The ugly truth: the real cost of cyber breaches to SMEs

Submitted by: PR Artistry Limited
Wednesday, 9 December 2020

Cyber security preparedness is more than a nice to have, an SME's survival can depend on it. Guy Lloyd at CySure explains why.

Small and medium sized enterprises (SMEs) rarely trigger national headlines for breaches in data security and compliance, not because they aren't a target but because the monetary impact is small compared to the big corporations. However, breaches are all too common and the while the cost of cyber breaches to SMEs, including the impact to business operations, remediation work and resultant fines, may not run into millions, it can do untold damage. SMEs are agile and lean in their business operations, and so unbudgeted costs can severely impact finances.

Such is the concern about the UK economy's resilience to cyber attacks that the UK Government recently commissioned a study (i) to analyse the cost of cyber breaches. It found that organisations are being hampered from managing and mitigating cyber risks by a lack of transparency, awareness and understanding of the costs. UK businesses tend to overlook indirect and long-term costs when assessing the impact of a cyber breach. This leaves organisations woefully unprepared for the financial impact, which in the most extreme cases, can spell an end to the business. SME's in particular are most likely to underestimate the costly impact from non-compliance with cyber security breach-related laws and regulations, therefore leaving them unprepared for any potential fines.

Bumper year for cyber crime

The Coronavirus pandemic has provided cyber criminals with a fertile ground to execute scams and reap a bounty of riches. Attacks designed to steal valuable company and customer information have skyrocketed in 2020. Interpol(ii) reported that in a four-month period some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs, all related to COVID-19 were detected. With many of us working/schooling from home, our concentration levels have been tested to the max. When under pressure and distracted it is easy to click on a phishing email or unknowingly visit a scam website. The rush to remote working has opened up opportunities for hackers and any company with lax security measures makes easy pickings.

Work smarter, not harder

In today's GDPR world no company can afford to be naïve or negligent about regulatory compliance. Cyber Essentials is the UK Government-backed scheme that aims to help organisations protect themselves against common cyber threats. It offers organisations a way to demonstrate to customers and suppliers a commitment towards cyber security and data protection by achieving an accredited and registered certification standard. It lays the foundation to developing policies and procedures to mitigate against threats that can impact business operations.

Getting started can seem daunting but achieving certification doesn't have to be. Using an online compliance risk management system that incorporates GDPR and Cyber Essentials Plus is a simple and cost-effective way to achieve certification. SMEs should look for a solution that can guide them through a gap analysis to highlight the business areas to focus on.

Cyber security doesn't need to be complex, costly or confusing. A low cost, simple set of actions as defined in Cyber Essentials can go a long way to protect against common attacks.

Preparedness in uncertain times
Business confidence comes from understanding the risks involved and the knowledge that should the worse happen it is possible to keep calm and carry on. Being certified with a creditable scheme delivers the assurance that SMEs can demonstrate their commitment and attention to bolstering cyber defences.

Uncertain times can hit when we least expect but the benefit of certification through with help from an information security management system (ISMS) is knowing your business is prepared. Now more than ever we should be celebrating business resilience and preparedness.

Guy Lloyd – Director at 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 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

(i) Analysis of the full cost of cyber security breaches Report
(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/901569/Analysis_of_the_fu

(ii)Interpol report shows alarming rate of cyberattacks during COVID-19
(https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COV