# CYBERRISKS+LIABILITIES

January/February 2017

## IN THIS ISSUE


**Cyber Criminals Can Exploit Any Organisation's Weaknesses, No Matter the Size**

*In 2016 alone, businesses of all sizes received an average of 230,000 cyber attacks. Learn about the weaknesses in their cyber defences in order to bolster your own.*

**Most Pay Ransomware Despite Claiming They Never Would**

*Within the last two years, nearly half of all UK businesses have been infected with ransomware, a malicious and dangerous piece of software that could bring your business to a grinding halt.*

**Recent Cyber Security News and Prosecutions**

*Read about how the British Heart Foundation and the Royal Society for the Prevention of Cruelty to Animals were fined by the ICO for secretly screening millions of their donors, how fines under the General Data Protection Regulation (GDPR) could cost the UK economy £122 billion, and about three former Enterprise Rent-A-Car employees that used their positions for personal gain before being caught by the ICO.*


Packetts

## Cyber Criminals Can Exploit Any Organisation's Weaknesses, No Matter the Size

On average, each UK business was subject to 230,000 cyber attacks in 2016, according to research provided by internet service provider, Beaming. Very few of these attacks were successful, but the sheer volume is noteworthy. In November, for the first time ever, more than 1,000 attacks per day hit individual company firewalls, contributing to an overall cost to the UK economy of £34.1 billion. What's more, is that 2 out of 3 large businesses and SMEs were hit with cyber attacks in 2016, according to research from the government and the Federation of Small Businesses. Even though businesses of all sizes are being targeted by cyber criminals, the methods that they use to get past the various cyber defences can be drastically different.

Below are some common trends among both large businesses and SMEs that your organisation can review in order to better prepare itself.

### Large Businesses' Cyber Weaknesses

- **Overconfidence.** According to a report published by multinational professional services firm, EY, 50 per cent of the organisations surveyed stated that their cyber defences would be able to detect a sophisticated cyber attack. However, 86 per cent of the surveyed organisations also stated that their cyber security does not adequately meet their organisation's needs.
- **Lack of a formal cyber security breach programme.** Sixty-four per cent of organisations do not have a cyber security breach programme in place. This includes cyber security training for all employees in order to help them identify, handle and report cyber threats. What's more, 55 per cent of organisations are unable to identify vulnerabilities in their cyber security.

### SMEs' Cyber Weaknesses

- **Lack of cyber defences.** Despite the potential risks that cyber attacks pose, 45 per cent of SMEs still do not have a cyber breach response plan. Even worse, only 7 per cent of SMEs have cyber insurance, according to industry research.
- **Doubt.** According to market research specialists, Juniper Research, 27 per cent of SMEs believe that they are too small to be of any interest to cyber attackers. This perception of invulnerability can be rather costly, as the average cost of a cyber breach is between £75,000 and £310,000. Furthermore, this does not include costs due to a loss of reputation or business disruptions.

# Recent Cyber Security News and Prosecutions

### British Heart Foundation and Royal Society for the Prevention of Cruelty to Animals Fined

Both the British Heart Foundation (BHF) and the Royal Society for the Prevention of Cruelty to Animals (RSPCA) were fined for secretly screening millions of their donors. The intent of the organisations was to identify wealthier donors and target them specifically in order to receive more donations. Upon completing its investigations, the Information Commissioner's Office (ICO) issued a substantial fine to each organisation (£18,000 to BHF and £25,000 to RSPCA) and instructed them to cease their data-matching activities to obtain data that donors had not freely provided.

### Fines Under GDPR Could Cost British Businesses £122 Billion

According to new findings from the Payment Card Industry Security Standards Council, UK businesses could experience up to £122 billion in fines for cyber security breaches in 2018. The estimate is based upon the new EU legislation that will set regulatory penalties for cyber security breaches at 4 per cent of global turnover. In addition, the council has stated that the cap for the penalty will be set at £18 million. Whilst the United Kingdom may have already left the EU by 2019, Prime Minister Theresa May has stated that she intends to sign all current European law into UK law and repeal it gradually. That means that the forthcoming cyber security legislation would still apply to UK businesses even after Brexit.

### Individuals Fined for Violating Data Protection Act

Three former employees of Enterprise Rent-A-Car—Andrew Minty, Jamie Leong and Michelle Craddock—pled guilty to conspiracy to steal customer information. At different times, each of the former employees obtained personal data from the company's systems and passed it along to claims management companies in order to pursue personal injury claims. Minty was fined £7,500. Leong was sentenced to a conditional discharge for 12 months, with prosecution costs of £3,000 to be paid within two years. Craddock was also sentenced to a conditional discharge for 12 months, with prosecution costs of £1,200 to be paid within two years.

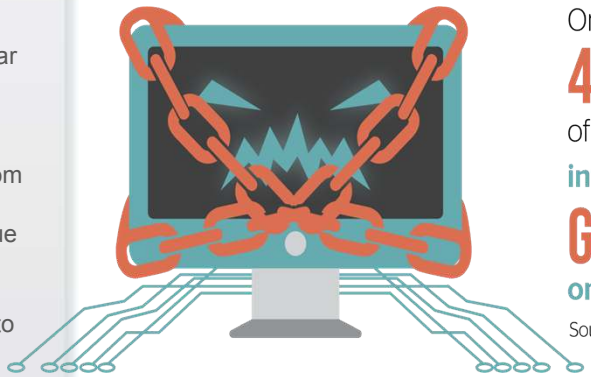
# Most Pay Ransomware Despite Claiming They Never Would

Within the last 24 months, 44 per cent of all UK organisations have been infected by ransomware, and 27 per cent of those were infected more than once, according to recent research published by cyber security firm, Trend Micro. Ransomware is a type of malicious software (malware) designed to block access to specific data, files or even the entire computer until a designated sum is paid to the cyber criminals responsible for the attack. Of the organisations that have been infected with this type of malware, 1 in 3 stated that their employees were affected by the attack along with an estimated 31 per cent of their customers. This type of cyber attack can be especially dangerous if an organisation does not have any sort of digital backup for the data and files that could be sequestered by malware.

Despite the potential damage that this type of cyber attack could cause, nearly 75 per cent of surveyed organisations who have not been infected by ransomware stated that they would never pay cyber criminals. Yet, 65 per cent of organisations that have been infected end up paying the ransom. The average cost for an organisation is £540, but 1 in 5 businesses have paid more than £1,000. Unfortunately, less than half of those organisations actually get their blocked data back.

The effects of a cyber attack are not just financial, as an organisation infected with malware may also be affected by a loss of reputation and business interruptions. In fact, it takes an average of 33 hours to repair the damage caused by ransomware. To ensure that your organisation is protected from ransomware, follow these simple best practices:

- Provide all employees—from the directors and officers to the interns—with comprehensive data security training to ensure that they know how to identify and manage cyber security threats, such as suspicious email requests or webpage prompts.
- Purchase cyber insurance and install security software on each computer in your organisation to detect and stop malware and viruses. In addition, you may want to consider drafting a non-work mobile device policy to minimise the potential of a data breach caused by an employee's personal device.



Only
**45 PER CENT**
of organisations that have been
**infected by ransomware**
**GET THEIR DATA BACK**
**once they have paid.**
Source: Trend Micro

*Contains public sector information published by the ICO and licensed under the Open Government Licence v3.0.*

Design © 2017 Zywave, Inc. All rights reserved. This publication is for informational purposes only. It is not intended to be exhaustive nor should any discussion or opinions be construed as compliance or legal advice. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.

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