PROTECTING YOU FROM CYBER AND DATA LOSS

FROM EVERY POSSIBLE ANGLE

Made possible

QBE

Contents

We're the buffer between the best laid plans and an uncertain reality

The security of your organization's information, whether it be in digital format or on paper, is under greater threat than ever before. To combat this threat, companies are allocating significant resources to fortify their networks to prevent access by hackers. While such measures are critical, no IT solution will ever be enough. A recent Net Diligence survey found that 30% of cyber losses (52 out of 176) were attributable to employees of the organization – of those, 77% were unintentional, caused primarily by staff mistakes and errors in paper handling [1].

For publicly traded corporations, cyber security has quickly evolved into a board issue, a risk for which they have a fiduciary duty to understand and manage. For board members, a cyber incident or privacy breach could prompt shareholder lawsuits for security failures, declines in a company's stock price, and allegations of management negligence. Impacted clients can also bring a class action lawsuit, even where there is "no evidence that a Class Member absorbed a fraudulent charge. [2]"

Smaller and mid-sized organizations are not immune to this risk. The majority of claims submitted for the Net Diligence Claims Study (87%) were from organizations with less than $2B in revenue [3]. It is a relatively new trend that hackers will target smaller organizations as they are seen as being more vulnerable. Where such a breach becomes public knowledge, the reputational damage and loss of business could put the viability of a smaller business into jeopardy.

Please read on to find out what we can do for you.

Scott Pidduck
Senior Underwriter - Professional Lines And Cyber
QBE Canada

[1] 2016 Net Diligence Cyber Survey
[2] www.canadianunderwriter.ca/insurance/data-breach-settlement-approved-canadian-class-action-lawsuit-home-depot-1004099522
[3] 2016 Net Diligence Cyber Survey

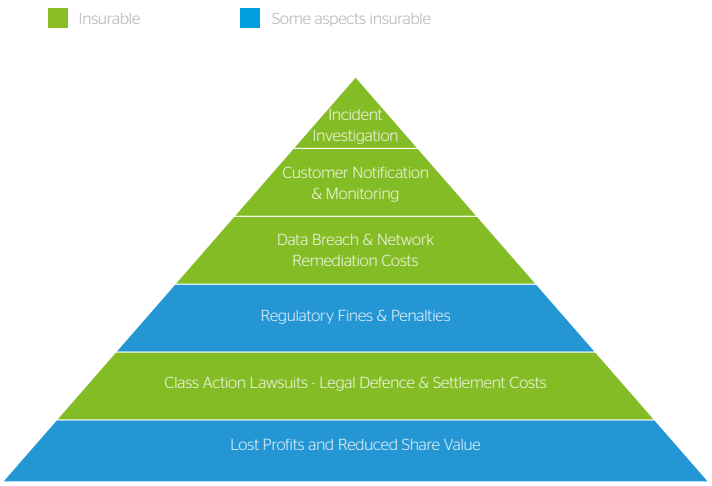
Real cost of a claim

The cost of a cyber breach or data loss incident is often only considered in terms of the cost to repair the damage incurred. However, most often the biggest cost resulting from an event is the legal defence costs and the resulting legal settlement to injured plaintiffs. Recent claims have demonstrated that legal costs can be extremely high, even when the number of records or individuals impacted is relatively small.

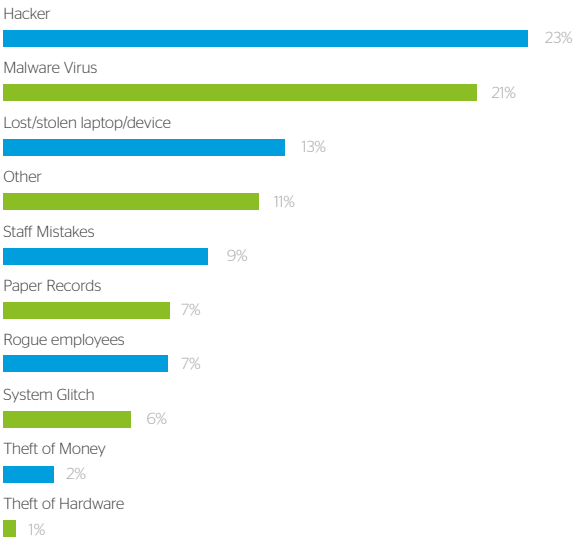
While risk management strategies can help to reduce the risk of loss, insurance is an optimal solution for most any organization. Keeping this in mind, the coverages offered by insurers do vary and it may not always be clear what is actually insured. Our goal at QBE is to be clear on what we cover. More critically, while some insurers only provide indemnification for costs incurred, QBE's approach is to provide you with a team of specialists who can work with you through the crisis, quickly and effectively, minimizing the impact to your organization and on your reputation.

For most organizations it is not a question of if but when will it have a breach – will you be ready?

How the Costs Add Up



Distribution of Cyber Losses by Type in 2016 [4]



[4] Based on 176 cyber loss events reported by participants in the 2016 Net Diligence Cyber Survey

What is my exposure?

Where an organization holds personal information of others, the risk of it being stolen or lost is easy to understand. For other organizations, the risks they face may not be so clear. The current reality is that any organization which uses computers has some exposure. Furthermore, any organization which has physical papers containing sensitive information in its possession could also benefit from cyber and data security insurance.

The sources of exposures and potential risks are long. Luckily, these risks are insurable. If you're still in doubt as to whether you might benefit from cyber and data security insurance just ask yourself "If my staff were unable to use their computers tomorrow, could my organization continue to function?"

Potential Risk	Potential Exposure
Do you allow staff to use the internet or e-mail?	Libel and Slander
	Damage to your systems due to virus or hacking
	Damage to third party systems by forwarding a virus
	Employees hacking your network
	Breach of Canadian Privacy Legislation
Do you have a website?	Breach of Intellectual Property Rights
	Misleading Advertising
	Libel and Slander
	Unauthorised access
Do you hold HR/payroll data on your network?	Breach of employees privacy rights
	Failure to handle, manage, store or destroy data correctly
Do you hold Third Party data?	Breach of Canadian Privacy Legislation
	Failure to handle, manage, store or destroy data correctly
Do you allow Third Party access to your network?	Damage to your computer system due to virus or hacking attack.
	Consequences to your business due to down time, business interruption exposure
	Potential for that access to be threatened by a hacker - extortion
Do you hold sensitive data that is accessible via your web server?	Libel and Slander
	Breach of intellectual property rights or confidentially
	Potential for that data to be threatened by a hacker - extortion
	Breach of Canadian Privacy Legislation
Do you transact any business via a website or rely on e-mail to communicate with clients?	Damage to your systems due to a virus or hacking attack
	Lost revenue or assets due to a virus or hacking attack
	Breach of statutory duties regarding the advertising or sale of goods or services by e-commerce
Do you have any business control systems or processes that are stored on maintained and controlled on your network?	Hacker/competitor infiltration of your systems and corruption of their working
Do you hold any customer's credit card or personally identifiable information on your network?	Breach of Canadian Privacy Legislation
	Potential for that data to be threatened by a hacker - extortion
	Financial loss by a third party due to dishonesty of your employees

Did you know? Your cloud provider is not responsible

It might not surprise you to learn that data outsourced to a cloud provider could be anywhere in the world. What is more interesting is that if you ask your cloud provider where it is, they can't tell you.

Why? Because it's always on the move and that is by design. While this may not raise any alarm bells at first thought, if your data is breached, you will be held to the legal standard of the country where the data resides at the time of the breach. To add complexity to this situation, you could also be held liable to the standard of each country where a resident is impacted by the breach. As an example, if your business physically operates in Canada but you hold data for a client who lives in California, it is conceivable that you could be held to the laws and standards of California, which are currently some of the strictest in the world.

Many cloud providers hold themselves harmless for any breach of your data. In other words, this is not a risk that is transferable via contract.

The good news is that there are active steps you can take to mitigate your risk of having a breach:

- Careful choice and contracting with your cloud computing is critical. To help, accounting companies with consulting arms can put together a strong vendor outsourcing contract including with cloud computing companies.
- There is an app for that – BlackCloudRX rates the various cloud computing companies and also tracks security breaches, lawsuits and major outages impacting cloud service providers.
- Service providers, such as information security consultants, can work with you to test and improve your IT security and protocols.
  - Insurance companies providing cyber insurance often have established relationships with these companies and can offer preferred supplier discounts
- Some cloud providers will allow you to put physical security around the servers holding your data. Better still, ask to visit the location where the server is located so see you can see first hand the physical setup and security in place.
- Some cloud providers will keep your data in a single location and country of your choosing.

Canadian Privacy Legislation

Canadian privacy legislation, both federal and provincial, regulates the collection, use and disclosure of personal information, as well as the rights of access and correction of that information.

The definition of personal information varies amongst the legislations, but it is principally defined as any information capable of identifying an individual, either when used alone or in combination with other information.

Unlike in the U.S., personal information includes publicly available information about an identifiable individual.

All businesses are required to have a privacy policy and plan to safeguard information against unauthorized collection, use or disclosure. The legislations that govern these requirements are as follows:

Canadian Privacy Legislation

Province/Federal	Law/Regulation
Federal	Personal Information Protection and Electronic Documents Act (PIPEDA)
British Columbia	Personal Information Protection Act (PIPA)
Alberta	Personal Information Protection Act (PIPA)
Saskatchewan	Privacy Act
Manitoba	The Personal Information Protection and Identity Theft Prevention Act
Ontario	Personal Health Information Protection Act, 2004 (PHIPA)
Quebec	Act respecting the protection of personal information in the private sector
New Brunswick	Personal Health Information Privacy and Access Act (PHIPAA)
Newfoundland and Labrador	Personal Health Information Act (PHIA)
Nova Scotia	Personal Health Information Act (PHIA)

For more information, please find the Breach Notification Law Map contained on QBE's E-Risk hub. Informatoin on how to access the hub can be secured through your broker.

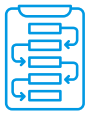
How can I reduce my risk?

Effective risk management can go a long way to prevent an event and can also help to minimize harm when an event does occur. The first step is to understand the exposures your organization faces and then build a plan based on your data protection priorities. Risk management is a continuous process that at no point can be considered complete.

Tips to Reduce your Cyber and Privacy risk

Identify Business Critical Data & Networks

Identify where your organization's most valuable intellectual property and sensitive data and informational assets are stored or are located and how it is being protected. Where there are budget constraints, prioritize IT spending to ensure that your most valuable assets receive the highest level of protection which can be afforded.



Create an Incident Response Plan

This plan should encompass the external parties you would want to engage if your systems or data were compromised. If you're unsure as to who should be included, please refer to the section "What Happens When You're Hacked?" found in this report. Your data breach plan should be linked with any business continuity plans your organization might have. It is important to train individuals based on their role in the plan. Most critically, the plan must periodically be tested to ensure it continues to be comprehensive and effective.

Train Your Employees

Create security policies relating to the use of the organization's systems, including access from home and mobile devices. Train and then test your employees on these policies, as well as on sources of malware and electronic scams. This is your best defence against having employees cause unintended harm.

Put Your Network Security to the Test

Let an independent third party test the robustness of your network security. QBE's preferred network security vendor can be hired at a special rate when cyber insurance is being purchased through QBE.

Avoid conflicts of interests

Make sure that the individual responsible for maintaining network security is not the same person who reports breaches to the board or management.

For more risk managements tips and guidance, you are invited to review the information and guidance contained on QBE's E-Risk hub. Information on how to access the hub can be secured through your broker.

What happens when you're hacked

It is an unfortunate truth that organizations which have had their systems breached are often treated more like criminals than the *victims they are*. As a breach becomes public knowledge, organizations face intense media scrutiny and are at risk of becoming defendants in class action lawsuits and other proceedings. Even when a cyber crime has undoubtedly occurred, the police often cannot assist and will instead suggest that you call your insurance company.

To learn more about QBE's team of preferred vendors who can work with you through a crisis, ask your broker for access to QBE's E-Risk hub or have your broker reach out to Scott Pidduck at QBE for additional information.

Here's what you can do if you have suffered a breach - and why it matters:

Engage A Breach Coach

When a breach event occurs, time is of the essence. QBE's experience is that breach remediation costs are significantly less when a breach coach is engaged immediately and manages the process on behalf of the organization. The coach's role is to manage and oversee the work being done simultaneously by different specialists as explained below.

Notify Your Insurance Company

Where insurance has been purchased, provide notice to your broker so that your insurance company is engaged.

Start the Process Under Privilege

Use a lawyer to hire an independent digital forensic firm. By having attorney-client privilege around the investigative efforts, you can carefully prepare and control how information is released publicly. This is a strong tactic if a government investigation or class action lawsuit is a possibility. The work relating to a cyber-attack should involve a team of lawyers with different skill sets and expertise. By engaging outside legal counsel who specialize in data breaches, you are assured that you will be compliant with breach notification requirements. Legal counsel is also the best party to share documented information with your insurance company around the time spent and cost incurred to remediate the event.

Save Your Network Logs

Have your IT staff gather and document facts surrounding the potential incident. Network security event logs are often vital in helping verify the date, time and machines involved in an incident. Your company should save these logs to support further investigation by the digital forensic firm and also for remittance to your insurance company.

Engage an independent digital - forensic firm

These firms can perform a timely and unbiased investigation to determine the extent of the damage and assess the options for remediation. Detecting and resolving a breach often requires malware reverse engineering expertise. As a consequence, even companies with large IT departments would not likely have the expertise required to remediate its organization's systems following an event. An additional benefit of engaging an independent outside firm to investigate the breach is that the results will be perceived as more objective and, therefore, are more defensible if challenged later on (e.g. by government, shareholders, customers, etc.). Where hired, your independent digital forensic firm can lead any briefings with your insurance company.

Consider Hiring a Public - Relations Specialist

Damage to the reputation of a business is one of the biggest risks following a breach and lost business can be the most costly consequence. To help manage messaging to the media and other impacted parties, it is beneficial to hire a public relations specialist to work with your organization through the crisis.

Risk transfer
What are the options?

At QBE, there is no "one size fits all" approach.

Not all companies face the same cyber security risks. The type and cost of crisis services are driven almost entirely by the type of data lost and the cause of loss.For companies in the financial services and hospitality sectors, the forensic costs incurred tend to be higher. For organizations in the retail sector, a large proportion of their loss stems from money spent on legal guidance and breach coach costs. For those in the healthcare sector, the highest cost incurred is for credit and ID monitoring.

To meet each organization's unique needs, we provide a comprehensive package as a standard offering, and then allow for additional coverages to be purchased as may be beneficial to your organization. In addition to tailored coverages, the limits purchased can also be customized based on your unique exposures, allowing you to pay only for the type and amount of coverage you need.

As standard, QBE's insurance policy includes protection for:

- Failure to correctly handle, manage, or store personal or third party corporate information
- A violation of data protection and privacy regulation and/or legislation
- A third-party's good faith reliance on a hacker's fraudulent use of your computer and telecommunication systems, including the fraudulent use of an encrypted electronic signature
- Unauthorized access to, unauthorized use of, or a denial of service attack
- Unintentional spreading of a computer virus
- Improper online activities such as web-scraping and web harvesting
- Third party allegations of defamation and breach of intellectual property rights arising from any matter or content you publish online, including the content on your website.

As standard, QBE's insurance policy also reimburses you for costs to deal with:

- Any financial benefit that has been transferred to a third-party that you cannot recover
- Public relations and crisis management specialists to help you respond and mitigate the damage to your reputation and business operations following an insured event
- Regulatory investigations and penalties (where insurable by law)
- The withdrawal of published content which is deemed to breach advertising standards
- Costs to have employee(s) in court to support the resolution of a claim insured under the policy.

Organizations may also purchase additional insurance protection as follows:

Data breach costs cover
Reimburses you for the costs incurred following a cyber or data security event, such as:

- The costs to notify individuals that their data has been breached, including legal costs to draft the notice
- The cost of credit monitoring where personal financial data has been breached
- The cost of a call centre to coordinate and handle the breach notification communication.

Cyber business interruption costs cover
This coverage replaces your lost business income resulting from:

- A total or partial interruption of your computer and telecommunication system
- A degradation in service, or
- A failure of your computer and telecommunication systems.

Information and communication asset rectification cost
This includes:

- Repairing, restoring or replacing the affected parts of your information and communication assets (including software, hardware, firmware and electronic data) following any damage, destruction, alteration, corruption, copying, theft, or misuse.

Cyber extortion cover
Reimburses you for the costs of:

- Responding to a threat from a hacker, including authorized ransom payments.

We are pleased to provide a copy of our policy wording and discuss questions upon review.

Additional support available to you

As a QBE policyholder, you'll receive complimentary access to the eRiskHub® portal. eRiskHub® provides tools and resources to help you understand your exposures, establish an incident response plan, and minimize the effects of a breach on your organization.

QBE eRiskHUB®

Incident Roadmap

A detailed overview of QBE's cyber claims process, including how our specialist providers will work together to give you immediate assistance.

In The News

Cyber risk stories, security and compliance blogs, security news, risk management events and helpful industry links.

Cyber Library

Best-practices articles, white papers and webinars from leading technical and legal practitioners.

Risk Manager Tools

Assists you in managing your cyber risk through useful online tools.

eRisk Resources

A directory that helps you quickly find external resources with expertise in pre- and post-breach disciplines, including interactive training manuals and videos.

Cover across the globe

We're well placed to help you.

If you have offices or clients abroad, multi-territorial controls, varying data protection laws and cultural differences expose you to a whole new level of risk.

With a network of office around the world - all operating to the same exacting QBE standards - we're well placed to give you the full support you need, whatever your operations take you.

With a global network of local offices, we offer you:

- A centrally co-ordinated global risk management service across 150 countries
- Dedicated multinational case handlers who can talk you through local practices and procedures
- A liaison service to ensure you're always issued with the appropriate plicy documentation
- Policies that are fully compliant with local regulatory and tax requirements
- Premium and tax payment tracking every step of the way
- A single premium wherever possible, however many countries you operate in.

Our QBE offering

Whatever business you're in, chances are QBE has an expert in insuring it.

The breadth of industry sectors we insure is almost as diverse as our range of insurance solutions.

- Agriculture
- Aviation
- Communication/Media
- Construction
- Education
- Energy (Oil & Gas)
- Motor
- Financial institutions
- Forestry/wood products
- Healthcare
- Hospitality
- Life sciences
- Manufacturing
- Marine
- Mining, metals, minerals
- Power & utilities
- Professional services
- Public sector
- Real estates
- Sports & recreation
- Technology
- Trucking
- Wholesale, Retail & Distribution

Here's a selection of what we can insure across many industry sectors.

- Automobile Fleets
- Automotive Product Recall
- Builder's Risk/Course of Construction
- Clinical Trials
- Crime
- Cyber Liability
- Directors and Officers (D&O) Liability
- Environmental Impairment Liability (EIL)
- Energy
- General Liability
- Group Programs
- Hull Insurance
- Kidnap & Ransom
- Marine
- Medical Malpractice
- Mortgage Impairment
- Pharmaceutical & Medical Devices
- Professional Liability/E&O
- Property
- Specie
- Terrorism and Political Risk
- Wrap-up (Construction) Liability

Please visit QBEcanada.com to learn more.
www.qbecanada.com/insurance-solutions

Contact us

We welcome your inquiries or questions.

For cyber and data security insurance inquiries, please contact:

Underwriting

Scott Pidduck
Senior Underwriter - Professional Lines And Cyber
Tel: +1-416-682-5925
Scott.Pidduck@ca.qbe.com

Angela Feudo
Underwriter - Professional Liability
Tel: +1-416-682-5924
Angela.Feudo@ca.qbe.com

Claims

Michael Bourgeois
Senior Claims Examiner
Tel: +1-604-558-5773
Michael.Bourgeois@ca.qbe.com

Darren Goldman
Claims Manager
Tel: +1-416-682-5901
Darren.Goldman@ca.qbe.com

For all other general inquiries, please contact:

Kimberly Fernandes
Business Development Manager
Tel: +1-416-682-5944
Kimberly.fernandes@ca.qbe.com

Futher reading

Please visit our website:
www.qbecanada.com/insurance-solutions

Made possible

QBE Services Inc.

Bay-Adelaide Centre, 333 Bay Street, Suite 520, Toronto, Ontario, M5H 2R2, Canada
Tel +416 682 5930 Fax 416 682 5948
Visit QBEcanada.com

Registered in the Province of Ontario, Canada No. 002193827

7489/CanadaCyberReport/MAY2017