identify weaknesses. The UK Government Cyber Security Breaches Survey 2020 (i), reveals that many businesses are confused about audit best practice, supplier risks and the reporting of breaches. Half of businesses (50%) say they have carried out an internal or external audit in the last 12 months, but the quality of the audits varies greatly. In some cases, external audits were more financial based and only touched upon some aspects of cyber security.

This vulnerability poses a danger to the larger organisations which SMEs do business with. Hacking into a poorly-secured supplier is now how many of the most sophisticated threat groups start their campaigns. So, while other suppliers in the chain are stepping up and securing their networks, applying patches and software updates as soon as they are released, the effort could all be for nothing if a hacker can get access to the whole chain via a poorly secured SME. In short, if security isn’t a priority for everybody, then it may as well not be a priority at all.

Personal responsibility for cyber physical security incidents

Too many SME’s assume international criminals aren’t interested in their computer system. But in an age where information is currency, your customers, your suppliers and your data are extremely valuable. A data breach could not only cause huge financial and reputational damage, but business leaders could find themselves personally liable for cyber physical security incidents. A cyber physical attack is a security breach in cyber space that can impact on the physical environment by way of critical infrastructure i.e. an oil pipeline or electricity generating plant etc.

The influx of technology, like the Internet of Things (IoT), increases the variety and potential damage that hackers can achieve. By 2024, Gartner predicts that 75% of CEOs will be held personally responsible and accountable for failing to protect systems from cyber incidents (ii). Business leaders won’t be able to plead ignorance to the ramifications of cyber incidents, particularly as government cyber security agencies have increased the details and frequency provided around threats.

Be prepared – get cyber ready
Business owners need to get proactive in understanding their security responsibility, failure to do so could result in a hefty fine, the termination of lucrative contracts and even risk personal liability. Commercially, if your business cannot show that it takes cyber security seriously, it risks falling at

the first hurdle of any future contract tender.

Becoming certified with a credible scheme provides a practical framework for an SME to assess its current cyber security and compliance levels. The benefit is that demonstrates to customers and suppliers that you take cyber security and the protection of data seriously. Getting started can seem daunting but achieving certification doesn't have to be difficult or expensive. Using an online information security management system (ISMS) that incorporates GDPR and Cyber Essentials Plus is a simple and cost-effective way to carry out an audit and highlight the areas that your business needs to focus on.

CySure's cyber-security solution is designed to deliver these quick wins. Our system provides businesses with a staged approach to compliance and certification, guided by a virtual online security officer (VOSO). At less than the cost of a daily coffee, SMEs can pave the path to cyber resilience. To read more download our latest white paper entitled "Small business and cyber security: The importance of being cyber ready in an online world (https://cysure.ltd/resources/)

Guy Lloyd is Director at CySure.

(i) UK Government Cyber Security Breaches Survey 2020
(https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020#cha

(ii) Gartner CEO liability report
(https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liable)

About CySure

CySure is a cyber security company founded by experts with extensive experience in operational and risk management. The company has offices in London (UK) and California (USA) and CySure's flagship solution – Virtual Online Security Officer (VOSO) is an information security management system (ISMS) that incorporates GDPR, US NIST and UK CE cyber security standards to guide organisations through complex, emerging safety procedures and protocols, improve their online security and reduce the risk of cyber threats.

For more information please visit CySure (http://www.cysure.ltd)

Press contact: Mary Phillips/Andreina West
PR Artistry Limited
T: +44 (0)1491 845553
E: mary@pra-ltd.co.uk