UNIVERSITY OF TORONTO | SECURE of TOGETHER

ANNUAL REPORT
May 2023 – April 2024

INFORMATION SECURITY AT U OF T:

SECURE **TOGETHER**

TABLE OF **CONTENTS**

INTRODUCTION

Securing our community, data and systems

As we reflect on the fiscal year 2023-2024, we celebrate the achievements of the University of Toronto's tri-campus information security program and bring our attention to what lies ahead. This annual report provides insights into our progress, key risks and the path forward.

Over the past year, we have continued to focus on mitigating security risks stemming from remote work and ransomware by prioritizing efforts to maximize risk reduction and measuring progress.

We built on our commitment to collaboration across the tri-campus community. Learning from the success of the multi-factor authentication project, we have developed new and better structures for collaborative efforts that transcend unit boundaries. This is evident in the tri-campus commitment to the information security strategic initiatives we launched during the year.

Our accomplishments include the increased adoption of next-generation endpoint protection and enhancement of our ability to proactively identify, track and report security vulnerabilities. We continue to foster a security-aware culture through curated and context-rich information security training. Additionally, we have bolstered our capacity to swiftly detect and respond to security threats by upgrading our infrastructure, refining firewall management, integrating superior threat intelligence and fortifying our partnership with the Canadian Shared Security Operations Centre.

Our success and achievements are a collective endeavor, uniting us across tri-campus units and institutional teams.

However, we cannot become complacent. The work of security is ceaseless. Just as we enhance our capabilities, so do our adversaries. To keep pace, we must continue to elevate our cyber security posture, but we cannot do it alone. The path to staying ahead lies in our collective efforts. Indeed, **we are secure together**.

A VIEW INTO **KEY HIGHLIGHTS**

Highlights

- Released the University of Toronto's Information Security Strategy.
- Deployed next generation endpoint protection for more than **10,000** endpoints across the tri-campus community.
- Onboarded over **7,000** staff and faculty onto the Security Awareness training platform.
- Security incident response tabletop exercises completed by **seven** academic and administrative divisions.
- Enhanced **network security** by upgrading University's edge firewall.
- Published **four** new security guidelines including security guidelines on operational technology.
- Released official guidance on secure handling of Social Insurance Numbers.
- Expanded network scanning, resulting in an **eightfold** increase in institutional visibility into security vulnerabilities.

U of T Information Security Strategy

In August 2023, the office of the CISO officially released University of Toronto's Information Security Strategy to provide a shared direction for security and privacy at the University. The strategy drives institutional and unit level efforts to enable the mission of the University, reduce our top security risks and improve alignment with regulatory and compliance requirements.

This annual report highlights progress made against the four strategic objectives:

1. Secure University digital transformation
Ensuring security and privacy is at the core of emerging technologies and new ways of teaching, learning and working adopted by the University.

2. Trustworthy teaching, learning and research
Enabling structures to ensure scholars, researchers, academics and staff feel safe when using University infrastructure, systems and resources.

3. Resiliency through effective risk management
Strategically assessing and managing risk to prevent security attacks and minimize their impact through timely detection and response.

4. Excellence through collaboration
Harnessing the power of partnerships to solve bigger and more complex challenges.

SUCCESS STORIES FROM ACROSS THE TRI-CAMPUS **COMMUNITY**

Securing the University's digital transformation

Empowering security through endpoint protection

The institutional rollout of **next-generation endpoint protection** has garnered support from the community, with **over 10,000 endpoints enrolled**. This is a significant step towards bolstering the University's defenses against sophisticated attacks and enhancing our capacity for timely detection and response.

This collaborative effort, co-led by University of Toronto Mississauga and ITS Information Security, spans all three campuses, with 40 participating units. Institutional funding and support have made it easier for units to adopt this capability.

Key benefits:

- **Endpoint management:** A single integrated view for managing endpoints and responding to alerts.
- **Threat hunting:** Incident investigation and identification of known or emerging threats.
- **Vulnerability management:** Visibility into endpoints running vulnerable applications.
- **Live threat updates:** Real-time enhancements to detection capabilities via live threat updates.

"The Faculty of Music was invited to participate in the pilot phase of the endpoint protection project. We had an incredibly positive experience. The next-gen anti-virus agents were easily deployed and had little to no impact on device performance, giving us the benefit of real-time threat detection and analysis."

Sebastian Bisciglia, Director, Information & Learning Technology, Faculty of Music, U of T

"In recent years, we've witnessed an increase in cyber attacks targeting educational institutions. In response, the Faculty of Applied Science and Engineering has adopted the institutional endpoint protection platform. The platform is not just another anti-virus solution; it's a next-generation defense system designed to shield against a broad spectrum of cyber threats. The success of this initiative hinges on the collaborative teamwork and active engagement of all IT personnel across academic units. It embodies the essence of IT@UofT, while showcasing an excellent example of the Secure Together model, emphasizing that cyber security is a shared responsibility."

Alex Tichine, Director, Information Technology, Faculty of Applied Science & Engineering, U of T

Information Security team members accepting an award for the success of the MFA program.

Strengthening network security for digital transformation and hybrid work

Robust network security provides the foundation for rapid digital transformation and hybrid work models. The unification and alignment of network security practices across the University is a key element of our strategy. By doing so, we aim to create common, cost-effective solutions that benefit everyone and ensure a secure and seamless experience for all. As we work towards this long-term goal, here are highlights of key accomplishments from this year:

- **Secured VPN access** through multi-factor authentication. This has drastically reduced unauthorized access while ensuring that community members have secure network access regardless of where they are.
- **Upgraded admin VPN** to optimize the service and make it more resilient to cyber attacks.
- **Upgraded the University's edge firewall** to further enhance our network security, increase our resilience to denial-of-service attacks and enable common protections across the tri-campus community.

Secure cloud transformation

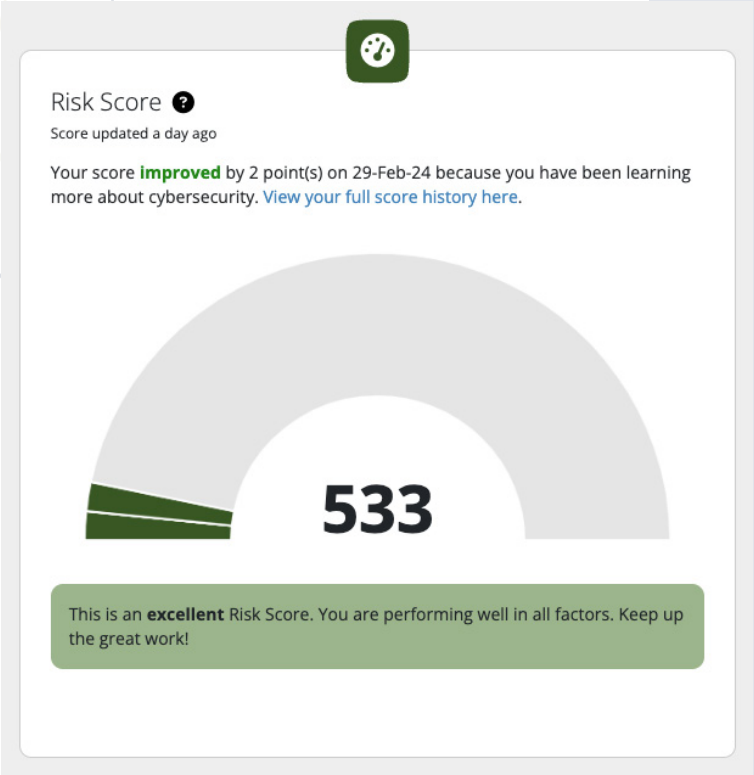
Core enterprise applications, which are integral to the University's key business processes, are progressively leaning on cloud services. ITS has securely connected on-premises resources with the Microsoft Azure Cloud, offering a cost-effective, consistent and secure model to leverage cloud services across U of T. This has not only improved resilience of critical applications but also given community members access to enhanced business solutions such as PowerBI and Database-as-a-Service from wherever they are.

WE AIM TO CREATE COMMON, COST-EFFECTIVE SOLUTIONS THAT BENEFIT EVERYONE AND **ENSURE A SECURE AND SEAMLESS EXPERIENCE FOR ALL.**

Enabling safe and trustworthy teaching, learning and research

Empowering the community: U of T's Security Awareness and Training Program

This year, U of T placed security awareness at center stage, launching a program to equip staff, librarians and faculty members with essential security knowledge. Co-led by UTSC and the ITS Information Security team, the Security Awareness and Training Program has achieved significant milestones.



Key accomplishments of the program:

1. **Learning platform deployment:** Established a user-friendly learning platform that is accessible to all enrolled users and leverages gamification to keep users engaged.
2. **Curated learning content:** Curated content, ensuring that platform users receive targeted guidance on security topics ranging from social engineering to data protection.
3. **Phishing simulations:** Launched monthly phishing simulations for all onboarded users, empowering participants to recognize and respond to phishing attempts.
4. **Tailored spear-phishing campaigns:** Ran customized spear-phishing simulations for senior executives who face targeted attacks.

The program thrives on community engagement and has leveraged **champions** within the U of T community to actively promote security awareness.

Program impact:

- As of March 2024, **41 U of T units** have joined the program, collectively onboarding over **7,000 staff, faculty and librarians** onto the learning platform.
- Over **2,800 U of T community members** have completed the learning modules.

"Understanding the importance of having a knowledgeable and empowered community, UTSC has put significant emphasis on enrollment in the Information Security Awareness and Training Program. As of early 2024, nearly 640 appointed staff have been enrolled; with work continuing to soon extend this training to non-appointed staff and then to faculty members."

Romel Sargezi, Information Security Analyst, UTSC, U of T

Building self-serve community-focused cyber security resources

The Information Security team has curated a collection of concise guides addressing common cyber security queries. These resources provide actionable steps on various security topics to all U of T community members, ranging from researchers to staff and curious learners.

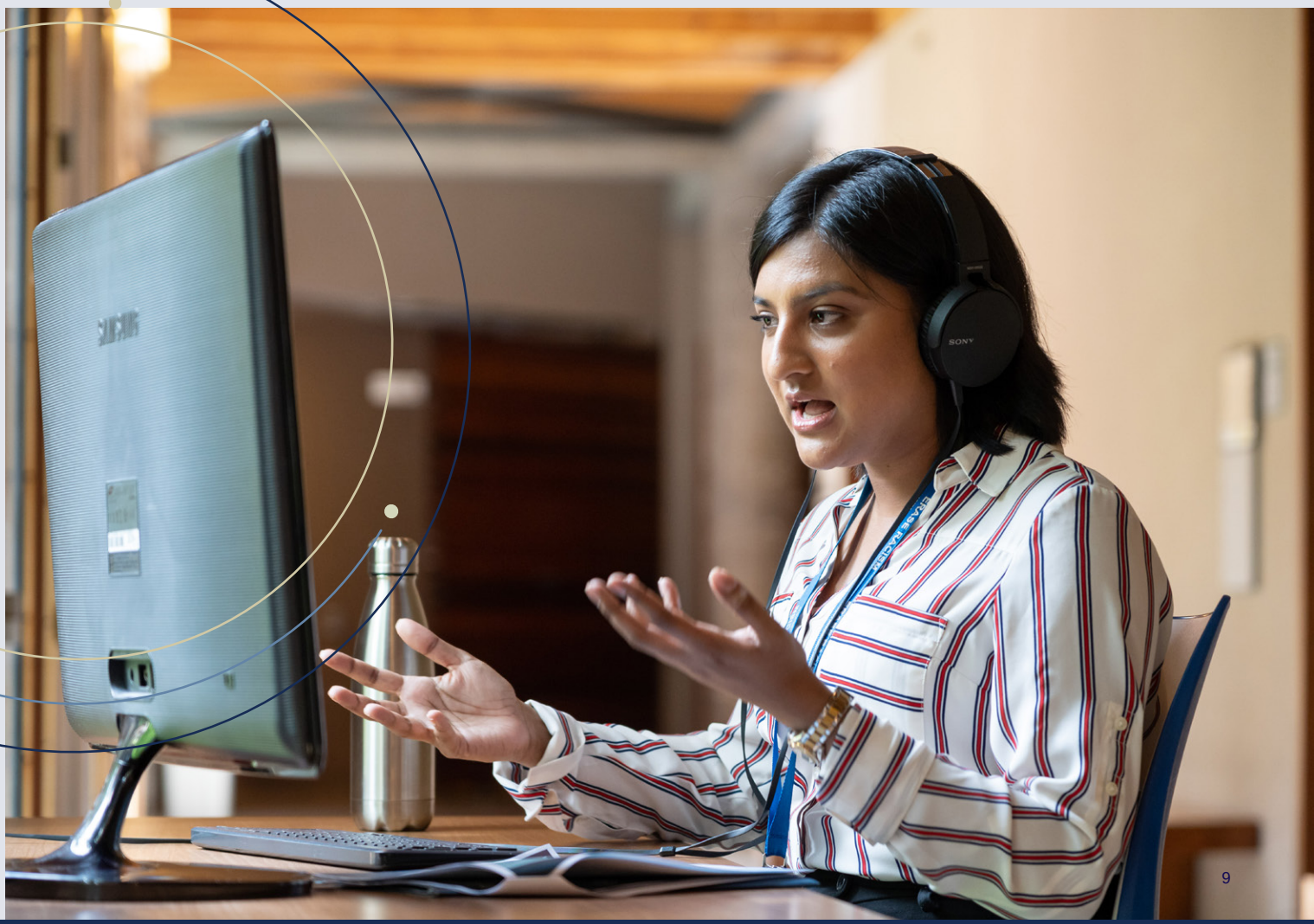
Framework for trusted and vetted research infrastructure

Led by the Information Security team, experts from across the University are working together to develop a framework to evaluate research infrastructure against the University's Information Security Control Standard.

For researchers who opt to use these vetted systems, interactions with sponsors, data providers and research ethics boards will be streamlined, allowing them to focus on their core research activities.

"The context of scholarly activity at U of T has has expanded rapidly over the last 10 years. The emergence of new technology has increased the capacity to access sensitive data from multiple devices, and thus brought forward new considerations for how sensitive data should be protected. In parallel, new models of data sharing have emerged which extend beyond the traditional boundaries of data access restriction within a laboratory or network of collaborators. U of T's Research Information Security Program has developed resources to support faculty, staff and trainees as they engage in their scholarly activity."

Dr. Karl Zabjek, Associate Professor, Department of Physical Therapy, U of T and Affiliate Scientist, KITE Research Institute, University Health Network



Resilience through effective risk management

Enhancing vulnerability management for a more secure environment

Effective vulnerability management is critical to a strong information security program, particularly as the number of compromises via known vulnerabilities are on the rise. The ITS Information Security team has enhanced the institutional vulnerability management service, offering deeper insights into security vulnerabilities within our environment. In the past year, institutional visibility into security vulnerabilities has **increased eightfold.**

Key highlights of the improvements:

1. **Expanded scanning coverage:** Extended network and web application scanning capabilities, providing a more comprehensive view of security vulnerabilities.
2. **User-friendly portal:** Provided units with access to an intuitive portal to review vulnerability scan results and take informed actions.
3. **Vulnerability rating system:** Introduced a rating system to streamline remediation efforts by prioritizing vulnerabilities based on their severity, allowing teams to focus on critical issues first.
4. **Automated progress tracking:** Enabled automated reporting system to keep stakeholders informed of ongoing remediation efforts.

IN THE PAST YEAR, INSTITUTIONAL VISIBILITY INTO SECURITY VULNERABILITIES HAS **INCREASED EIGHTFOLD.**

Driving ransomware preparedness

The office of the CISO launched a campaign to bolster unit-level preparedness against ransomware attacks, focusing on greater adoption of ransomware-resilient backups, endpoint protection, ransomware playbooks and tabletop exercises.

- **Building a community of ransomware responders:** Fostered collaboration across divisions by creating a community of ransomware responders responsible for driving preparedness efforts at the divisional level.
- **Guidance and tool support:** Provided support for divisional contacts through guidance and practical tools to implement best practices and enhance readiness.
- **Metrics-driven progress tracking:** Collected relevant data to measure progress against key focus areas and guide continuous improvement.
- **Tabletop exercises for real-world scenarios:** Ran third-party facilitated security incident tabletop exercises for **five divisions** to validate and reinforce ransomware preparedness. Additionally, conducted a business continuity tabletop exercise, attended by leaders from various shared services units, to assess our institutional preparedness.

"The institutional Business Continuity Working Group partnered with the Information Security team on a tabletop exercise in December 2023. The team provided leadership and guidance as they navigated the working group through an information security issue. The scenario and the discussion that followed was invaluable. We are delighted to be partnering with Information Security again on a similar tabletop in June 2024, this time to include tri-campus academic and shared services divisional representatives."

Elizabeth Cragg, Director, Office of the Vice President, Operations & Real Estate Partnerships, U of T

Advancing U of T's Information Risk Management Program

The Information Security team has continued to build upon established risk management practices. This includes enhancements to the **Data Asset Inventory-Information Risk Self-Assessment** program with new guidance for completing the data asset inventory, managing data assets and identifying critical digital assets.

The office of the CISO released guidance for units to mature their risk management programs. This included tools and templates to build key components such as risk registers, risk acceptance processes and clearly defined risk management roles and responsibilities.

"It's amazing to see the growth of information risk management at the University with tools like the DAI-IRSA. There is plenty of room to improve and I'm looking forward to the evolution of Information Risk Management Programs over the next five years."

Jeff Waldman, Manager, Institutional Data Governance, U of T

Risk management journey spotlights from across the tri-campus community

Student Life:

- **Automated SharePoint access synchronization:** Developed an automated process to synchronize SharePoint access, ensuring user permissions remain up-to-date and aligned with organizational roles. Solution will be deployed in 2024.
- **Enhancing web application security:** Exploring the use of web application scanners during software development and as part of periodic security reviews.

University of Toronto Mississauga:

- **Risk management program:** Formalized UTM's risk management program by leveraging a customized solution for efficient risk identification, mitigation and tracking.
- **Automated patch management:** Deployed automated patch management solution, thus reducing time and effort for applying security updates.
- **Incident response:** Developed an Incident Response standard and refined it through a third-party led ransomware tabletop exercise.

"University of Toronto Mississauga is committed to enhancing its security maturity. Key future initiatives include formalizing asset management and access controls, implementing centralized security logging and monitoring, encouraging departmental participation in the annual Data Asset Inventory and Information Risk Self-Assessment cycle, and enrolling all staff and faculty in the institutional security awareness program."

Akshat Mishra, Information Security Program Manager, UTM

University of Toronto Libraries:

- **DAI-IRSA for UTL digital assets:** Participated in DAI-IRSA to assess and manage security risks to UTL.
- **Endpoint protection:** Deployed next-generation endpoint protection to over **1,000** UTL servers and staff workstations as part of the institutional initiative.
- **Secure storage:** Conducting gap analysis to enhance U of T Dataverse's ability to securely manage Level 3 and 4 research data.
- **Security awareness training:** Successfully onboarded users to the institutional security awareness training platform with **256** users having completed the training.

"I am immensely proud of the strides we have made in enhancing our security. Our team's dedication and expertise have not only ensured the safety of our digital assets but also fostered a culture of security awareness and vigilance. It is also important to recognize the fantastic initiatives spearheaded by the CISO's office. Their visionary projects and collaborative efforts have significantly benefitted our operations, reinforced our security posture, and guided our strategic approach. As we move into the next year, we are committed to building on this momentum, continuing to innovate and improve our security measures to meet evolving challenges."

Amaz Taufique, Manager, Enterprise Infrastructure and Staff Technology, UTL

Medicine:

- **Web application firewall:** Deployed a high-availability firewall to protect web applications against malicious attacks.
- **Endpoint protection:** Implemented next-generation endpoint protection solution as part of the institutional rollout.
- **Security awareness and training:** Onboarded users to the institutional security awareness training platform, with training completed by 78 per cent of participants.

"From re-building our entire VLAN infrastructure, to implementing next-gen endpoint protection, adding web-application firewall capabilities, rolling out a faculty-wide cyber security training program, and setting the groundwork for transitioning to a fully-managed digital asset infrastructure and role-based access with real time HR updates, our incredible partnership with IS, and the other teams in ITS has tangibly showcased that working together as IT@UofT professionals we can make significant leaps in protecting our people and systems and a real difference. I'm truly humbled by what this partnership has already achieved and looking forward to the future as we work towards being Secure Together."

Dimitris Keramidas, Director, Information Technology Temerty Faculty of Medicine, U of T

Pharmacy:

- **Endpoint protection**: Deployed next-generation endpoint protection on 138 endpoints as part of the institutional rollout and built capability to respond to alerts in a timely manner.
- **Asset and data inventory:** Building an inventory of data, hardware and software for improved management of assets and data.

"In 2024, we will collaborate with ITS to implement Intune. We will also initiate a project to isolate different subnets using Virtual LANs to prevent spread of malware. All personal devices will be required to use the guest Wi-Fi network to enhance security."

Byron Qu, Manager, Information Security, Leslie Dan Faculty of Pharmacy, U of T

Security awareness champions from across the tri-campus community celebrating their efforts.

Information Security staff engaging with the community at the Cyber Security Awareness Month booth.

Excellence through collaboration

Preparing for the future: Experiential learning for students

The office of the CISO has been actively cultivating cyber security expertise among students. Noteworthy initiatives include:

- **Capture the Flag event:** Sponsored a successful event organized by the CTF Student Club. The event drew 2,400 participants, including over 300 students from U of T.
- **Hands-on security lab:** Provided free training resources to students for honing their security skills.
- **Security Operations Center:** Hired student workers to augment the institutional incident response team, providing vital support for security event monitoring.

Harnessing the power of community

Throughout the year, we came together as a community to spread security awareness, discuss security matters and build shared solutions. Key highlights include:

- **Listening to researchers:** Information Security, in partnership with offices within the Vice-President, Research & Innovation, convened a panel to actively listen to researchers, understand challenges related to sponsor-imposed requirements and identify areas where research facilitation can be improved.
- **Empowering students:** Security experts from across the tri-campus community visited over 20 classrooms, educating students about security best practices.
- **Cyber security-as-a-service:** The office of the CISO has initiated a program to offer security support to single department faculties by embedding dedicated resources directly within these faculties.

"The FIPP Office enjoys a very felicitous, close, and collaborative relationship with University IT offices and staff. We meet regularly and address issues at the intersection of technology and privacy, comprising information security, information sharing, systems design, audit, compliance, data classification, and many more, and we believe that our ongoing collaboration is very helpful for the University."

Rafael Eskenazi, Director, Freedom of Information and Protection of Privacy Office, U of T

Partnering to safeguard research at the University

The **Research Information Security Program**, under the umbrella of **Information Security**, and the Research Security team, operating within the Office of the Vice-President of Research and Innovation, have collaborated with other University partners on initiatives to secure and facilitate research. Key among them is the **supply chain risk management** initiative. The enactment of the U.S. National Defense Authorization Act, Section 889 has acted as a catalyst for the creation of a supply chain risk assessment methodology. This methodology enables more risk-informed procurement decisions by assessing both information security and geo-political risks associated with third-party relationships.

"The Research Security Team and the Research Information Security Program maintain a close and collaborative relationship that yields several effective outcomes: geopolitical risk analysis as part of large institutional procurement; awareness among the research community about requirements for information security and research security in grant applications; and support for researchers regarding security-related inquiries."

Paul Jarrett, Director, Research Security, U of T

Strengthening sector partnership

We have continued to build strong partnerships across the sector and contributed to addressing shared security challenges.

- We actively champion efforts to understand and enhance cyber security maturity of the sector by participating in the National Cybersecurity Assessment developed by partners in Canada's National Research and Education Network and the CANARIE cyber security benchmarking program.
- Our commitment to our strategic partnership with CanSSOC extends beyond utilizing its services. We are also actively contributing to its evolution by supporting Research Intensive Group projects focused on advancing CanSSOC operations.

…A CLOSE AND COLLABORATIVE RELATIONSHIP THAT YIELDS **SEVERAL EFFECTIVE OUTCOMES**

WHAT LIES **AHEAD**

These are exhilarating times, fueled by advancements in artificial intelligence that have created new risks and opportunities. We need to be ready to capitalize on these developments so we can reap the benefits while minimizing risks to security and privacy.

Whether tackling existing security risks or navigating through emerging ones, the same foundational principle persists – doing what's right. As individuals, we must recognize that our work carries profound implications for security. We must weave security and privacy into the very fabric of everything we create and do. This shared responsibility demands vigilance and collaboration from each of us.

Safeguarding the University against risk is not a task that any single unit can accomplish in isolation. Our collective strength hinges on the preparedness of every unit.

Together, we can confidently navigate this transformative landscape.

Office of the CISO focus areas

In the coming year, the office of the CISO will continue to drive security initiatives that enable teaching, learning and research in alignment with U of T's Information Security Strategy.

- Transform identity at the University by kick-starting a multi-year effort to consolidate identities, enhance identity systems and streamline identity lifecycle management.
- Continue to make security learning available to more users across the community.
- Set the groundwork for secure data management by fostering efforts to implement data sensitivity labeling and develop more comprehensive data inventories, thus paving the way for secure adoption of AI.
- Enhance detection and response capabilities by expanding coverage of next-generation endpoint protection, maintaining investment in CanSSOC, upgrading threat analysis platform, increasing capacity for security event logging and automating alerts for rapid response.
- Continue to bolster U of T's network security by offering firewall management as a service to the community.

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