Cybercrime & the bottom line: 5 Reasons why SMEs can’t ignore cyber security

Submitted by: PR Artistry Limited
Wednesday, 29 May 2019

The digital world offers many opportunities for business growth however it exposes organisations to new cyber risks. Weak cyber security can leave organisations exposed and the revenue repercussions can be severe. Joe Collinwood, CEO at CySure identifies the risks and how to mitigate them.

The benefits of operating in the digital world presents many opportunities to small and medium enterprises (SMEs) however it opens organisations to a host of cyber risks. Although cybercrime is the biggest challenge for many organisations, and often leads to financial loss. Changes in business practice in addition to technological changes are opening up threats which need to be managed to avoid negatively impacting revenue. Here we explore 5 ways cyber security issues can impact the bottom line.

1. Business disruption

Too many SMEs hold the belief that they are too small to be attacked and that their sector would be of no interest to a cyber-criminal. Unfortunately, SMEs are as much at risk from cyber security risks as large organisations. 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. Depending on the severity of the attack, SMEs can suffer severe disruption, including impacting business operations and preventing staff from carrying out their day to day work. The U.S National Cybersecurity Alliance(ii) found that 60 percent of small companies are unable to sustain their businesses over six months after a cyber-attack. Being prepared for when, not if, the inevitable happens is key to recovery. SMEs that view cyber security as an essential foundation, with documented policies and processes, will be better positioned to withstand the after effects of a cyber security incident.

2. Data loss and regulatory fines

Data breaches are costly, not only in regulatory fines but in lost business confidence from customers, suppliers and partners. According to the Ponemon Institute’s 2018 Cost of Data Breach Study(iii), the average cost of a stolen or lost record is $148, while the average annual overall cost of a data breach is nearly $4 million. This is irrespective of the fines and sanctions under the new EU General Data Protection Regulation (GDPR) and California’s Consumer Protection Act which comes into effect on 1st January 2020 which will surely add to those costs. EU GDPR is the most significant change to data protection legislation in Europe for over two decades and puts individuals back in the driving seat of how their data is used. There’s no exemption for small businesses or sole traders. By taking a proactive stance towards data protection, SMEs can take control of their data and engage with customers and prospects on a deeper and more personalised level, maximising on the opportunity to differentiate themselves from the pack.

3. Intellectual property

The current cyber landscape is chaotic, from state-sponsored hackers to financially motivated cybercrime gangs. In a rapidly evolving landscape of increasingly sophisticated cyber-attacks, there is a very real risk of a hacker gaining access to intellectual property or other sensitive commercial information and using it to their advantage. Whilst no security strategy can stop 100% of attacks, the aim is to mitigate the risk as much as possible. The majority of attacks exploit basic weaknesses in IT systems and

software, which can be straightforward to defend against. It's time for SMEs to redefine their approach to information security and view it as a way of life aligning security concerns with business goals. By having a top-down, consistent approach to data governance, backed up with the necessary resources and employee training, SMEs can ensure compliance becomes an integral part of the operation.

4. Reputational damage

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 the erosion of customer and supplier trust. However, the real expense of an attack against an organisation is the damage to brand reputation. Suffering a cyber-attack can cause customers to lose trust and spend their money elsewhere. Additionally, having a reputation for poor security can also lead to a failure to win new business or government contracts.

5. Third party relationships

Many organisations often rely on a vast network of agile SME suppliers and partners. However, with so many prolific data breaches occurring due to flaws in third-party partners, SMEs are coming under increasing pressure to prove their security credentials – or risk missing out on lucrative business opportunities. The cyber threat landscape is more real and harmful than many businesses want to accept. However, cyber security need not be complex or prohibitively expensive. SMEs need to seek solutions matching their size and needs which may not necessarily be the same solutions used by a big organisation.

SMEs have an inherent advantage over larger companies, 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. By giving cyber security the same priority as other business goals, SMEs can maintain their advantage and thrive in the new digital world.

Joe Collinwood is CEO of CySure Limited

(i) Cyber Security Breaches Survey 2018
(http://www.Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf)

(ii) The U.S National Cybersecurity Alliance - Small Companies Cyber Attack
(http://www.small-companies-cyber-attack-60%-out-of-business/)

(iii) Ponemon Study (https://costofadatabreach.mybluemix.net)

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