
UNIVERSITY OF TORONTO
Information Security
Information Security at U of T
SECURE TOGETHER
ANNUAL REPORT FISCAL YEAR 2024 – 2025

# TABLE *of contents*



# A MESSAGE

## *from the Chief Information Security Officer*

Over the past year, cyber security has dominated headlines, with stories ranging from major data breaches to evolving regulatory requirements. According to a report from IBM, Canadian organizations pay an average cost of $6.32 million per data breach. In 2024 alone, the Canadian Anti-Fraud Centre received 108,878 fraud reports, totaling over $638 million in losses. Additionally, AI-powered cyber attacks have enabled attackers to inflict more damage with fewer resources.

This challenging reality demands our continued focus on cyber security priorities. As individuals, we must recognize that our work carries profound implications for security. We must ensure that the data in our care is not only secure but also managed with integrity and ethical considerations. It's about doing what is right, not just what we think is possible.

There are challenges ahead, but I am reassured by the support of this amazing community. I am incredibly proud of what we have achieved together, and I am confident that, together, we can continue to secure our digital ecosystem and build trusted experiences for all.

**"I am confident that, together, we can continue to secure our digital ecosystem and build trusted experiences for all."**

Deyves Fonseca

**Deyves Fonseca**
Acting Chief Information Security Officer
University of Toronto

# OUR YEAR *in review*


## SPRING

- Institutional incident response plan is reviewed and refreshed
- The Digital Asset Classification Standard is released by the Office of the CISO with endorsement from the Information Security Council
- Cyber security-as-a-service program is initiated to provide support to single-department faculties

## SUMMER

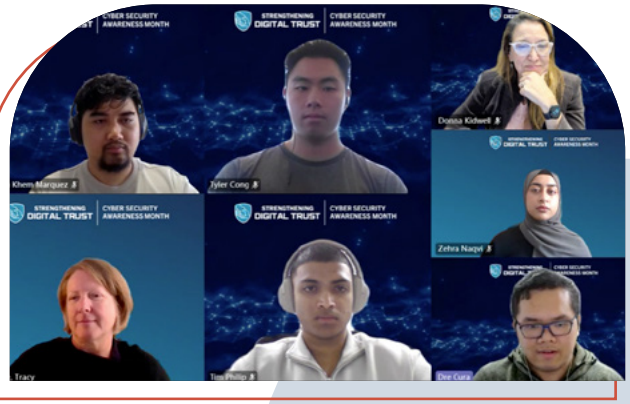
- Dr. Donna K. Kidwell joins U of T as the new Chief Information Security Officer
- Virtual platform to conduct tabletop exercises is released
- Institutional initiative to provide firewall management-as-a-service is kicked off
- General-purpose password manager is launched for faculty, librarians, staff and students

## FALL

- Student orientation programs feature information security booths to prepare students for a secure digital experience
- Call-to-action for divisions to address key security risks is released by the Office of the CISO
- University-wide attention on risk posed by end-of-life-systems is urged by the Information Security Council
- The role of Acting Chief Information Officer is taken on by Dr. Donna K. Kidwell
- The role of Acting CISO is taken on by Deyves Fonseca for the second time, after holding the role previously for five months in early 2024
- U of T celebrates Cyber Security Awareness Month
- Data Asset Inventory and Information Risk Self-Assessment (DAI-IRSA) 2024-25 is kicked off
- Next-generation anti-virus (endpoint protection) project is completed and transitioned into a sustained service
- Migration to the new Information Security website is completed
- The SailPoint Identity Governance and Administration project marks the start of U of T's identity modernization journey


## WINTER

- Data Privacy Day is celebrated at U of T with focus on data literacy
- Cyber security-as-a-service is renewed for another year
- Data Asset Inventory and Information Risk Self Assessment cycle closes with participation from 110 units
- Units learn how to build their incident response plans through in-person workshops
- A method for assessing and attesting to the security of U of T's IT systems is established by the trusted digital infrastructure framework




Time needed to reset compromised accounts reduced from

**ONE DAY TO 10 MINUTES**

**3,237**

data assets inventoried by

**127 UNITS**

**143 PER CENT** increase since last year

**4,500**

compromised device alerts detected and actioned

**47 PER CENT**

reduction in critical vulnerabilities open for longer than 30 days

# OUR CYBER SECURITY *maturity journey*

## Strategic objective #1:
*Securing digital transformation*

### Tri-campus teams expand protections for user devices and servers

Teams across U of T added next-generation anti-virus (endpoint protection) to 10,000 additional user devices and servers, bringing the total to over 20,000. Next-generation anti-virus safeguards systems against advanced security threats that traditional anti-virus solutions cannot detect. As a result of this and other security measures, over 4,500 compromised device alerts were detected and actioned.

### U of T takes a bold step towards establishing firewall management as an institutional service

The institutional Information Security team worked with U of T units and divisions to establish firewall management-as-a-service and replace outdated firewalls with those offering advanced capabilities. So far, 40 units have transitioned to this new service model, which offers scalability and cost savings while maintaining expert-driven protection against security threats. Participating units receive greater support in managing their firewalls. Additionally, the service provides baseline security protections and a secure method for addressing unit-specific needs, ensuring firewall configurations align with U of T's security policies.

# Driving digital transformation:
## *An OISE story*

**The digital transformation at the Ontario Institute for Studies in Education (OISE) is not just about technology; it's about people. It's about advancing scholarship, enhancing pedagogical practices and supporting research excellence through innovative technology and strategic partnerships. At its heart, this transformation prioritizes the human aspect of digital change, ensuring that technological advancements are inclusive, equitable and accessible, and actively bridge the digital divide in academia.**

What has made this possible is the dedication and foresight of OISE's Education Commons team and their commitment to service excellence, collaboration and continuous learning.

Over the past three years, Education Commons has successfully migrated all systems and applications to U of T's cloud environment. This shift has improved scalability, significantly reduced OISE's digital footprint and strengthened cyber security. Additionally, it has freed up resources to focus on collaborating with faculty and researchers, understanding their needs and co-creating solutions.

Further, Education Commons' adoption of real-time secure data feeds has not only improved data security but also unlocked new possibilities that weren't available before. One notable example is the doctoral tracker, which provides up-to-date information and supports students throughout their academic journey.

In collaboration with the institutional Information Security team, Education Commons has enhanced cyber security through network segmentation, endpoint protection and the adoption of secure practices such as role-based access and segregation of duty. Additionally, by partnering with the University's Information Technology Services team, Education Commons has eliminated redundancies and streamlined operations, achieving economies of scale and allowing greater focus on divisional priorities.

***"Through the strategic integration of secure and sustainable digital solutions, OISE has cultivated a data-driven academic ecosystem that advances world-class research, teaching and learning. By prioritizing technological security and innovation, OISE strengthens its mission as a globally recognized faculty of education and a cornerstone in the evolution of higher education."***

-Julia Duncan, Director, Education Commons, OISE

# Strategic objective #2:
## *Enabling safe and trustworthy teaching, learning and research*

### Training platform brings cyber security best practices to the community

Teams across U of T worked together to expand security awareness training to over 14,000 staff and faculty. To date, over 7,000 individuals have completed learning modules. Monthly simulated phishing exercises reach over 7,000 staff and faculty, training them to recognize and appropriately respond to malicious emails.

### Password managers reduce risk of account compromise

The institutional rollout of the 1Password general-purpose password manager provided individuals with an effective way to securely store their digital credentials and protect their accounts against compromise. So far, 30 units and three research labs have been onboarded, safeguarding accounts belonging to over 1,500 staff and faculty, and 650 students.

### New framework to assess U of T's digital infrastructure enables research

Recent years have seen an increase in cyber security requirements from institutions and government agencies sponsoring research. This has created an urgent need to identify and establish trusted digital infrastructure at the University, leading to the creation of the Trusted Digital Infrastructure Framework. This framework provides a consistent method to assess and attest to the security and trustworthiness of U of T's digital infrastructure. SciNet is already using this framework to secure SciNet4Health infrastructure, as are U of T Libraries as they move to further secure their research data portal. Initially designed to help researchers comply with sponsor requirements, this framework has applications across all University systems to identify security gaps and work towards building more trusted digital experiences.

# Bridging the gap between policy and process:
## *A UTSC story*

**Often, policies fail not due to their inherent flaws, but because of poor implementation. The University of Toronto Scarborough's (UTSC) response to the updated guidance on protecting social insurance numbers (SINs) is a great example of how to successfully implement a policy.**

In early 2024, the Information Security Council officially designated SINs as level 4 data and issued updated protection guidelines. Processes for handling SINs had shifted during the pandemic and in some cases did not fully align with the new guidelines. Responding to the situation at hand, UTSC's Information and Instructional Technology Services (IITS) team initiated a campus-wide effort to help departments meet the new security requirements.

The first step was to build a secure platform for collecting and storing SINs. But that was not enough. Teams across the campus needed training and support to adopt the new platform and evolve their business processes. This is when the journey of organizational change, involving multiple human resources teams, payroll departments and business officers, started. This was no easy endeavour, but UTSC successfully moved 48 departments to the new platform within six months.

Today, all employee onboarding processes at UTSC follow secure protocols for handling SINs, protecting not just the University but also its people.

***"It is truly amazing how the UTSC community came together to make this transition happen in such a short amount of time. This reflects the power of collective action. We are secure together."***

– John Stewart, Information Security Program Manager, IITS, UTSC

# Strategic objective #3:
## *Resilience through effective risk management*

### Units build cyber resilience by focusing on preparedness

When it comes to responding to a cyber security incident, preparedness is key. This year, the institutional Information Security team ramped up efforts to prepare units to respond to security incidents. The team conducted in-person workshops to help units build their incident response plans. Additionally, units across U of T were given access to a virtual platform with pre-built scenarios that simulate real-world security incidents, allowing them to run tabletop exercises and practice their response on their own schedule. So far, the tool has been used to run 39 tabletop exercises.

### Dedicated support for single-department faculties helps bridge the cyber security gap

Safeguarding the University is a collective effort that no single unit can achieve alone. Our collective strength hinges on the preparedness of every unit. This sentiment inspired the cyber security-as-a-service program, which provides support to single-department faculties by embedding dedicated security resources directly within them.

Currently, eight single-department faculties participate in this program. One year into the program, the results have been more than promising. Participating faculties have adopted stronger vulnerability management practices, evident in the faster rate of closure of open vulnerabilities. Additionally, faculties have improved their incident preparedness, with five faculties having drafted their incident response plans and completed tabletop exercises. This program has also been instrumental in increasing engagement with research groups and driving rapid adoption of institutional security solutions, including next-generation anti-virus, password manager and security awareness training.

### Administrative and IT teams partner to identify and protect data assets

The Institutional Research and Data Governance (IRDG) team, in collaboration with Information Security, has been supporting units in cataloguing their data assets and identifying where level 4 and level 3 data exist within their environment. This initiative has increased awareness about data classification, the roles of data trustees and custodians and secure data management practices such as data minimization. To date, 3,237 data assets have been inventoried by 127 units, representing a 143 per cent increase since last year.

**Safeguarding the University is a collective effort that no single unit can achieve alone. Our collective strength hinges on the preparedness of every unit.**

# Unlocking cyber resilience through security log management: *A UTM story*

**If you've visited the University of Toronto Mississauga (UTM) campus, you're likely familiar with its advanced digital classrooms and strong commitment to sustainability. It's no surprise that UTM is part of a tri-campus system that has been ranked the most sustainable university in the world. However, alongside building resilience against climate threats, another story of resilience is unfolding at UTM—this time against cyber threats.**

UTM is enhancing its ability to detect malicious activity by centralizing log collection and analysis. Starting in 2024, UTM initiated a campus-wide effort to collect security event logs from servers, firewalls and cloud services, sending them to the institutional platform for analysis. This initiative involved collaboration between UTM I&ITS team and the institutional Information Security team.

The cloud-hosted solution, adopted as part of this initiative, integrates with many on-premises systems, requiring the team to develop new, complex skills and capabilities. With that effort, over the last six months, UTM has deployed log collection agents on over 300 assets and deployed over 320 rules to detect anomalous activity.

Even though the initiative is still underway, UTM is already seeing benefits in the form of greater visibility into its environment.

***"This initiative marks a major milestone in UTM's cyber security journey, ensuring a safer digital environment for students, researchers and staff."***

- Anthony Betts, Director, I&ITS, UTM

# Strategic objective #4:
*Excellence through collaboration*

### Information Security website serves as a resource hub for the community

This year, the institutional Information Security team completed work on the new Information Security website. Designed with the community in mind, the website provides ready answers to common questions about the institutional information security programs, services, ongoing projects and security standards and guidelines. Additionally, it features specially curated security resources for staff, faculty and students. So far, the website has attracted an impressive 281,000 visits and boasts over 91,000 active users.

### Community engagement drives security awareness

Throughout the year, the Office of the CISO sponsored a variety of events to raise security awareness within the community. These initiatives included security booths at new student orientation, privacy clinics to help individuals configure privacy settings on their social media apps and expert panels during Cyber Security Awareness Month and Data Privacy Day. Additionally, Information Security team members collaborated with faculty to bring short, security-focused talks directly to classrooms.

### Research Security and Information Security partner to support researchers

The institutional Information Security and Research Security teams have been collaborating to provide support to researchers. They have released security guidance on international travel and conduct security briefings for researchers traveling abroad. Additionally, the Information Security team has been hosting office hours to bring direct support to researchers and research staff. A year ago, the Information Security team set a goal to double their engagement with researchers from five researchers to 10 within a year. They have far exceeded this goal by engaging with over 140 researchers to date, with many repeat engagements.

### U of T leverages sector partnerships to build shared cyber security solutions

U of T has provided funding to establish the Canadian Shared Security Operations Centre's (CanSSOC) dark web monitoring service, which has been instrumental in aiding investigations during security incidents. We have also been working with CANARIE and other Canadian universities to build a federated Security Operations Centre aimed at detecting and responding to cyber security threats across the sector. U of T has been a key participant in the pilot phase, providing feedback for the design and implementation of this new model.

***"Research Information Security has been invaluable in helping us navigate the complexities of the cyber security assessment world."***

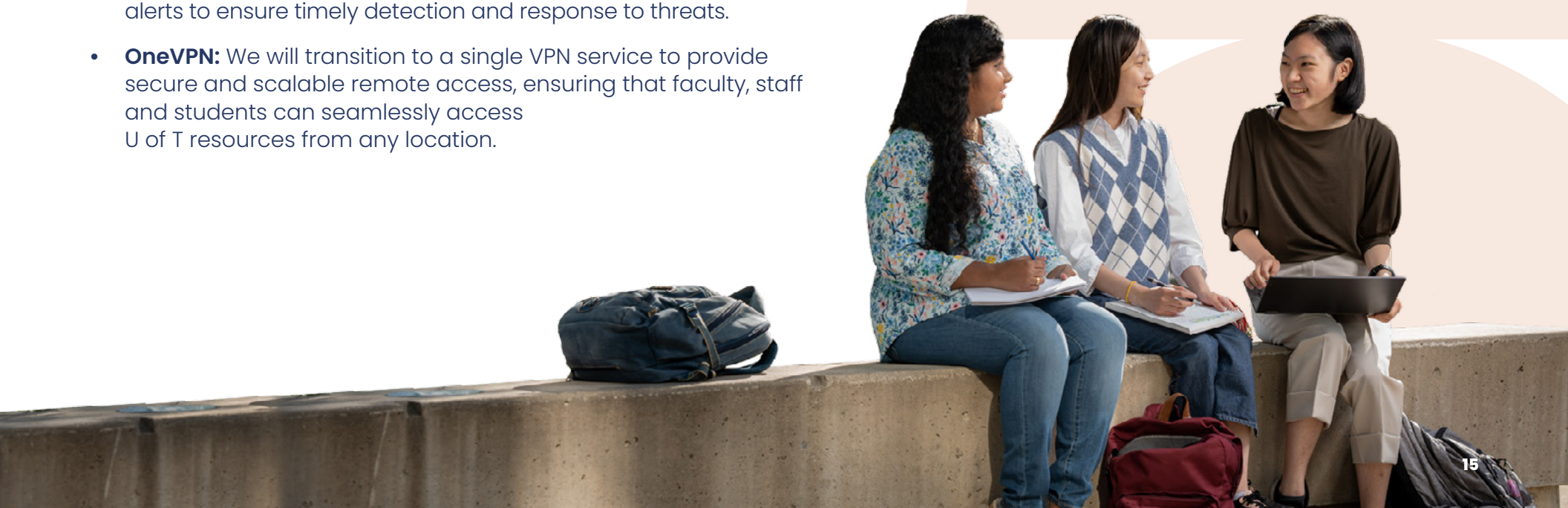
- Shawn Winnington-Ball, Manager, Information System Security, SciNet

# WHAT LIES *ahead*

## Office of the CISO's focus areas

In 2025-2026, the Office of the CISO will prioritize the following areas, along with advancing strategic initiatives that are already underway. These also align with the IT@UofT strategic plan.

- **Identity governance and administration:** Identity underpins all digital experience at the University and is essential for U of T's digital transformation. We will focus on replacing legacy identity infrastructure to enhance user lifecycle and access management processes. This marks the first step in a long-term initiative to modernize our approach to identity.
- **Research competitiveness:** We will support researchers in successfully competing for grants by helping them meet cyber security requirements set by research sponsors.
- **Timely detection and response:** We will continue to increase our capacity for security event logging and implement automated alerts to ensure timely detection and response to threats.
- **OneVPN:** We will transition to a single VPN service to provide secure and scalable remote access, ensuring that faculty, staff and students can seamlessly access U of T resources from any location.



UNIVERSITY OF TORONTO | Information Security

**Office of the Chief Information Security Officer**
University of Toronto
Simcoe Hall
27 King's College Circle, Room 5E
Toronto, ON M5S 1A1, Canada

ciso@utoronto.ca | Tel: 416-978-7857
security.utoronto.ca

DEFY GRAVITY