CYBERRISKS+LIABILITIES

March/April 2017

IN THIS ISSUE

CIAT Insurance Services
Administered by McPartland Finn Ltd

March 2017 Government Report: 'Cyber Threat to UK Business is Significant and Growing'

'The Cyber Threat to UK Business', the first joint report by the new National Cyber Security Centre (NCSC) and the National Crime Agency (NCA), presented a rather disheartening outlook for the digital safety and security of UK organisations. In fact, three months after it became operational in October 2016, the NCSC has had to address 188 high-level cyber attacks, including Russian state-sponsored hacks.

Whilst most UK organisations will likely not be targeted for state-sponsored attacks, each business was subjected to 230,000 cyber attacks in 2016, according to internet services provider, Beaming. In addition to noting the high volume of cyber attacks experienced by organisations, the report also identified current trends in cyber threats, which include the following:

- The technical skill required to successfully carry out a cyber attack continues to decrease, as malware and services, such as distributed denial of service (DDoS) attacks, can be acquired on the dark web without much difficulty.
- The ever-increasing number of internet-connected devices—including mobiles, wearables and smart appliances—provides cyber criminals with significant opportunities for attacks.
- Threat actors, which are either individuals or software that are responsible for incidents that breach an organisation's security, are learning skills and methodologies from one another.

In response to these cyber threats, 28 per cent of UK businesses indicate they plan on taking out cyber cover this year, and 59 per cent plan on increasing their cyber security budgets, according to industry research. To protect your business, the NCSC offers the following tips:

- Report cyber attacks to Action Fraud at 0300 123 2040.
- Invest in cyber security, which should include robust anti-virus and malware detection software, as well as cyber cover.
- Provide your employees with basic cyber security training, which outlines risky online behaviour.

For more help managing cyber risk, contact the professionals at CIAT Insurance Services today.

Recent Cyber Security News and Prosecutions

Businesses Could Face Fines for Not Registering CCTV Cameras with the ICO

A Coventry business owner was fined £200 and ordered to pay £439.28 in prosecution costs and a £20 victim surcharge after she plead guilty to violating Section 17 of the Data Protection Act (the Act). The business owner was using in-store closed-circuit TV (CCTV) cameras as part of her business but was unaware that she had to register them with the Information Commissioner's Office (ICO). However, the ICO had sent her letters explaining that she was in violation of the Act and needed to register her cameras along and pay the £35 annual fee. Whilst the business owner received the ICO's letters, she chose to ignore them, as she thought they were spam.

ICO Issues One of Its Highest Fines to Firm Behind 22 Million Nuisance Calls

Media Tactics, a telemarketing services firm for businesses, was fined £270,000—one of the highest fines that the ICO has issued for nuisance calls—and given a legal notice to stop making unlawful calls after it was found guilty of making more than 22 million nuisance calls. In its investigation, the ICO found that the firm not only did not have permission to make the calls, but that the list of numbers used were gained from untrustworthy third parties. If the firm does not comply with the ICO's legal notice, it could result in further court action.

ICO Issues Guidance for Consent Under the GDPR

The government announced that it will be adopting the General Data Protection Regulation (GDPR), which will come into force on 25th May 2018. The GDPR will affect companies that conduct business with mainland Europe. In order to prepare your company for the GDPR, the ICO released guidance for consent. Since the GDPR builds upon the Data Protection Act, there is a high standard of consent that companies have to meet during the process of gaining customers' consent. Your company can review the ICO's guidance by clicking here.

Apps and Smart Appliances May Pose a Significant Cyber Security Threat

Despite the fact that 79 per cent of surveyed UK organisations have some type of cyber defences, 57 per cent of those organisations have experienced at least one cyber attack within the last 12 months, according to a recent survey from multinational defence and security company, BAE Systems. On average, these cyber attacks cost organisations £330,000. However, that figure does not include the cost of business disruptions or the loss of reputation.

These numbers are so high because hackers have more routes than ever to breach your defences—including mobile apps and smart appliances. Whilst mobile apps—such as Slack, Evernote, WhatsApp and Dropbox—may help your employees complete their tasks more efficiently, your IT department may not approve them for official use due to the potential security threats that they pose. Some apps—such as those that are cloud-based—are often granted access to the mobile's camera, location, data and contacts, which means that a cyber criminal could hack the device through an app and spy on your organisation.

Similarly, smart appliances—including TVs, thermometers and refrigerators—can also provide cyber criminals with access to your organisation. Not only can cyber criminals spy on your organisation through the microphones installed in your smart appliances, but they could also adjust the settings on the devices, which could potentially impact efficiency and quality.

To ensure that cyber criminals cannot gain access to your organisation via mobile apps and smart appliances, follow these four best practices:

1. Develop a mobile device management programme.
2. Encrypt and install anti-virus software on all corporate mobile and smart devices.
3. Explain to your employees what corporate data can and cannot be shared with third-party apps.
4. Have IT monitor what apps and data are being accessed on company networks.

THIRTY-FIVE PER CENT
of UK businesses have admitted that they changed nothing after a cyber security incident.

CIAT Insurance Services
Barlow House, Minshull Street
Manchester, M1 3DZ
(0161) 233 4497
http://www.ciat-insurance.co.uk