Information in the event of a

DATA BREACH

SEPTEMBER 2020

INSURANCE BROKERS
ASSOCIATION OF CANADA

CYBER RISK

What you should do **before** a Data Breach

"IN 2019, OVER 28 MILLION CANADIANS WERE IMPACTED BY DATA BREACHES." — PRIVACY COMMISSIONER

TYPE OF INCIDENT	TOTAL BREACH REPORTS
ACCIDENTAL DISCLOSURE	147
LOSS	82
THEFT	54
UNAUTHORIZED ACCESS	397
TOTAL	680

No business owner would want to experience a data breach that exposes customer data, or suffer the reputational harm that would bring. Protecting client data and the IT Systems your business depends on should be a top of mind priority for every business. Canada's data privacy and data protection laws continue to evolve, with mandatory record keeping and reporting of data breaches now required, and a risk of financial penalties for non-compliance.

NOW IS THE **TIME TO PLAN, HARDEN AND TEST YOUR I.T. SYSTEMS** TO REDUCE THE RISK OF A DATA BREACH.

MITIGATION OF CYBER RISK

CRITICAL RISK:

Insurance brokerages are exposed to a number of potentially devastating risks including flood, fire, earthquake, data breach, and cyber attack. Cyber risk is on the rise, and will only get worse. The Office of the Privacy Commissioner of Canada (OPC) noted: "Since November 1st, 2018, (when reporting became mandatory) we have received 680 breach reports. That is six times the volume we had received during the same period one year earlier. It's a staggering increase and higher than we had anticipated." Brokerages must acknowledge all risks and be prepared to take action with mitigation strategies that will help to avoid a disaster.

POSSIBLE SOLUTIONS

The primary requirement is planning – a brokerage must develop a written plan to address each risk. For a natural disaster, work with your broker management system provider on how to access data if your office is shut down (an ASP is a solid choice). Find a secondary site from which to work and arrange for your staff to work remotely. Find alternate power sources: i.e., generators. You can also contract with disaster relief providers.

Security risks require even more extensive planning to address issues such as customer communications, reputational protection, and legal implications. In addition to having a plan to respond to an attack, you must have in place a written security procedure plan to prove that you have done your best to protect your customers' data. Written – and regularly updated – plans are critical for mitigation of risk.

RESOURCES:

Government of Canada - CyberSecureCanada

Government of Canada - Emergency & Disaster Planning

Canadian Centre for Cyber Security

CSIO eLearning - Cybersecurity eLearning

Ins Institute - Develop a Small Business Disaster Recovery Plan

BROKERAGE PASSWORDS

CRITICAL RISK:

Sloppy password management makes protecting private client information extremely difficult. Writing down user ID and passwords or putting them in an unsecured electronic document does not provide adequate security.

POSSIBLE SOLUTIONS

Ensure that employees are familiar with password best practices.
There are three parts to effective *password management:*

- Use the password management capability built into your brokerage management system, including Single Sign-On.
- Adopt two-factor authentication where available.
- Use a third-party enterprise Single Sign-On (SSO) solution for all other passwords.

RESOURCES:

Office of the Privacy Commissioner of Canada - Passwords

Password Managers 2020

REAL TIME MONITORING OF BROKERAGE EQUIPMENT FOR DATA BREACH

CRITICAL RISK:

Understanding the content of data that flows in and out of an organization's network is critical. Monitoring through the use of Data Loss Prevention (DLP) solutions has become increasingly popular to protect sensitive data and provide insight into the use of content within an organization.

RESOURCES:

SANS - Data Loss Prevention Hardware & Education

Broadcom - Data Loss Prevention Products

POSSIBLE SOLUTIONS

DLP solutions range from simple desktop-based clients to extensive inline network-based appliances designed to analyze traffic for sensitive data such as credit card and social security numbers. In recent years, SAAS or cloud based DLP solutions have become another option for organizations looking to utilize a 3rd party or service provider to perform this function. The resource center at SANS.org provides information on the types of DLP solutions available; choose one that will best fit your organization's needs.

USING ASP SYSTEMS FOR SECURITY

CRITICAL RISK:

ASP (Application Service Provider) or web-based systems ensure that data from brokerage management and other systems is always accessible, data backed up with multiple redundant copies, and automatically updated with all software upgrades as they occur. In comparison, LAN-, desktop-based, and even Thin Client systems can more easily be compromised due to damage, require brokerage staff time to backup and upgrade, and are not as mobile-accessible.

POSSIBLE SOLUTIONS

Almost all major industry software vendors offer ASP versions, and many offer only ASP. Whether you are using a management system, comparative rater, or CRM, check with your vendor on availability and pricing.

Due diligence should be exercised when selecting an ASP; assess what security measures they have implemented to harden their environment and reduce the risk of cyber threats that could compromise their environment.

Note: ASP systems tend to have higher price points than desktop, as the vendor incurs costs for data hosting, management, access, software updates, and other security. Also keep in mind that anti-virus and other protection software still needs to be in place.

RESOURCES:

Gartner Reviews - Data Loss Prevention tools

CISCO - Evaluating ASPs

Top Anti-Virus Software

WEBSITE DESIGN WITH SECURITY IN MIND

CRITICAL RISK:

Even if your website is basic and only used for informational purposes, it is still important that you keep security in mind, whether you build your own site or have a company do it for you. There are several ways your website can be compromised: hijacked to redirect visitors to another site, infected with malicious code or viruses and Denial of Service (DoS), to name a few.

POSSIBLE SOLUTIONS

Install SSL (Secure Socket Layer) encryption. This adds the "s" to https:// indicating that the site is secure and also adds the lock icon in front of the website url. Adding SSL has become a design best practice, and is a must if you accept payments from customers. It also prevents a browser from warning visitors that the site is not secure, which may discourage existing or potential clients. HTTPS is also a factor that Google takes into account when ranking your website.

Use strong administrative passwords to secure your website and always be sure to back up your website files in case of disk failure or simple corruption of your html files.

RESOURCES:

Google Support: Secure your site with HTTPS

Why am I seeing a 'Not Secure' warning?

MOBILE DEVICES

CRITICAL RISK:

If you are using mobile devices to conduct any type of business, you are exposing your company to additional security threats that can compromise your business network and data. One of the biggest challenges can be data loss or breaches caused by lost or stolen mobile devices. Another threat targeting mobile devices is the introduction of attacks, malware and high-jacking your account.

POSSIBLE SOLUTIONS

Create an approval process for any mobile device used to conduct business. This should include a written statement of company policy that is reviewed and signed by the user, and outlines the following.

STEPS TO TAKE

1 All devices must be password protected.

2 Use secure wireless connections when transmitting business information – no free services from coffee shops or airports.

3 A reporting process for lost or stolen equipment (immediate located or wiped).

4 All devices are securely wiped prior to disposal or trade in.

5 Use Encrypted drives and memory cards.

6 Use security on all mobile devices, keep software updated, use only trusted apps.

7 Apply business workflows and procedures to mobile use (proper client file documentation in the brokerage management system).

8 Apply business email policies and best practices to mobile devices as you would in your office.

RESOURCES:

Office of the Privacy Commissioner of Canada - Keeping your Information Safe

Office of the Privacy Commissioner of Candada - SIM Card Swap Scam

DOCUMENT RETENTION

CRITICAL RISK:

The longer an organization keeps client information, the more documents could be lost in the event of a data breach.

RESOURCES:

Managing the Security Risks of Portable Devices
"Bring Your Own Device" Opportunities & Risks
Office of the Privacy Commissioner of Canada - Protecting Personal Information on your mobile device

POSSIBLE SOLUTIONS

Keep information only for as long as legally required and as needed by the brokerage. Federal legislation and provincial insurance regulators have requirements for a proper document retention policy as well as requirements for proper disposal of private client information. The organization should create a document retention policy that all brokerage systems can fully support, and monitor for compliance.

ENCRYPTING DATABASES

CRITICAL RISK:

With the continuing complexity and sophistication of hackers, and increased electronic transmission of data, this is possibly the single most critical business risk for businesses today.

RESOURCES:

Microsoft Device Encryption - Windows 10
McAfee - Endpoint Encryption Helps Keep Your Data Safe

POSSIBLE SOLUTIONS

Compliance with provincial privacy and personal information regulations is critical, adhering to the strictest province in client database. Use readily available encryption tools such as Microsoft Device Encryption to encrypt hard drives, backup media and other devices so that if they're lost or stolen they can't be read. Make certain that you don't lose the encryption key and that it's kept safe and secure.

EDUCATION & TRAINING

CRITICAL RISK:

Brokerage employees have access to vast amounts of private information that can be susceptible to theft. One of the most important pieces of a security policy should be ongoing education and training outlining employees' roles and responsibilities in safeguarding company assets and client information.

POSSIBLE SOLUTIONS

Have written security policies and breach notification procedures that are reviewed in detail with all new employees and periodically with all staff so that security and data safeguarding are a part of the insurance brokerage's culture. Undertake an annual review of the entire security policy as well as the breach notification procedures, awareness of threats and all privacy responsibilities.

Undertake an annual review of the entire security policy as well as the breach notification procedures, awareness of threats and all privacy responsibilities. Specific aspects of a security policy, real world breach examples or current "lessons learned" can be reviewed on a monthly or quarterly basis to keep security and the safeguarding of information top of mind, and show management's support and expectations for policy adherence.

Establish a training calendar for each of the following: IT, security compliance officer, privacy officer, executive management, supervisors, mobile employees and all employees. This will ensure that employees know their responsibilities and are familiar with the brokerage's security policies and privacy statements.

RESOURCES:

Office of the Privacy Commissioner of Canada - Employee Snooping

Office of the Privacy Commissioner of Canada - Privacy Toolkit

DATA BREACH LAWS

CRITICAL RISK:

Brokerages possess data that, if breached, could cause significant harm to the affected individuals and organizations. It is critical that the brokerage understand the federal data breach laws (PIPEDA) and those of their home province, as well as any other province (and/or foreign jurisdiction) where they do business.

POSSIBLE SOLUTIONS

- Develop an Incident Response Plan (IRP) to ensure that you know what to do and how to do it in the event of a data breach. The IRP should describe what an incident is, when and how to report it, and to whom (internally, and externally if required).

- PIPEDA defines what specifically constitutes a Data Breach, and outlines the mandatory reporting requirements, as well as potential fines and penalties. The Office of the Privacy Commissioner of Canada (OPC) provides a wealth of definitive information on PIPEDA in general, applicable provincial regulations and specific actions to take in the event of a breach.

- In addition, the Payment Card Industry (PCI) has its own set of security standards and compliance requirements that apply to any business that accepts, transmits or stores any cardholder data.

- For brokerages conducting business in the United States, Mintz-Levin outlines by state, the definition of breach, covered entities, notice procedures, and penalties. It is also incumbent upon the brokerage to understand where the Federal Trade Commission (FTC) stands on protecting personal information. Brokerages that write group health insurance are also required to meet the standards of the HIPAA HITECH breach rules.

RESOURCES:

Office of the Privacy Commissioner of Canada - For Businesses

Office of the Privacy Commissioner of Canada - Provincial and Territorial privacy laws and oversight

Office of the Privacy Commissioner of Canada - PIPEDA fair information principles

Office of the Privacy Commissioner of Canada - What you need to know about mandatory reporting of breaches of security safeguards

Office of the Privacy Commissioner of Canada - Ten tips for avoiding complaints to the OPC

PCI Compliance FAQ

Minz-Levin - State Data Security Breach Notification Laws

GDPR (General Data Protection Regulation) - Toughest Privacy and Security law in the world

Deloitte - GDPR and Canadian organizations

ELECTRONIC COMMUNICATION

CRITICAL RISK:

With electronic communications, there are key areas that the brokerage must address. Canada's Anti-Spam Legislation (CASL) and PIPEDA create obligations on the part of both carriers and brokerages regarding proper recordkeeping of consumer consent. Measures to improve efficiency and security should also be implemented.

POSSIBLE SOLUTIONS

Know and understand federal and your provincial laws regarding electronic communication. Utilize a best practices approach and CSIO standards with electronic communication. Start with a single business process and product line and create a process map for the ideal workflow and security in each area. Sensitive personal information should not be sent via email, whether in the email text or as an attachment. Instead, send emails with links to a secure site.

RESOURCES:

CSIO Advisory Report: Electronic Signature and Delivery

Canada's Anti-Spam Legislation

IP PHONE SYSTEM SECURITY

CRITICAL RISK:

The convergence of voice and data networks presents a multitude of advantages and cost savings; however, there are associated security and fraud risks that must be addressed. Three of the more prevalent risks are: interception of calls and privacy concerns, interruption of service, and theft of service or toll fraud.

POSSIBLE SOLUTIONS

Compliance with provincial privacy and personal information regulations is critical, adhering to the strictest province in client database. Overall security of your data infrastructure becomes increasingly important when implementing a VoIP system. Unencrypted VoIP traffic can easily be captured. Use encryption protocols such as TLS, so that voice traffic is encrypted the same as data traffic for secure transmission over a network. Implementation of larger premise-based VoIP systems should also consider the use of a Session Border Controller (SBC).

RESOURCES:

VoIP -Info.org - VoIPO Phone Security Issues

SANS - Security Issues Countermeasures

SANS - VoIP Security Issues

DOCUMENT DESTRUCTION

CRITICAL RISK:

Document destruction is not just about paper files. It also includes electronic files and emails (retention) as well as files that may be located on LAN's, cloud drives, local hard drives, mobile devices and USB or external drives. Federal and provincial laws require businesses to properly destroy customer records that no longer need to be retained. Destruction includes shredding or otherwise modifying the personal information in those records so that it is unreadable.

POSSIBLE SOLUTIONS

Establish a policy and processes for the proper destruction of documents following these 5 steps:

1. Take stock and inventory of where information is stored (brokerage management systems, fax, email, paper, physical drives, cloud services, 3rd party).
2. Scale down – consolidate and restrict the storage of information to controlled and manageable locations.
3. Secure it – lock paper drawers, secure server access, password protect files, screen savers.
4. Pitch it – properly destroy or remove documents and files that no longer need to be retained.
5. Plan – establish procedures, train employees and monitor for compliance.

RESOURCES:

Office of the Privacy Commissioner of Canada - Safeguarding Data

REMOTE ACCESS OF BROKERAGE SYSTEMS

CRITICAL RISK:

Remote access adds flexibility for brokerage operations; however, steps must be taken to adequately mitigate risks associated with this capability. To reduce the risk of a security breach via remote access points, three primary areas should be addressed: improved authentication, entry point validation, and security of data during transmission.

POSSIBLE SOLUTIONS

Use strong authentication with two-factor capability. Available solutions include remote access, certificates, SMS PIN codes, or biometric validation. Consider restricting remote access to some systems. Use an Intrusion Detection/ Prevention System (IDS, IPS) sitting in-line between the remote access point and your internal network, to prevent security exposure. This reduces risk from hacking software and viruses from the connecting device. Use a Virtual Private Network (VPN) to secure data during the transmission from remote locations.

RESOURCES:

Best Remote Access Software

PAPER VERSUS PAPERLESS

CRITICAL RISK:

When a brokerage moves from paper to paperless environment, important decisions must be made in a number of areas. These include: data storage (local vs. cloud), consistent workflows and continuity, staff training and requirements, retention of documents-histories, access to documents via the carrier websites and user access based on need.

POSSIBLE SOLUTIONS

Analyze current workflows and amend them according to new requirements for paperless process. Have a good communications plan and train and monitor staff for adherence and continuity. Decide where to host data (stored locally on server or in the cloud) and understand the security vulnerabilities and precautions needed for each. Be aware that each choice has a different financial impact and either choice may not be financially feasible for a brokerage. Adhere to provincial and federal retention guidelines for documents when moving from paper to paperless. Paper copies of documents may no longer be necessary when the brokerage has access to client documents on the carrier website.

RESOURCES:

CIO 14 Tips for Creating a Paperless Office

Phase 1 - Improving Workflows by Going Paperless

Phase 2 - Turning off Paper

ACT Article - Creating an Information Security Plan

PROTECTING CONFIDENTIAL INFORMATION

CRITICAL RISK:

The risk to brokerages has increased significantly regarding Protected Health Information ("PHI") and Personally Identifiable Information (PII). Brokers must be aware of the provincial and federal laws regarding this information, and know what data is kept, where it is stored, and who has access to it.

POSSIBLE SOLUTIONS

Conduct a risk analysis to identify and document where all the PHI and PII is located in your organization. Complete a compliance gap assessments. Minimize the amount of PHI and PII that the brokerage retains if possible. Develop, train and monitor policies and procedures with staff. Implement a "need to know" access policy. Be aware of the **Breach Notification Rule.**

RESOURCES:

Office of the Privacy Commissioner of Canada - For Businesses

Office of the Privacy Commissioner of Canada - Provincial and Territorial privacy laws and oversight

Office of the Privacy Commissioner of Canada - PIPEDA fair information principles

Office of the Privacy Commissioner of Canada - What you need to know about mandatory reporting of breaches of security safeguards

IT ENVIRONMENT & TESTING

CRITICAL RISK:

No plan is perfect. Don't wait until after a breach to find that out - test your system before anything bad happens. There are companies that specialize in analyzing your security employing tactics that criminal enterprises use. They can expose vulnerabilities that may have been missed when designing your IT security, and help resolve gaps before they can be exploited.

POSSIBLE SOLUTIONS

Use an outside consultant to perform a security audit of both physical and technical security. Use the review of policies and procedures to improve your security policies, record retention and data collection policies. Have a security company conduct a Pen test, (Penetration Test) of your IT environment. Ask your IT professional to verify that all devices are configured to optimize security and set your Operating Systems to automatically apply patches.

RESOURCES:

InfoSecurity - Call in the White Hats - It's Time to Reboot External Testing

DISASTER RECOVERY PLANNING (DRP)

CRITICAL RISK:

Failing to contemplate and plan for disasters can have serious consequences and may even result in the failure of your business. According to FEMA (Federal Emergency Management Agency), following a disaster 90% of smaller companies fail within a year unless they can resume operations within 5 days. The COVID 19 crisis has exposed weaknesses in many DRPs and will likely result in reassessing the range of risks facing businesses and how to plan for them.

RESOURCES:

Canadian Centre for Cyber Security

Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

POSSIBLE SOLUTIONS

Decide on either outsourcing or using internal management to create your DRP. A comprehensive plan will include:

- Communications plan and role assignments.
- Plan for your equipment.
- Data continuity system.
- Backup check.
- Detailed asset inventory.
- Pictures of the office and equipment (before and after).
- Vendor communication and service restoration plan.

Once your DRP has been created, test it a minimum of once per year using various disaster scenarios. Test data backup sub-systems quarterly. Use the results to refine your DRP. Make sure that employees are adequately trained on the plan and that they have the tools they need to continue their assignments in the event of a disaster.

AFTER A DATA BREACH - HOW TO RESPOND

CRITICAL RISK:

A brokerage that has suffered a data breach faces several risks such as reputational harm, unexpected costs to investigate the breach and close any gaps in your IT environment, potential loss of business, legal action and risk of financial penalties imposed by the OPC. A critical first step is determining whether there is a duty to report, as getting this wrong will likely bring financial penalties and unwanted publicity, potentially at a national level. Using third parties to process or manage data does not transfer your responsibilities regarding record keeping or reporting of a breach.

POSSIBLE SOLUTIONS

1 Contain it! (e.g., stop the unauthorized practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security).

2 Designate someone to lead the breach investigation. This individual should have appropriate authority and knowledge to conduct the initial investigation and make preliminary recommendations. If necessary, a more detailed investigation may subsequently be required. It may be necessary to hire an outside expert.

3 Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage. Escalate internally as appropriate, including informing the person within your organization responsible for privacy compliance. Make sure to review our document **What you need to know about mandatory reporting of breaches of security safeguards** to fully understand your obligations.

4 Be careful not to destroy evidence that may be valuable in determining the cause of the breach, or allow you to take appropriate corrective action.

RESOURCES:

Office of the Privacy Commissioner of Canada - Mandatory Reporting of Breaches; What you need to know

GLOSSARY

ASP An application service provider (ASP) is a business that provides computer-based services to customers over a network, for example, access to a particular software application (such as customer relationship management) using a standard protocol (such as HTTP).

CLOUD COMPUTING Is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet.

INTRUSION DETECTION SYSTEMS (IDS) Analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) also analyze packets, and can also stop the packet from being delivered based on what kind of attacks it detects, which helps to stop the attack.

DLP (DATA LOSS PREVENTION) Is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response.

VIRTUAL PRIVATE NETWORK (VPN) Extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

SAAS (SOFTWARE AS A SERVICE) Is a method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers.

SBC (SESSION BORDER CONTROLLER) Protects the network and other devices from:

- Malicious attacks such as a denial-of-service attack (DoS) or distributed DoS
- Toll fraud via rogue media streams
- Malformed packet protection
- Encryption of signaling (via TLS and IPSec) and media

APPENDIX

Adapted from 'How Do You Protect Your Agency's Data?' courtesy of ACT (Agents Council for Technology) and used with permission.

NEED MORE INFO?

IBACTECH@IBAC.CA

INSURANCE BROKERS
ASSOCIATION OF CANADA