MARSH & McLENNAN
AGENCY

WORLD CLASS. LOCAL TOUCH.

BEWARE OF THESE 4 MYTHS OF IT DATA SECURITY

FEBRUARY 2012

Beware of These 4 Myths of IT Data Security

By Dan Hanson
Director of Management Liability

While we reap the benefits of information technology in all aspects of our daily lives, we seldom comprehend what's going on in the background or consider the potentially costly risks it ushers into our organizations.

Effective enterprise risk management requires knowing and evaluating exposures throughout your systems, including your cyber and data breach risks. The fact that you may not easily relate to the IT staff or comprehend all the technical details does not mean that you can neglect these that are becoming more important, and more risky, all the time.

Unfortunately, many business leaders don't consider their own cyber risk correctly or accurately. In my business, I help employers manage and prevent risk. When we discuss the risks associated with IT and cyber security, I hear some common myths as to why the employer does not need to be concerned.

Myth #1: We really don't hold any confidential information.

While financial institutions, healthcare organizations and retail companies are rightly seen as high-hazard businesses when it comes to holding a lot of confidential data, all businesses hold some.

Many may think an old line manufacturing company has little or no exposure to a network security event. However, they undoubtedly hold data on their current employees, and probably have information on employee prospects as well as recently-terminated employees. They also likely hold the design plans of key customers, acquisition targets and partners. Virtually any business has billing records of many customers on hand, which often contains sensitive data.

There are virtually no businesses without any exposure to a network security event. The exposure varies from business to business in differing levels of financial or reputation implications, but every business has risk. It is important to understand the type and amount of information your firm holds, and also the ramifications if a breach were to occur.

Myth #2: We use a third party vendor so we do not have the exposure.

If your client, employee or business partner trusts you with confidential data and it is compromised, it will certainly cause frustration, but it could also result in a lost customer, damaged reputation or financial loss. The perception will be that it was your fault and that it's your responsibility to repair any damages.

Using a third party vendor may actually present more exposure to your business. As your systems link with other systems and connect with other companies' data, you take on the added exposure of potentially corrupting or breaching the data of multiple businesses due to your processes and your people.

Also, just because a third party vendor is providing a service for you, it does not mean that they are assuming all of your liability. It's important to fully understand the indemnification agreements and hold-harmless contractual wording in place with the third party vendors, and to verify that they have adequate resources, including insurance, to back their indemnification obligations to your business.

Myth #3: Our IT Department assures us that we do not have any exposure.

Bank robberies still occur despite protective measures like time-lock safes, armed guards and other security measures because that is where the money is. The same is true of data breaches. They occur multiple times every day to all sizes and kinds of businesses because that is where the data is.

Consider the recent Sony case. This is an example of a large, sophisticated company with the latest and greatest technology protection that was hacked with apparent ease. Businesses with the best controls still have data breaches. You can't engineer the people-factor out completely: Laptops get stolen, and PDAs get left in airports.

There have been reports of the FBI, the State Department and multiple Fortune 500 companies being hacked despite sophisticated control measures and teams of people working to protect their systems. When an IT manager says their systems are impenetrable, that person is either extremely naïve or horribly overconfident.

Myth #4: Hackers only attack large companies.

This is very untrue. In fact, the *Wall Street Journal* reported that many small to midsize companies are being targeted by sophisticated, organized crime units because of their naïve approach to data security.

According to the report, "In 2010, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit, which investigates cyber attacks, responded to a combined 761 data breaches, up from 141 in 2009. Of those, 482, or 63%, were at companies with 100 employees or fewer. Visa Inc. estimates about 95% of the credit-card data breaches it discovers are on its smallest business customers."

Defending against cyber crime

Accepting that your business has technology or cyber risk is the first step toward protecting your operations against harm. The next step is to gain a basic understanding of the systems you have in place – what do they really do, what information is collected, how are they are interconnected, which vendor relationships are data sensitive, and what protections have already been established. But this is only a start.

There are several other things to consider:

- Understand the amount and potential exposures associated with the confidential data held within your firm.
- Realize that your IT risk does not stop at the four walls of your business. It is important to understand the contracts in place with vendors or partners who have access to your systems and data.
- Understand the controls that your vendors and partners have in place to protect your confidential data when in their control, and also understand the insurance they have backing them if a data breach should occur. Consider establishing formal requirements for your vendors.
- Constantly update and monitor the controls your business has for managing confidential data. For example, limit access to data, update software protections, keep abreast of the latest cyber attacks and trends and maintain adequate insurance.
- Understand it is not if, but when, your business may be subject to a data breach incident. Being small does not make you immune from attack, but may actually make your business a more likely target if the attacker feels you are not sophisticated.

Just like your business would have a disaster recovery plan for a natural disaster, it's important to have in place an IT or cyber security breach disaster recovery plan as well to minimize damage to your firm if does experience a breach.

A key to this is to find help where you can. High-priced cyber security consultants are great, but they just aren't feasible for many businesses, especially as margins are tightening for so many employers.

Finding a qualified insurance agent or broker who can help you diagnose your risk and then help design measure to reduce the risk you and your company face is a great start. The best agents or brokers are able to provide this service as an added value.

About the Author

Dan Hanson is Director of the Management Liability Group at risk prevention firm RJF/ Marsh & McLennan Agency, based in Minneapolis. He designs programs to help companies manage and reduce risk exposures.

How do I get more information?

- Dan Hanson, Director of Management Liability Group, at hansond@rjfagencies.com or 763 548 8599
- Ask your RJF/MMA representative
- Find other Cyber Liability content at www.rjfagencies.com/CyberLiability

MARSH & McLENNAN
AGENCY

Marsh & McLennan Agency LLC
7225 Northland Drive North, Suite 300
Minneapolis, MN 55428
+1 763 746 8000
+1 800 444 3033
www.rjfagencies.com