CYBERRISKS&LIABILITIES_

NEWSLETTER

December 2013 / January 2014

IN THIS ISSUE

Voice Over Internet Protocol Security

The allure of Voice over Internet Protocol (VoIP) technology—using an Internet connection to make phone calls—is dazzling, but do not get blinded by the novelty. Although the benefits of VoIP seem prepared for long-term sustainability, the technology is not without its flaws. Before adopting VoIP for your business, consider its unique benefits and risks.

VoIP, also known as IP telephony, relies on digital technology rather than traditional analogue phone lines to place calls. It requires a high-speed broadband connection such as DSL or cable, but can contact people over a broadband connection or with a personal telephone. Depending on the service provider, callers can access VoIP wherever they have a high-speed Internet connection, making the technology much more mobile and reliable than other telephone services.

The Benefits
The Internet is everywhere. Because VoIP capitalises on existing Internet connections, many businesses that already have a viable Internet connection are poised to take advantage of VoIP's many benefits, including:

- **Efficient bandwidth use.** VoIP requires less bandwidth to do more.
- **Low transmission costs.** VoIP typically costs less than using a normal telephone. Many services even offer free international calls.
- **Consolidated network expenses.** Consolidating connections lowers operating costs.
- **Increased employee productivity.** VoIP facilitates more communication.

The Security Risks
Do not let VoIP's benefits overshadow its security risks. Any threat to your computers' security is a threat to your VoIP connection. The technology is relatively new and users may be unaware of additional security risks, some of which are enumerated below:

- **Call fraud.** A caller impersonates another user to gain system access or data.
- **Phishing.** A user falls victim to a ruse and voluntarily provides information to a malicious party.
- **Eavesdropping.** A hacker can listen in real time to a conversation or reconstruct it after the fact.
- **Intercepted calls.** Attackers can listen to calls and intercept any data transfers.

As technology develops, so do the threats. But a proactive approach can help curb any malicious attacks. Contact Crendon Insurance Brokers Ltd for tips on keeping your VoIP system secure.

Crendon
Insurance
Brokers

The Necessity of Encryption

Storing valuable information securely is important—your business may need to store sensitive data such as customers' personal information, but storing that data also creates the risk of losing it and paying large fines for data breaches. Simply storing your sensitive information behind passwords or firewalls is not enough—if attackers break through your business' cyber security measures, they will have access to all of your sensitive and valuable information. One way to help protect your data is to encrypt it.

Encryption is not foolproof in prevent hacking or the unauthorised access of information, but it does prevent third parties from reading it. Encryption uses mathematical algorithms and an encryption key to encode data so that only someone who has the encryption key can read the data.

Protecting the encryption key is therefore crucial. Never store it in the same place as the encrypted data. Likewise, never send encrypted data and the key to unlock it in the same message. If you need to send encrypted data via email, provide the key over the telephone to the message's recipient. This prevents an inadvertent or malicious interceptor from reading its contents.

The best encryption method for your business will depend on the sensitivity of its information and its data storage methods. There are many different types of encryption, including the following:

- **Full disk** encrypts an entire disk, including all its data. This method is used to encrypt laptops, desktops and mobile devices.
- **Individual file** encrypts a single file or creates an encrypted repository for file storage.
- **Data transit** encrypts during a transfer, but does not guarantee encryption once the data reaches its destination.

Contact Crendon Insurance Brokers Ltd for more information on encryption and different ways to protect your sensitive data.

Council ordered to pay £80,000 for losing unencrypted data

The Information Commissioner's Office (ICO) served North East Lincolnshire Council with a penalty of £80,000 after a serious data breach exposed hundreds of local children's personal information and special educational needs. The data was stored on an unencrypted memory stick left attached to a laptop in the Council's offices by a special educational needs teacher. When the teacher returned, the memory stick was missing and has still not been recovered. The data was unencrypted even though the Council had introduced a policy that required the encryption of mobile devices three months prior to the incident.

Company failed to register with ICO, fined £1,010.66

The director of a pay day loans company based in London that processes personal information was prosecuted for failing to register his business with the ICO. The Data Protection Act requires that all organisations processing personal information must register with the ICO by paying an annual fee of £35 and providing details about the type of information they process. The director was fined £150 and ordered to pay £1,010.66 in prosecution costs and £20 in victims' surcharge. The company was fined £500, and also ordered to pay £1,010.66 in prosecution costs and a £50 victims' surcharge.

Barclays employee prosecuted for accessing customer data

A 27-year-old former employee of Barclays Bank was fined £3,360 after illegally accessing a customer's information while still employed by the bank. The employee accessed the same customer's information on 22 separate occasions, passing this information onto her friend who was, at the time, the customer's partner. Information shared by the employee included details about the customer's children. The former employee was aware that her actions were against Barclays' policy, as the bank had informed its staff that they should not access customers' accounts unless required. The employee became a former employee shortly after the customer raised concerns with Barclays that his account was being compromised.

CYBERRISKS&LIABILITIES_
NEWSLETTER

Crendon Insurance Brokers Ltd
11 Greenfield Crescent
Birmingham, West Midlands, B15 3AU
0121 454 5100
www.crendoninsurance.co.uk

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.