Cyber resilience in uncertain times: 5 steps for SMEs to survive and thrive

Operating online brings benefits to SMEs, but it also brings the risk of cyber attacks. Joe Collinwood, CEO at CySure, details five steps to cyber resilience

LONDON, UK, June 26, 2019 /EINPresswire.com/ -- When it comes to cyber crime, small businesses are not exempt from the disruption that impacts large organizations. If anything, their size can make them more vulnerable as they are perceived as a softer target. That isn't to say that SMEs are unaware of cyber risks - according to the Cyber Security Breaches Survey 2019[i], 78% now see cyber security as a high priority. However, only 15% of small businesses have a formal cyber incident management process.

> By developing a cyber resilience stance based on following a few simple steps, SMEs can not only survive but thrive in the new digital world."
>
> *Joe Collinwood, CEO, CySure*

Two-thirds of SMBs have suffered a cyber attack in the past 12 months[ii] according to the 2018 State of Cybersecurity in Small & Medium Size Businesses report. No business is too small to be attacked, nor too small to protect itself. SMEs can pave the path to cyber resilience by following 5 simple steps:

1. Maximise your best asset – your people

Your employees are your greatest asset and the first line of defence. Training is absolutely vital. Among the SMEs that identified a breach or attack in the 2019 survey, 63% had their most disruptive breach reported by staff rather than by antivirus software. People are the only link that can bind technology, processes and policies together to ensure business goals are met. By having the right policies, processes and training in place for preventing, as well as reacting to a cyber threat, SMEs can create the best scenario to restore operations post incident.

2. Invest in cyber insurance

Becoming more resilient to cyber risks in an age of digital disruption increasingly means understanding how to restore operations quickly should the worst happen. Cyber insurance is specifically designed to cover the unique exposure of data privacy and security and can act as a backstop to protect a business from the financial and reputational harm resulting from a breach. Standard policies are often inadequate to cover the likely cost of even a more "standard" security breach, let alone cyber attack or 'hacktivism'. Only specialist cyber insurance policies provide extensive cover.

3. Secure and back up data

Data is the lifeblood of any organisation yet many SMEs either fail to back up their data or they are not doing so effectively. Losing the ability to restore business critical data, such as customer data and financial information after an incident can be catastrophic. Data loss can damage reputations and paralyse businesses, but these are by no means the only problems. Since the EU General Data Protection Regulation (GDPR) came into force on 25 May 2018, organizations of all sizes can face hefty fines should they suffer a data breach. SMEs must take control of their data and ensure business critical information is securely backed up and can be restored at speed.

4. Ensure good malware and virus protection
Good cyber resilience goes hand in hand with good cyber hygiene. Whilst cyber resilience is all about ensuring a business can continue to operate after or even during an event, cyber hygiene is about proactively offsetting those risks in the first place. Phishing emails and malware infections caused by attachments and links to hacked web sites have become common occurrences. To counter act these evolving threats organizations should focus on getting the basics right and developing a cyber hygiene habit. The benefit of regular maintenance is that it identifies potential issues early, before cyber security risks become a problem. SMEs should invest in effective firewalls, anti-virus and anti-malware solutions and ensure any updates and patches are applied regularly, ensuring that criminals can't exploit old faults or systems. The National Cyber Security Centre advises updating software as soon as a new patch or update is available. Additionally, user passwords should be changed regularly and unused equipment disposed of securely.

5. Demonstrate commitment to security – get certified!
Cyber Essentials (CE) in the UK and the NIST Cybersecurity Framework in the US are government and industry backed voluntary schemes to help all organisations protect themselves against common cyber-attacks. The CE and NIST schemes aim to provide businesses with a structured framework and continuous process that implements the minimum standards to mitigate the risk from cyber attacks.

For example Cyber Essentials certification in the UK can help SMEs implement strong, cyber security hygiene practices. Being fully Cyber Essentials compliant mitigates 80%[iii] of the risks faced by businesses such as malware infections, social engineering attacks and hacking. By utilising an online information security management system (ISMS) that incorporates Cyber Essentials Plus, SMEs can undertake certification guided by a virtual online security officer (VOSO) as part of its wider cyber security measures.

Agile and resilient
According to the Business Population Estimates conducted by the UK Government, small and medium businesses make up 99.9%[iv] of all private sector businesses in the UK. However, almost half (43%) of British SMEs admit to having no business continuity, disaster recovery or crisis management plans in place, despite almost the same number of UK businesses (46%) suffering at least one cyber security breach or attack.

Smaller organisations are by nature agile and innovative, harnessing the power of technology and the internet to reach their customer base, however this also increases the attack surface. The path to becoming cyber resilient can be daunting but it is not insurmountable. By developing a cyber resilience stance based on following a few simple steps, SMEs can not only survive but thrive in the new digital world.

[i] Cyber Security Breaches Survey 2019
[ii] 2018 State of Cybersecurity in Small & Medium Size Businesses report
[iii] https://www.cyberessentials.ncsc.gov.uk/
[iv] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663235/bpe_2017_statistical_release.pdf

Mary Phillips
PR Artistry
+44 1491 845553
email us here