CYBERRISKS+LIABILITIES

September/October 2018

IN THIS ISSUE

These Two Cyber-attacks Are on the Rise—Here's How to Protect Yourself

Although clicking on and responding to emails in the workplace is a common practice, recent research revealed it's also a top cyber-security concern. Indeed, among the methods cyber-criminals use to attack organisations, social engineering scams and ransomware are on the rise.

Social engineering scams, such as email attacks and phishing scams, accounted for over 25 per cent of cyber-incidents earlier this year, affecting organisations across various industry sectors. These incidents can cause serious damage, compromising sensitive data at the click of a button. And although social engineering schemes can cost organisations over £1 million, they are preventable.

You can help your business avoid social engineering scams by communicating with your staff about phishing attacks and providing them with proper training to identify fraudulent or suspicious emails. Emphasise the importance of checking that the sender's email address seems valid (this includes reaching out to the user to confirm their identity), the message doesn't contain any typos or grammatical errors, and the links don't have lengthy, suspicious URLs when your mouse hovers over them.

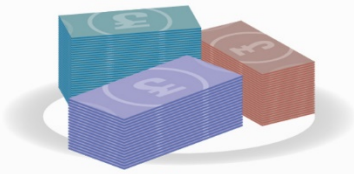
Ransomware, which is a form of malicious software (malware) that blocks access to a device until some form of ransom is paid (such as large amounts of money), has impacted nearly 60 per cent of organisations in the past year—up 10 per cent from 2016, according to research from cyber-security experts, SentinelOne. What's more, incidents such as WannaCry highlight cyber-criminals' ability to use ransomware to attack hundreds of devices across the globe at one time.

To decrease your organisation's risk of a ransomware attack, routinely update your company's operational systems and antivirus software to avoid vulnerabilities from outdated technology. In addition, ensure these systems are effective by running tests and conducting frequent assessments. You should also have a plan in place in case an attack occurs. Communicate the plan to all employees so everyone knows how to respond in this situation.

For more tips regarding cyber-security, contact Robison & Co Ltd today.

SMEs Suffer Greater Loss in the Event of a Cyber-attack: **Here's the Evidence**

Although rising cyber-attack methods such as phishing and ransomware can impact all organisations, SMEs face significant risk because:



They are more willing to pay **ransoms.**

They likely have fewer cyber-security measures in place.

In the past year, **42%** of all cyber-attacks occurred against small businesses.

60% of small businesses fail within 6 months of a cyber-attack.

Source: ICO and industry research

Here's Why You Can't Make the Mistake of Mishandling Your Customers' Data

Between the implementation of the GDPR and a frenzy of high-profile data breaches, this past year has strengthened public concern over personal data protection and misuse. Not to mention, now that the public has more rights regarding the details of their personal data collection, processing and use, they are more likely to join in the efforts to hold organisations accountable for their mistakes.

In the ICO's 2018 Information Rights Survey, data revealed a range of public opinions surrounding organisations' use of their personal data. The main research findings include the following:

- **Improvements in overall trust and confidence**—The amount of people who trust businesses with their personal data has risen slightly since 2017. Specifically, the proportion of the public that places high trust in companies storing and using their data has significantly increased—from 21 per cent in 2017 to 34 per cent in 2018. But, it's important to note that despite this change, the amount of people that possess low trust in these practices remains greater.
- **Technology troubles**—The data revealed that the public is divided on whether or not organisations protect their personal data from technology risks. Alongside this suspicion, the public said their biggest concern when organisations use their personal data is the risk of personal information being stolen by criminals.
- **GDPR support**—Although the survey found that public awareness of the GDPR varies considerably, more work is being done to increase awareness about the regulation than the Data Protection Act did in the past. A majority of the public agrees that it's important to protect any personal information they share, and almost 20 per cent of adults feel they have a good understanding of how their personal data is used and made available by UK organisations (an 8 per cent increase from last year). Lastly, there has been a significant rise in people seeking information from public bodies, like the ICO, following the GDPR.
- **Room for concern**—Despite improvements in overall trust and confidence, suspicion and concern remain prevalent in the realm of data collection. The survey found over 50 per cent of people are still concerned about automated decision-making. Not to mention, the proportion of people stating that they or a close family member have heard about a data breach has risen. In addition to these concerns, nearly 80 per cent of people felt that if an organisation who used their data suffered a data breach, then that company should be held responsible for the loss.

Robison & Co Ltd
6 Rotherbrook Court, Bedford Road
Petersfield, Hants, GU32 3QG
01730265500
www.robison.co.uk