Keeping Your Data Secure

Data security is crucial for all businesses. Customer and client information, payment information, personal files, bank account details—this information is often impossible to replace if lost and is extremely dangerous in the hands of criminals. Data lost due to disasters such as a flood or fire is devastating, but losing it to hackers or a malware infection can have far greater consequences. How you handle and protect your data is central to the security of your business and the privacy expectations of customers, employees and partners.

What kind of data do you have?
Your business data may include customer data such as account records, transaction accountability and financial information, contact and address information, purchasing history, and buying habits and preferences, as well as employee information such as payroll files, direct payroll account bank information, home addresses and phone numbers, and work and personal email addresses. It can also include proprietary and sensitive business information such as financial records, marketing plans, product designs and tax information. If you collect personal information, make sure you have a privacy policy that explains how the information will be used and what individuals' rights are regarding the data.

Complete a data inventory to identify and classify all of your potential areas of vulnerability. Common data classifications include the following:

- **Highly confidential**: This classification applies to the most sensitive business information that is intended strictly for use within your company. Its unauthorised disclosure could seriously and adversely impact your company, business partners, vendors and/or customers in the short and long term. It could include credit card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs and employee payroll files.
- **Sensitive**: This classification applies to sensitive business information that is intended for use within your company; information that you would consider to be private should be included in this classification. Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.
- **Internal use only**: This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within your company. While its unauthorised disclosure to outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to negatively impact your company, employees, business partners or vendors.

Classifying your data allows your company to set parameters for how the data is accessed, transported, shared and ultimately kept secure.

Where is your data stored?
Data is most at risk when it's on the move. If all your business-related data resided on a single computer or server that is not connected to the Internet, and never left that computer, it would be very easy to protect. But to be meaningful, data must be accessed and used by employees, analysed and researched for marketing purposes, used to contact customers and even shared with key partners. Every time data moves or changes hands, it can be exposed to different dangers.

It's important to create a company policy that dictates safe data transfer and storage. The policy should include information on how to back up, transport and safely store physical and virtual data.

- **Physical data:** Keep in mind that physical media, such as a disc or drive used to store data or a data back-up, is vulnerable no matter where it is located, so make sure you guard any physical data stored in your office or off-site, and make sure that your

physical data storage systems are encrypted. As much as possible, try to avoid data transport on physical media such as flash drives or CDs. These media can easily end up in the wrong hands.

- **Website data:** Your website can be a great place to collect information, from transactions and payments to purchasing and browsing history, and even newsletter signups, online inquiries and customer requests. This data must be protected, whether you host your own website and manage your own servers or whether your website and databases are hosted by a third party. If a third party hosts your website, be sure to discuss systems it has in place to protect your data from hackers and outsiders as well as employees of the hosting company.
- **Virtual data:** Storing data virtually is a very common practice, but it has certain risks you need to consider. If your company contracts with a third party to house data virtually, be sure to keep an updated, thorough contract that outlines who accesses your data, how it is encrypted and how it is backed up. Additionally, be sure you are aware of the location of the company you are trusting with your data.

Who accesses your data?
Once you have identified, classified and located your data, you must control access to it. The more sensitive the data, the more restrictive the access should be. As a general rule, access to data should be on a need-to-know basis. Only individuals who have a specific need to access certain data should be allowed to do so.

Not every employee needs access to all of your information. For example, your marketing staff shouldn't need or be allowed to view employee payroll data, and your administrative staff may not need access to all your customer information.

The first step in controlling access to your data is assigning rights to that data. Doing so simply means creating a list of the specific employees, partners or contractors who have access to specific data, under what circumstances, and how those access privileges will be managed and tracked. As part of this process, you should consider developing a straightforward plan and policy—a set of guidelines—about how each type of data should be handled and protected based on who needs access to it and the level of classification.

How do you protect your data?
Once you understand the type of data your company makes use of, where it is located and who accesses it, you can begin planning how you will protect it. Protecting data, like any other security challenge, is about creating layers of protection. The idea of layering security is simple: You cannot and should not rely on just one security mechanism—such as a password—to protect something sensitive. If that security mechanism fails, you have nothing left to protect you.

Businesses have many affordable backup options, whether it's backing up to an external drive in the office, or backing up online so that all data is stored at a remote and secure data centre.

Are you planning for the future?
Every business has to plan for the unexpected, and that includes the loss or theft of data from your business. Not only can the loss or theft of data hurt your business, brand and customer confidence, it can also expose you to the often costly violations of the Data Protection Act that cover data protection and privacy. Data loss can also expose you to significant legal actions.

That's why it's critical to understand exactly which data or security breach regulations affect your business and how prepared you are to respond to them. At the very least, all employees and contractors should understand that they must immediately report any loss or theft of information to the appropriate company officer.

Identifying your exposures will help you figure out how to protect your data. In additional to data security measures, insuring your data is crucial. For more information, contact your Crendon Insurance Brokers Ltd representative.