Cyber incidents increased by 1000% in the finance sector alone - 3 reasons why businesses need to be cyber ready

Submitted by: PR Artistry Limited
Thursday, 17 October 2019

The number of cyber-crime incidents recorded by the UK's Financial Conduct Authority (FCA) increased from 69 in 2017 to 819 in 2018 - an increase of 1000%. However, the finance sector is not alone. Joe Collinwood, CEO at CySure explains why in the technological age no business can afford to be under prepared when it comes to cyber security.

The finance sector regulator, the FCA, has recorded a ten-fold increase in cyber-crime incidents (i), however, across all sectors more businesses are reporting being impacted by a cyber incident year-on-year. According to a recent report conducted by Hiscox (ii), there has been a sharp increase in the number of cyber-attacks this year, with more than 60% of firms having reported one or more attacks, up from 45% in 2018.

The same report shows that cyber security incidents cost the average small business (under 50 employees) $29,000. Cyber related costs typically include ransoms paid, hardware and software systems replaced, the impact of losing customers and difficulty attracting future business and damage to reputation, all of which can be difficult if not terminal for a small business.

In a rapidly evolving landscape of cyber threats it is vital that organisations of all sizes and sectors understand the risks and act fast. Often hardest hit is small to medium enterprises (SMEs), that lack the expertise and financial resources to withstand the fallout from a cyber incident. Here are three reasons why SMEs need to become cyber ready:

1. Missing out on lucrative supply chain contracts
The Hiscox report revealed that supply chain incidents are now common place and contributing to the rise in cyber-crime. Nearly two-thirds of firms surveyed (65%) have experienced cyber-related issues in their supply chain in the past year. Whilst not always the case, it is often SMEs with their limited IT expertise and resources, that have the weakest cyber-security arrangements.

In addition organisations that are subject to the EU General Data Protection Regulation (GDPR) have a limited time to report a data breach to the Information Commissioner's Office (ICO). Under GDPR, data controllers are responsible for their own compliance as well as that of any third-party processors. As a result, organisations are closely examining the security practices of any potential third party and seeking agreements to the measures it will take to secure its systems. It's time for SMEs to step up and prove their security credentials – or risk missing out on lucrative business opportunities.

2. Data loss, fines and tarnished reputations
The sharp rise in the number of cyber-incidents reported by the UK's financial sector is likely to have been driven in part by the GDPR. The regulation introduced an obligation on all organisations to report certain types of security breaches. Data is a lucrative currency and cyber criminals are motivated by financial gain. Organisations such as legal and accountancy firms are viewed as rich pickings, as they are a "gateway" to client information. SMEs in these sectors are perceived as soft targets with few security barriers, limited cyber security tools and little or no in-house expertise. Regardless of size,

if your business handles personal information then data protection laws apply. Failure to comply could result in a hefty fine and a tarnished reputation. Should a business be implicated in a data breach it may be forced to cease operating during an investigation if data procedures are classed as unsafe. The temporary barrier to access market opportunity could prove impossible to recover from.

3. Cyber resilience = Business resilience

The risk of an attack cannot be minimised, cyber criminals are business like in their approach, for them attacks are a low-risk, high-reward model. This particularly applies to SMEs and sectors such as accountancy and law firms where the criminal gains can be significant. A recent poll conducted by the UK Law Society (iii) showed that approximately 80% of firms have reported phishing attempts in the last year. SMEs need a strategy to identify and proactively minimise risks. Certification provides a practical framework for an organisation to assess its current cyber hygiene levels and take steps to protect itself against common cyber-attacks.

Increasingly we are seeing company boards requesting assurance on how a company is preparing for cyber breaches and how it will deal with the aftermath through agreed protocols. Part of a board's fiduciary responsibility is to identify and mitigate those risks that could impact the organisation. Good cyber hygiene not only demonstrates good information governance; when performed properly it results in the protection of stakeholder assets and the potential mitigation of legal and compliance risks.

Don't get caught out

Criminals are continually lowering technical barriers to entry, making crimeware-as-a-service available on the dark web. Being unprepared is no longer an option, organisations need to get proactive in protecting their data and that of their customers – or risk the consequences.

Cyber Essentials in the UK and National Institute Standards and Technology (NIST) in the US can help organisations implement strong, cyber security hygiene practices. Being fully Cyber Essentials compliant is said to mitigate 80% of the risks faced by businesses such as phishing, malware infections, social engineering attacks and hacking. By utilising an online information security management system (ISMS) that incorporates NIST and Cyber Essentials Plus, organisations can undertake certification, guided by a virtual online security officer (VOSO), as part of their wider cyber security measures. To download CySure's latest white paper entitled "Small business and cyber security: The importance of being cyber ready in an online world" visit CySure (http://www.cysure.net)

Joe Collinwood is CEO of Cysure

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

(i) SC Magazine|https://www.scmagazineuk.com/third-parties-contribute-1000-increase-finance-sector-cyber-crimes/article/1589653]
(ii) Hiscox Cyber Readiness Report 2019
(iii) Law Society (https://www.lawsociety.org.uk/communities/the-city/articles/cybersecurity-biggest-threats-legal-sector/)