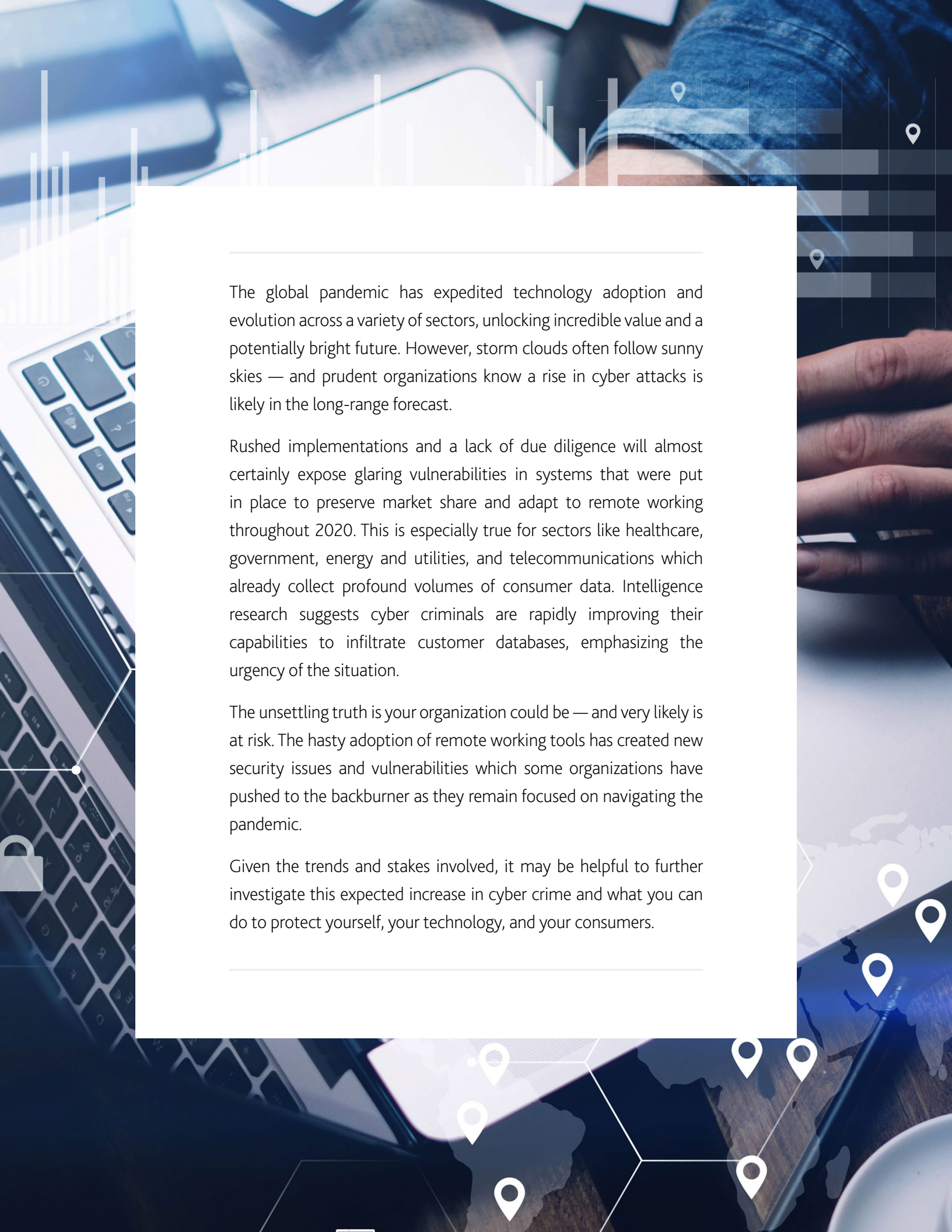
Planning for increased cyber risks in an age of digital transformation

MNP.ca



The global pandemic has expedited technology adoption and evolution across a variety of sectors, unlocking incredible value and a potentially bright future. However, storm clouds often follow sunny skies — and prudent organizations know a rise in cyber attacks is likely in the long-range forecast.

Rushed implementations and a lack of due diligence will almost certainly expose glaring vulnerabilities in systems that were put in place to preserve market share and adapt to remote working throughout 2020. This is especially true for sectors like healthcare, government, energy and utilities, and telecommunications which already collect profound volumes of consumer data. Intelligence research suggests cyber criminals are rapidly improving their capabilities to infiltrate customer databases, emphasizing the urgency of the situation.

The unsettling truth is your organization could be — and very likely is at risk. The hasty adoption of remote working tools has created new security issues and vulnerabilities which some organizations have pushed to the backburner as they remain focused on navigating the pandemic.

Given the trends and stakes involved, it may be helpful to further investigate this expected increase in cyber crime and what you can do to protect yourself, your technology, and your consumers.

4 Four key challenges

1. An expected rise in operational technology targeting and compromise

The rate of cyber attacks is expected to increase as political powers and organized crime groups continue to realize their full potential to impact operational technologies. Where hacks and breaches have historically focused on espionage — with a goal to secure research and close the competitive advantage — it is now routine for attacks to directly compromise operations and cause entire systems to fail. The TRISIS attack in 2017 is a startling example which saw malware developers specifically target Schneider Electric's Triconix safety instrumented system (SIS); a failure of which could have resulted in significant physical damages.

The Canadian government's intelligence and security arm, Communications Security Establishment (CSE), noted increased threat levels as "cyber threat actors are almost certainly improving capabilities to exploit industrial control systems (ICS)" in their National Cyber Threat Assessment of 2020 and Cyber Threat Bulletin to Canada's Electricity Sector.

The threat landscape for supporting operational technologies is also increasingly complex and deep. Attackers are pinpointing areas throughout the supply chain to compromise both physical units and software technologies. In other words, technologies are often arriving at organizations with pre-installed vulnerabilities which provides attackers with a seamless foothold in the environment at the point of implementation. Organizations can offset this increased targeting capability and threat complexity by addressing risks and gaps and planning their next moves before the attacker makes their play.

2. Ransomware increasingly capable of adversely affecting operational technology (OT)

Ransomware is a staple in the cyber criminal's toolbelt which has repeatedly proven effective against increasingly digital corporate environments. Notable ransomware attacks have succeeded in taking over financial processes, customer and partner web services, and communications. But the shift toward more integrated operational technologies raises the alarm such breaches will likely spread to these systems as well.

The consequences are increasingly significant, too. In their most recent National Cyber Threat Assessment the Canadian government reports the average ransom demand increased more than 1,500 percent between 2018 and 2020 — from approximately $9,000 to $150,000. Recent ransomware variants "EKANS" and "MegaCortex" foreshadow the potentially widespread prevalence of operational technology compromises, as both were found to have industrial control system interruption modules built-in.

While organizations are increasingly implementing controls to prevent and mitigate the occurrence of ransomware, attackers' capabilities are generally evolving far more quickly. Attacks will likely continue — and continue to be more severe — until enterprises recognize the need for a more progressive and proactive approach.

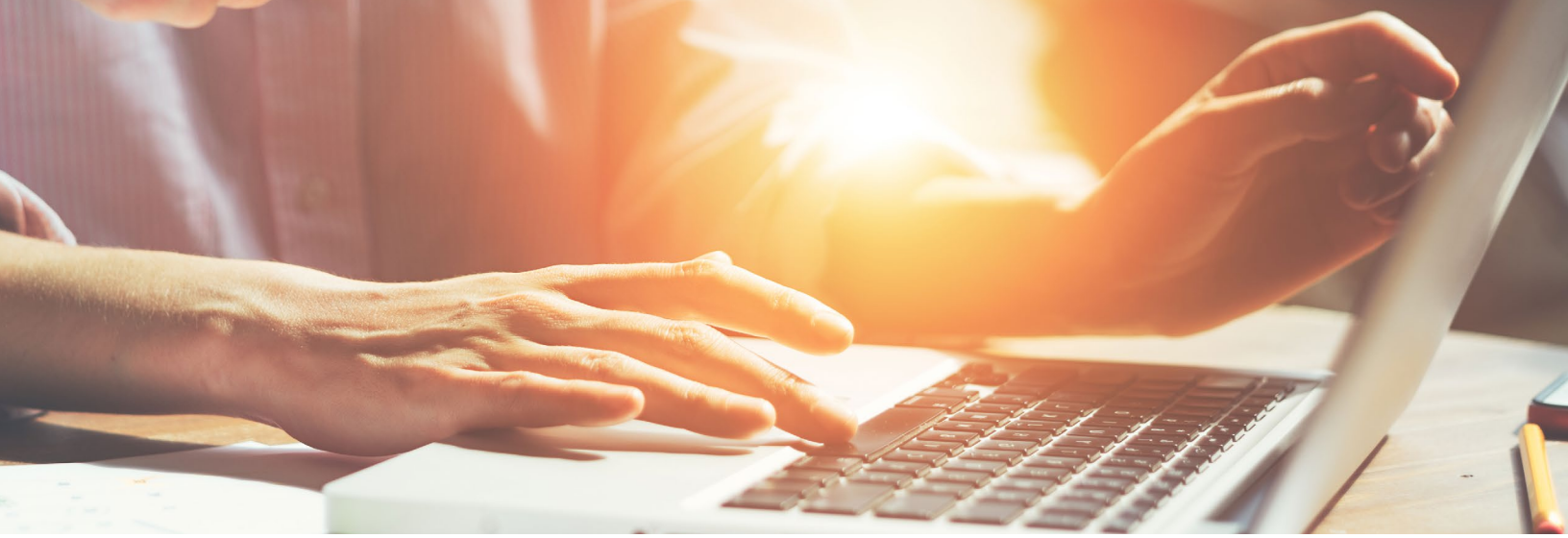
Organizations must be willing to stretch beyond traditional methods if they're to reduce the impacts of ransomware on information and operational technology environments. Improved threat detection and environmental redundancy are a good first step, but conventional methods alone may not be enough to stop an adversary that doesn't always follow convention.

3. Effective incident response planning and practice

Business resiliency and contingency planning have been highly effective in addressing environmental, organizational, and operational impacts in the critical infrastructure space. These types of risks are well known and have existed for a very long time. However, cyber security is a relatively new domain for contingency planning. It's therefore understandable that organizations have historically underprepared or failed to thoroughly consider the range of potential scenarios.

Effective incident response planning may be the necessary antidote. This approach helps decision makers thoroughly consider how technologies, risks, the threat landscape, staff structuring, vendor resources, physical locations, and the organization's culture could impact a potential crisis. Policies, plans, playbooks, and procedures are all staples of the program which outline expected responses to anticipated incidents, and how to practice them.

Organizations which embrace effective incident response planning benefit from scenario planning and practice now — which in turn, lays down a solid foundation to build from as threats adapt and evolve.



4. Enhancing data governance

Data, as they say, is the new oil. Its already astronomical value will only continue to grow as the world becomes more digitized and organizations increasingly turn to analytics to eek out even the slightest competitive edge. Collecting, using, and sharing personal data is already an integral part of stakeholder interactions for most organizations. Now many are looking to secondary uses for transactional data — from enhancing the customer experience, to developing new products, or improving the efficiency of business operations.

Consolidated data lakes (i.e. a centralized repository for storing all structured and unstructured data) and new technologies like analytics and AI are lucrative targets for attackers. Organizations are at growing risk of both breaches and leaks and the potentially significant financial, reputational and competitive damages that go in hand. Especially with tightening global privacy legislation lead by the European Union (GDPR), California (CCPA), and, most recently, Canada (PIPEDA).

Customers are more aware of their privacy rights and demanding that new products and services have privacy and security embedded in them. Organizations operating in multiple jurisdictions have additional challenges in meeting their regulatory and legal obligations and could face significant fines in the event of a compromise.

Preserving customer privacy and ensuring responsible and ethical data use may require some organizations to completely rethink their approach to data governance. Leaders need a comprehensive understanding of what data their systems are collecting, who owns it, how it's being tracked and managed, along with the organization's myriad legal and regulatory obligations. This may mean introducing new processes and practices to support decision making around new products or methods to extract additional value and insight from existing data.

An effective privacy program management framework is key for organizations to understand and manage their growing privacy risks.

Start building your cyber security system

The average breach lingers for a staggering six months before it's detected, which can lead to significant consequences in the interim. A poor security posture has the potential to compromise billions of dollars in personal, payment, or proprietary information — or worse: growing concern around cyber terrorism and state-sponsored attacks reveals it's not just information attackers are after anymore, but the ability to destabilize and take essential businesses offline.

This makes continued investment in cyber maturity far more than a strategic imperative, but a potential matter of national security. And its importance will only increase as Canada becomes more digitized, and remotely connected due to the pandemic. The economy — and perhaps even our lives — depend on robust, resilient, and reliable cyber solutions to combat the growing list of threats.

What steps should my organization take?

MNP has worked with many of Canada's largest municipalities, healthcare providers and government agencies to secure their data and assess weaknesses in their technology infrastructure. Our services run the entire lifecycle from putting an initial cyber security program in place to responding and remediating systems after an attack.

We recognize many organizations may worry about resourcing, expertise and where to focus their cyber security investments for maximum impact. However, it's important to recognize the biggest risk isn't in doing the wrong things, but in doing nothing at all. If an organization does nothing else, the following case study outlines our top recommendations to rapidly shore up gaps in their cyber defenses.

Know where you're vulnerable

We previously collaborated with a large enterprise client to conduct an initial stage Maturity Threat Assessment. This involved a comprehensive review of their entire business, competitive, governance, and technology landscape and helped to identify:

- Technology and information assets most at risk of an attack,
- Areas within their technology infrastructure where a breach was most likely to occur,
- Key gaps in their technical controls, policies, procedures, and training, and
- How best to allocate of cyber security funding and oversight.

Our assessment helped the client understand key vulnerabilities in their technology systems, and where they would get the greatest return on their cyber security investments. Most importantly, it allowed the organization to target specific, cost-effective improvements. The result was greater peace of mind that their team, customers, and systems were all optimally (though not necessarily universally) protected from the attacks they were most likely to face.

Test your assumptions

Having put our recommendations in place, the client's leadership approached us about a year later to find out whether their improved focus and enhanced controls were delivering the expected level of resilience. Rather than waiting for a breach to come to them, though, the client wanted MNP to penetration test their systems — which we call a Red Team Exercise or, in essence, a simulated cyber attack.

What follows is a step-by-step overview of our approach, which we try to keep as close to a real-world scenario as possible.

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 was able to evaluate a wide range of security factors and gauge many of the client's potential vulnerabilities, including:

Ease of access / quality of physical security: How easy is it to access 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 sensitive wired / wireless networks? How forthcoming are employees with passwords? Are employees accessing or disseminating information on unsecured guest networks (e.g. smartphone, tablet, etc.)?

Step 2:
Test existing controls to understand efficacy and resilience

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

Known vulnerabilities / patches: Has 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 in line with the most recent standards? Has it changed default passwords, adequately encrypted stored passwords, and adequately 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 gain access to 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?

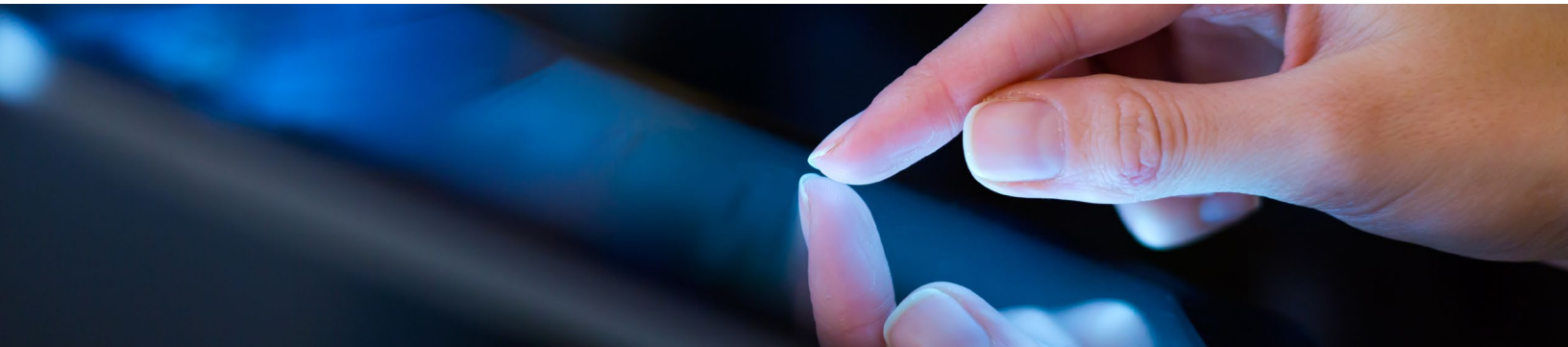
Step 3:
Map potential spread and infrastructure vulnerabilities

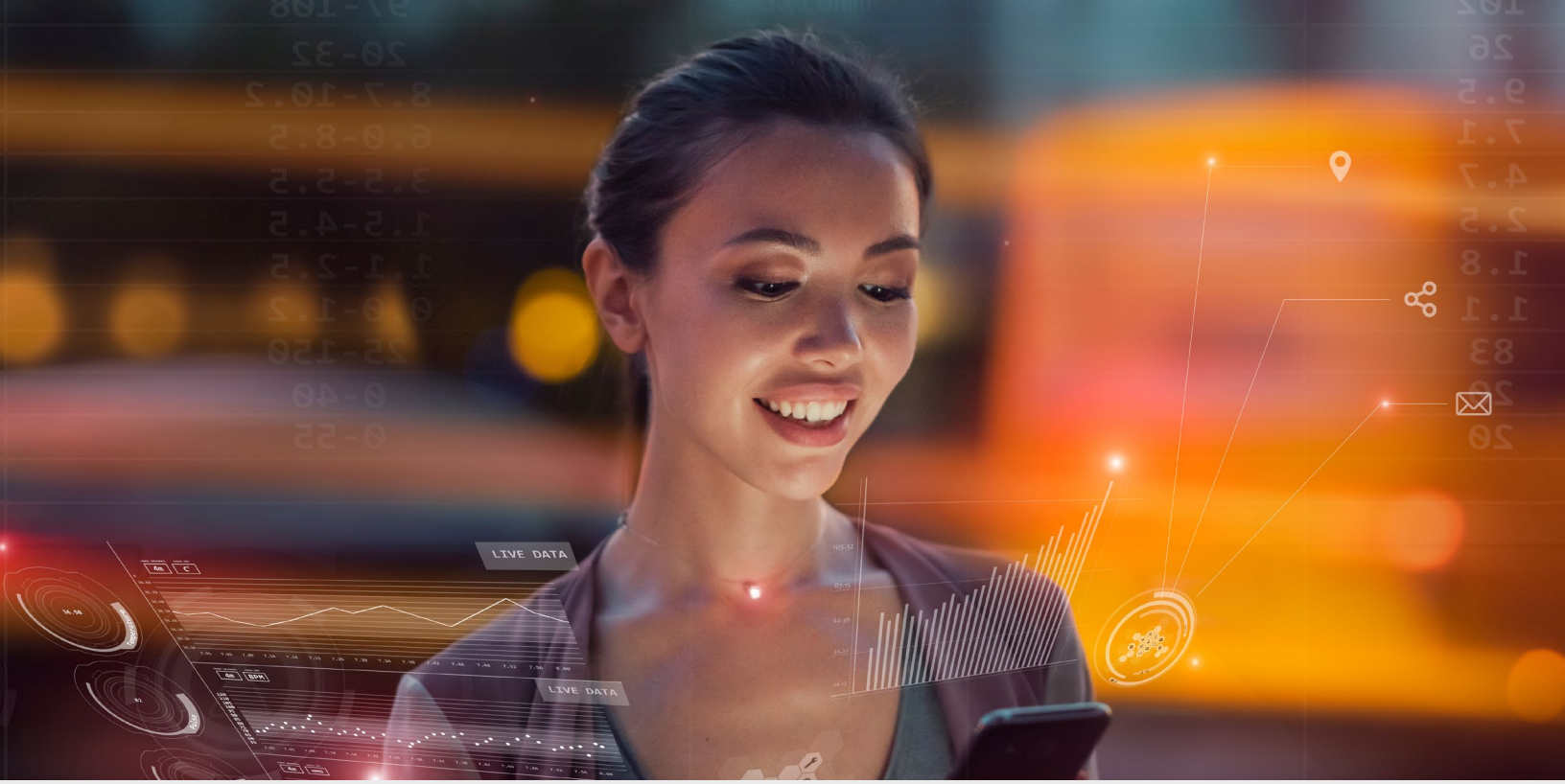
The final step in our Red Team's process always works on the assumption that we've managed to gain access to our client's systems. Whether we did or didn't is less important than what happens next, because it can mean the difference between a near miss, and a potential catastrophe.

It all comes down to one question: Is the client operating on the assumption that they can — and eventually will be — breached?

Properly segmented IT and OT systems are essential for slowing and ideally preventing a breach from spreading to other high value systems. Keeping critical systems independent from one another helps to minimize the potential damage of any given cyber incident. It also buys critical hours to recognize the breach and action an incident response plan to contain the attack and ultimately recover the systems.

For example, if a team member inadvertently installed a ransomware program on a local business network, that same software should not be able to replicate into a nearby control room. If an attacker manages to access a single transformer station, they should not be able to also access every other transformer station on the grid. If one database becomes compromised, it should not provide a pipeline to every sensitive database across the organization.





It’s always better to know

Like nearly every organization we work with, our specialists were able to spot and leverage several gaps that eventually helped us succeed in our breach. However, thanks in large part to the client’s significant recent investments, we were severely limited in what we could access and the amount of damage we could theoretically cause. Most importantly, the client was able to action our feedback to immediately patch the vulnerabilities we opportunistically capitalized on.

Consider how much data your organization collects, processes, shares, and stores on your network every day, in a week, in a year. Six months is a long time for a cyber incident to go undetected. Not to mention potentially hundreds of thousands of dollars in fines, and many years of regulatory hurdles to overcome thereafter.

Thankfully for our client, we were able to complete our Red Team exercise, issue a comprehensive report on our findings, and offer a wide range of action items in a similar timeframe. And with none of the legal or reputational damage — showing it’s always cheaper and easier to test your vulnerabilities and find out where you stand now.

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.

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

PRAXITY™
Empowering Business Globally