CYBERRISKS+LIABILITIES

July/August 2017

IN THIS ISSUE

Petya and WannaCry Highlight Need for Robust Cyber Security and Cover

After the two major cyber attacks earlier this year, your organisation can no longer be passive with cyber security. Learn how you can better protect your organisation from cyber threats.

One Year Countdown Until GDPR: Is Your Organisation Compliant?

The GDRP will come into force in less than a year. You should start reviewing now how your organisation can prepare.

Recent Cyber Security News and Prosecutions

Read about how a supermarket chain was fined for ignoring customers' marketing wishes, a firm that was fined £50,000 for nuisance calls and how a used-car dealer was fined for sending over 300,000 spam text messages.

Packetts

Petya and WannaCry Highlight Need for Robust Cyber Security and Cover

The global cyber attacks caused by the ransomware programs, WannaCry and Petya, spread to more than 150 countries. WannaCry alone infected more than an estimated 230,000 computers. Ransomware is one of the most common cyber attacks, accounting for 17 per cent of all security breaches in the United Kingdom in 2016, according to government research. Even worse, an estimated 54 per cent of UK organisations have been the victims of ransomware.

The attack's effects can be quite severe, causing business disruptions, financial loss, and partial or total loss of data. There can also be 'slow burn' costs, including reputational damage, litigation and loss of competitive edge. What's more, if your business is hit by a cyber attack and criminals breach personal customer data, you'll have to deal with business disruption and those slow burn costs as well as an Information Commissioner's Office (ICO) fine. In fact, cyber breach fine amounts are expected to raise significantly after the General Data Protection Regulation (GDPR) comes into force in May of next year.

With the potential devastating effects and exploitable gaps in cyber defences, robust cyber security and cover is no longer an option, it's a necessity. To ensure that your organisation is adequately protected from cyber threats, consider implementing the following practices:

- Update your network security.
- Install and update anti-virus as well as anti-malware software on all your organisation's computers.
- Provide your employees with cyber security training. This should include best practices, such as how to recognise and respond to a cyber attack.

Yet, the most vital component of a solid cyber defence is purchasing comprehensive cyber insurance to ensure that your organisation cannot only sustain but overcome a cyber attack. For more information, contact Packetts today.

Recent Cyber Security News and Prosecutions

Morrisons Supermarket Chain Fined for Ignoring Customers' Marketing Wishes

After sending out 130,671 emails to people who had previously opted out of receiving marketing related to their Morrisons More card, Morrisons was fined £10,500. In its investigation, the ICO found that the company's actions deliberately broke the Privacy and Electronic Communication Regulations (PECR). What's more, the GDPR, a new data protection law concerning organisations receiving consent from customers, comes into force next year. That means incidents, such as this, will have much more severe penalties.

Maidstone Firm Responsible for Nuisance Calls Fined £50,000

The ICO received 169 complaints about receiving unwanted calls from MyHome Installations Ltd. Over a period of 18 months, the company bought customer data from third-party companies in order to make unsolicited phone calls, even to individuals on the 'no call' register. As these actions violated the PECR, the company was fined £50,000.

Radcliffe Used-car Dealer Fined £40,000 for Sending 336,000 Spam Texts

Concept Car Credit Limited sent more than 300,000 spam-marketing text messages without ensuring that it was only contacting individuals that had consented to receive the marketing. In addition to a £40,000 fine, the ICO also issued the company an enforcement notice, ordering it to stop sending unlawful texts. If the company does not comply with the notice, it could face additional fines and penalties.

One Year Countdown Until GDPR: Is Your Organisation Compliant?

In less than a year, the EU General Data Protection Regulation (GDPR) will come into force. The forthcoming guidelines are intended to create uniform data protection rules for EU member states. Despite Brexit, UK organisations that want to conduct business in the EU must also comply with the GDPR. The government has confirmed that the United Kingdom's decision to leave the EU will not affect the commencement of the GDPR.

As the GDPR will be formally adopted on 25th May 2018, your organisation must begin taking the necessary steps, if you have not already done so. By that date, your organisation should complete the 12 steps outlined by the Information Commissioner's Office (ICO), which can be found here. Especially if your organisation relies on a constant stream of prospect data for its sales pipeline, now is the time to audit that data to ensure you can keep prospecting and selling after the GDPR commences. If your organisation fails to comply with the new regulation and does not provide adequate cyber protection for your customers, you could receive sizeable fines and penalties. The GDPR has a simple, two-tiered fine structure:

1. An organisation may be fined up to €10 million (roughly £8 million) or 2 per cent of its annual turnover—whichever is higher—for not properly filing and organising its records, for not notifying the supervising authority and data subject about a breach, and for not conducting impact assessments.

2. An organisation may be fined up to €20 million (roughly £16 million) or 4 per cent of its annual turnover—whichever is higher—for violating the basic principles related to data security or for violating consumer consent.

To assess how prepared your organisation is for the GDPR, you can complete this five-step self-assessment from the ICO. For more information about what cyber precautions your organisation can take in order to defend itself, contact the professionals at Packetts today.

Had the GDPR been applied to ICO's 2016 fines, the total would have been a staggering

£69 MILLION

rather than merely

£880,500.

Source: NCC Group

Packetts
Salts Wharf, Ashley Lane
West Yorkshire, BD17 7DB
01274 206 500
http://www.packetts.com