Feature

Time for a privacy check-up

It's getting scary out there. Make sure your security systems are protecting your business and the personal information you have.

By Trudy Lancelyn

Advisen, a company that provides proprietary databases, analytical tools and customer applications to the insurance industry, hosted a Cyber Risks Insights Conference Oct. 20 in New York City, at which Michael Chertoff, co-founder and executive chairman of The Chertoff Group and Secretary of the U.S. Department of Homeland Security from 2005 to 2009, delivered the keynote address. He noted that of all the risks businesses face, in his view cyber is the greatest one, and the one that should get the most attention. "The fear is that a cyber attack could cause a loss of life and property as well as disruption of the global economy."

Advisen surveyed more than 27,000 companies in 22 industries and found that half of them had "botnets" on their systems, i.e., malicious software that allowed the systems to connect with other computers and forward spam or viruses without the owners knowing it was happening. Another term for botnets is "zombie army", which leads one to suspect that, for some, the zombie apocalypse isn't going to look like an episode of *The Walking Dead;* it's going to occur when a region or industry sector finds itself closed for business.

In its *2015 Internet Security Threat Report*, Symantec, the provider of anti-virus software, reported:

"Attackers clearly have retailers in their crosshairs if the increase in data breaches containing financial information is any indication. The retail industry again has the dubious distinction of being the industry liable for the largest number of identities exposed, accounting for almost 60% of all identities reported exposed, up from 30% in 2013. Financial information has moved to the fourth most common type of information exposed in a breach. In 2013, 17.8% of breaches contained financial information, but in 2014 this number jumped to 35.5%." In most cases, this breached information was credit or debit card details.

In its Nov. 16 edition, *Thompson's World Insurance News* reported on an address by Beth

Pearson, president of the Registered Insurance Brokers of Ontario (RIBO), to its members in Toronto earlier that month.

"The impact of PIPEDA (the *Personal Information Protection and Electronic Documents Act,* which was amended in June) and similar statutes heighten our obligations and encourage a more formal process for the collection, use, sharing and destruction of personal information," said Pearson, of AP Insurance Brokers in Hamilton, Ontario.

"We need to make sure our office data-handling systems are up to date and ensure that the policies and procedures reflect what is happening in our shops – with a keen eye on protecting the personal information in our possession." Stressing the importance of technology tools such as data encryption, she said, "And it is also important that we raise awareness of data protection amongst our staff through, for example, training sessions on office policies and procedures," adding that it is particularly important to enhance security when data is at its most vulnerable – when it is accessed via mobile electronic devices.

Insurers are moving quickly toward e-commerce, and the brokerages that are best able to integrate with insurers' technology, not just for business-to-business communications but for business-to-consumer interactions as well, will have a leading edge as consumer expectations and buying habits evolve. But the basics of information collection, sharing and storage must be covered as well, and frustratingly, those goalposts are constantly moving. Even if you underwent a thorough assessment within the past year, there may be something new to consider and implement. Regulators and systems providers are making sure business people get the memo by downloading onto them increasingly more responsibility for compliance.

Over the next few pages we'll review some of the basics of privacy compliance, look at recent changes and provide some links and resources to assist you.

Guard against identity theft

By Romal Brice

Identity theft represents one of the most troubling results of privacy breaches; this kind of fraud has affected thousands of British Columbians.

This is of particular concern for insurance brokers, with the privacy of confidential information becoming increasingly important in client – broker relationships. In the normal course of their business, brokers receive key personal and business data that must be protected – a privacy breach can cause significant and long-term harm to both a customer and to the broker, given the loss of trust.

Brokers, like any business that collects personal information, can take the lead in stemming the rise of identity theft – helping their clients and protecting their own reputation and profits at the same time. It's essential for them to develop a comprehensive plan to protect their clients' personal information. It's not just the right thing to do – it's the law. As well, knowing what personal information you have in your possession, and what you are doing with it, is fundamental to protection of that information.

Fortunately for brokers, useful resources are available to help them comply with the law and protect their clients' information. Canada's Office of the Privacy Commissioner suggests following a number of measures.

First, limit the amount of information you collect. Not only does collecting less information reduce the potential damage from a breach, it also lowers the costs of collecting, storing, retaining and archiving data.

Next, limit the amount of time you retain the information. There's no need to keep a client's information beyond what's necessary for your purposes. Make sure you have guidelines and procedures for retention and destruction of personal information.

It's also important to ensure client information is protected against loss or theft. This requires that your brokerage have a security policy. Prevent unauthorized access, disclosure, copying, use or modification; lock paper files and computers; and maintain areas with restricted access and alarm systems. Encrypt all computerized records, whether they are on computers, networks or remote access devices. Educate your employees so that they know the procedures and how to follow them.

Brokers must also ensure they have good authentication processes. If someone claims to be a particular customer, the broker needs to be able to authenticate that the customer is who he or she claims to be. In a financial business like insurance, where a customer may wish to obtain sensitive records, such processes are critical. This can be a difficult task; the creation of an authentication process that's too rigorous or asks unnecessary questions can be too intrusive in and of itself. Create a process that's appropriately designed given the sensitivity of the particular information and the risks associated with it.

Despite our best efforts, data breaches can still occur. Brokers need to have a plan ready to implement if the worst happens and a breach takes place.

In particular, you must tell those affected as soon as possible. This is most important in a situation where there's a risk of identity theft or some other kind of harm.

Notification should include the following information:

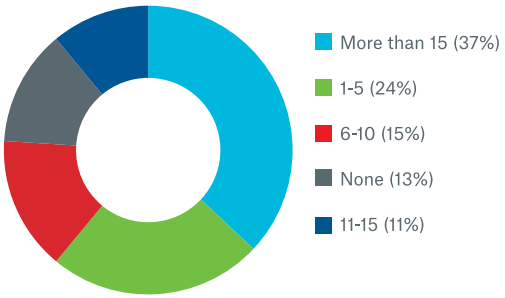
- A list of the type of personal information disclosed;
- An assessment of the risk of identity theft as a result of the breach;
- A description of the measures taken or that will be taken to prevent further unauthorized access to personal information;
- Contact information for affected individuals to obtain more information and assistance; and
- Information and advice on what individuals can do to protect themselves against identity theft and fraud.

What's more, a broker must be prepared to provide assistance to all those

Cyber risk survey

A survey of business risk managers released in October by the Boiler Inspection and Insurance Company of Canada revealed that 87% of Canadian businesses have experienced at least one hacking incident in the past year. *www.munichre.com/HSBBII/en/home/index.html* > Press & News

How many hacking scares/incidents have you experienced in the last year?



affected by the breach. This assistance can include paying for credit monitoring.

Of course, such a breach may be the result of a crime. In the case of a breach where theft is suspected, contact police immediately. As well, if there's a risk of identity fraud, you should also contact credit reporting agencies.

Finally, be sure you notify the Office of the Privacy Commissioner of Canada whenever there is any kind of breach involving personal information. Brokers also fall under provincial regulations; you should also contact the Office of the Information and Privacy Commissioner for B.C. in the event of a breach.

Brokers are gatekeepers for the privacy of client information. Their efforts to safeguard personal data are critical to the safety of their clients and the reputation of their own businesses and the industry at large.

Insurance Council's Client Confidentiality Guidelines

On May 13 the Insurance Council of B.C. issued a notice advising that it has incorporated Client Confidentiality Guidelines into the Code of Conduct. In 2009 Council advised that there would be no tolerance of intentional unauthorized access to, or use of, a person's information. Since then, Council has identified situations where licensees failed to appreciate that even seemingly innocuous activities could result in a breach of privacy. The Guidelines define client personal information, and reference the *Personal Information Protection Act* for direction on the privacy requirements when a licensee's book of business is being sold to another licensee. They also reiterate that agents' nominees are responsible for the actions of their employees and the systems used within their offices.

New *Digital Privacy Act* amends PIPEDA

Bill S-4, the *Digital Privacy Act*, the federal government's latest amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), came into force on June 18. Here are some of the key features of the legislation that would be of interest to insurance brokers:

Changes to consent

The "valid consent" provision is revised, putting more onus on organizations to make a reasonable effort to ensure that customers are not only *advised* of the purposes for which their personal information will be used, but *that they also understand it*.

Disclosure without consent

Organizations that collect personal information may disclose it to certain third parties without obtaining prior consent in a few circumstances:

- in order to investigate a breach of an agreement or a contravention (or anticipated contravention) of a federal or provincial law,
- to detect or suppress fraud, or
- when there are reasonable grounds to believe that an individual has been the victim of financial abuse.

Disclosure in a business transaction

During a negotiation for the purchase/sale of a business, the selling business can share personal information about clients or employees to the prospective buyer where such information is necessary to determine whether to proceed with the transaction or to complete it. The organization that receives the personal information must:

- use and disclose it solely for purposes related to the transaction,
- protect it with appropriate security safeguards, and
- return the information or destroy

it within a reasonable time if the transaction does not proceed. Once the business transaction is completed, parties to the transaction can use and share personal information as long as certain steps are followed.

Employees' personal information

The original PIPEDA did not extend to the personal information businesses have about their employees, although B.C.'s *Personal Information Protection Act* did include such provisions. Bill S-4 brings into federal law provisions with which B.C. businesses have complied for many years: that employers are able to collect, use and disclose employee information without consent if it is needed to establish, manage or terminate employment, provided the employee in question has been notified why the information is being or may be collected, used or disclosed.

Breach notification requirement

Bill S-4 introduces new requirements for reporting security breaches. These requirements are not yet in force, but are worth noting because they are coming.

Organizations that suffer a security breach of the personal information they store about employees and customers will have to notify individuals of the breach, and report it to the Office of the Privacy Commissioner of Canada (OPC), if it is "reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual."

Organizations will be required to keep and maintain records of every breach of security safeguards involving personal information under their control. These records must be provided to the Privacy Commissioner on request. Because there is no threshold regarding the size of the breach, one may consider that all breaches, no matter how trivial or inconsequential, must be logged.

The latest and greatest in TLS

When information is being transferred over the internet from a computer on one system to a server on another – for example, between brokerage and insurer, or brokerage and debit/credit card provider, or via an email message – it can transfer in a public manner that can be intercepted and read by a third party or it can be encrypted (converted to code) so that it can be read only by the sender and the intended recipient.

For more than 20 years, Secure Sockets Layer (SSL) was one of the most widely used encryption protocols, and it remains in widespread use today. About 15 years ago SSL v3.0 was superseded by Transport Layer Security (TLS) v1.0; today the current version is 1.2 and v1.3 is being drafted.

Retail merchants using electronic payment systems for taking debit/credit card payments at point of sale must meet system requirements known as Payment Card Industry Data Security Standards. These standards are maintained and enforced by the PCI Council, a body founded by major credit card providers American Express, Visa, MasterCard and others.

Earlier in 2015, the PCI Council released new v3.1 requirements. Merchants must not implement new technology that relies on SSL or early TLS, and merchants using SSL and TLS v1.0 and 1.1 must discontinue the use of those systems and devices before June 30, 2016. Only TLS v1.2 is PCI DSS compliant.

Merchants are required to upgrade their payment-card systems to the latest version of TLS (V1.2) by June 30, 2016.

Where do B.C. brokerages stand in their TLS compliance?

In May, the Centre for Study of Insurance Operations (*www.csio.com*) released its finding that 81% of B.C. brokerages have adopted TLS email security. CSIO used *www.checkTLS.com* to determine whether brokers with CSIO accounts were TLS-enabled, and concluded that the brokerages tested were representative of the entire P&C brokerage community across Canada. The results are online at *https://csio.memberclicks.net/transport-layer-security-tls*.

While this level of TLS adoption can be seen as a glass-half-full story – B.C.'s 81% adoption rate is the second-highest in Canada, shared with Alberta and exceeded only by Saskatchewan brokers' 91% level – it also reveals that 19% of B.C. brokerages are not TLS-enabled. In addition, it does not determine to what degree insurance brokerages are compliant with TLS v1.2 – the level needed for PCI 3.1 compliance.

CASL fines show government is serious

Canada's Anti-Spam Legislation (CASL) came into force on July 1, 2014. All Canadian businesses are now subject to this legislation that limits the sending of commercial electronic messages without prior consent. Violations of this legislation may be investigated by the Competition Bureau, the Canadian Radio Television and Telecommunications Commission (CRTC) or the Office of the Privacy Commissioner of Canada.

In 2015 the CRTC imposed a penalty of $1.1 million against Compu-Finder, which provides training services to businesses, for promoting its courses through email messages sent to recipients without consent; some of the email solicitations did not have properly functioning unsubscribe mechanisms. The CRTC imposed a $48,000 administrative monetary penalty against Plentyoffish Media Inc., operator of an online dating site, for sending unsolicited email messages that contained a deficient unsubscribe mechanism.

Every business in Canada should ensure that it has express or implied consent, or an exemption, prior to "e-blasting". In addition, every promotional email message must properly identify the sender, and provide an unsubscribe mechanism.

RESOURCES:

CRTC's Bulletin 2014-326 *Guidelines to help businesses develop corporate compliance programs* contains practical steps that companies can take to implement a CASL-compliant culture. *www.crtc.gc.ca/eng/archive/2014/2014-326.htm*

New guidance for "Bring Your Own Device" privacy

At first blush, it may appear to be a win/win situation when employees opt to use their own cell phones, tablets and laptops for work: a savings for the employer and convenience for the employee. But businesses have security and privacy responsibilities for the information their employees collect and store, and when this information is spread over multiple devices beyond the businesses' control, they face increased management costs and reputational risks.

To support businesses in developing "Bring Your Own Device" (BYOD) policies, the Office of the Privacy Commissioner of Canada, along with its provincial counterparts in Alberta and British Columbia, recently released a new joint guidance document – *Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?* Among the considerations and suggestions:

- Conduct a privacy impact assessment and risk assessment: Identify and address risks associated with the collection, use, disclosure, storage and

retention of personal information.

- Develop, communicate, implement and enforce a BYOD-specific policy: Such a policy should address issues such as user responsibilities, acceptable and unacceptable uses of BYOD devices, application management and access requests. Internal departments, such as information technology, information management, legal, finance and human resources, need to develop an enforceable, easy-to-understand BYOD policy.
- Mitigate risks through containerization: Have employees keep corporate information compartmented from other information on their mobile device.
- Formalize a BYOD incident management process: In the event of a privacy or security breach involving an employee's device, have a process in place to help with the identification, containment, reporting, investigation and correction of that breach in a timely manner.
- Maintain an inventory: Keep a list of authorized mobile devices and apps participating in each BYOD program.

Intrusions upon seclusion

In 2012 the Ontario Court of Appeal in *Jones v. Tsige* recognized a "new" common law tort of "intrusion upon seclusion".

Jones and Tsige were both employed at a bank, but did not know or work with each other. Tsige had become involved in a common-law relationship with Jones' ex-husband. Jones maintained her primary bank account at the bank. Given her position, Tsige accessed the banking information of Jones 174 times over a four-year period, contrary to the bank's policy. When Jones discovered the unauthorized access of her bank account she complained to the bank, which suspended Tsige for a week without pay, and commenced an action against Tsige in the Ontario Superior Court of Justice for invasion of privacy, seeking damages of $70,000 plus punitive damages of $20,000. At the first level the action was dismissed on the grounds that the tort of invasion of privacy did not exist at common law in Ontario. Jones appealed. The Court of Appeal overturned the first decision, recognized the new common law action of "intrusion upon seclusion", and awarded $10,000 to Ms. Jones.

Intrusion upon seclusion is not common law in all Canadian provinces. B.C., along with four other provinces, has a statutory tort for the invasion of privacy. The case provides a reminder for all employers:

- Employers should implement policies that articulate the right of the employer to monitor employees' use of company systems to ensure privacy is being maintained.
- Those policies should be in writing and communicated to employees. The policies should make clear that employees who engage in personal use on the company's technology systems should have no expectation of privacy and should know that the employer may view all information, including personal information, on its systems.
- Employers that take steps to define expectations in the workplace will be better equipped to defend against invasion of privacy claims, and will also be better positioned to argue that they should not be held vicariously responsible for employees who act outside the scope of their employment and breach privacy policies.

PRIVACY RESOURCES:
For a list of privacy resources and guidance documents, go to ***www.ibabc.org*** *> Members' Area > Links & Resources.*