RISK INSIGHTS

Crendon Insurance Brokers

Notable Cyber Security Fines

The amount of UK businesses falling victim to cyber-attacks has steadily grown over the past several years. Cyber-attacks do not discriminate—businesses, both big and small, urban and rural, and across all industries have been targeted.

It is dangerous to believe that cyber-attacks can only happen to other businesses or that the fines will be miniscule. Cyber-attacks threaten the survival of every business, and the fines can be ruinous. As a business owner or manager, you need to be aware of the risks associated with cyber-attacks and the strategies for bolstering cyber security.

Learn from the mistakes in the following Information Commissioner's Office (ICO) prosecutions to ensure that your business does not suffer the same consequences.

Notable Cyber Security Fines

Charity Fined for Cyber Security Ignorance

- **Background:** The British Pregnancy Advice Service was fined £200,000 after a hacker gained access to thousands of individuals' personal information.
- **What Went Wrong:** The charity was unaware that its official website had been storing the names, addresses, birthdates and telephone numbers of individuals who requested advice on pregnancy issues. A vulnerability in the site's code allowed a hacker access to the system and the collected library of personal information.

Broker Fined After Cyber Criminals Raid Records

- **Background:** Staysure, a personal lines broker, was fined £175,000 after a hacker gained access to the credit card information and medical records of more than 100,000 of its customers.
- **What Went Wrong:** The Company failed to review and update its IT security systems as well as its database software, which generated security gaps. These gaps, coupled with the company's noncompliance of the Data Protection Act, allowed the hacker to gain access to the personal financial information of the company's clients.

The consequences from a cyber-attack are severe, long lasting and potentially ruinous. Do not let your business become a cautionary tale.

Council Penalised for Releasing Sensitive Details

- **Background:** The Islington Council was fined £70,000 after the personal details of more than 2,000 residents were made available to the public on the Web.
- **What Went Wrong:** The council had received a freedom of information request from the What Do They Know website, which enables individuals to submit requests for information to public authorities. Complying with the site's request, council members provided three spreadsheets—which they failed to review for the presence of sensitive private information. The spreadsheets contained information on the housing needs of 2,375 residents, whether they had a history of mental illness or had been victims of domestic abuse. Despite being notified after the first

spreadsheet was released, the council failed to take action, which resulted in the other two spreadsheets being released. This breach occurred, in part, due to the council members' failure to remove the source data of the residents' private information from the spreadsheets.

Company Fined After Sensitive Hard Drive Stolen

- **Background:** Jala Transport Limited, a Wembley-based loans company, was fined £70,000 (which was later reduced to £5,000 due to the company's limited financial resources) after an unencrypted hard drive containing customer data was stolen.
- **What Went Wrong:** The sole proprietor of the business kept the hard drive, along with several other business materials, stored in a case in his car. The case was later stolen as the car idled at a red light. The hard drive—which contained information on the names, birthdates, addresses, the identity documents used to support loan applications, and the payment details of the business' 250 clients—was password protected but not encrypted.

Council Fined for Lax Laptop Security

- **Background:** The Glasgow City Council was fined £150,000 after two unencrypted laptops, which contained personal information of more than 20,000 individuals, were stolen from its building.
- **What Went Wrong:** While the city council building was undergoing refurbishment, lax security allowed an unknown individual access to the office where the laptops were stored. Despite previous warnings from the ICO, the council failed to provide its faculty with laptops capable of encrypting private and sensitive information.

Travel Company Fined for Cyber Negligence

- **Background:** Think W3 Limited, an online travel services company, was fined £150,000 after a hacker gained access to more than 1 million credit and debit card numbers.
- **What Went Wrong:** The company failed to periodically empty its cache of customer information—which it had been collecting since 2006—as well as to perform security checks of its site, which led to the development of gaps in the site's code. These gaps provided the hacker with the opportunity to access the company's library of more than 1 million customer credit and debit card numbers.

Council Fined After Leaving Memory Stick Unattended

- **Background:** The North East Lincolnshire Council was fined £80,000 after an unencrypted memory stick was stolen, which contained sensitive personal information of nearly 300 children.
- **What Went Wrong:** The memory stick—which contained information on the mental and physical health and special educational requirements of 286 students—was left unattended but connected to a laptop in the possession of a special education teacher. After the educator had left the room, an unknown individual stole the device. While the council had introduced a policy of encrypting portable devices, it failed to check that existing devices could be encrypted.

Council Fined After Publishing Sensitive Information

- **Background:** The Aberdeen City Council was fined £100,000 after private information was inadvertently published.
- **What Went Wrong:** When a city council employee accessed documents from her personal computer at home, concerning the families of vulnerable children along with the details of alleged criminal offences, a file-sharing programme automatically uploaded them to the Web for public viewing. The breach occurred, in part, due to the council's lack of a policy concerning accessing documents from off-site personal computers.