Keep your cyber security in check – 4 reasons to get certified from CySure

When it comes to cyber security breaches – is it when, not if? Joe Collinwood at CySure discusses how certification can give SMEs good cyber hygiene

LONDON, UK, January 17, 2019 /EINPresswire.com/ -- Cyber security has become a fundamental component of business operations. As cyber criminals get more sophisticated and threats continue to evolve it is vital that companies invest in security policies, procedures and products regardless of size, market or location.

Small and medium-sized enterprises (SMEs) are as much at risk from data breaches as large organisations. According to the Cyber Security Breaches Survey 2018, 42% of small businesses identified at least one breach or attack in the last 12 months. This is a significant problem which is set to increase as criminals find new ways to digitally delve into organisations for increasingly valuable personal information.

> Certification has many benefits; it ensures standardisation within the supply chain and is a good differentiator for SMEs who provide services as it shows a diligence to information security. ”
>
> *Joe Collinwood, CEO, Cysure Limited*

However, it is not an insurmountable problem and SMEs can protect themselves against common cyber-attacks by undertaking a certification process. Cyber Essentials is a government and industry backed scheme to help all organisations protect themselves against common cyber-attacks. In collaboration with Information Assurance for Small and Medium Enterprises (IAMSE) they have set out basic technical controls for organisations to use which is annually assessed. Here are four reasons to get certified:

1. Mitigate cyber risks
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, and these can be quite straightforward to defend against. Being fully Cyber Essentials[i] compliant mitigates 80% of the risks faced by businesses such as malware infections, social engineering attacks and hacking. The Cyber Essentials scheme aims to provide businesses with a strong base from which to reduce the risk from these prevalent cyber-attacks.

2. Identify weak security links in your supply chain
As the saying goes, you are only as strong as your weakest link and this is especially true when dealing with third parties that are outside of your domain of control. The 2017 Data Risk in the Third-Party Ecosystem study found that 56% of respondent organisations had been affected by a third-party data breach, up from 49% the previous year. This should be a major concern to any organisation as GDPR makes it clear that organisations are accountable for data breaches

caused by any third-party service providers they appoint to handle data.

Organisations, or in GDPR speak, 'controllers', must only appoint third party 'processors' who can provide sufficient guarantees that the requirements of the GDPR will be met and the rights of data subjects protected. By using a third party that has achieved certification via a scheme such as Cyber Essentials or IASME governance standard, organisations can show that they have taken steps to conduct due diligence within its supply chain. Certification demonstrates that information security procedures within a third-party processor are certified to be the same, or more comprehensive than, the information security procedures followed by the controller organisation for the data involved in the contract.

3. Show commitment to cyber security
By displaying the Cyber Essentials badge on its website, an SME can demonstrate to customers, partners and investors their commitment to cyber security. This is particularly beneficial for organisations that are storing personal information on customers and employees, or hosting commercially sensitive data. Through certification, SMEs can proactively provide sufficient guarantees that regulatory requirements will be met and the rights of data subjects protected.

4. Competitive advantage
Improving cyber security within its supply chain is a priority for UK Government. It has decreed that suppliers must be compliant with the Cyber Essentials scheme in order to bid for contracts which involve the handling of sensitive information and the provision of certain technical services. However, Cyber Essentials presents a competitive advantage to certified SMEs when competing for all business or tendering for public sector proposals as they will be able to demonstrate their security credentials and their diligence towards defending the integrity of their customers' data.

Supported at every stage
Achieving safety and compliance doesn't have to be a costly or complex project. By utilising an online information security management system (ISMS) that incorporates Cyber Essentials, SMEs can undertake a certification route guided by a virtual online security officer (VOSO) as part of their wider cyber security measures. This will help the organisation to coordinate all security practices in one place, consistently and cost-effectively. Additionally, SMEs can take advantage of the expertise of online cyber security consultants at a fraction of the cost of a full time in-house security specialist or a team of consultants.

Certification has many benefits; it ensures standardisation within the supply chain and is a good differentiator for SMEs who provide services as it shows a diligence to information security. The UK National Cyber Security Centre has taken a leadership role in providing the technical expertise for the Cyber Essentials scheme, which ensures that it encompasses the county's best technical insight and experience. Cyber Essentials certification can help SMEs implement strong, cyber security hygiene practices and benefit from the new digital world.

[i] https://www.cyberessentials.ncsc.gov.uk/

Joe Collinwood is CEO of Cysure Limited

Mary Phillips
PR Artistry
+44 1491 845553
email us here