

Wednesday, September 6th, 2006



Information requires safekeeping

Wednesday, September 6, 2006

On the cutting edge / Brian T. D. Bowman

IN today's economy, information is the most valuable corporate asset. And for this reason, businesses of all sizes should take steps to protect corporate information regardless of whether it is stored online or off-line.

Whether it's customer or supplier lists, intellectual property or employees' personal information, it's information that needs safekeeping.

Think of what would happen if a company's biggest competitor were able to secretly sift through its filing cabinets. New inventions, trade secrets, customer lists and business processes would be in the hands of the competitor. In another scenario, think of what would happen to a company if its computers were hacked by online thieves. Regrettably, a number of companies do not have to imagine this. It seems like every day this scenario plays out in the news headlines. The effects are predictable -- lost goodwill for the company and reduced public confidence in online transactions.

Statistics Canada recently released the results of an Internet use survey, which showed that 75 per cent of Canadians have strong concerns about online privacy and security. Partly to combat these concerns, most businesses invest in online security.

But what about "off-line" security breaches? There doesn't seem to be as many headlines on these occurrences, which results in many corporate decision-makers overlooking corporate vulnerabilities.

Off-line breaches can easily occur because of disgruntled employees, industrial espionage or human error.

A good example is this summer's U.S. Department of Veteran Affairs public relations fiasco. A Veteran Affairs employee had taken a work laptop and external hard drive home, even though not authorized to do so. The employee's home was then burgled. *InformationWeek* later reported that the laptop and hard drive contained 26.5 million veteran and active-duty personnel identities. The security breach has reportedly resulted in proceedings against the U.S. government.

The biggest error that some businesses make securing corporate information is pigeonholing their security practices. For example, some companies build high security fences around electronic information, but fail to protect hard-copy information. The important thing

to do to secure corporate information is to focus on the information itself, rather than where the information is stored.

A company's intellectual property, for example, is often stored electronically and also on paper. Privacy laws require organizations to protect personal information regardless of the format. The first step is to determine what information needs protecting. And this will be different for every business. A technology company will primarily value its intellectual property. A marketing company will need to protect customer lists. Manufacturing businesses will safeguard supplier lists.

Each business will also need to identify what laws apply to relevant corporate information. For instance, privacy laws will apply to personal information; the Copyright Act will apply to copyrightable works. Next, businesses should develop security policies for online and off-line activities. Such policies should include computer use policies for staff and privacy policies for managing personal information.

Once security policies are created, it is important that they be monitored and enforced. Policies should be reviewed and revised regularly to ensure they remain relevant. The last step is to adopt a security breach protocol to help the company prepare for when a breach occurs. If information really is the most valuable corporate asset, it deserves protection.

Protect your No. 1 asset

- ❖ Steps to protecting corporate information:
- ❖ Determine the data key to your corporation;
- ❖ Identify any legal requirements;
- ❖ Develop security policies;
- ❖ Monitor and enforce those policies;
- ❖ Finally, determine what to do when something goes wrong, with a security breach protocol.

Brian Bowman specializes in privacy, access to information, advertising and marketing, intellectual property and technology law with the Information & Ideas Group of Pitblado LLP. He can be reached at 956-3520 or bowman@pitblado.com.