

Redefining cyber security as a business enabler - 3 ways SMEs can benefit

Submitted by: PR Artistry Limited

Wednesday, 8 May 2019

In an era defined by cyber crime it is easy to take the view that cyber security is exclusively an IT cost and the necessary price of doing business. Joe Collinwood, at CySure explains why it's time to look beyond the traditional defensive role of cyber security and recognise its innovative possibilities.

The consequences of a data breach can be a disaster for small and medium-sized enterprises (SMEs) which is why cyber security should be a fundamental component of business operations. The repercussions of a breach extend far beyond the costs that are easiest to calculate, such as incident response, external technical services and communications. The indirect financial cost can be far harder to calculate and remediate such as lost business stemming from reduced customer and supplier trust, damage to brand reputation and fines from the Information Commissioner's Office (ICO). The biggest killer for businesses is the disruption to the business and the time lost while trying to get the business operational again

With the constant threat of a potential cyber attack it is easy to see why some companies develop a defensive and reactive cyber security posture. However, if SMEs are to remain relevant and competitive in the digital economy, it is vital they ensure innovation isn't stifled by rigid security practices. A cyber security strategy developed in line with business goals can support business agility, develop customer loyalty and facilitate operations.

Here are 3 ways SMEs can achieve business growth through effective cyber security management.

1) Support business agility

Digital transformation has changed the business landscape creating a competitive and fast paced world. In this intensely competitive environment, start-ups and online companies are damaging traditional brands with innovative digital business models, products and services. SMEs can adapt swiftly to changing environments, embracing digital technologies to improve their internal processes, product offering and enhancing the customer experience.

Providing services in the connected world is increasingly more risky but SMEs that view cyber security as an essential foundation will have the confidence to implement digital processes and technologies that fuel innovation and growth. Without it, companies may hesitate to start digital projects, therefore stifling their innovation potential and opening the door to competitors.

2) Improve data management – the positive impact of GDPR

The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 and is designed to govern how every organisation treats the personal information it has collected by putting individuals firmly in charge of the way their data is used. The processes necessary for GDPR compliance can deliver many commercial advantages, after all data is the lifeblood of any organisation.

By taking a proactive stance towards GDPR, SMEs can take control of their data and engage with customers

and prospects on a more personalised level. By developing a reputation for safeguarding sensitive information and providing transparency to customers, businesses can improve brand loyalty while gaining new customers. Business growth is dependent on customer trust. Security savvy organizations that can demonstrate a trusted track record and commitment to protecting customer information can maximise on the opportunity to differentiate themselves from the pack.

3) Smoother operations

SMEs are more at risk from data breaches than large organisations because cyber criminals recognize that SMEs do not have the money or resources to launch a legitimate defence and therefore are easy prey. According to the Cyber Security Breaches Survey 2018 (i), 42% of small businesses identified at least one breach or attack in the last 12 months. In a rapidly evolving landscape of cyber threats, SMEs which understand the risks and have a robust cyber security strategy are more able to recover business operations when a breach happens.

This ability to demonstrate cyber resilience is becoming a contractual requirement to many large organisations that rely on a vast network of agile SME suppliers and partners within their supply chain. SMEs that invest in cyber security can show they are less likely to be a conduit for criminals to access a larger organisation, and are better placed to demonstrate their ability to recover business operations and performance in the event of an attack, therefore protecting the supply chain. While no security strategy can stop 100% of attacks, the aim is to mitigate the risk as much as possible.

Positioned for growth with cyber security

SMEs have an inherent advantage over larger companies as their agility enables them to be flexible and adjust to changes quickly. The lack of red tape and corporate complexity means they can act and adapt fast. A strong cyber security posture encourages data management leading to better customer profiling and greater customer loyalty. Good cyber hygiene practices demonstrate to customers, partners and investors that the organization is a trustworthy provider of goods and services, and protector of customer data.

Cyber security need not be prohibitively expensive. SMEs should seek solutions matching their size and requirements. By utilizing an online information security management system (ISMS) that incorporates Cyber Essentials Plus in the UK and NIST controls in the US, SMEs can be guided by a virtual online security officer (VOSO) to understand just how safe and compliant to regulations they are as part of wider cyber security measures.

A cyber security strategy creates a culture of innovation and trust, both essential for business growth. By giving cyber security the same priority as other business goals, SMEs can position themselves for success and thrive in the digital age.

(i)Cyber Security Breaches Survey 2018, gov.uk
(<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018>)

Joe Collinwood is CEO of Cysure Limited

ENDS

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.

CySure also supplies organisations with cyber insurance to supplement their security strategy and offset crippling forensic and remediation costs in the event of a cyber breach.

For more information please visit CySure (<http://www.cysure.net>)

Press contact: Mary Phillips/Andreina West

PR Artistry Limited

T: +44 (0)1491 845553

E: mary@pra-ltd.co.uk