Deloitte.

Building an informed community

New cyber threat landscape makes sharing intelligence imperative

The complexity of cyber threats has evolved rapidly in recent years – with highly specialized criminal, political, and government networks overtaking random small-scale hackers and criminals as the foremost threat to organizations.

These specialized networks represent an elaborate mix of cyber threats that can target specific organizations, regions, and customer profiles through a sophisticated set of malware exploits and anonymization systems.

Organizational leaders increasingly understand that the new cyber reality means more new and sophisticated threats - and as threats continue to increase, cyber criminals' capabilities will grow as well. Leaders also understand that combatting the new threats will depend on more than tweaking security policies and executing technical fixes.

To meet new enemies on the cyber battlefield, organizations will need new intelligence. They'll need strong cyber threat intelligence (CTI) capabilities as well as the ability to share information to ensure that intelligence about cyber threats gets to the right people and the right systems for proactive decision making. The challenge is one that will require broad vision, executive guidance, and an ability to create new models of cooperation within and across industries.

Cyber criminals know the importance of intelligence. They actively profile organizations to help them develop highly customized malware code and attack techniques for exploiting specific security weaknesses. On top of gathering intelligence, they're sharing it, helping one another to exploit organizations' vulnerabilities.

For Canadian businesses, the result is a league of cyber adversaries that is persistent, motivated and agile – sharing and employing a variety of tactics, techniques and procedures (TTPs) that can compromise systems, disrupt services, perpetrate financial fraud, expose sensitive information, and steal intellectual property.

Organizations could benefit by taking a page from the playbook of modern cyber criminals. If cyber attackers can devote resources to leveraging intelligence from their community as a way to advance their efforts, what's stopping industry from doing the same thing?

What is Cyber Threat Intelligence (CTI)?

CTI is an organizational capability, not a data set. It is an intelligence-led approach to manage cyber risk and build cyber resilience. It requires continuous awareness of relevant, current and emerging threats to your organization where you can proactively identify and mitigate incoming attacks.

The value to organizations

While cyber attackers have long shared security-related information for their mutual advantage, business organizations have been slow to cooperate among themselves. Only recently have business leaders begun to fully recognize the need to engage in CTI sharing as a way to help combat cyber threats.

And the need is great, with cyber crime activity continuing to increase. According to a joint McAfee-Center for Strategic & International Studies report released in June 2014, the cost of cybercrime in Canada is estimated at 0.17% of the country's gross domestic product[1], and according to Ponemon Institute, the cost of cybercrime is $7.6 million on average per company in 2014, a 10.4 percent net change from previous year's study[2].

The growth in cyber-attacks has fueled discussion of information sharing across all sectors and industries. Many organizations, however, have not moved past the discussion stage. A majority of business leaders polled say they are willing to share cyber information and would do so voluntarily. Nonetheless, more than 40 percent aren't sharing any information at all, citing legal reasons or business concerns as the main factors.

But the case for CTI sharing is growing clearer and being proclaimed loudly, with key organizations such as the U.S. National Institute of Standards and Technology (NIST) asserting that "to enhance incident response actions and bolster cyber defences, organizations must harness the collective wisdom of peer organizations through information sharing and coordinated incident response"[3].

Moving forward on CTI sharing remains a challenge for organizations. And to overcome their persistent reluctance to share information, businesses need to better understand exactly how they can share intelligence safely and effectively, how they can preserve privacy, and how they can realize significant overall benefits from sharing.

One path forward begins with setting up information sharing communities – a move that can boost the ability to defeat advanced, persistent threats across individual organizations, industries, and geographies while heightening cyber resilience in the face of targeted attacks. Unlocking the value of CTI sharing requires an understanding of key prerequisites – to understand the features of an enabling technology platform/infrastructure and to understand what the lifecycle of a CTI sharing initiative should look like.

A recognized need

Recognizing the importance and need for a threat intelligence sharing community, Deloitte has been involved in the creation of the Canadian Cyber Threat Exchange (CCTX). Leveraging our global knowledge and expertise of threat intelligence and cross intelligence sharing, we have helped defined the requirements and elements of the CCTX and developed the governance model which explains how it will work and how organizations can benefit from participating in it.

Creating a CTI sharing community

The current threat landscape may serve as the vital motivator to prompt organizations to collaborate on a robust CTI sharing community within Canada. But before such a community can become operative, the Canadian business community must address certain considerations from the outset. The following is a list of actions that includes leading practices for developing an effective CTI sharing community:

Develop community oversight and governance structures

Clearly established structures can help drive the community's vision and provide a level of assurance that procedures exist for addressing concerns. An intelligence-sharing community requires a strong oversight board and clear rules for seating that board. Beyond a board, the community will need a code of conduct as well as procedures and penalties for handling disputes or breaches of membership. Strong oversight means members can trust that their rights and obligations are clearly governed and that security measures are in place to prevent sharing or leaking of unauthorized data.

Implement community membership criteria

A defined process and criteria can help ensure that new members are evaluated on their willingness to share intelligence, on best practices, on know-how, and on experience. A strong CTI community should also include a specific "member intelligence" onboarding process where analysts can obtain key and relevant information from the member's organization. It will also allow the member to receive customized reports on threats to specific assets.

Make cross-sector sharing a priority

Cyber attackers are not always industry-specific when seeking out new targets. While it is of great value for CTI communities to rely on industry-specific intelligence such as the Financial Services - Information Sharing and Analysis Centre (FS-IFAC), it is equally important to have cross-sector sharing as part of the community's plan with appropriate controls and agreements in place.

Leverage cybersecurity expertise

Gathering and analyzing community intelligence requires subject-matter experts who can produce reports and identify trends. A CTI sharing community also requires specialized day-to-day operational personnel to assist with program management and administration.

Support open discussions on threat intelligence

Periodic open group discussions can help community members share best practices, insights, and perspectives in an engaging and meaningful way, while also helping to build trust within the group.

Comply with regulatory, privacy and legal obligations

Complying with regulatory, privacy and legal requirements for information sharing remains a key concern. This enables an organization to define, publish, and disseminate any potential civil/criminal responsibilities so all members understand their obligations.

However, understanding the regulatory landscape provides only the baseline. If customer information is being collected, used or disclosed, take measures to ensure the appropriate privacy controls are embedded into the technology design and privacy infrastructure. Depending on the type and quantity of information disclosed or compromised, potential liability issues could ensue given the rise in class action law suits in Canada.

A competitive advantage is to take a proactive risk management approach to privacy. Adopt a "Privacy by Design" mindset to ensure that information practices and privacy standards are not only compliant with regulatory requirements, but adhere to privacy best practices. Deloitte offers a Privacy by Design certification program[4] to demonstrate that processes, solutions and programs meet privacy best practices, minimizing the risk of compromise and reputational harm.

Develop a community funding framework

Acquiring the right technologies, platforms, and resources to generate actionable intelligence requires funding commitments from members. Explore cost-sharing methodologies to determine what is right for the community.

For example, tiered membership fees rather than fixed contributions might work well for some communities. Funding amounts should cover not only operational and technology costs, but developmental and research costs as well.

Initiate government relationships

Private-sector communities should immediately begin developing reciprocal relationships with government bodies – to provide and to be provided with security breach notifications that can help organizations prevent, detect, and respond to threats.

What to share?

There's a wealth of information that organizations can share as they seek to collaborate among themselves to combat and prevent cyber attacks. Shared information can include:

- Intelligence on potential targets and attackers
- Vectors an attacker is known to use
- Methods and impacts of a successful attack
- Lessons learned and defence guidelines

The key success metrics of creating a successful CTI sharing community include:

1. Having a central and secure ability to **share information,**
2. Established **trust** across a unique blend of public and private, cross-sector community members,
3. **Member sharing of best practices, concerns and discussion items,** and
4. **Documented outcomes** usable to create internal awareness on CTI.

The power of sharing

A community in which organizations can share real-time intelligence on constantly evolving threats can deliver broad benefits, including:

- Access to relevant, actionable intelligence
- Enhanced threat understanding
- Cost savings through elimination of duplicated effort
- Increased efficiencies in risk assessments
- Implementation of sharing models without new legislation
- Identification of trends and indicators of compromise
- Prioritization of threats and vulnerabilities by importance and imminence
- Improved security through shared best practices
- Development of shared situational threat awareness
- Correlation of seemingly unrelated indicators
- Better defensive agility with shift from reactive to proactive strategies
- Improved, more timely decision making via shared, real-time information
- More rapid customer notification of potentially impactful incidents

Developing a CTI sharing platform

The next step beyond the basic components of a CTI sharing community involves putting in place an appropriate technology platform. The effort will include systems, tools, and controls for sharing threat knowledge in a timely manner while protecting organization-specific corporate knowledge.

As with building the overall CTI community, there are essential actions and best practices involved in developing an effective CTI sharing platform:

Create an intelligence sharing taxonomy

An explicit taxonomy will help ensure that all participants use and understand a common language and terminology. The taxonomy should include trusted intelligence classification standards, such as the Traffic Light Protocol (TLP). Communities also should set boundaries to define which members and which sectors can access which levels of information. Confidence-level ratings also should be developed and included in reports for members – to let them know how trusted specific intelligence sources are.

Operationalize the platform

If a community decides to create its own intelligence sharing platform, it will have to develop both applications and infrastructure. Such an approach requires developing a robust broadly functional application interface, as well as acquiring and implementing infrastructure components that will ensure constant availability.

Instead of creating its own platform, a community might opt to save time and resources by leveraging partnerships with CTI experts and using existing technologies. Such an approach might include, for example, implementing a MISP (malware information sharing platform) – an open-source platform for sharing, storing, and correlating "indicators of compromises" targeted attacks – or a Soltra Edge, an industry-driven threat intelligence sharing platform.

Ensure anonymization capabilities

Any platform should allow members to share intelligence either openly or anonymously. To support anonymization, the community should create an accepted definition and develop the necessary controls. All members should know what aspects of the sharing process are or can be anonymized without risk of misinterpretation.

Control the volume of shared information

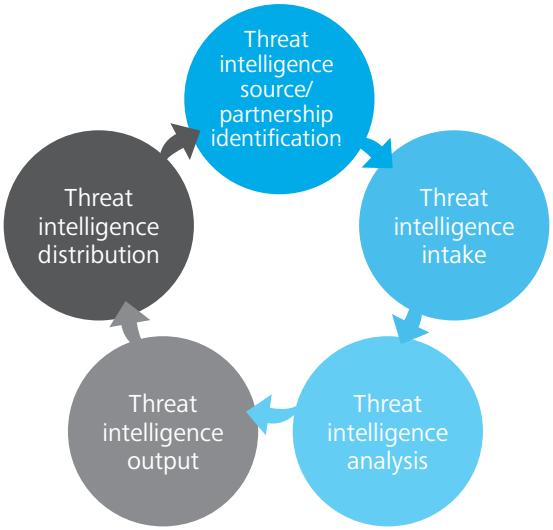
Developing clear intelligence triaging and analysis process can help ensure that the most critical information is shared first, while limiting the amount shared. Too much information can consume valuable resources, meaning critical items might not be addressed rapidly enough.

Create actionable intelligence

Intelligence sharing holds limit value if reports and discussions fail to outline potential actions that members should take to proactively secure their operations against identified threats or vulnerabilities.

The CTI sharing life cycle

Once the requisite platform is in place, the ongoing cyber threat sharing process can begin. In its most effective form, the process is an end-to-end endeavour that involves acquiring, assessing, disseminating, and applying knowledge about cyber adversaries, with the goal of producing "actionable intelligence." The vision is to maximize value for individual organizations as well as for the community at large.



Protective power

A CTI sharing community with a cross-sector focus and access to real-time intelligence holds the potential to help organizations respond more effectively to threats and to better protect their assets.

Establishing such a community and making it operational requires a multiphased approach – with the first true step being a group of committed, forward-thinking leaders coming together and establishing a guiding structure. Once leaders have set core requirements and expectations, they can begin crafting a pilot program and set in motion a truly cutting-edge cybersecurity strategy.

Ultimately, embracing established best practices for CTI sharing can provide a strong baseline for organizations looking to establish not only a CTI sharing community but a community that serves as an active, effective, sustainable mechanism for collective cyber threat protection.

The first true step is a group of committed, forward-thinking leaders coming together and establishing a guiding structure.

Sharing what we know

Deloitte has experience helping organizations address cyber threats through a variety of tools, processes, and tactics – including CTI sharing initiatives. We're happy to share what we know. To learn more about our approach to CTI and to discuss steps for building a CTI sharing community, please contact us.

Dina Kamal

National lead, Cyber intelligence
and Analytics services
dkamal@deloitte.ca
+1 416-775-7414

[1] McAfee and Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime.* Date accessed: August 20, 2015. http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf

[2] Ponemon Institute. *2014 Global Report on the Cost of Cyber Crime.* Date accessed: May 31, 2015. http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime

[3] National Institute of Standards and Technology. *Guide to Cyber Threat Information Sharing* (Draft). Date accessed: July 9, 2015. http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf

[4] Deloitte LLP, & Ryerson University, & Cavoukian, Dr. Ann., & Kingsmill, S. (2014). *Privacy by Design - Setting a new standard for privacy certification.*

www.deloitte.ca

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.

Designed and produced by the Deloitte Design Studio, Canada. 15-3128H