CYBERRISKS&LIABILITIES_

Protecting Against Online Fraud

While computers have improved the speed and efficiency of how we work, they have also allowed thieves and con artists an easier avenue by which to steal from people and businesses. One of the ways these cyber criminals use computers to steal is through online fraud, one of the fastest-growing crimes today.

Types of Online Fraud
Your company's intangible assets could be at risk if you or your employees are not mindful of online fraud attempts. Understanding and identifying different types of online fraud could save your company thousands, or even millions of pounds in lost sales, damaged reputation, legal expenses, etc.

- **Social engineering** is the act of taking advantage of human behaviour to commit a crime. Social engineers can gain access to buildings, computer systems and data simply by exploiting the weakest link in a security system—humans. For example, social engineers could steal sensitive documents or place key loggers on employees' computers at a bank—all while posing as an IT consultant from a well-known company. Social engineers can be tough to spot because they are masters at blending in.
- **Phishing** is attempting to acquire information such as usernames, passwords, credit card numbers and other sensitive information by pretending to be a trusted entity in an electronic communication, such as email. One of the more common phishing scams is receiving an email that asks the user to verify his or her account information. A quick check of your email's Spam folder would likely result in a few examples of phishing.
- **Pagejacking and pharming** occurs when a computer user clicks on a link that brings them to an unexpected website. This can happen when a hacker steals part of a real website and uses it in the fake site, causing it to appear on search engines. As a result, users could unknowingly enter personal information or credit card numbers into the fake site, making it easy for a hacker to commit online fraud. Pharming is the name for a hacker's attack intended to redirect a website's traffic to a fake site**.**
- **Vishing** is similar to phishing and pharming, except victims of vishing attacks are solicited via telephone or another form of telecommunications. The hacker can easily pose as a representative of a bank or other institution and collect personal information that way.

Corporate Identity Theft
It doesn't matter if you are a large international company or a local shop, cyber thieves are always looking for their next score. It is often assumed that smaller businesses are too small to escape attention from cyber crooks, but according to Verizon Communication's *2012 Data Breach Investigations Report*, 72 per cent of the 855 data breaches analysed were at companies with 100 or fewer employees. No company of any size is completely safe from cyber thieves.

There are many ways a cyber-thief can steal a company's identity in addition to the various types of online fraud listed above:

- **Stealing credit history** – A cyber thief could steal and use a company's credit history for his or her own financial gain, and then use it to set up a dummy company, racking up huge debt for the real company.
- **Rubbish bin diving** – All too often, papers with sensitive information are recklessly tossed in the rubbish bin instead of being properly shredded and discarded.
- **Hacking** – Having proper security measures in place for your computer system is essential to keep intangible assets safe. Make sure you are using firewalls, routers and other security devices to protect your assets.

Crendon Insurance Brokers

Prevent Online Fraud
Understanding and being able to identify potential online fraud techniques is the key to keeping your company safe. Use the following tips to protect your intangible assets and ensure protection against a data breach:

- Never give sensitive information like credit card numbers out over the phone unless you know the person on the other line.
- Shred all credit reports and other sensitive data before disposal.
- Educate employees about phishing and pharming scams. Remind them to not click on anything that looks suspicious or seems too good to be true.
- If your company doesn't have an IT department, hire an outside company to set up the proper security measures for your computer network.
- Always monitor credit reports and other financial data for the company. If you see things that don't belong, investigate.
- Do not allow employees to write down passwords in the office.
- Always encrypt sensitive data.

If You are a Victim
It is common to have an "it will never happen to us" philosophy when it comes to fraud. Unfortunately, that thinking can lead to lax security measures and carelessness when it comes to protecting intangible assets. If you become a victim of online fraud:

- **Act quickly.** Report the fraud immediately to local police. Notify important suppliers, vendors and partners.
- **Alert your customers.** If there is a data breach involving customers' personal information, activate your plan to alert them. This information could be incredibly harmful to your customers, so alert them as soon as possible.
- **Do an investigation.** If you do not have the resources to do an internal investigation, consult a third party. The quicker the breach can be dealt with, the fewer negative effects your company will endure.
- **Take measures to lessen the chance of a future breach.** Fortunately, cases of online fraud can be good learning tools for your company. Analyse why the breach happened and take steps to make sure it doesn't happen again.

Count on Our Risk Expertise
A data breach as the result of online fraud could cripple your company, costing you thousands or millions of pounds in lost sales and/or damages, not to mention sanctions under the Data Protection Act. Contact Crendon Insurance Brokers Ltd today to learn more about our resources and ensure you have the proper cyber liability cover to protect against losses from fraud.