The MEARIE Group

Reciprocal News

Cyber Risk: “Think Global, Act Local”

Previously, locking up your files was perhaps the best defense against allowing a privacy breach to occur. Today, with the majority of your business being conducted electronically - on your office computers and servers, through your networks, over the internet or through cloud computing – your data is being exposed to the risk of a leak in a multitude of ways. And it isn’t just your confidential company data – the exposure of your customers’ data could cause a loss if it were to be mishandled or somehow leaked. Unfortunately, it is not only your organization’s policies which form part of this risk; your networks now expose you to threats on a global level as well. As such, it is a real challenge to keep your data and systems protected.

There have been many privacy breaches in the news lately, involving large companies’ failures to protect their customers’ data. These incidents cost an organization through personnel costs, legal counsel and time lost to managing the crisis; after the incident, an organization may need to communicate to customers, repair the system to prevent further incidents or perhaps face a law suit.

According to Gartner Inc. the top five privacy issues* facing business today are:

1. Data Breaches

Data breaches rank high on the priority list because of their visibility, but preparing for and following up on breaches is actually straightforward. Most controls exist anyway if security management is working properly. Organizations should compartmentalize personal information, restrict access, encrypt data when transmitting it across public networks, encrypt data on portable devices, and encrypt data in storage to protect it from users who have been given too much privilege, from rogue administrators and from hackers. Consider data loss prevention tools, tokenization, data masking and privacy management tools.

2. Location-Based Services

Location information can be GPS information, smart meter identification, the nearest cell tower, information about wireless access points, indoor positioning information, speed, altitude, smart meter identifiers and IP addresses. Not every organization processes geolocation data, but the area is evolving rapidly, and a specific way of processing may suddenly surface as a privacy scandal (eg. smartphones storing more location information than expected). Many providers are still in the “collect” stage rather than the “use” stage. They compile vast amounts of information, often without a clear plan of what to do with it. This violates a fundamental privacy principle – collect information only for the purpose for which you need it.

3. Cloud Computing

Cloud computing and privacy are innately at odds. Privacy laws apply to one country; the public cloud is not related to any country. Privacy officers should not accept “no” for an answer when asking whether the processing of personal information in the cloud or abroad is allowed. Most privacy laws have some flexibility, guidance is evolving slowly and, in many cases, there are legally acceptable solutions. Organizations should focus on the location of the legal entity of the provider, not on the physical locations of its operation centres.

4. The Value of Privacy

The value of privacy and the sensitivity of personal information are impossible to determine without context. Personal information has hardly any value or sensitivity. Rather, it depends on how data is being processed. There is no right or wrong. Finding the balance between "not enough" protection and "too much" protection is an ongoing process. Legal requirements are a bad guideline as they trail technical innovation and cultural change by several years. Privacy officers should set up a process to identify stakeholders for personal information, gather requirements from them, influence the design of the business process and applications, and plan for adjustments.

5. Regulatory Changes

Regulatory changes should not distract privacy officers from pursuing their strategies, because most regulatory changes will only have a mid- to long-term effect. Absent of any specific laws or regulatory guidance, organizations must interpret existing, generic privacy legislation for emerging technologies like smart meters, indoor positioning, facial recognition on smartphones correlated to photo databases, vehicle and device locators, presence detection, body scanners, and others.

More than ever you depend on your network for your important business operation, the use of smart meters, online billing, smart grid and related activities. Network security will continue to be a major issue.

Following risk management best practices and ensuring your Policies and Practices are in place will help you in mitigating cyber risk and privacy liability exposures for your operations. If you have questions or would like assistance with your Cyber and Privacy exposure contact Gary Durie, Manager Risk Management and Underwriting Services at 905.265.5355 or gdurie@mearie.ca

* "Top Five Issues and Research Agenda, 2011 to 2012: The Privacy Officer", June 14, 2011, www.gartner.com

The MEARIE Group's Reciprocal News is an electronic publication intended for Subscribers of The MEARIE Group's Insurance programs. It is published on a periodic basis and is intended for information purposes only. In the event of specific claims, incidents or legal actions against the Subscriber, coverage will be determined by MEARIE policy interpretation.

Tips on Updating Your Privacy Policy

Hearing about these incidents will cause many organizations to review, change or update their Privacy Policies. As such, it is important to be informed and consider the full extent of this exposure. The following tips may help you either develop or continue to support an effective network security plan:

- Focus on return on value rather than return on investment. Consider the harm a network security breach could do to your business, such as lost revenue or customer litigation.
- Never assume that network attacks will come only from outsiders. Your employees can accidentally create security vulnerabilities, and disgruntled or former employees can cause considerable damage.
- Don't be tempted to confront security concerns with a piecemeal approach rather than a unified strategy that protects your whole network.
- Work with others in your company to develop and roll out security strategies, focusing on technology, training, and physical site security with tools like surveillance cameras.
- Find the right balance between security and usability. The more secure your network is, the more difficult it can be to use.

The MEARIE Group

Gary Durie, *Manager, Risk Management*
& Underwriting Services
T:905.265.5355 or 1.800.668.9979
3700 Steeles Ave West, Suite 1100, Vaughan, Ontario L4L 8K8
gdurie@mearie.ca
www.mearie.ca