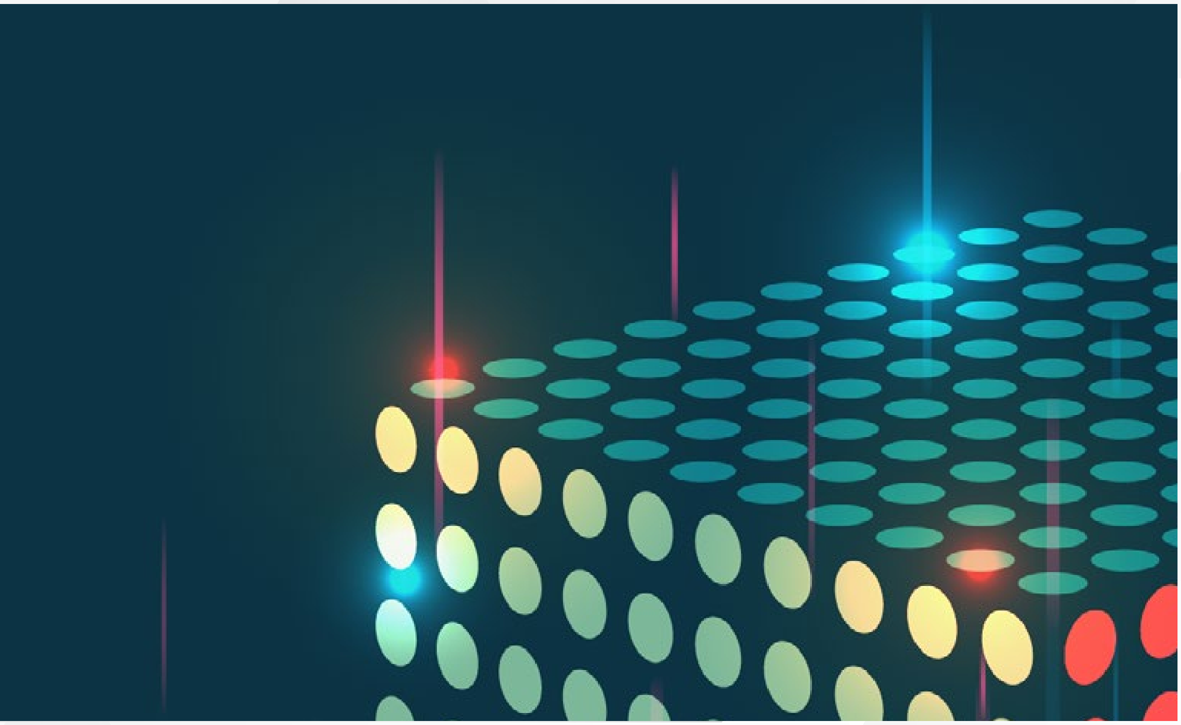
MNP DIGITAL



The perfect storm

Why cyber awareness is more important than ever

MNPdigital.ca

Organizations throughout the private, public, and not-for-profit sectors have faced a myriad of strategic and operational hurdles over the past two years. Arguably, none have been so disruptive as the growing cyber security and privacy threat.

By every measure, 2020 was yet another record-breaking year for breaches, and the COVID-19 pandemic has deservedly taken its fair share of the blame. But leaders would be wise to heed the other factors at play — including risks that emerge through digital transformations, growing reliance on third-party technology providers, and increasingly sophisticated machine learning and AI hacking tools.

As we near the end of 2021, organizations must be prepared to protect against not only the sheer volume of attacks, but a widening array of tactics and vulnerabilities.

Following is an overview of five contemporary risks and steps organizations can take to reduce the risk of a breach.

Remote work continues to pose risks

Perhaps the biggest and most publicized concern around the shift to remote work is the notable growth in extant threats like phishing and ransomware attacks. According to Verizon's 2021 Data Breach Investigation Report & Analysis, phishing was present in 36 percent of breaches in 2020, a 10-percent increase year over year. The office seems to provide a natural defence to this type of attack in that employees can verbally flag a suspicious email to a peer across the hall or at an adjoining workstation. Remote workers appear not only less inclined to vocalize concerns over email or instant messaging, but also more vulnerable to clicking suspicious links or downloading unsolicited attachments.

With the growth of remote work, it's also inevitable that cyber criminals will continue to spend more time in residential areas looking for unsecured or poorly secured internet connections. Cyber criminals have long used wireless access points and open wi-fi hotspots to compromise corporate networks. Remote workers who haven't updated the default passwords on their router or don't regularly connect to the employer network via a secure VPN are at significantly higher risk of a breach.

Online collaboration tools are another lingering concern. While these have been a lifeline for organizations throughout the pandemic, they've also been mired in developer shortcomings and security vulnerabilities due to rushed implementations. An area which is perhaps not getting enough attention is employees independently seeking out additional platforms and software to enhance the remote work experience. Without proper vetting from IT security professionals, these too can leave networks vulnerable.

The challenges of a hybrid workforce

Even as a return to the office is becoming possible in many parts of Canada, more employers are opting for a hybrid approach. While potentially beneficial for employee engagement and wellbeing, this partial return to the office will likely do little to reduce cyber risks. In fact, the opposite may be true. Without knowing who or how often team members will be in the office, a hybrid workforce effectively doubles the security environment and the risk factors for organizations to monitor and mitigate moving forward.

Cyber security training is necessary to support the successful transition to a hybrid workforce, but is insufficient as a standalone solution. Organizations must embrace a robust and ongoing effort to regularly assess, detect and mitigate threats, and regularly test human and technical controls across internal and remote networks.

Digital identity management: Vaccine passports

Digital authentication is not an entirely new concept, but the implementation of vaccine passports has been divisive as it relates to privacy. A host of privacy and data security concerns have emerged around the collection of biometric data, management of sensitive information, and protection of individuals' intrinsic right to privacy.

MNP's Privacy and Data Protection Lead, Adriana Gliga suggests organizations can manage the issue by creating different access levels to see user data based on need. No external party would be able to save or use the data beyond the stated purpose, and — much like physical ID cards — the individual who owns the data would retain the source.

However, while this can mitigate the likelihood of a privacy leak or breach, it will not absolve organizations of the duty to protect individuals' sensitive information. Those entities requiring digital IDs, be they governments or employers, will still be responsible for securing user data. They must be transparent around the collection and use of sensitive information — and accountable for building digital trust via robust privacy programs, standardized privacy frameworks, and keeping user data secure.

Global semiconductor chip shortage: What's the knock-on effect for digital security?

Demand for semiconductor chips skyrocketed through the pandemic. Yet manufacturing supplies were unavailable for months as thousands of factories shut down due to COVID-19 restrictions. The resulting backlog has worsened an ongoing global chip shortage and supply chain crisis which some experts believe could take another two years to resolve.

It's not just everyday items like computers, video game consoles, automobiles, and smartphones that are affected. Semiconductor chips are also a crucial part of secure payment services as well as digital passports and ID cards.

According to EUROSMART, "The security chip is the only tamper resistant technology that guarantees that user data, cryptographic keys and the applications handling them remain protected at rest and during execution."

The shortage directly impacts the ability to keep user data secure when using applications which have become increasingly essential and commonplace in a pandemic-afflicted world. If the situation doesn't improve, it's foreseeable banks and credit card providers may need to issue temporary chip-less cards to consumers — and retailers may struggle to upgrade aging payment terminals. It's also possible emerging vaccine passports may lack critical chip-enabled security features necessary to protect sensitive personal information.

An increase in state-sponsored hacking?

A major U.S. pipeline fell victim to a serious, albeit relatively unsophisticated ransomware attack in May 2021. This led to a days-long shutdown resulting in fuel shortages, panic buying, and significant price increases.

The breach illustrates just how vulnerable organizations and governments can be to even simple attacks. More important, it highlights a growing focus on critical infrastructure among cyber criminals — and the looming threat to national power grids, water supplies, and the natural resource sector. While the pipeline attack was allegedly carried out by an independent group of hackers, there's growing concern state-sponsored groups may use similar techniques to wreak havoc and further geopolitical goals.

Even the largest organizations will struggle to prevent an attack from a sovereign state with virtually limitless resources at its disposal. However, there is still wisdom in regular cyber maintenance such as requiring employees frequently update passwords and immediately installing software patches and updates. Attackers — even those with government backing — will always take the path of least resistance. Embracing these and other best practices such as multi-factor authentication are often enough to persuade a would-be hacker to pursue an easier target.

Those organizations who view themselves as particularly vulnerable to critical infrastructure and state-sponsored attacks may also consider increasingly affordable AI tools to track network users and identify suspicious activity.

Ransomware attackers are targeting large reputable organizations

Ransomware attacks, a perennial concern for the better part of a decade, have risen sharply since the start of the pandemic — particularly among large enterprises. Increasingly, cyber criminals are targeting reputable organizations which store large volumes of sensitive information and therefore risk significantly higher fines and PR damage in the event of a breach. Organizations such as law firms, physicians, financial institutions, etc. are more likely to pay ransom demands if it means resolving the issue quietly and avoiding any unwanted media attention.

The tactic appears to be working, too. A recent report from CrowdStrike found the average ransomware payout now exceeds $1,000,000.

Problem is, paying a ransom doesn't necessarily guarantee a swift and amiable conclusion. There's nothing stopping attackers from perpetually increasing payout demands, stealing and selling records on the dark web, or simply disappearing without restoring access to critical systems. That's why a comprehensive breach response plan is critical.

Everyone in the organization should understand their role in a breach — including how to report a suspected breach internally, which third parties to contact and when (e.g., cyber professionals, legal advisors, PR firms), how to prevent further damage, and the organization's breach reporting requirements. Moreover, organizations need to ensure they're regularly backing up (and testing) critical systems and information to an offline server. This can help to both support business continuity throughout the breach, as well as validate the recovery process.

Implementing proactive steps like multi-factor authentication and employee training can help to reduce the likelihood of a successful ransomware attack. However, nothing is 100 percent effective. While cyber insurance is not a silver bullet, it can often help offset the cost of a breach — particularly for organizations which have a lot to lose in a ransomware situation.

A rise in surveillance software

Employers are increasingly turning to remote monitoring tools (i.e., surveillance software) to keep a watchful eye on their remote workforce. Supervisors can now view employees' screens, webcams, keystrokes, and computer activity to verify they're showing up at their desk on time and staying on task for the full working day. While this may provide an initial boost of confidence for employers concerned about teams running errands or streaming video on company time, it also begs the question of employees' right to privacy.

According to a study released by Top10VPN, "demand for employee monitoring tools surged by 87 percent in April [2020] then remained 71 percent above the pre-pandemic average the following month."

Employee surveillance is arguably as old as work itself. However, until recently it's been unthinkable that employers could (or would want to) track individuals in their own homes. Most employees are aware their employer can access their emails or browser history — or even that their in-office activities may be captured on CCTV. However, home surveillance raises a new level of concern.

What's to stop a wayward leader from turning on the webcam during off hours? Or a cyber criminal from prying into individuals' private lives during a cyber breach? What many may want to rationalize as a necessary check against lazy home office habits may expose both organizations and individuals to more legal, reputational, and ethical risk than anyone bargained for.

Effects on your business

A cyber attack typically ends with the mitigation of malicious code and restoration of services. However, that only marks the beginning of an organization's recovery. Lost revenues and reputational damages can be much more difficult to quantify and often take months, if not years to recuperate.

Critical questions organizations must consider in the aftermath of a breach include:

- Have ransomware originators stolen personal client / employee information, intellectual property, etc.? What information has been compromised, and what is the organization's legal and ethical duty to the affected parties (e.g., credit monitoring, financial compensation, etc.)?
- Has the attack compromised other servers and / or login credentials that could lead to another breach in the future? What steps are necessary to fully secure the organization and prevent another similar attack?
- Has the attack impacted the functioning and integrity of a physical system (e.g., drilling rig)? What are the costs and necessary steps to get systems back to nominal operating parameters?

Most organizations can expect a general loss of trust and confidence among clients, customers, and employees in the aftermath of an attack. This can materialize in everything from depressed revenues and lost productivity, to lawsuits and regulatory investigations. These damages are difficult to quantify but often include fines, extensive public relations and outreach investment, credit and identity monitoring for affected parties, costs to third party advisors, investments in training and security improvements, and more.

You recognize the threat... How do you respond?

Best practices such as quality perimeter controls, aligning with compliance programs, employee training, and incident response planning will form the foundation of any effective cyber security program. However, every organization must also approach their planning with two assumptions:

1. It's not a matter of if they'll face a cyber attack, only when.
2. It's virtually impossible to protect against every potential breach scenario.

It is therefore imperative organizations do not focus their limited security dollars on minimally protecting everything, but maximally addressing the highest priority risks and highest value assets. It is recommendedevery client begin with a baseline assessment of their overall cyber security maturity and risk exposures — and review this annually at a minimum.

Increasingly, we're also recommending clients assess the effectiveness of their risk management strategies through offensive security exercises such as ethical hacking and penetration testing. These allow organizations to understand their overall resilience in a real-world scenario without the real-world consequences.

Following is an overview of a typical Red Team exercise:

Step 1: Assess physical security and workplace habits

A single cursory site visit can reveal an astonishing amount about an organization's cyber posture. Even without sitting down at a computer monitor, our team can evaluate a wide range of security factors and gauge many of potential vulnerabilities, including:

Ease of access / quality of physical security: How easy is accessing common working areas and infrastructure? Are doors locked and functioning properly? Are employees consistently greeting, logging, and supervising guests or contractors while on-premises? Do team members frequently share swipe passes? Is tailgating a common practice?

Security education, awareness, and training (SEAT): Do employees consistently lock workstations when away from their desks? Do employees consistently share or discuss sensitive information in common areas? Are sensitive information and / or systems visible to visitors in common areas?

Network security and access: Is guest wireless access adequately firewalled and / or segmented from sensitive networks? Are there adequate restrictions and multifactor authentication requirements to access sensitively wired / wireless networks? How forthcoming are employees with passwords? Are employees accessing or disseminating information on unsecured guest networks (e.g., smartphones, tablets, etc.)?

Step 2: Test existing controls to understand efficacy and resilience

Leveraging both the information gathered in step one and the typical attack techniques used by cyber criminals, the team will then penetration test (i.e., attempt to breach) the organization's information (IT) and operations technology (OT) systems. Some common areas we typically look to gain access to include:

Known vulnerabilities / patches: Have the organization and its employees been vigilant in updating software and firmware to take advantage of the latest security features? These so-called zero-day vulnerabilities are a common point of access for many breaches.

Build / hardening standards: Has the organization taken adequate steps to configure firewalls, servers, switches, and routers according to the most recent standards? Has it changed default passwords, adequately encrypted stored passwords, and sufficiently restricted access privileges? Is disused or outdated hardware and software still connected to the network?

Encryption standards: Does all information that flows in, out, and through the network meet industry encryption standards? Do any gaps and / or shortcuts in encryption allow malicious actors to harvest information or access the network?

Social engineering: How effective are team members at identifying and reporting malicious emails? How many (if any) login credentials were harvested from a simulated phishing attack? Are current education and warning measures adequate to prevent a social engineering breach?

Step 3: Map potential spread and infrastructure vulnerabilities

Properly segmented IT and OT systems are essential for slowing and ideally preventing a breach from spreading to other high-value systems. Once the team accesses the client’s network, they attempt to spread the simulated attack and compromise as many systems as possible.

Organizations that work on the assumption they will inevitably be the victim of an attack keep critical systems independent from one another to minimize the potential damage of a breach. This can also buy critical hours to action an incident response plan, contain the attack, and ultimately recover the systems.

Embrace cyber security and privacy as a core business objective

Today's organizations are embracing more digital tools and collecting more sensitive data than ever before. At the same time, cyber criminals are continuing to evolve their tactics to take advantage of human and platform vulnerabilities, and global uncertainty in a changing world.

There is little organizations can do to prevent becoming the target of an attack. But every organization can take meaningful steps to improve their preparedness and minimize the short- and long-term damage of a breach, including:

- Regularly assess key vulnerabilities and cyber risk exposures
- Ensure compliance with all industry and regulatory requirements is up to date
- Build cyber and privacy risk assessments into all strategic and tactical planning
- Provide frequent cyber security training for all employees
- Implement and update security and privacy governance programs
- Create and regularly practice an incident response plan

At MNP Digital, our multidisciplinary team can support you through all phases of your cyber security planning and execution — whether you're just getting your program off the ground or looking to achieve ever greater levels of maturity. Visit us MNPdigital.ca to find a local advisor and for more information on how we can help.

About MNP

MNP is a leading national accounting, tax and business consulting firm in Canada. We proudly serve and respond to the needs of our clients in the public, private and not-for-profit sectors. Through partner-led engagements, we provide a collaborative, cost-effective approach to doing business and personalized strategies to help organizations succeed across the country and around the world.

Author:

Danny Timmins, CISSP
National Cyber Security Leader
905.247.3290
danny.timmins@mnp.ca

Contributors:

Adriana Gliga CISSP, CIPM, PCIP
National Privacy Leader
647.480.8489
adriana.gliga@mnp.ca

Eugene Ng , BComm, CISSP, PCI QSA, ISO 27001 LA
Partner, Cyber Security
905.247.3280
eugene.ng@mnp.ca

Chris Law , BS
Partner
604.817.4852
chris.law@mnp.ca

Tom Beaupre , QSA, CISSP, CISA, BS
Partner, Risk Management
514.228.7844
tom.beaupre@mnp.ca

PRAXITY™
Empowering Business Globally