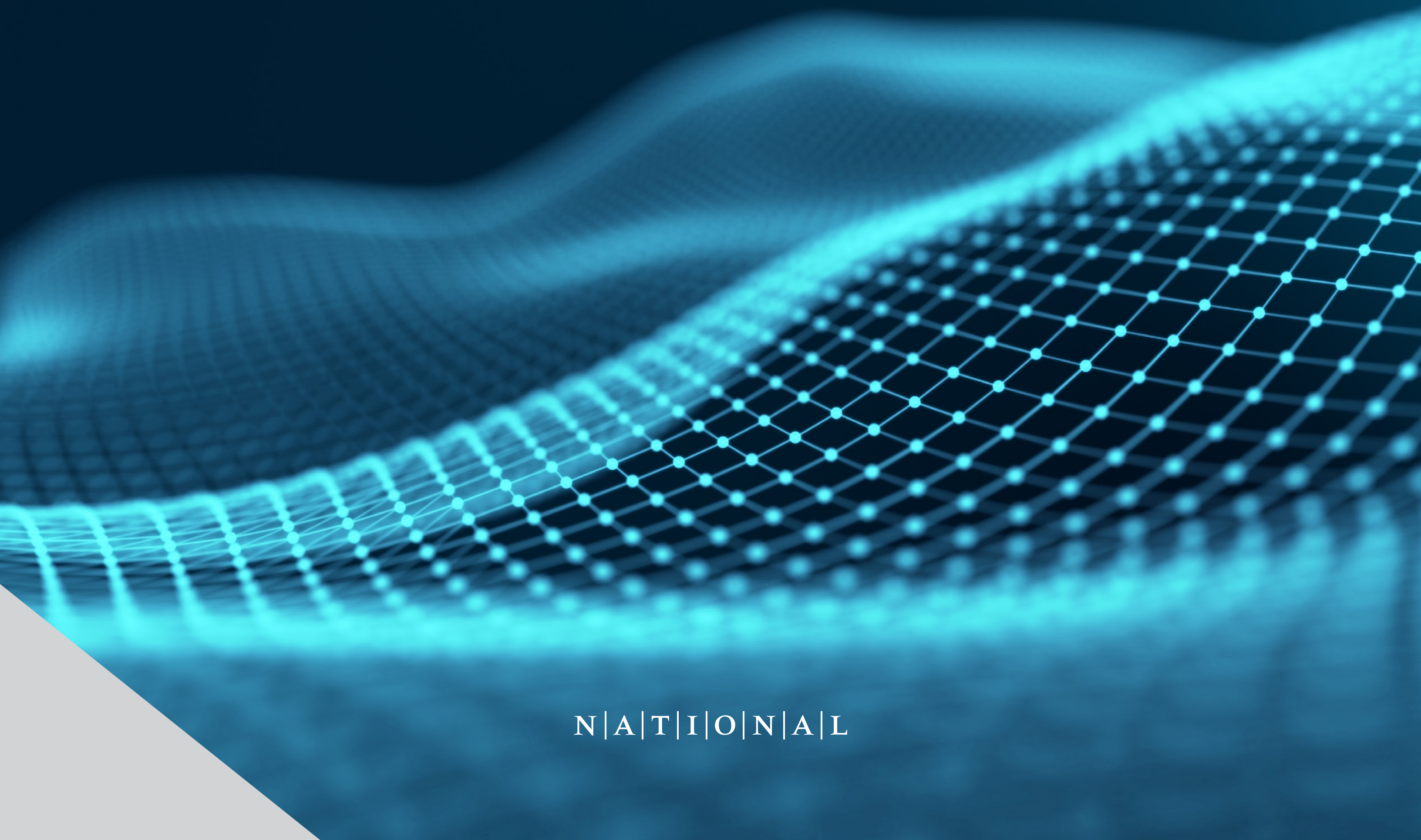
CYBER SECURITY AND
CRISIS COMMUNICATIONS

How to effectively navigate and prepare for a cyber attack

March 2021



N|A|T|I|O|N|A|L

AUTHORED BY:
Karen White, Vice-president, Crisis and issues management
Larry Markowitz, Senior advisor, Financial communications and Investor relations
Odane Finnegan, Associate, Public affairs

Overview

At NATIONAL, we know that good execution is based in good planning, and that this rule is magnified in the intensity of a crisis.

There is arguably no greater crisis for an organization than to suffer a cyber security breach. Regardless of industry, the security of your clients' data is critical to the health of the customer relationship. As the work environment has become increasingly digitized, new avenues of attack by malicious cyber actors have opened. **In the light of this new reality, we have decided to share some best practices for when (not if) your organization faces a cyber security crisis.**

The new environment

Data moves quickly. As we transition to a digital-first, work-from-home culture, your digital landscape must become more of a priority for decision makers in your organization. In this section, we will highlight the heightened risk in the current standard infrastructure. We will outline recent transitions in the regulatory environment and changes in consumer perceptions.

New attack vectors

Let's start by stating the obvious: Last year changed the world. There's no caveat needed because in every aspect of life, the events of the last twelve months changed standard operating procedures for all. One such change was the wide-scale adoption of work-from-home protocols for companies of all sizes. As employees logged in from home, the number of entry points open to infiltration by bad actors increased by several orders of magnitude. Individual home networks are more susceptible to attack for numerous reasons (that we won't explore in this paper). This has translated into significantly more attempts on corporate networks.

According to the CIRA Cybersecurity Report, three-in-ten organizations have seen a spike in the volume of attacks during the pandemic. This number is likely a conservative estimate, as within that same survey, 38% of respondents did not even know whether they had experienced a breach of customer and/or employee data within the last year. Indeed, we have seen many breaches that only came to light after a list of confidential customer data was discovered on the dark web.

In the face of such uncertainty, how would you even know if your data has been exfiltrated? This requires a thorough audit of current data storage and data sharing practices, as well as a process to identify when something outside of that standard practice has occurred. As our work becomes increasingly virtual, the importance of securing vulnerable information has never been greater—whether you are in the private sector or the public sector.

Organizations who store any customer, client, or employee information (in other words, every organization) need to be acutely aware of the impacts that a data breach or other cyber security incident would have on their operations and their reputation. They need to plan accordingly and understand what steps need to be taken (a) before an incident happens, (b) while it's happening, and (c) after it has ended.

Changing regulations

Once an issue has been identified, a litany of questions follows. However, there is one set of questions the answers to which have changed significantly in recent times: What am I legally required to do? Who am I required to notify? Within what timeline?

Federal and provincial legislators have instituted clear expectations for organizations that suffer a breach: communicate clearly, honestly, and often. As cyber attacks that breach Personally Identifiable Information (PII) become more common, governments have recognized the need to update legislation to protect their citizens.

On November 17, 2020, the federal government tabled Bill C-11, the Digital Charter Implementation Act, 2020, which seeks to significantly overhaul Canada's federal privacy laws, providing individuals with greater control over their data and holding companies that handle personal data accountable for protecting that data. The proposed legislation creates a new data management framework under which consumers are granted greater control over how their data is used and must consent to any lessening of control. There will also be a new enforcement regime, which will represent a significant departure from the previous system. It provides for significant fines of up to $10 million or 3% of global revenues against companies that fail to protect their users' data, meaning that protecting the data and privacy of Canadians will become a higher-level priority for organizations.

Shifting consumer expectations

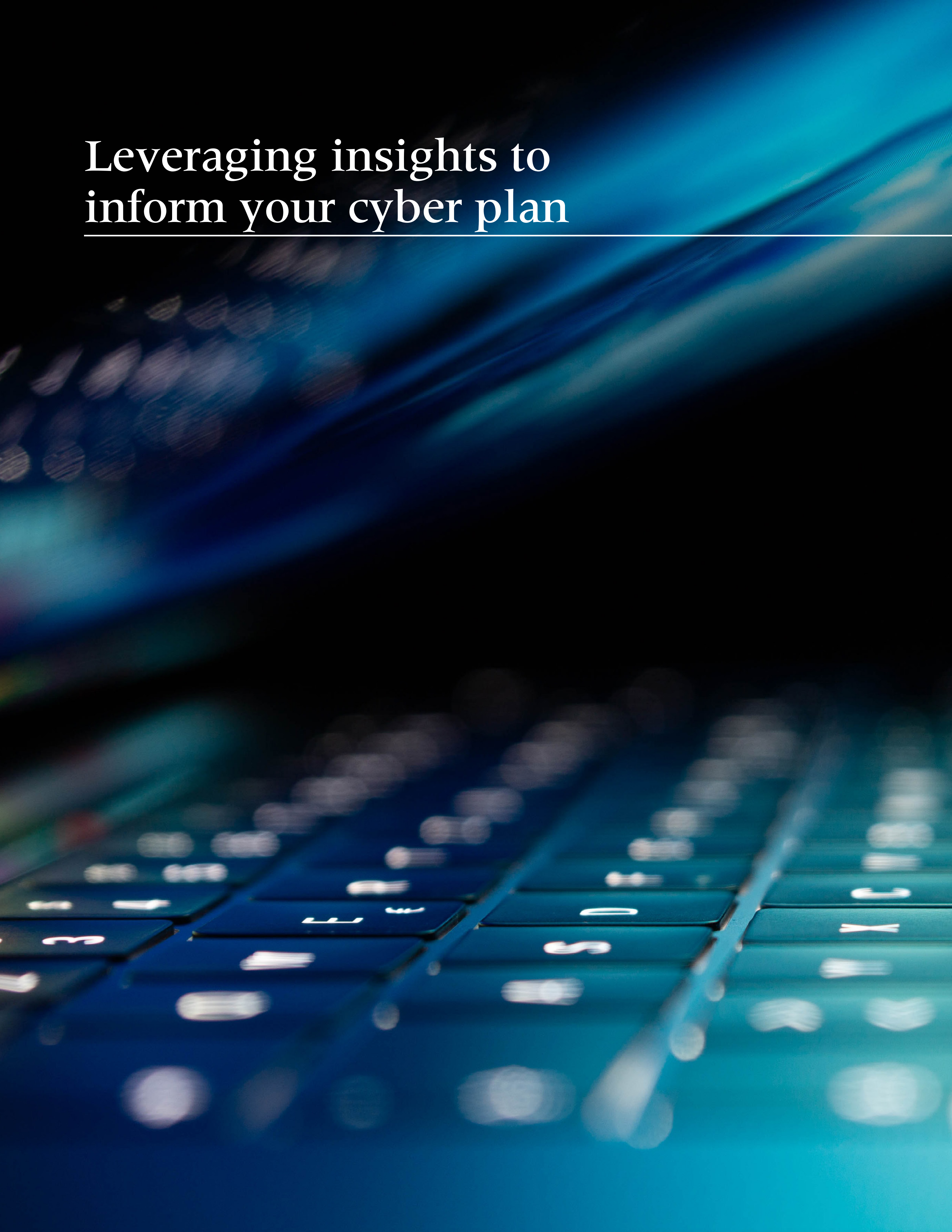
There is an adage in Silicon Valley along the lines of, "If the app is free, you're the product." Capitalizing on the time users spent on an app or platform has become the prominent feature of our digital economy. However, users are often left with the feeling they have no control over their digital footprint. As a result, when data breaches started coming to light, consumers are unforgiving in their response.

A survey sponsored by the Privacy Commissioner of Canada found that the proportion of Canadians who have adjusted their device settings to limit the amount of personal information that is shared had steadily increased from 40% in 2011 to a high of 76% in 2016. In addition, 82% of respondents indicated they would uninstall an app based on the information it is requesting; 92% expressed some level of concern about the protection of their privacy; and nearly 60% are concerned about the potential for their posts on social media to harm their reputation. These figures are indicative of the importance of control over the use and privacy of personal data.

This desire for control does not only relate to security issues. Another notable addition to that survey, conducted by the Privacy Commissioner of Canada, was regarding the public's views on the economics of data as it currently exists. The top three concerns listed were firms like health insurance providers using data on them to make decisions; marketing agencies analyzing likes and dislikes to target advertising; and personal information being used in a hiring process. The level of knowledge and awareness of consumers is increasing and as that happens, they expect a level of clarity from the business and organizations with which they engage.

In the face of everything listed above, there is some good news in this report for businesses. The survey found a few key areas that business leaders can focus on to improve trust and engagement in their platforms, products, and services. When asked what practices or laws ought to be prioritized, there were two responses that received more than 70% support. The first was ensuring that companies would face a "large" financial penalty under Canadian law with the ability to levy fines up to 5% of global revenue. The second was that Canadians were "definitely" or "probably" more willing to do business with a company if that "company provides clear, easy to understand information about its privacy practices".

Leveraging insights to inform your cyber plan



Armed with a better understanding of the regulatory landscape and the expectations of consumers, it is up to business leaders to implement proven best practices.

A data breach is a critical moment for any organization. How you respond and how you communicate that response will impact your brand identity—be it positively or negatively.

At NATIONAL, we have identified several best practices you can implement in the face of a data breach. We have divided these recommendations into (a) what you can do now, (b) what you can do during an attack, and (c) what you ought to do after you've identified the issues and contained the breach.

Pre-event

Assuming you would rather not "build your plane in flight", it is best to do some planning prior to experiencing a cyber attack or other data breach.

Taking the time to audit and reflect on your organization's crisis communication vulnerabilities, preparedness, procedures, and resources, is a critical step in pre-event planning. This will help identify gaps in the current state of preparation and inform recommendations and actions. The findings of the pre-breach audit phase, which typically includes consultation with legal, security, and information technology experts to review and strengthen your organization's cyber response manual, will help you anticipate and manage issues that could potentially result in a cyber breach.

Now, what should you put in your cyber breach document? Begin with a list of questions. This will lead you to look around your organization, and outside your organization, for those who can help you answer them. As you go through this process and begin to answer those questions, it will help craft your future response to any security issue or data breach. You will have begun to build your plane before it needs to "take flight". To that end, we thought we might help elaborate on some of the questions you should be asking.

The first question is: What data are we holding? This might seem straightforward, but depending on the size of your organization, there may be multiple answers to this question. If that's the case, your first aim should be to get down to one organization-wide answer. Even if not everyone has access to all the data, it is important to know what information is being kept about customers and where. What data you're keeping is going to influence the rest of the process, as different types of data require different levels of security protocols. Are you merely storing a name and order sheet? Or does that data come associated with credit card or other payment info?

Next, you should assess where that data is being stored and what protocols are in place to identify when and where a breach has taken place. There are additional technical questions that should be asked and answered regarding passwords, third-party integrations, and a whole list through which data and privacy experts could take you. For our purposes, as we look at how to communicate during that time and how to best prepare for it, we need to address these questions in order to have a better and clearer understanding of the level of risk you face and to what potential issues that can lead.

The end-goal when creating a compliance program is to have a base understanding of your risks and effective measures in place to mitigate potential risks. By answering these questions, you will have established the framework to draft your communications and identify risk scenarios. By the time you're done with this planning, you should have a folder that is both secure and also accessible when nothing else is (the last thing you want is to create a plan and then have that plan locked away behind a hacker's paywall). This folder will address your data concerns, what data is in your possession, where you are holding that data, and how you know it's being held safely. Your folder will contain your immediate contact list and a checklist of questions, such as:

- » Who are the audiences impacted by this incident?
- » Have we notified employees? Customers?
- » Have we notified regulators? What notifications are required?
- » What do we tell each stakeholder audience?
- » When do we communicate? And, how often?
- » How will we know if we've been successful?

All of these questions will help inform your checklists and crisis preparedness plan. They will also form the basis of testing of your crisis plan, so you are prepared to response in the event of a cyber attack.

PRE-BREACH PLANNING INCLUDES:

- ✓ Overall crisis preparedness audit
- ✓ Communication planning and material audit
- ✓ Social and traditional media insights and research
- ✓ Executive coaching and media training
- ✓ Development of a cyber crisis playbook, which includes:
  - » Scenario development
  - » Established crisis team and approval protocols
  - » Identified spokespeople
  - » Audience and channel identification and prioritization
  - » Key message development
  - » Measurement and evaluation
- ✓ Crisis simulations and tabletop exercises

During the breach

Armed with a cyber crisis playbook, organizations can immediately activate their team of experts including crisis communications, legal, insurance, and cyber security to navigate cyber incidents.

Cyber incidents can be disruptive and have an impact on company operations and business continuity. Many organizations are able to efficiently create a virtual or on-site "situation room" or emergency operations centre and layer in experienced staff to effectively manage all crisis components including IT, operations, HR, legal, insurance, and communications. When a breach occurs, you will immediately have three major concerns:

» How can we secure and protect our data from the attack?

» What is the nature of the data that was compromised?

» Who are the individuals or stakeholder groups impacted by this and how will we communicate with them?

Regardless of the specifics of the incident, the first guiding principle is that **communication must be accurate and timely.** By timely, we mean it is important to understand from your investigation who the impacted audiences are and what is the nature of data that has been compromised. If personal information has been compromised, this will trigger more formal regulatory requirements for notification. Remaining silent risks creating a vacuum that will be filled by rumours and speculation. As you investigate and gain further insight into what has occurred, you can update your initial communication with additional detail. Whatever you do say should be accurate and concise, and the information you're sharing should be consistent and communicated with purpose.

The second principle is that you must **communicate directly with impacted stakeholders**—be they employees, customers, suppliers, or others. It is said that it costs five times more to attract a new customer than it does to retain an existing one. This demonstrates the importance of communicating effectively following a cyber attack, as the sentiment among your key audiences will be the driving force behind your ability to maintain trust and confidence in your organization. Communicate with priority audiences early and as necessary as new developments arise. Even without a wealth of detail, you can let them know an investigation is underway and provide further updates as the investigation proceeds.

Allowing your stakeholders to be notified by media or to stumble upon news of the breach themselves are worst-case scenarios. Your goal from the outset should be to control the channel of communication between your organization and key audiences. Once these communication channels have been established, you will want to keep them updated, allowing you to address stakeholder concerns

COMMUNICATIONS DURING THE RESPONSE PHASE OF A CYBER ATTACK INCLUDE:

- ✓ Cyber response team activation
- ✓ Integration into cyber response team of cyber security, legal, insurance, and operations
- ✓ Work with cyber experts to contain breach and determine scope (i.e. type of personal identifying information [PII] that was breached and who was impacted)
- ✓ Consult with legal on preparing formal notification letters
- ✓ Determine if privacy commissioner(s) or police need to be notified, based on jurisdiction
- ✓ Strategic counsel and communications planning
- ✓ Issues monitoring and management
- ✓ Employee and stakeholder relations
- ✓ Media relations and management
- ✓ Writing/editing and content development, Q&As, and statements
- ✓ Traditional and social media monitoring and issues analysis

directly, keep them up to date with the progress of the investigation, and inform them of any steps taken after the fact. As communications go in both directions, having an open line of communication will also help you assess the level of support or frustration with your organization and gauge an appropriate response.

If you are facing a ransomware incident, that adds an extra layer of complexity to your response. Typically, a ransom attack involves cyber criminals accessing and encrypting your data and demanding payment to restore access to your information and threatening to release it on the dark web. This means your information is compromised and available for others to see. The prevalence and risk of ransomware continues to grow. In a 2020 global survey from Sophos, a U.K.-based security firm, in Canada, 96% of organizations whose data was encrypted got it back, with twice as many (56%) through back-ups than by paying ransom (26%). About 39% (80) respondents in Canada (total 200) were hit with ransomware in 2020, and 68% of Canadian companies not hit by ransomware expect to be impacted in the future. Interestingly, 20% of respondents have holes in cyber insurance policy, meaning ransomware attacks are not covered by insurance.

Finally, when drafting your communications, do not start in the middle of the story. Start from the beginning in a spirit of transparency. The brand loyalty you will garner is priceless.

Post-breach recovery

When a cyber attack is over, it is important to assess your incident response and help maintain trust and confidence among your key stakeholders. By assessing your breach response through reputation audits and social media intelligence reporting and analysis, organizations have an opportunity to reflect on lessons learned and apply these learnings to their cyber security and crisis communications plan.

It is important to document what steps you took to contain the breach and what new processes will be put in place going forward. This is critical information to share with your key audiences to demonstrate you've learned from the incident and are doing everything you can to prevent a similar attack from happening again.

In many cases, companies offer support services like credit monitoring to provide added protections if personal information has been compromised. Some companies will provide one-to-three years of credit monitoring for impacted individuals, and on the high end of the scale, up to up to five years.

Assessing the effectiveness of training on enhanced protocols and implementation of additional security measures (i.e. antivirus software) following an incident are also critical following a cyber incident. In some cases, this involves brining in third-party experts in cyber security to audit and complete a scan of your IT infrastructure and continuing to update security monitoring protocols and prevention measures.

Finally, it is important that organizations consider how to rebuild their brand image and maintain the trust and confidence of your key audiences. A thoughtful approach to brand recovery and reputation management will help transform this crisis into an opportunity by sharing learned lessons and demonstrating effective leadership.

COMMUNICATIONS DURING THE EVALUATION AND RECOVERY PHASE INCLUDE:

- ✓ Post-incident analysis and reputation review
- ✓ Communications planning to rebuild stakeholder relationships, trust, and confidence
- ✓ Post-incident evaluations - "Lessons learned" workshops and report
- ✓ Reputation audit and management plan
- ✓ Updates to crisis communications plan
- ✓ Reputation management plan and communications

Conclusion

One thing we know is true, when it comes to cyber attacks, it's not a question of if. It's a matter of when.

With the growing threat and prevalence of cyber attacks, it's critical that companies have effective communications hard-wired into their crisis plan. Layer on the risk of increased exposure with dispersed workforces and greater regulatory scrutiny, and companies are under tremendous pressure to handle these threats in real time.

While the best strategy is prevention (and many companies successfully fend off attacks), the increased frequency and sophistication of attacks is making it increasingly difficult to keep your data safe in a virtual world. Despite these challenges, there are steps you can take to protect your data and respond swiftly if you are the victim of cyber attack.

We hope this document provides some thought starters for how you can effectively prepare to respond and recover from a cyber attack. We'd welcome the opportunity to review your plans.

References

1. **“2020 CIRA Cybersecurity Report”**
   Canadian Internet Registration Authority

2. **“New data breach reporting requirements come into force this week”**
   Office of the Privacy Commissioner of Canada
   October 29, 2018

3. **“Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia”**
   Report of findings
   PIPEDA Report of Findings #2019-002
   April 25, 2019

4. **“Strengthening Privacy for the Digital Age”**
   Proposals to modernize the Personal Information Protection and Electronic Documents Act
   Innovation, Science and Economic Development Canada
   May 21, 2019

5. **“2016 Survey of Canadians on Privacy”**
   Prepared for: Office of the Privacy Commissioner of Canada
   Phoenix Strategic Perspectives Inc.
   December 2016

6. **“National Cyber Security Strategy: Canada’s Vision for Security and Prosperity in the Digital Age”**
   Ministry of Public Safety and Emergency Preparedness Canada
   May 28, 2019

7. **“Does It Still Cost 5x More To Create A New Customer Than Retain An Old One?”**
   Blake Morgan
   Forbes Magazine - April 29, 2019

About the authors

KAREN WHITE

leads the NATIONAL Public Relations crisis team and is one of our leading cyber security experts.

LARRY MARKOWITZ

is a lawyer and financial communications expert and a lead member of the cyber security communications team.

ODANE FINNEGAN

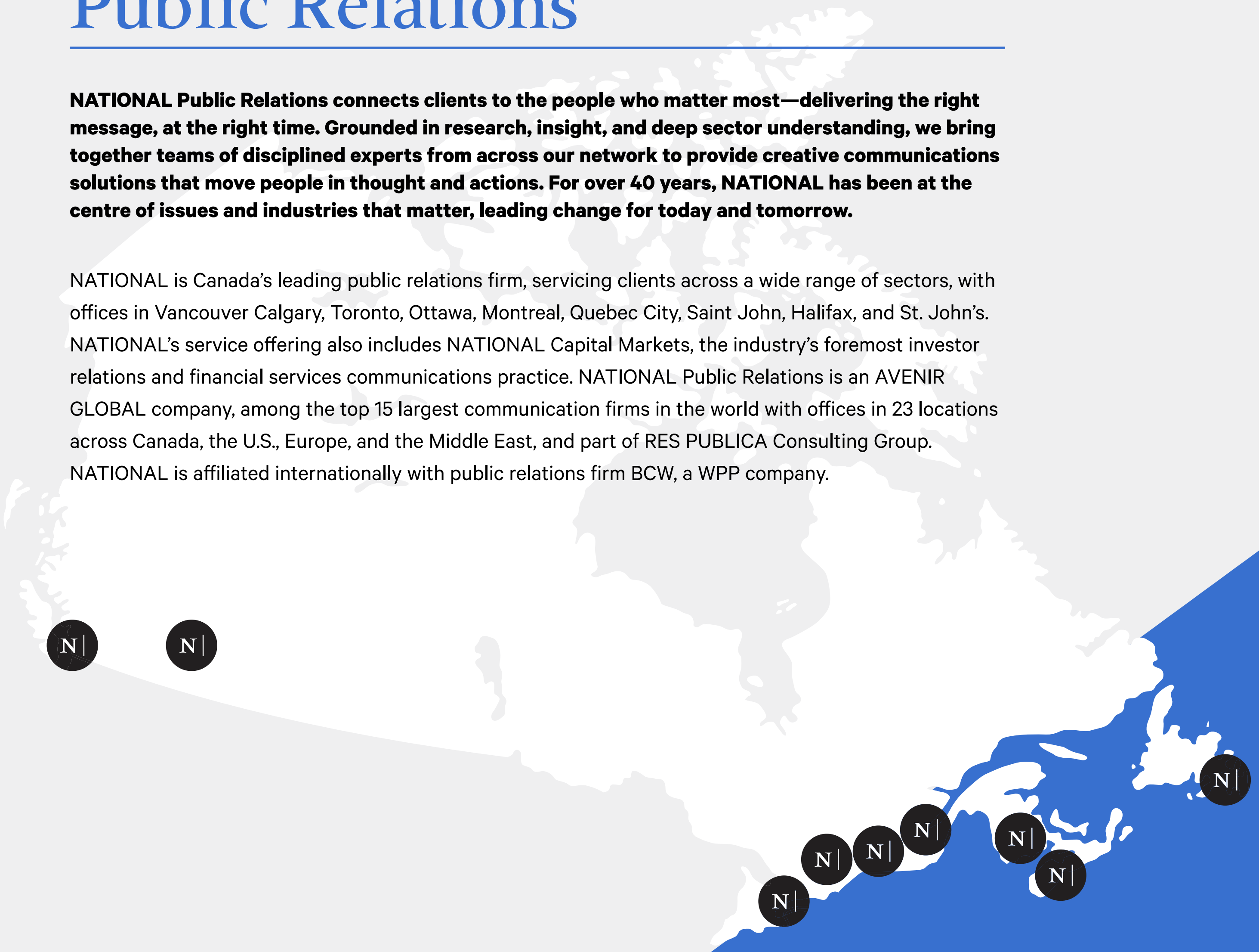
is a member of our social intelligence team with an interest in leveraging data and insights to inform communications strategy.

Learn more about our expertise in cyber security at national.ca/cybersecurity.
Contact our cyber security experts: cyber@national.ca.

About NATIONAL Public Relations

NATIONAL Public Relations connects clients to the people who matter most—delivering the right message, at the right time. Grounded in research, insight, and deep sector understanding, we bring together teams of disciplined experts from across our network to provide creative communications solutions that move people in thought and actions. For over 40 years, NATIONAL has been at the centre of issues and industries that matter, leading change for today and tomorrow.

NATIONAL is Canada's leading public relations firm, servicing clients across a wide range of sectors, with offices in Vancouver Calgary, Toronto, Ottawa, Montreal, Quebec City, Saint John, Halifax, and St. John's. NATIONAL's service offering also includes NATIONAL Capital Markets, the industry's foremost investor relations and financial services communications practice. NATIONAL Public Relations is an AVENIR GLOBAL company, among the top 15 largest communication firms in the world with offices in 23 locations across Canada, the U.S., Europe, and the Middle East, and part of RES PUBLICA Consulting Group. NATIONAL is affiliated internationally with public relations firm BCW, a WPP company.



national.ca

N|A|T|I|O|N|A|L

national.ca