


BREACH, PRIVACY, AND CYBER COVERAGES:

Fact vs. Fiction





Misconceptions about data breach, privacy, and cyber coverages abound. In fact, financial institutions may be as confused as their clients, and that can put businesses at risk. After all, if you don't believe you need certain coverage, or if you think you're covered when you're not, a cyber event could spell disaster for your operation.

The solution? A deeper understanding of the various types of cyber coverage available, and guidance on which may be best for your unique company. Financial institutions who keep abreast of the latest programs can be in a better position to assess options for their clients, and informed clients can ensure all aspects of their business are considered.

This white paper will help arm you with the information you need to work with a provider to choose the cyber coverage that could save your business in a crisis.

How cyber coverage has evolved	4
Different programs for different goals	6
Understanding the differences between coverages	8
Size and industry determines relative risk	10
A sound cyber strategy for your business	12
How we can help	13





How cyber coverage has evolved

Cybercrime may seem like a recent affliction, but it's been around for quite a while – and so has cyber coverage. Since the first coverage solutions appeared in the early 1990s (as technology began to play a larger role in daily life and the internet was emerging as a viable business tool), inaugural service interruption and website liability coverages have led to a wide range of identity and data breach solutions.

But have these responses evolved enough to handle today's risk?

How far we've come

As websites evolved from the digital equivalent of billboards into active business platforms, connections grew exponentially. Programs that spoke to network liability soon followed, gaining prominence among larger companies and specialized online businesses.

The scope of risks businesses face today has prompted financial institutions to create a broader array of identity and data breach management service solutions. These new options are designed to address not only the conventional issues of doing business online, but also the dangers surrounding consumer data breaches and cyber business interruption, as well as emerging threats like data ransom and cyber extortion.

While there may be more variety in the program options available to businesses, cyber coverage isn't as widespread as it could be: many carriers don't offer cyber policies, and those that do will vary in what they're offering, [making it difficult for clients to compare policies](#).

Where we're headed

Despite the media attention given to major data breaches, there continues to be a misperception (if not apathy) among business owners: many believe they don't need coverage for cyber or breach risks, or that their current umbrella policy already includes this type of coverage, and so they don't bother purchasing cyber policies for their businesses. However, as more big breaches dominate headlines, the fear of cybercrime is spreading, and that's pushing people to act.

If you don't know where to start, you're not alone: many of your peers are in the same boat, as it can be difficult to get familiar with the depth and breadth of available cyber policies. Financial service organizations can play a big role in helping you choose and develop a cyber risk program that's tailored to your business, as they continue to build on their solid understanding of the current cyber risks at play.

Know your risk to understand your options

An awareness of risks and mitigation best practices is at the heart of proactive protection. You may have the tools to improve your security posture and reduce your risk of a breach, but identifying and implementing effective measures requires a better understanding of today's cyber threat environment and how your operation compares.

The move from narrowly focused programs to programs that address multiple risks in interrelated areas had led to some confusion. Knowing which risks your company faces and how best to mitigate them isn't nearly as straightforward as it was even five years ago, but expert insight into the evolving world of best practices can help marry risks with appropriate mitigation strategies.

If you don't know where to start, you're not alone: many of your peers are in the same boat, as it can be difficult to get familiar with the depth and breadth of available cyber policies.

Different programs for different goals

An important first step is to differentiate between a few common – yet different – digital defence programs.

Here are some explanations of specific program features.

1. Cyber Programs

These focus on services and systems related to technology and their use in business. Risks addressed include website and software design, network equipment, damage caused by service interruptions and computer viruses, and much of the work performed by technology vendors and consultants.

Customers are also commonly covered for damages if they inadvertently transfer a virus to a network owned or operated by someone else.



2. Data Breach Programs

Often used interchangeably with privacy breach programs and/or security breach programs.

A data breach program provides protection for businesses in the event sensitive data is compromised or exposed. Many program policies also cover costs associated with first-party response and third-party liability exposures.

3. Privacy Breach Programs

A more broadly defined program, a privacy breach program can protect businesses in the event customer, consumer, or patient data is compromised or exposed.



A data breach program provides protection for businesses in the event sensitive data is compromised or exposed.

Understanding the differences between coverages

The terms “cyber coverage” and “privacy breach coverage” are often used interchangeably when referring to the policies available, but there are significant differences between them.

Cyber coverage:

Typically focuses on services and systems related to technology and their use in business.

Risks addressed include website and software design, network equipment, damage caused by service interruptions and computer viruses, and much of the work performed by technology vendors and consultants. Commercial depositors are also commonly covered for damages

if they inadvertently transfer a virus to a network owned or operated by someone else.

Privacy breach coverage:

Protects businesses in the event customer, consumer, or patient data is compromised or exposed. Costs associated with first-party response and third-party liability exposures may also be covered under such a policy.



First-party coverage:

Provides for legal expenses associated with regulatory compliance, such as federal mandates and financial industry regulations, including contractual agreements surrounding compliance.

This program also covers expenditures incurred during a forensic investigation into the duration and extent of the exposure, to determine specifically what data was compromised and who was impacted. First-party coverage also extends to the costs involved with responding to a breach, notifying the affected parties and any applicable regulatory agencies, and providing victims (and potential victims) with credit monitoring tools and identity theft remediation services.

Third-party coverage:

Focuses on liability costs related to defending against consumer-based litigation or regulatory actions that arise as a result of a breach.

Cyber crime vs cyber risk coverage

Though the terms may sound alike, cybercrime and cyber risk will fall under different coverage categories. Cybercrime is a peril within crime policies, while cyber risk is something separate.

Let's take social engineering as an example, which refers to deceiving and manipulating people to perform certain actions or reveal sensitive information. When social engineering results in a financial loss, it would fall under cyber crime. However, if social engineering leads to a loss of confidential data, this would be considered a cyber risk peril.

According to a [recent FICO survey](#), 40% of Canadian firms have a full cyber security program in place – one that covers all risks – while 50% of respondents in the retail and e-commerce sector don't believe their coverage matches their risk profile. How can businesses reconcile this issue? First, they must assess their individual risk based on their unique profile.



40% of Canadian firms have a full cyber security program in place – one that covers all risks – while 50% of respondents in the retail and e-commerce sector don't believe their coverage matches their risk profile.

Size and industry determines relative risk

Is your company small, mid-size, or large? Size matters when it comes to cyber risk, as the amount of data as well as your approach to storage can expose certain vulnerabilities.

Large companies

The nature of big companies and their operations typically calls for strong privacy breach and cyber coverage. Since they tend to gather, process, and store large amounts of information – and they often have complex technology and network infrastructures supporting their operations – big companies have more potential points of weakness (and likely more money to lose).

These companies often deploy and manage much of the underpinnings

that drive wider activities, such as the processing of financial transactions and the compilation and analysis of large databases. This can require many connections to outside partners, such as suppliers and client organizations, which enlarges the network of potential victims. An extensive use of external vendors also leads many big businesses to allow network access to companies and people outside their own workforce, increasing the risk of a breach.



The factors laid out above put the typical large company at significant risk of cyber exposure. Privacy breach risks, on the other hand, are often managed through the proactive policy making and robust security measures available to big firms that have sufficient funding and ample internal resources.

Small businesses

In contrast to large organizations, many small and mid-sized businesses won't face the same levels of risk when it comes to cyber exposure. They may rely primarily on their own internal systems while only occasionally working with other companies to use their networks for connected activities.

While small businesses may not have the same general cyber risk as large businesses, they often have a higher privacy breach risk. Since most don't employ data protection experts or large technology teams, the information they collect and manage can potentially be more vulnerable to exposure.

Small businesses are also less likely to implement strict data retention policies, plus they may not be familiar with the safest ways to store and dispose of information. In many cases, non-digital breach risks remain a top concern among small and midsize businesses: mailing hard-copy invoices and patient statements to the wrong address, for example, or improperly disposing of obsolete paper files, may pose as great a breach risk as any electronic network intrusion.

Other factors to consider

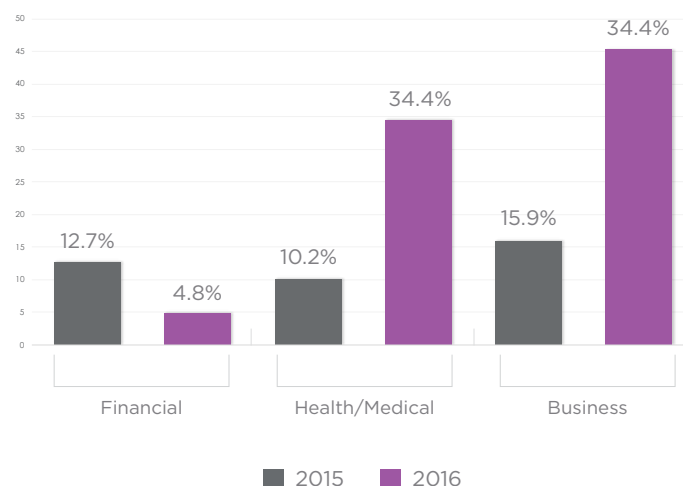
A subset of firms both large and small have risk profiles shaped by more than just their size. Companies that operate in specific industries, such as healthcare, legal, or financial sectors, often require more robust privacy breach programs.

These types of businesses are responsible for managing particularly sensitive information, and if that data is exposed, those impacted

could suffer significant harm. Whether it's a large hospital organization or a smaller clinic, a nationwide law firm or a small-town attorney, these companies have valuable and highly confidential information that attracts hackers – and that the businesses must vigorously strive to protect.

A review of breach statistics over the past decade shows trends within several key industries:

BREACHES BY INDUSTRY: 2005–2016



This data reveals that the financial and credit sectors may be preventing exposures more successfully now than in years past, but the health and medical services and general business industries have experienced a worrying uptick in breach events.

A sound cyber strategy for your business

The needs for both cyber and privacy breach protection solutions rest on business size, but other risk factors could influence the ideal program for a business, too.

Big companies generally have a number of other value-add products in their portfolios, and cyber risk programs can naturally align with existing initiatives that are overseen by the organization's risk management group. It's likely that these internal teams already have identified where potential liabilities lurk and what can be done to mitigate them. And while large firms regularly absorb significant levels of risk for financial reasons, most have also accepted sizable insurance premiums as a normal cost of doing business.

In comparison, the small business sector has been largely overlooked as a segment of the marketplace that was either uninterested or unable to secure robust programs. However, many small businesses (particularly those in the high-risk sectors) will often benefit from highly targeted and carefully underwritten policies. In many cases, add-on coverages can strengthen an existing commercial insurance policy, but the danger remains: without comprehensive cyber coverage, is your business truly protected across the range of existing cyber risk scenarios?



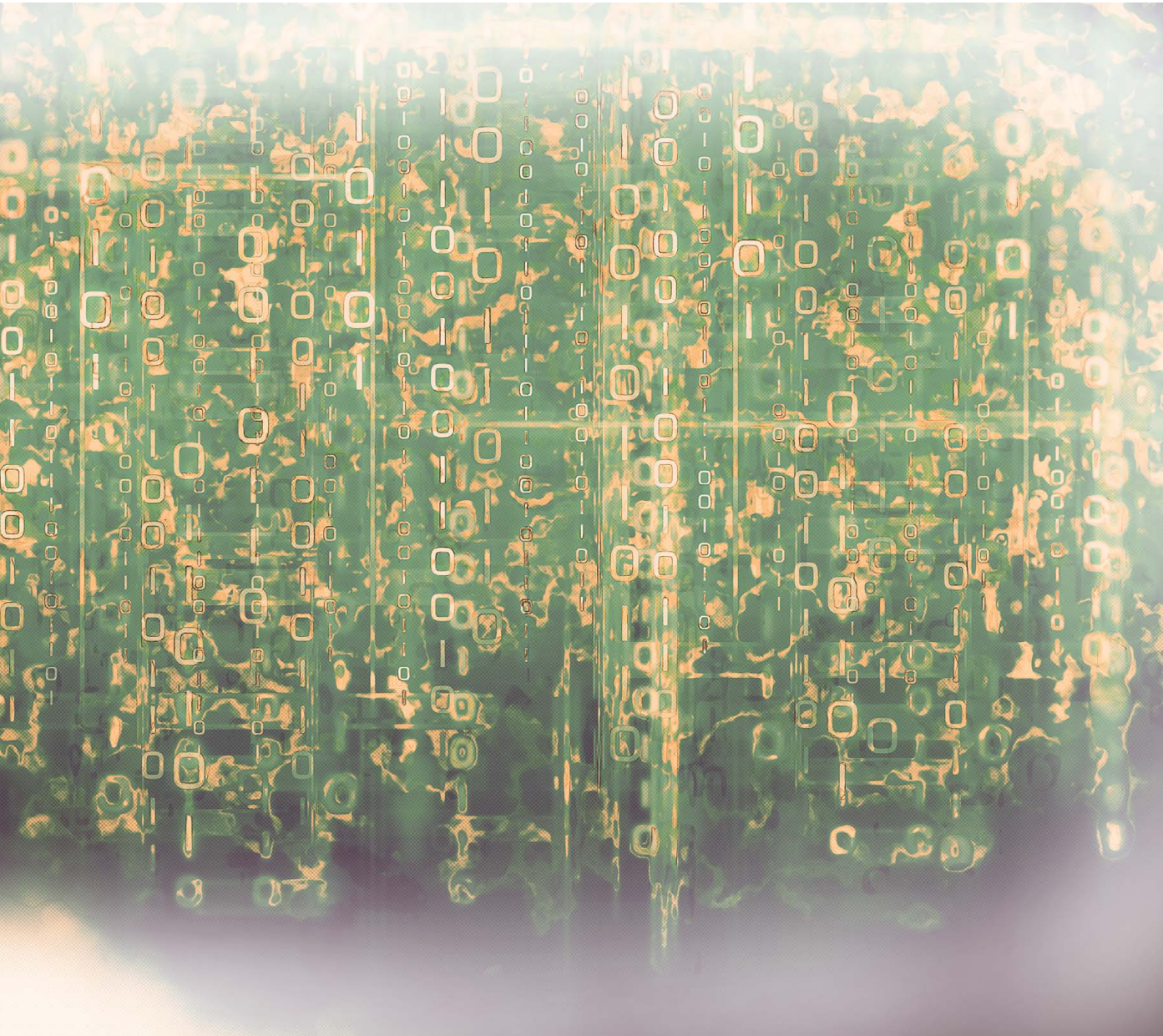
How we can help

Cyber risk comes in many forms, and it's crucial that you know your relative risk if you aim to build a strong defence. But while it's important to protect your business as well as you can, the right insurance can come to your rescue if your efforts fall short.

Not all cyber risk insurance is created equal. Without the right coverage, legal fees and fines, repair costs, and business interruption expenses that come with a cyber attack could fall on your shoulders. And as weapons like ransomware become more sophisticated and far-reaching, a single attack can bring on serious financial trouble.

Together with CyberScout, Northbridge Insurance has developed a versatile [cyber risk insurance](#) product: your policy can protect your bottom line if you suffer a breach, but it also grants you access to extensive cyber resources to help you protect, assistance to help you react, and personalized guidance to make sure the same thing doesn't happen again. After all, risk management is an ongoing responsibility, and Northbridge takes that seriously with comprehensive policies that keep your company's long-term success in mind.





This whitepaper is provided for information only and is not a substitute for professional advice. We make no representations or warranties regarding the accuracy or completeness of the information and will not be responsible for any loss arising out of reliance on the information.

Northbridge Insurance and Northbridge Insurance Logo are trademarks of Northbridge Financial Corporation, licensed by **Northbridge General Insurance Corporation** (insurer of Northbridge Insurance policies). [3808-002 ed01E]