Case Studies

In Data We Trust

Unlocking the Value of Data in Ontario

Claudia Dessanti
Senior Policy Analyst, Ontario Chamber of Commerce

CASE STUDY: TD FUSION CENTRE

Financial service providers are faced with rapidly changing cybersecurity environments, geopolitical complexities, and an expanding attack surface as banking becomes increasingly digital. TD Bank Group (TD) responded to these challenges by taking a multi-disciplinary, data-driven approach to protect the data and financial assets of its customers, stakeholders, and the broader economy.

In September 2019, TD launched its Fusion Centre in downtown Toronto, an 8,000 square foot state-of-the-art operational hub that incorporates a best-in-class, multidisciplinary approach to risk management. The hub is focused on improving prediction and prevention of enterprise threats, detecting new threats, and enabling incident response driven by a shared view of TD's threat landscape.

The Fusion Centre relies on cross-functional teams to avoid the siloed nature of threat management that often exists within large organizations. The Centre's "teams of teams" approach integrates different groups from across the Bank, representing cyber operations, incident response, cyber intelligence, information protection services, global security and investigations, fraud management, anti-money-laundering, legal, communications and compliance. Each team brings unique expertise and perspectives to facilitate "shared consciousness" and a culture of collaboration across the organization.

Multi-disciplinary cooperation leads to more effective threat intelligence and faster response times. It allows TD to keep pace with nimble cybercriminals who learn to adjust their tactics and techniques faster than businesses can hire and train employees to respond.

In June 2020, TD will open its Singapore Fusion Centre, while continuing to expand teams and tools across multiple locations. Using a "follow-the-sun model," teams are currently situated in Toronto, New Jersey, Tel Aviv, and Singapore – allowing for continuous coverage across time zones. Ongoing investments in people, processes, and capabilities are informed by best-in-class industry standards such as NIST's Cybersecurity Framework.

TD's approach to threat management is also supported by data, aggregating thousands of disparate data sources through a centralized platform. Artificial intelligence and machine learning tools are coupled with a diversity of employee talents to help improve threat detection and more efficiently protect data and technology assets. TD is also part of a larger network in which cyber threat intelligence and best practices are shared among industry peers, global law enforcement, and government agencies to enhance collective capacity.

Finally, as we all respond to the global implications of COVID-19, TD via the Fusion Centre created a virtual war room to proactively monitor for potential frauds and phishing campaigns related to government relief programs in Canada and the United States. The virtual war room has also been instrumental in helping the bank to coordinate the successful transition of TD's employees from physical locations to working from home as they continue to provide vital banking services to its 25 million customers. By mid-March, TD had approximately 100,000 employees working remotely, up from fewer than 20,000 prior to the pandemic, reflecting the fastest technology pivot in TD's history.

As the threat and cyber landscape grows more complex, TD continues to strengthen its innovative approach to the everchanging environment.
The Fusion Centre is an important evolution in TD's ongoing efforts to deliver meaningful innovations that safeguard customers' privacy, security, and trust.

CASE STUDY: DATA FOR GOOD BY TELUS

TELUS has long recognized the value of using data to achieve social good. During the COVID-19 pandemic, the Canadian telecommunications and health care technology company put this commitment into action by launching a new initiative called Data for Good.[55]

The Data for Good program provides governments, health authorities, academic researchers, and other stakeholders with access to de-identified network mobility data and insights to help them respond more effectively to COVID-19. By giving stakeholders free access to its TELUS Insights service, TELUS is supporting a variety of efforts to stem the spread of the virus, lessen impacts on health and the economy, coordinate health care responses, and carry out research that could mitigate or prevent future phases of COVID-19 or future pandemics.

For example, data scientists can analyze network mobility data from TELUS in conjunction with case counts of COVID-19 in different regions to help governments develop public policy responses and decide where to allocate limited resources. Similarly, data showing the number of people visiting certain locations can help research and academic institutions assess the economic impacts of COVID-19.

Data for Good is a privacy-first program, reflecting TELUS' long-standing commitment to using data responsibly. The TELUS Trust Model, which centres around the core principles of accountability, ethical use, and transparency guides all data-driven practices across the business.[56] TELUS worked with privacy and technology experts to develop models that allow insights to be derived from network mobility data without compromising individuals' privacy. The result is that when data is shared with third parties, it is strongly de-identified and aggregated in accordance with leading industry standards to ensure privacy is fully protected at all times without compromising the utility of the data and the insights it provides.

With a robust data governance framework in place, TELUS was able to develop and launch Data for Good swiftly as the need for network mobility data became apparent earlier this year. The program is run by the TELUS Data & Trust Office and powered by TELUS Insights, a data analytics practice that has received Privacy by Design certification.[57] To further protect privacy, stakeholders are required to limit their use of the insights and datasets to the ethical purposes outlined on the TELUS website.[58]

TELUS remains committed to leveraging de-identified network mobility data for a variety of public purposes beyond COVID-19. The TELUS Insights service helps government agencies, non-profits, and other organizations make more informed and strategic decisions.[59] For communities, it contributes to emergency response, improved health outcomes, and better public services. For customers, this leads to best-in-class services, optimized reliability, and superior customer experiences. As opportunities to use data to improve the lives of Canadians increase, TELUS will continue to build trust with stakeholders by using data in a way that generates value, promotes respect, and delivers security.

[55] TELUS. "Data for Good: Leveraging TELUS data against COVID-19." *https://www.telus.com/en/about/covid-19-updates/privacy-statement.* Accessed June 1, 2020.

[56] TELUS. 2019. "The TELUS Trust Model." *https://www.telus.com/en/about/privacy/trust-model.*

[57] Professional Evaluation and Certification Board. "Certifications Granted." *https://pecb-ms.com/en/certifications-granted.* Accessed June 1, 2020.

[58] TELUS. "Data for Good: Leveraging TELUS data against COVID-19."

[59] TELUS. "TELUS Insights." *https://www.telus.com/en/on/business/medium-large/enterprise-solutions/big-data-analytics.* Accessed June 1, 2020.

CASE STUDY: CYBERSECURITY & THREAT MANAGEMENT AT SENECA

In January 2020, Seneca launched a new graduate certificate in Cybersecurity & Threat Management. This eight-month program responds to the high demand for skilled cybersecurity professionals in the IT and financial service sectors.

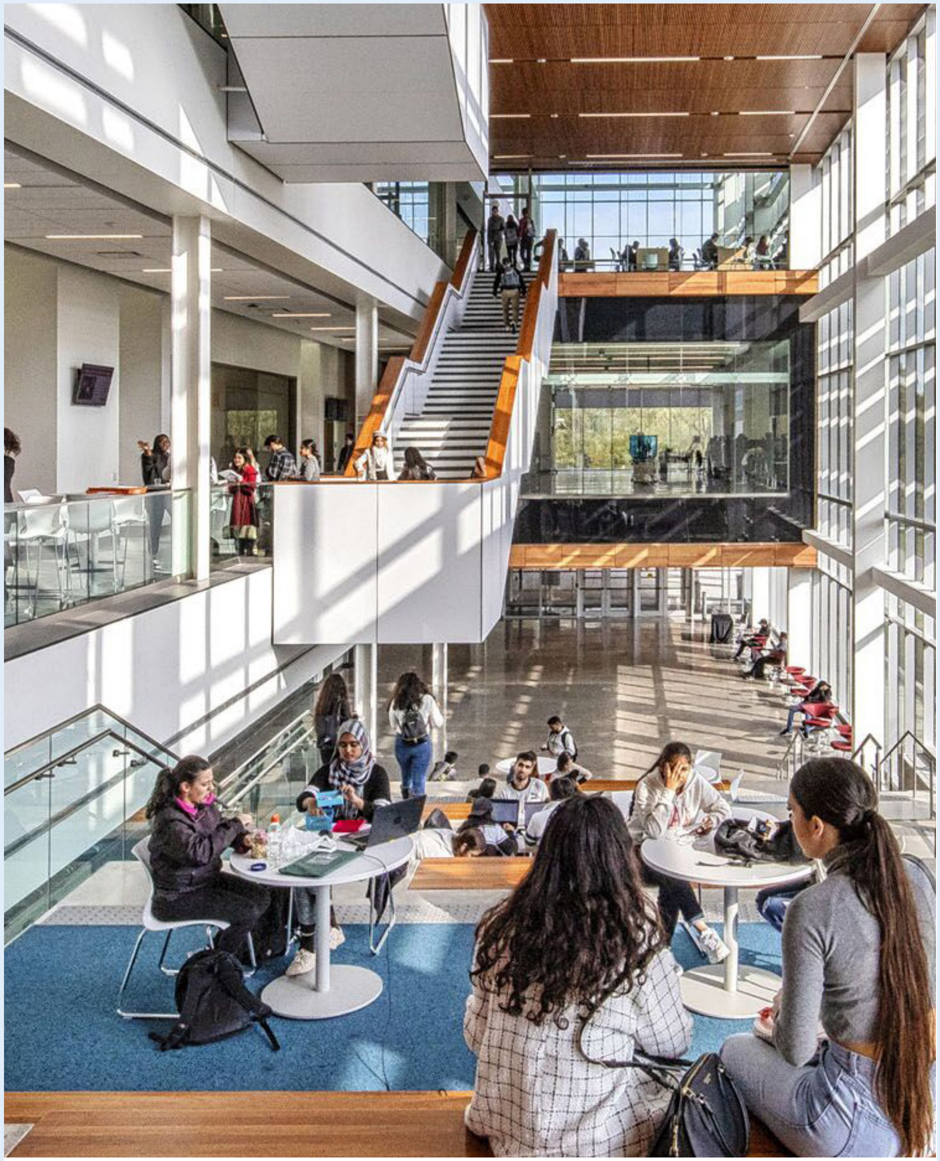
Designed to reflect the industry's cybersecurity needs, the new credential prepares graduates for successful careers in the field. The curriculum was developed in partnership with Toronto Finance International, a public-private partnership between financial institutions, government and academia. Courses are taught by industry professionals, further aligning the skills being taught with the needs of employers.

Most students enrolled in the Cybersecurity & Threat Management program are professionals looking to upskill or reskill. Courses are designed to build technical specialization as well as complementary skills in project management, communication, and data analysis. On site, students are able to practice their knowledge in applied activities in Seneca's new state-of-the-art cybersecurity labs. The program's industry capstone project and optional work term give students additional industry experience that employers often look for.

Graduates are equipped for careers as information security analysts, threat analysts, IT systems and network administrators, risk analysts and ethical hackers. Their skills will directly help address the complex and evolving challenges faced by banks, investment firms, insurance providers and more.

The inaugural intake for the program has been unprecedented with additional spots created to support the demand. Seneca accepts two cohorts per year, starting in January and September. Courses are primarily being offered at Seneca Downtown with the labs delivered at Seneca's Newnham Campus. A part-time option is also available. Courses are delivered in late afternoons, evenings and on Saturdays to accommodate students who are employed.

Through its many industry partnerships, Seneca will continue to adapt the program to reflect the changing cybersecurity needs of employers. This ongoing collaboration with businesses is critical, particularly in a field as rapidly changing, complex and consequential as cybersecurity.



Seneca

CASE STUDY: NERDS ON SITE

Founded in London, Ontario, Nerds On Site is an all-inclusive IT service provider with over 75,000 residential and business clients across North America. What follows is a real example of how Nerds On Site was able to thwart a cybersecurity attack on an international company, bring systems back online with minimal downtime, and secure the company's systems against future attack.

ATTACK

In January 2019, ACME Inc. (not the company's real name) received a ransomware email attachment (a phishing scheme) that launched a PowerShell script – a tool that falls under the radar of traditional endpoint security products. Over the next six months, the undetected threat continued to infect systems across the company's global locations.

ASSESSMENT AND RESPONSE

In July, after realizing they were under attack, ACME Inc. contacted Nerds On Site. The Incident Response Team quickly responded, assessed the situation, and found that ransomware had not yet been deployed. Isolation steps were then taken, prompting attackers to launch the ransomware encryptor, which the Incident Response Team immediately detected. The encryptor and ransom note (demanding $600,000, increasing by $120,000 per day) warned against shutdown and internet disconnection, but the team did just that, shutting down every device in the data centre and the internet connection itself. This allowed full preservation of at least one Active Directory domain controller.

Nerds On Site relied on its Three-Phase Incident Response Protocol:

- Phase One (Isolate): existing Cisco ASA gateways at site-to-site VPN infrastructure were removed and replaced with adam:ONE, a DNS-based firewall and gateway solution.

- Phase Two (Remediate): computers were set up to boot into safe mode, and Webroot was deployed to do a thorough scan. Global IT teams were given step-by-step instructions in their respective languages, communicated across a central dashboard. Once Webroot removed infections, the system was re-scanned to ensure a clean status.

- Phase Three (Fortify and Maintain): adam:ONE technology was used to reconfigure the systems using whitelisting. In contrast to blacklisting, this approach begins from a zero-trust standpoint and only allows users to access resources that have been determined to pose no threat (whitelisted).

RESULTS

Rapidity on the part of the Nerds On Site Incident Response Team stopped the attackers in their tracks. Systems were brought back online with only one shift of downtime and without paying the ransom. Importantly, the team deployed advanced technologies to ensure ACME Inc. is properly fortified against future attacks.

ontchamberofcommerce

@OntarioCofC

company/ontario-chamber-of-commerce

www.occ.ca

ontario
chamber of
commerce

Indispensable Partner of Business

© 2020. Ontario Chamber of Commerce. All rights reserved.