Worried about the financial impact of data breaches? 5 reasons for cyber insurance

Joe Collinwood at CySure explains why cyber insurance is a business essential for companies

LONDON, UK, January 31, 2019 /EINPresswire.com/ -- Cyber risk remains a key concern for every boardroom and small to medium enterprise (SME) business owner. The current cyber landscape is chaotic including state-sponsored hackers, financially motivated cybercrime gangs and simple negligent data loss. Risk is everywhere and liabilities are high. Cyber threat remains one of the most significant and growing risks facing organisations today and too few are prepared.

> Insurance should be viewed as an important addition to a company's overall risk management"
>
> *Joe Collinwood, CEO, CySure*

The global average cost of a data breach per compromised record in 2018 was $148, a 6.4% increase from 2017, according to the Ponemon Institute 13th-annual Cost of Data Breach Study. Interestingly, locations that experienced the most expensive data breaches include the US and the UK, where notification costs are nearly five times the global average. It is clear the problem isn't going away. Although cyber security most often makes it into the headlines because of large breaches, the most frequent threat is actually to SMEs. 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. Research conducted by the National Cyber Security Alliance revealed that 60 percent of hacked small and medium-sized organisations go out of business after six months.

Five reasons for cyber insurance
Becoming more resilient to cyber risks in an age of digital disruption means understanding the full scope of cyber governance responsibilities. Here are five reasons why every business, regardless of size or ownership, needs cyber insurance:

1. Cyber crime is growing exponentially – an overwhelming majority of businesses are reliant

on online services, which exposes them to cyber security risks. The 2018 Cyber Security Breaches Survey, conducted on behalf of the UK Government, revealed that 43% of UK organisations surveyed had experienced a cyber security breach or attack in the last 12 months. With highly sophisticated attacks now commonplace, businesses need to assume that they will be breached at some point and have coverage to mitigate the risk.

2. Data breaches are costly – as mentioned before, in Ponemon Institute's 2018 Cost of Data Breach Study, the average cost of a stolen or lost record is $148, while the overall cost of a data breach is nearly $4 million. This is irrespective of the fines and sanctions under the new General Data Protection Regulation (GDPR) within the EU and California's Consumer Protection Act, which comes into effect on 1st January 2020 and will surely add to those costs.

However, the real expense of an attack against an organisation is not just the financial damage suffered or the cost of remediation, a data breach can also inflict untold reputational damage. 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.

3. Organisations can be held legally and financially liable if third party data is compromised in a breach – emerging regulation as announced by the US Department of Defence (DoD) and the EU's GDPR, places the responsibility on organisations to only appoint third parties who can provide sufficient guarantees that the requirements of NIST 800-171 and GDPR will be met. Both the DoD and the UK's Information Commissioner's Office (ICO) will hold liable, and may, fine any organisation that has not carried out due diligence to ensure third parties are compliant. Regulatory fines have become synonymous with data breaches and the fact that cyber risks are now global, makes complying with various regulatory responses across different geographies all the more challenging.

4. Standard insurance policies do not cover cyber risk - 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. While some categories of losses might be covered under standard policies, many significant gaps often exist and cyber events can impact numerous lines of insurance coverage. Standard policies are often unlikely to cover the cost of even a "standard" security breach, let alone cyber-attack or 'hacktivism'. Only specialist cyber insurance policies provide extensive cover. However, organisations need to research policies carefully to understand the level of cover offered and their responsibilities to stay within the conditions of the policy.
5. Improved cyber awareness and risk management – insurance is just one piece of the puzzle and solely taking out a cyber insurance policy won't protect an organisation from a cyber-attack. Given that the single greatest cyber risk is social engineering, ie employees voluntarily but unknowingly allowing an attack to occur, it's critical that organisations get the basics right, such as putting every employee through training on how to avoid and recognize cyber threats. The fact is that the vast majority of damage done by cyber-attacks is due to an inability of the party

being attacked to respond. Organisations need a comprehensive risk management plan that details how the company will respond in the face of a cyber-attack, that includes unknown threats.

Getting the basics right
Given the complexities and ever-changing threats it is important to be proactive as possible. Cyber Essentials is a UK government-backed and industry supported scheme that guides organisations on how to protect themselves against the most common cyber threats. Undertaking a certification route will help organisations, especially SMEs which may not have a dedicated cyber security specialist, to coordinate all security practices in one place, consistently and cost-effectively.

Certification is a valuable indicator of a mature approach to cyber security in organisations. It helps to guard against the most common cyber threats and demonstrate a commitment to cyber security. Whilst cyber insurance can provide a layer of protection when an organisation is faced with a cyber threat, it is no substitute for good cyber hygiene. Insurance should be viewed as an important addition to a company's overall risk management, but organisations should not wait for a breach before confronting their cyber risks and exposure.

Joe Collinwood is CEO of CySure

Mary Phillips
PR Artistry
+44 1491 845553
email us here