Cyber Risks & Liabilities

March/April 2019

Protect Your Organisation from These New Cyber-threats

As technology continues to advance in the workplace, it has become even more critical to ensure proper cyber-security measures within your organisation. And one of the best ways to ensure robust cyber-risk management practices is by staying updated on the latest cyber-threats.

In the recently released European Union Agency for Network and Information Security (ENISA) Threat Landscape Report 2018, ENISA identified Europe's top 15 cyber-security threats from the past 12 months. While the top four threats remained identical to previous years (eg malware, web-based attacks, web-application attacks and phishing), the report discovered a rise in two relatively new cyber-threats—cryptojacking and denial of service (DoS) botnets.

Don't let these evolving concerns cause disaster within your business—use this guidance for an overview of the new threats and best practices to reduce your risk:

- **Cryptojacking**—This threat takes place when cyber-criminals hijack the victim's computer power via an internet browser or email to mine cryptocurrencies (eg Bitcoin or Monero) without consent from the victim. Cryptojacking is a serious concern, as it can cause significant financial loss in seconds. Consider these tips to protect your business:
    - Keep your internet browsers secure by installing ad-blocking and anti-cryptomining extensions.
    - Prevent email hacking by reminding staff members to never click on suspicious websites or links in their emails.
- **DoS botnets**—While normal botnets can be beneficial, malicious botnets hack into your device and trick you into downloading software that allows the botnet's owner to gain full control of your device. From there, the botnet owner can execute a DoS attack to shut down your organisation's website or email spam to millions of internet users. Use this advice to avoid botnet issues:
    - Never download attachments or software without confirming its validity.
    - Routinely update your devices' operating systems. In addition, be sure to implement hacking safeguards such as firewall and anti-malware software.

As cyber-threats continue to evolve, so do your insurance needs. You can ensure ultimate peace of mind against data breaches with robust cyber-cover. For more information and insurance solutions, contact Blackfriars Insurance Brokers Ltd today.

BLACKFRIARS GROUP INSURANCE

Blackfriars Insurance Brokers Ltd
6 Congleton Rd
Sandbach, CW11 1HN
0161 300 2930
www.blackfriarsgroup.com

The GDPR Is in Full Effect: An Overview of the Latest Fines

It has been nearly a year since the GDPR went into effect, and several organisations have since been exposed to the costly non-compliance price tag. While high-profile prosecutions have yet to occur within the UK, the following incidents emphasise the importance of GDPR compliance:

- **Failed consent policies in France**—French regulators gave Google a record-setting GDPR fine of €50 million (£42.7 million) for failing to provide transparent and accessible information on its data consent policies in January 2019.
- **Password problems in Germany**—In September 2018, a German social media company suffered a cyber-attack that compromised the personal data of over 800,000 users. An investigation revealed that the users' passwords had been stored in unencrypted text. The financial penalty was €20,000 (£17,000).
- **Camera concerns in Austria**—In October 2018, an Austrian business received a GDPR fine of €4,800 (£4,100) for installing a CCTV camera in front of their establishment that also recorded a portion of the public pavement.
- **Safeguard slip-ups in Holland**—In November 2018, the Dutch government discovered that Microsoft had failed to follow GDPR privacy guidelines when handling 300,000 Dutch workers' information. No fine has been issued, but the company could face millions of pounds in punishment.

Take Steps to Mitigate These Common Causes of Data Breaches Within Your Organisation

Recent reports identified the following factors as top causes of cyber-attacks:

External attackers **48%**

Human error and negligence **27%**

Technical error **25%**

Addressing the Gap in Your Cyber-security Approach: Staff Training

In the midst of the GDPR and a growing risk of cyber-attacks across industry lines, your organisation has more than likely bolstered their cyber-security practices in the past year. But have all of your staff members received the message?

Recent reports revealed that despite increased efforts and spending in the realm of reducing cyber-risk**,** over 60 per cent of UK businesses identified that they have a cyber-security skills gap. What's more, over half of these organisations believe they have an increased risk of suffering a data breach as a result.

Such startling statistics emphasise that your organisation can't ignore the gap in your cyber-security approach any longer. Indeed, it's crucial to ensure that all staff members are updated and aware of cyber-related risk management practices in your workplace to avoid suffering the costly consequences.

Make sure all of your employees can help prevent a cyber-attack and comply with the GDPR with this staff training guidance:

- **Keep it specific**—Avoid using a generic presentation or guide to communicate your cyber-security measures to staff. Make sure employees understand the specific role they play in helping prevent a cyber-attack. This entails identifying threats that different departments are more likely to face (eg phishing, insecure networks or dated software) and ensuring they know how to mitigate their daily risks.
- **Make it entertaining**—No one wants to listen (nor will they pay proper attention) to a lingering lecture on cyber-security. Be sure your training programme is fun and captivating for employees by utilising hands-on activities or acting out different cyber-attack scenarios.
- **Offer incentives**—Employees will be much more motivated to practise proper cyber-security measures if they feel valued for doing so. If a worker recognises a cyber-concern and follows correct protocol, make sure you praise their achievement with an award or an all-staff congratulatory email.
- **Stay updated**—Staff training shouldn't be a single occurrence. Keep employees updated on the latest threats and risks with a routine training schedule and additional resources.