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. Before adopting VoIP for your business, you should consider its unique benefits and risks.

The Technology
VoIP, also known as IP telephony, relies on digital technology rather than traditional analogue phone lines. It requires a high-speed broadband connection such as DSL or cable, but can contact people with either 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.

You can configure VoIP in one of the following four ways:

- **Dedicated routers** let you use your traditional phones to make VoIP calls. You connect the router to the high-speed Internet source, then connect your phone to the router. With an appropriate VoIP provider and service plan, dedicated routers require little added software or extra setup. You can use your router to make calls while travelling provided you have high-speed Internet access.
- **Adapters** plug into your computer, usually through the USB port, and feature a socket where you connect your phone. The call is made through your computer's Internet connection and works for a standard or mobile phone.
- **Softphones** are software applications that allow you to place calls directly from your computer using a headset, microphone and sound card. Users can typically talk to other people using the same service for free, with other calls costing a small fee. Softphones require the least bit of investment since most businesses already have most of the necessary components.
- **Dedicated VoIP phones** look just like regular phones but connect directly to a computer network rather than a phone line. Some have a base separate from the phone that facilitates the Internet connection, while others may simply be a normal-looking phone.

The Benefits
The Internet is everywhere. Most businesses already possess a viable Internet connection, making them poised to take advantage of VoIP's many benefits, including the following:

- **Efficient bandwidth use.** Compared to regular telephone networks, VoIP is more efficient in terms of bandwidth and equipment use, requiring less to do more.
- **Low transmission costs.** Less bandwidth and equipment means each call your employees place will cost less than one made on a normal telephone. Many services even offer free international calls.
- **Consolidated network expenses.** Businesses normally have a separate telephone line and computer network, but consolidate these two networks for their VoIP connections, saving on operation costs in the process. Internal calls between employees are much cheaper by using the business' already existing Internet connection.
- **Increased employee productivity**. VoIP phone calls are not just phone calls—they allow employees to send data files while talking and without being hindered by a lack of mobility. Employees can take advantage of multiple-party calls or video conferencing, which are impossible on a normal phone. They can also access their offices from home via a VoIP connection.
- **Access to more communications devices.** Unlike standard or mobile phones, VoIP phone calls are not limited to only contacting other telephones. Users have increased access to other communication devices, expanding businesses' reach.

The Risks
Although the benefits of VoIP seem poised for long-term sustainability, the technology is not without its flaws. Consider the security risks and quality drawbacks, enumerated below, before committing to VoIP for your business.

- **Less security.** Calls over the Internet are much less secure than calls over a traditional phone network. This gives rise to several possible security vulnerabilities, including:
    - Call fraud, where a caller impersonates another user, potentially gaining valuable information or access
    - Phishing, when a user falls victim to a ruse and voluntarily provides sensitive information to a malicious party
    - Eavesdropping, where a hacker can listen in real time to a conversation or reconstruct it after the fact
    - Viruses, which damage your network
    - Intercepted calls, meaning attackers can not only listen to a call, they can intercept any data files sent via the VoIP connection

  Any threat to your computer's security is a threat to your VoIP connection. VoIP can actually render your system more vulnerable to attack because increased connections mean increased pathways for hackers or malicious programs to gain access.
- **More spam.** Because VoIP communication is generally cheaper, telemarketers can send more messages, and their messages can be much bigger, requiring more storage on the recipient's end and potentially interrupting service.
- **Slight delay.** There is a small but noticeable delay between a speaker saying something and the listener hearing it.
- **Variable echo.** Call quality is worse with VoIP connections—a variable echo can appear, ranging from only annoying to completely distracting and ruining the efficacy of a phone call.
- **Additional upgrades.** A VoIP system needs regular software upgrades, called patches, unlike a traditional phone system. This means that businesses will need to set aside downtime for telephony upgrades, even though many businesses have never established telephony maintenance time before and may find it difficult to schedule.

Top Security Tips
The risks of VoIP need not outweigh the benefits—implementing a stringent security plan when adopting and maintaining a VoIP system can help curtail many of the nascent technology's risks. Use the following top security tips to keep your system secure:

- **Update software.** If your VoIP software provider releases patches, also called firmware updates, for the program you use, install them. They will ensure your program is protected from any known vulnerabilities in the old version.
- **Install and maintain anti-virus software.** Wield anti-virus software as a persistent guard against viruses and other malicious attacks. Because hackers are continuously developing new ways to attack, make sure you keep your anti-virus software up to date.
- **Capitalise on security options.** VoIP providers usually offer several security options, such as free encryption. Take advantage of any available security incentives.
- **Enable a firewall.** Firewalls help prevent malicious attacks and virus infections. Your system may already have a firewall that just needs to be enabled. Make sure it is up and running.
- **Evaluate security settings.** Before implementing a VoIP system, assess your security infrastructure and toughen it up based on your findings.
- **Secure and back up personal and financial data.** If attackers do gain access to your system, minimise the damage by securing and backing up your most important data. That way you will still have it in the event of a loss, and your attackers will have to work even harder to get it.
- **Create strong passwords.** Security starts within your own organisation—apply tough requirements for password creation to deter attackers.
- **Encrypt communications.** Either use your provider's encryption services or purchase your own. If your VoIP communication is intercepted without being encrypted, attackers will be able to eavesdrop with little effort.

As technology develops, so do the threats. But a proactive approach and the support of the insurance professionals at Crendon Insurance Brokers Ltd can help you stay ahead of the curve and plan a successful future for your business.