Wedgwood
INSURANCE LIMITED

6 WAYS TO HELP PROTECT YOUR BUSINESS FROM CYBER CRIME

CYBER RISK IS NOT AN "I.T." PROBLEM FOR BUSINESS

Cyber Risk is the newest "buzz" risk facing business, in fact, it's probably the biggest story around technology risk since the "Year 2000" bug back at the turn of the century. In the past, most of the stories were around large corporations being hacked (Target), government agencies (Heartbleed shutting down CRA for a day), or international cyber espionage, usually involving far-east countries.

What doesn't get discussed is the growing problem for small and medium size enterprises (read most businesses) that are now in the sights of hackers, thieves and cyber criminals. This trend has been quietly growing for some time, but rarely makes the news in Canada. Canada has few laws about public disclosure of security breaches.

What business is going to publicly discuss the fact that there computer systems were hacked, especially if they have sensitive or proprietary data belong to customers, employees or vendors?

The potential damage to their business and especially their reputation is a major risk for businesses in many sectors. Until now, we've heard about issues such as personal information belonging to clients being stolen; one of the newer trends is hackers gaining access to systems, changing administrative passwords, and locking the businesses network down. Then, they charge a ransom to have the system unlocked, or threaten a wipe of all the data…..

Scary stuff, right? What to do?

The sensible approach (and a nice start) is to ensure that a good anti-virus program installed that is regularly updated and that there is some kind of hardware/software based firewall so your system isn't open to the outside world. Most businesses would have a vendor, or in-house capability to do this, so let's just accept that fact that any responsible business owner will take these basic steps to secure their network, and the personal information that it may contain.

These are great "IT" related solutions. But……..

YOU CANNOT SOLVE YOUR CYBER RISK EXPOSURE WITH AN I.T. SOLUTION ALONE! HERE'S 6 WAYS TO HELP DEAL WITH THIS RISK…….

A complete approach to dealing with the problem cannot be left solely in the hands of your in-house network people, your system vendor, or the software/hardware your purchase. It requires a company-wide approach that starts at the top. Here are some steps you take can begin to secure your information.

1. **Make system security a priority at the top level of your company.** This doesn't mean the Owner/CEO/Leader needs to get directly involved but they should ensure all team members/employees are aware of, trained about and understand the importance of cyber security. It can reside solely with IT.
2. **Have an outside expert test your network**. As recently as two months ago, Bank of Montreal had an ATM machine hacked by some kids who found an old manual and discovered the default password for the machine. BMO had forgotten to change it. Outside firms are well aware of typical security holes, hardware defaults etc; that many clients may forget to change. Sometimes IT people can feel uncomfortable with this. It's not about lack of confidence in IT, it's about using expert resources that can specialize in this area.
3. **Train your staff**. Firewalls and software are fine, but many times hackers gain access to your business through many simple exploits of human nature. Phishing emails, phone call where they pose as a vendor and get pieces of information, password scams etc; are common ways to get access to your business network. Your team needs to be trained on how to recognize these scams, and how to properly verify that callers are legitimate.
4. **Policies to control password usage**. Passwords are the gateway to your network. Most businesses would be shocked to know how many employees use default passwords,

keep them on sticky-notes around their desk or share them with other employees. This is a recipe for disaster and one of the easiest ways for your system to be compromised.

5. **Mobile devices are small and easily lost stolen or damaged.** If they are not owned by the company, there is even more room for problems, if confidential client data is residing on personal mobile devices. There should be policies around automatic lock, encryption, etc so that data on mobile devices remains secure and doesn't become a gateway into your network.
6. **Look at Cyber Insurance products**. The average cost per record stolen in 2012 was $188 according to a study by the Ponemon Institute. If you have 10,000 client records, that would be a loss just to replace/notify/mitigate of $1,800,000. Can your business absorb this loss, if your best prevention/mitigation efforts failed? These policies are often quite inexpensive and are an affordable way to finance some of the cost of this risk.

No system can be completely bulletproof, but think of a burglar roaming a neighborhood. They'll check various homes, looking for the house without a security system, low level lighting, without a dog on the premises, or an unlocked door. They'll often pick the easiest target.

As cyber criminals scan the internet, is your business the one with unlocked ports into your network and staff inadvertently giving hackers the tools they need to break your security, or is it the one with solid security, trained staff and secure passwords and mobile devices? If it is, they'll likely move on to an easier target, if not, be prepared for a potentially significant financial loss, a damaged reputation and lots of lost clients.