CYBERRISKS+LIABILITIES

November/December 2016

IN THIS ISSUE

Crendon Insurance Brokers

5 Social Engineering Strategies That Threaten Your Company

Regardless of how much your company may have invested in its cyber security, there will always be one glaring vulnerability—the people that work there. Instead of using sophisticated and malicious computer codes, cyber criminals employ social engineering strategies to gain access to your company's confidential information. These strategies are meant to persuade, trick, blackmail, threaten, or deceive you and your employees in order to help cyber criminals carry out their crimes. What's more, is that a recent study published by the Federation of Small Businesses found that 66 per cent of its members were victims of cyber attacks within the past two years—and that 86 per cent of these attacks were social engineering scams.

To help your company identify these types of attacks, be on the lookout for the five most common social engineering strategies:

1. **Phishing** is when emails are sent from an allegedly trusted source—such as your bank—and ask for sensitive information, such as your password(s).
2. **Spear phishing** is a specialised attack on a specific person—such as someone in the accounting department at your company.
3. **Physical baiting** is when a criminal leaves a piece of hardware—such as a USB stick or CD—that has been infected with malware at the office in hopes that someone will load it into an office computer.
4. **Pretexting** occurs when an attacker poses as someone within your company—such as a senior IT manager—or someone your company regularly does business with—like a supplier—and creates false, urgent circumstances to compel an individual to provide sensitive information.
5. **CEO fraud** is when a criminal poses as the CEO or another senior member of your company in order to pressure someone that is able to initiate payments to transfer money to a specific bank account.

Protecting against social engineering strategies is simple as long as you implement the following strategies:

- Establish a process for requesting and authorising payments that requires two points of contact.
- Organise a procedure for what employees should do if they receive an unusual or suspicious email.
- Provide your entire staff—from the directors and officers all the way down to the interns—with comprehensive cyber security training to ensure that they know how to identify and manage cyber security threats.

Risk management alone is no match for today's sophisticated cyber criminals. To ensure your company stays protected, pair your cyber security efforts with a comprehensive cyber insurance policy. For more information, contact the experts at [B_Officialname] today.

Recent Cyber Security News and Prosecutions

Confirmed: UK Government Will Implement the GDPR in 2018

In a recent announcement, the government confirmed that it will be adopting the General Data Protection Regulation (GDPR). The regulation will come into force on 25th May 2018, and will impact companies that wish to continue conducting business with mainland Europe once Brexit negotiations have been finalised. As your company now has less than two years to prepare and adopt the necessary measures, you should follow the step-by-step guidance that the ICO has outlined to ensure that your company is adequately prepared. The ICO's guidance can be found at https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when.

Cyber Insurance Vital After Worldwide October DDoS Attacks

On 21st October, a distributed denial of service (DDoS) attack caused an internet blackout on the US East Coast and affected access to the web all over the world. DDoS is a malicious attempt to make a server or a network resource unavailable to users—typically by overwhelming it with fake traffic. Within the past year, the frequency of this type of cyber attack has increased by 125 per cent. This shocking growth is due in part to companies' challenges with adequately defending their IT networks. It is therefore absolutely essential that your company—regardless of size or industry—protect itself with cyber insurance. In addition, you should implement robust technology-based cyber risk mitigation strategies—such as installing security software to detect and stop malicious malware and viruses.

TalkTalk Fined Record £400,000 for Failing to Prevent October 2015 Attack

TalkTalk was fined £400,000—the largest fine issued by the ICO—after security failings allowed a cyber criminal to easily access its customer data. Between 15th and 21st October 2015, a cyber criminal accessed the personal data of 156,959 customers—which included names, addresses, dates of birth, phone numbers and email addresses. In its investigation, the ICO found that the company failed to properly scan Tiscali after acquiring it to ensure that there were no gaps in Tiscali's cyber defences. Upon delivering its fine, the ICO emphasised that the security breach was entirely preventable had TalkTalk taken the proper precautions.

Why Data Transparency Is Vital to Your Firm

The Information Commissioner's Office (ICO) recently released a new code of practice, which outlines how organisations should explain to people how their personal information is being collected, stored and used. What's more, is that this is the first piece of guidance that the ICO has published that provides organisations with instructions on how to comply with both the existing Data Protection Act and the EU's forthcoming General Data Protection Regulation (GDPR), which will enable the ICO to fine businesses 4 per cent of their global turnover for mishandling customer data. The code was written in order to emphasise the importance of trust and transparency for any organisation that handles sensitive customer information—especially since the ICO revealed that only 1 out of 4 adults trust businesses with their personal information.

This lack of trust has people being more proactive in protecting their personal information. Seventy per cent of people routinely check their bank and credit card statements for irregular activity and more than 50 per cent of people have antivirus software installed on their computers. The driving force behind people's behaviour is the concern that their personal information will be stolen by cyber criminals, used to make nuisance calls or sold to other companies for marketing purposes. This response should be treated as a wake-up call for your organisation to adopt more robust and comprehensive cyber security schemes along with a thorough customer privacy policy in order to regain the public's trust.

To ensure that your privacy policy is sufficient and easily understood, follow these guidelines:

- Ask customers to provide their consent to collect their personal information in a clear, obvious manner—such as a tick box that says, 'I agree' or 'I don't agree'. As a part of this process, you should explain what you will be doing with their information.
- Identify what customer information you currently collect that constitutes as personal data, which includes names, addresses, dates of birth, phone numbers, bank account information and email addresses.
- Map out how the information you collect travels through your organisation to identify what types of processes are used and if there are any vulnerabilities in your cyber security.

If you would like to review the ICO's code of practice in its entirety, you can do so by clicking here.

3 OUT OF 4 ADULTS
DO NOT TRUST businesses with their personal information.

Source: Information Commissioner's Office (ICO)

Crendon Insurance Brokers Limited
www.crendoninsurance.co.uk
0121 4 5 45 100
The CIBA Building
146 Hagley Road, Birmingham
B16 9NX

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

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.