CYBERRISKS+LIABILITIES

May/June 2017

IN THIS ISSUE

WannaCry Highlights Severity of Cyber Attacks

WannaCry, a ransomware program that targets a vulnerability in outdated versions of Microsoft Windows, has spread across 150 countries and infected more than 230,000 computers since it was launched on 12th May. It disrupted many NHS hospitals in England and Scotland, infecting up to an estimated 70,000 devices, including computers, MRI scanners, blood-storage refrigerators and theatre equipment.

Microsoft was aware of this cyber security gap and, as a precaution, released a Windows security update in March. However, many users had not run the update, which allowed WannaCry to spread quickly. After the initial discovery of the ransomware program, Microsoft issued a warning to the US government concerning its data-storing practices. According to Microsoft, the tool used in the WannaCry cyber attack was developed by the US National Security Agency and was stolen by hackers.

The danger that the ransomware program poses is based partially on how invasive it is. After infecting just one computer, WannaCry can spread to every device in a network within seconds. It works by locking users out of their computers before demanding money in order to regain control of their data. Initially, WannaCry requests about £230, but, if no payment is made within three days, it then threatens to double the amount. If no payment is made within that time, the ransomware program then threatens to delete the files after seven days.

While the spread of WannaCry has appeared to slow down, many firms have hired experts to prevent new infections. Some experts recommend that you should not pay the ransom, as there is no guarantee that the hackers will return the files unharmed, if returned at all. The government's National Cyber Security Centre recommends that you take the following precautions:

- Update your network security and keep a safe backup of your vital files.
- Run the Windows Update and turn on auto-updates, if available.
- Install and update anti-virus as well as anti-malware software on all of your organisation's computers.
- Provide your employees with cyber security training. This should include best practices, such as how to recognise a cyber attack.

However, the most beneficial practice that your organisation can invest in is to purchase comprehensive cyber insurance to ensure that your organisation can sustain a cyber attack. For more information, contact GS Group today.

Recent Cyber Security News and Prosecutions

Record Fine for Firm Behind Nearly 100 Million Nuisance Calls

Keurboom Communications Ltd was fined £400,000, the highest fine issued by the Information Commissioner's Office (ICO) for making nuisance calls. Over 18 months, the company made 99.5 million nuisance calls. In its investigation, the ICO found that the company hid its identity during the calls—making it difficult for people to complain—and made calls to some people without their express consent. In addition, the company and its director ignored the ICO's seven separate information notices, which has led to the company being placed in voluntary liquidation.

ICO Warns UK Firms to Respect Customer Data Wishes as it Fines Flybe and Honda

Flybe, an Exeter-based airline, and Honda Motor Europe Ltd were fined a collective £83,000 for breaking the rules about how customers' personal information should be treated when sending marketing emails. In its investigation, the ICO found that both companies had sent unwanted emails to customers that had already specified that they did not want to receive them. Both cases emphasise the importance of receiving and verifying customer consent.

Online Retailer Left Customers' Financial Details Vulnerable to Cyber Attack

Construction Materials Online Ltd was fined £55,000 after the company failed to protect its customers' personal information. In its investigation, the ICO found that the company did not have adequate cyber protection to prevent an attack. This security gap was exploited by a cyber criminal to access 669 unencrypted cardholder details, which included names, addresses, account numbers and security codes.

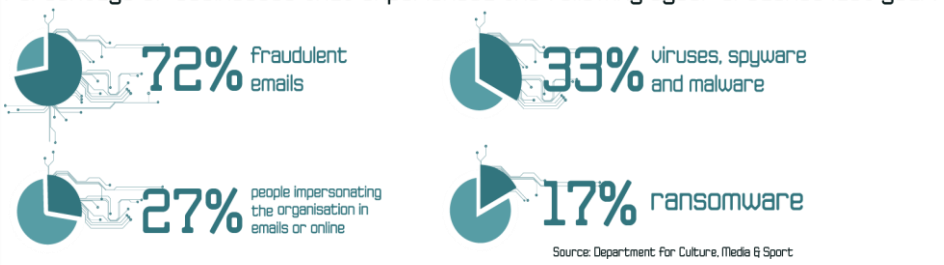
Government Releases 2017 Cyber Security Breaches Survey

The government recently published its 2017 Cyber Security Breaches Survey, which provides a way for you to compare the effectiveness of your cyber security efforts and learn how you can improve them. By examining last year's mistakes, your organisation can better adapt its cyber security efforts to protect the private data of customers and the organisation itself. Here are four key figures from 2016:

1. Forty-six per cent of all UK businesses reported at least one cyber breach or attack last year, a 22 per cent increase.
2. Seventy-four per cent of UK organisations have stated that cyber security is a high priority for them, an increase of 4 per cent over the previous year. The increase could be attributed to more organisations educating their staff about the dangers of cyber threats as well as the high volume of attacks on UK organisations.
3. Seventeen per cent of cyber security breaches experienced in 2016 were caused by ransomware, which was the fourth-most common type of cyber breach, after fraudulent emails, malware and people impersonating organisations, respectively. While ransomware may seem like less of a priority, its effects can be severe, causing business disruptions, partial or complete loss of important data, and loss of reputation.
4. Sixty-seven per cent of all UK organisations have spent money on their cyber security. What's more, is that 52 per cent of all organisations have enacted the basic technical controls that were outlined in the government-endorsed Cyber Essentials scheme.
5. Fifty-seven per cent of UK organisations have established procedures to identify cyber security risks, an increase of 6 per cent.

Whilst the majority of the figures outlined in the report saw an improvement over the previous year, cyber security should still be top of mind. To help ensure that your cyber security efforts are thorough and comprehensive, periodically have a cyber security professional inspect your organisation to identify any potential gaps in your cyber defences. In addition, provide your employees with annual training on how to identify and handle cyber threats.

Percentage of businesses that experienced the following cyber breaches last year:



GS Group
South Inch Business Centre
Perth, Perthshire, PH2 8BW
01738 441 555
www.gs-group.uk.com