Deloitte.

Deloitte 2015 Cybersecurity Survey:

Navigating a harsh cybersecurity landscape

Faced with evolving threats, many Canadian organizations are slow to adapt

Table of contents

Deloitte 2015 Cybersecurity Survey:

Navigating a harsh cybersecurity landscape

Avoiding a cyber attack is an impossible task these days. Cyber adversaries —whether motivated by economic or political gain—are determined and they’re highly sophisticated in their abilities. It’s no longer a question of *if* your business will be attacked. It’s a question of *when* and *what* will be the impact.

And, for some businesses, undetected attacks are already underway—carried out by savvy cyber adversaries who slither their way through vulnerabilities and weaknesses in IT systems, people, and processes and then remain undetected for months as they comb through critical data assets.

Deloitte Canada’s 2015 Cybersecurity Survey, which polled IT leaders at more than 100 major Canadian organizations across all major sectors, reveals that many Canadian businesses today have wrapped themselves in a false sense of security, leaving the door open even wider for would-be attackers. A majority of survey respondents (60 percent) said they had not experienced a cyber attack in the last 24 months—and most of that group (90 percent) reported that they felt protected against cyber attacks. In other words, those who had not reported being attacked generally felt protected—a potential set-up for developing a false sense of security.

But complacency is no longer an option. And simply reacting to threats is no longer sufficient. Organizations must get ahead of threats. They must become proactive and work diligently to mature their cybersecurity program.

The reality is that Canadian businesses, on the whole, are less mature when it comes to cybersecurity—registering at about 2.2 on a 5-point maturity scale in which Level 5 represents “optimized.” (It’s only slightly better in the U.S.—with U.S. readiness closer to a Level 3.) And businesses might actually be less mature than they realize—since survey maturity ratings are based on respondents’ self-reported data and their own understanding of what constitutes effective cyber procedures.

Although this sounds daunting, Deloitte does believe that with additional focus, investment, and increased maturity, not all breaches need to be the size or have the impact that we have recently seen reported. To improve their cybersecurity posture, Canadian businesses will need to get smarter in how they think about cybersecurity and take a holistic approach to ensure their systems are:

- **Secure**—the ability and effectiveness of security controls to protect critical data assets
- **Vigilant**—the ability to detect and where possible prevent cyber threats by having a clear view, understanding and monitoring for potential cyber threats that are specific to organization or industry
- **Resilient**—the ability to respond and recover quickly and unharmed from cyber threats

Untouched?

60%

of businesses said they had not experienced a cyber attack in the last 24 months and of that group 90% reported feeling protected against cyber attacks.

Unprotected?

Of the organizations that had been attacked in the past 24 months, only

55%

said they felt protected.

What it means to be secure, vigilant, and resilient

Secure

Secure businesses have strong "walls." They have in place a security-aware culture, effective procedures and technologies that are oriented toward keeping attackers from getting a toehold in their organizations. The concept of "secure" encompasses access management; data loss prevention; patch management; training and awareness; defined roles and responsibilities; and third-party management.

Vigilant

Vigilant businesses are those that place resources (people, technologies, and partners) high up in the "watchtower" to monitor the threat landscape—while also actively monitoring their perimeters and their internal organizations for potential breaches. Vigilance involves security event monitoring; advanced threat management; advanced malware detection; cyber profiling; intelligence collaboration and external threat intelligence; and security analytics.

Resilient

Resilient businesses are those that can do more than repel a variety of attacks from a variety of directions. They can recover effectively from those attacks and learn from them to become more resilient organizations. Resilience covers areas such as incident response, cyber attack preparation, and cyber risk management, as well as activities such as DDoS (distributed denial of service) response.

Maturity matters

When it comes to being secure, vigilant, and resilient, businesses surveyed are doing better in some areas than in others.

In the past, organizations focused much of their resources on becoming more "secure," not quite understanding the importance of also being "vigilant" and "resilient." For activities encompassing the realm of "secure," businesses had an average maturity score of 2.4—compared with a score of 2.2 in the realm of "vigilance," and a score of 2.0 in the area of "resilience."

Not surprisingly those organizations that also scored higher in "vigilant" and "resilient" had higher overall cybersecurity maturity. The survey revealed that there is a correlation between highly vigilant and highly resilient organizations and their overall maturity rating. The average maturity rating for organizations deemed "highly secure" was 2.9, and the average for "highly vigilant" organizations was 3.05. The average maturity rating for businesses considered "highly resilient," however, was 3.14.

So, how many of the 100-plus organizations surveyed are "highly secure," "highly vigilant," or "highly resilient"? Here's a snapshot:

- Highly **secure**: 36 percent
- Highly **vigilant**: 35 percent
- Highly **resilient**: 22 percent

Only nine organizations of 103 surveyed are highly secure, highly vigilant, and highly resilient.

Secure:

Just how protected are you, really?

Secure:
Just how protected are you, really?

Understanding the nature and anatomy of threats can prove increasingly difficult as attackers develop and fine-tune new strategies and tactics. And there's no shortage of imagination.

Only about **1/2** of businesses are **using MSSPs.**

More than 90% of MSSP-using organizations are monitoring publicly available information—monitoring their brand and policing information about their products, their IT, their procedures, and their people.

For example, to get to a target company, hackers have become highly adept at discovering ways to gain unauthorized access to IT systems of contractors or trusted partners—and then work their way into the networks of the target company. They also have excelled at collecting and leveraging personal data—using it both as a blackmail tool for gaining deeper access to systems as well as a "phishing" tool to deceive individuals and lure them into inadvertently providing hackers access to control their credentials.

The good news for Canada is that most organizations have a patch-management system in place. But only 30 percent report they have a fully integrated business-aligned patch-management capability. And while one-third of Canadian businesses have documented patch-management procedures, their activities don't prioritize patches based on business criticality. The bottom line: Many organizations still lack patch-management capabilities that can keep up with the fast pace of evolving threats.

One key element to effective patch management includes focusing on critical weaknesses as well as vulnerabilities that might not seem critical but that are known.

Organizations also should resist the urge to lean too heavily on regular patches from a single major software provider. Patch continuously, not just once per week.

Amid this landscape of hacker creativity, organizations increasingly "don't know what they don't know." They remain unaware of the many forms that threats can take. So they increasingly are turning to managed security service providers (MSSPs) that can offer a highly specialized "watcher in the tower" capability to help them broadly monitor the threat landscape, as well as to monitor and detect specific threats—to bolster their overall level of security. As a cost-effective alternative to handling all monitoring and response activities in-house, MSSPs play a critical role in providing round-the-clock security monitoring and proactive threat management for Canadian businesses.

Today, about half of the nation's leading organizations rely on the services of MSSPs—and they're seeing the value in it. Businesses using MSSPs report a greater sense of feeling protected against potential cyber threats—by about 18 percent—compared to organizations not using MSSPs.

MSSP customers also are more likely to have a defined cyber resiliency and recovery process—with 61 percent of MSSP customers having such plans, compared to only 52 percent across all organizations. They're also more apt to test the effectiveness of their procedures through cyber drills and simulations—with 52 percent of MSSP customers testing and simulating, compared to 41 percent across all organizations.

And they also take intelligence-gathering seriously. More than 90 percent of MSSP-using organizations are monitoring publicly available information—monitoring their brand and policing information about their products, their IT, their procedures, and their people. As a whole, only about 75 percent of Canadian organizations do such monitoring.

Working thoughtfully with an MSSP can help your organization develop a more proactive posture for detecting, preventing, and responding to cyber threats. A managed security services provider (MSSP) can provide 24/7 support to shoulder the cybersecurity burdens for your organization—from managing and interpreting security-related data to monitoring and responding to threats on a global scale. An effective MSSP serves as a partner that can offer more than monitoring, assume cybersecurity challenges on an outsourced basis, respond proactively to threats, and deliver an even greater level of protection.

Despite those advantages, 24 percent of organizations report seeing little to no value from managed security services. These organizations may be lacking a business and threat profile aligned management and engagement. Engagement is critical for an effective MSSP relationship. And an MSSP customer should not assume that an MSSP is doing everything according to the organization's vision. The key: ask questions, provide feedback, and require regular communications that represent more than a "news feed" on incidents.

Secure

Signs of strength

About one-third of businesses have a fully integrated business-aligned patch management capability for addressing weaknesses and vulnerabilities in operating systems and applications, and those organizations are 35 percent more likely to feel protected.

Across all organizations surveyed, the average maturity level for **patch management** was **3.0**.

Needs more work

But Canadian businesses could stand to do more work when it comes to shaping a security-aware culture by building employee awareness and developing internal know-how for cybersecurity. The average maturity level for **training and awareness** was **2.0**.

Vigilant: Know thy enemy

Vigilant:
Know thy enemy

Deloitte's 2015 Canadian Cybersecurity Survey shows that organizations are lagging when it comes to proactive threat management. Many of the organizations surveyed have fairly immature ability for monitoring and detecting cyber threats. Only 50 percent of organizations surveyed have a defined cyber resiliency and recovery process. And having such a process matters. Organizations with such a process are 33 percent more likely to feel protected, compared to organizations without a defined process.

About
75%
of companies say they monitor publicly available information.

But only
1/3
of organizations have a formal CTI process.

And less than
2%
perform global cross-site threat intelligence sharing.

Threats come in an abundance of forms—varying by industry, by geography, by type of target, by type of threat "actor," and by evolving threat vector. And they're evolving on a global scale daily, making it challenging to understand the risks and the realities—making it harder for you to better protect your organization as well as understand the degree to which you are actually protected. The good news is that a staggering amount of up-to-the-minute information about cyber threats is available and can be customized to your specific industry by select MSSPs. Yet many Canadian businesses consistently fail to tap into this information to understand what cyber threats exist, where their own weaknesses lie, and how their peer organizations are responding to threats.

This inability to develop strong cyber threat intelligence (CTI) capabilities continues to put businesses and their critical data assets at risk. Only a third of organizations have a formal process for gathering and sharing CTI. And only two organizations out of the 103 surveyed perform global cross-site threat intelligence sharing.

Organizations that do engage diligently in CTI activities—that have a formal process for gathering CTI—are 20 percent more likely to feel protected than those that do not. And CTI-focused organizations are 32 percent more likely to conduct infrastructure, network, and system-centric profiling.

They're also 16 percent more likely to engage in user-behaviour analysis and traffic-flow analysis. And they're 18 percent more likely to have real-time business-risk analytics and decision support. Why? Because intelligence needs to be integrated within security operations, monitoring technologies, analytics capabilities, and employee education programs.

To build CTI capabilities that can improve your overall security, you need to develop intelligence that is actionable—intelligence you can use to make informed decisions and actively bolster your security and threat-detection capabilities. Sharing intelligence with peer organizations within your industry or market also needs to be part of the picture. Greater CTI sharing can help businesses leverage attack techniques and procedures to provide relevant information and insights that can be used to configure security tools to better enhance cyber defence techniques.

Establishing a CTI-sharing community involves more than setting up a community. Collaborating with peers within a CTI community requires an ability to understand how to share intelligence safely and effectively, as well as how to preserve privacy. Done right, CTI and CTI-sharing capabilities take the form of an end-to-end function that steadily delivers actionable intelligence.

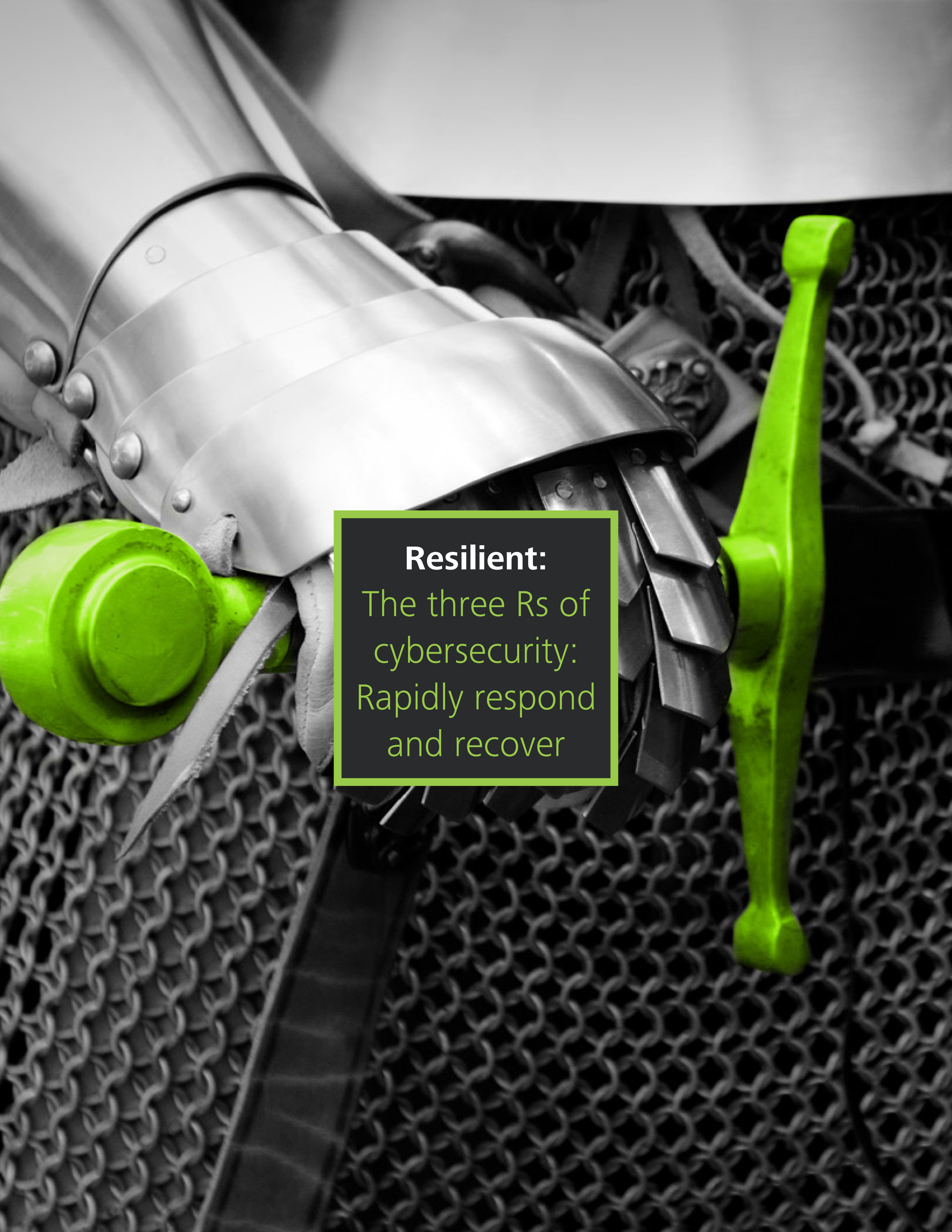
Vigilant

Signs of strength

Many Canadian businesses are taking security event monitoring seriously; 28 percent of organizations are logging, monitoring, and consuming threat intelligence. Across all organizations surveyed, the average maturity level for **security event monitoring** was **3.0**.

Needs more work

But Canadian businesses show a lack of maturity when it comes to activities around cyber intelligence. The average maturity level for **intelligence collaboration and gathering external threat intelligence** was **0.7**.



Resilient:

The three Rs of cybersecurity: Rapidly respond and recover

Resilient:
The three Rs of cybersecurity: Rapidly respond and recover

Canadian businesses remain largely in reactive mode when it comes to responding to cyber incidents, managing those incidents, and maintaining an ongoing compromise assessment capability for understanding the full extent and nature of threats—especially advanced persistent threats.

Compounding the challenge: the tendency of some organizations to focus only on technology when it comes to incident response and to overlook the people factor. Businesses need to keep in mind the impact an incident has on its people—the very people whose work, privacy, and morale suffer when there's a breach. Through regular tabletop and simulation training on cyber incident response, employers can prepare their staff for the issues that will arise during a cyber breach, helping to reduce the stress and the impact a cyber breach can have on both employees and external partners.

The path to improved incident response capabilities starts with process. The good news is that when it comes to incident management, most organizations (71 percent) have a documented *general* security incident response process, while 62 percent of organizations have *defined* incident response procedures. But only half have an idea of how effectively their procedures are; only 50 percent have documented incident procedures that are followed and tested.

But testing alone doesn't tell the whole story. Only 17 percent of Canadian businesses are including simulation and preparation drills in their testing—which is key to helping determine how effective your capabilities actually are. Tabletop and simulation exercises go hand in hand with a more comprehensive preparedness plan. The organization that prepares with drills and simulations is almost 45 percent more likely to have a defined resiliency and recovery process, and almost 30 percent more likely to conduct real-time business risk analytics, according to the survey.

Only **50%**

of businesses have documented incident procedures that are followed and tested.

Resilient

Signs of strength

When it comes to employing a basket of capabilities and resources to manage cyber risk, businesses are doing fair. Across all organizations surveyed, the average maturity level for **cyber risk management** was **2.5**.

Needs more work

Most organizations have only a basic level of DDoS mitigation capabilities. And only a small percentage of those organizations (8 percent) have undergone periodic testing of current solutions. For businesses surveyed, the average maturity level for **DDoS** was **1.2**.

At the heart of the need to address incidents in a resilient fashion is the need to think in terms of "incident response lifecycle." For most organizations, the ability to bounce back from a single attack belies the potential for ongoing, sophisticated threats. Advanced persistent threats (APTs) are one example. These threats aren't quick-hit attacks and data grabs. They start with an infiltration of your systems and then build as the cyber attacker gathers intelligence, digs deeper into your networks, covers its tracks, and then waits to exploit future vulnerabilities.

Combatting APTs and building incident response and management capabilities that are focused on threat lifecycles often begins with a deep compromise assessment—to determine proactively how your organization is being compromised. Such regular assessments can help you protect your critical systems and data from ongoing exposure, address threats before they become public news, understand your core cyber weaknesses, and build a case of support for improving your cyber defences. Yet only 43 percent of companies are performing only *periodic* vulnerability assessments.

43%

are performing only
***periodic* vulnerability assessments.**

Developing a cybersecurity posture that helps you become more resilient depends on thinking ahead of threats—on being proactive. Weathering advanced threats and enduring attacks with long, complex lifecycles requires a deep level of assessment and planning on the front end, not just strong reactionary capabilities on the back end of an attack.

Future realities

Deloitte Canada’s 2015 Cybersecurity Survey reveals that an overwhelming majority of respondents have opportunities to improve their overall cybersecurity posture by strengthening their ability to be more “vigilant” and “resilient.”

At the same time, a majority consider themselves prepared for a cyber incident—despite not having put in place the necessary procedures to operate as a secure, resilient, vigilant organization, and despite not having experienced a recent attack that would truly test their level of preparedness.

While many might consider their organizations to be protected, the reality is that Canadian organizations have *started* taking more secure measures with respect to cybersecurity but have been slow to adapt vigilant and resilient processes. Organizations that fail to proactively monitor for threats, inappropriate access and behaviour, and that are not aggressively gathering intelligence on threats, are less vigilant. If they fail to leverage the latest tools, processes, and skills for proactively responding to emerging threats, they should expect to face mounting challenges in managing their IT infrastructure and in achieving their business goals. And, as the competitive landscape continues to change, businesses that fail to develop a stronger cybersecurity posture may experience fresh challenges as they struggle to keep up with peers within their industry.

Improving your cybersecurity posture and becoming a more proactive organization requires more than awareness. It requires an ability to ask the right questions—and an ability to answer them. And it requires an ability to transform your business processes, to select the right technology solutions coupled with effective procedures and skills, and to weave it all together effectively and strategically—to evolve, just as the threats are evolving.

For more information on Deloitte’s insights into the evolving cyber threat landscape—and to learn how our global network of technology and business practitioners can help you build a proactive cyber strategy for the future—please contact us. Our deep experience across all sectors, our history of effective cybersecurity implementations, and our suite of tested preconfigured solutions and services enable us to provide the solutions your organization will need as you work to get ahead of cyber threats.

Discover more insights

To learn about what it takes to become a more secure, vigilant, resilient organization, read Deloitte’s Five essential steps to improve cybersecurity, at **www.deloitte.ca/5stepstocybersecurity**.

Explore **www.deloitte.ca/cyber** to find additional insights that can help you navigate the challenges of cybersecurity amid the landscape of emerging technologies.

Contact info

National

Nick Galletto

Partner
Cyber Risk Leader
ngalletto@deloitte.ca

Mark Fernandes

Partner
Cybersecurity Leader
mfernandes@deloitte.ca

Contributors

Dina Kamal

Partner
Cyber Risk Services
dkamal@deloitte.ca

Philip Fodchuk

Partner
Cyber Risk Services
pfodchuk@deloitte.ca

Rocco Galletto

Partner
Cyber Risk Services
rgalletto@deloitte.ca

Amir Belkhelladi

Partner
Cyber Risk Services
abelkhelladi@deloitte.ca

Robert Masse

Partner
Cyber Risk Services
rmasse@deloitte.ca

Cyber Intelligence Centre

www.deloitte.ca/cyber

Deloitte, one of Canada’s leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

The information contained herein is not intended to substitute for competent professional advice.