OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

November 2024

Safeguarding the City's Cyber Realm

Established in 2020, the Office of the Chief Information Security Officer (CISO) is dedicated to safeguarding the City against cyber threats, protecting sensitive information, and fortifying critical infrastructure through a multifaceted approach to cyber security.

Strengthening Business Resilience

Providing comprehensive cyber risk management and supporting City-wide strategic priorities

Enhancing Cyber Governance

Supporting strategic cyber governance and advisory as well as cultivating a cyber-aware organizational culture

OC | Senior Management Team

Maneesh Agnihotri
Chief Information Security Officer

Andree Noel
Deputy Chief Information Security Officer

David Hayes
Director, Cyber Threat Management

Paul Tsang
Director, Cyber Resilience

Sheri MacLeod
Director, Cyber Engagement

Mohsin Khan
Director (Acting), Cyber Advisory

Cyber Threat Management

Cyber Resilience

Cyber Engagement

Cyber Advisory

OC | Organizational Structure / Business Sections

Cyber Threat Management

Identifies, protects, and responds to cyber threats impacting the City, providing strategic and tactical guidance on offensive security, cyber intelligence, and application security

Cyber Resilience

Serves as a central point for cyber risk assessment and cyber advisory services

Cyber Engagement

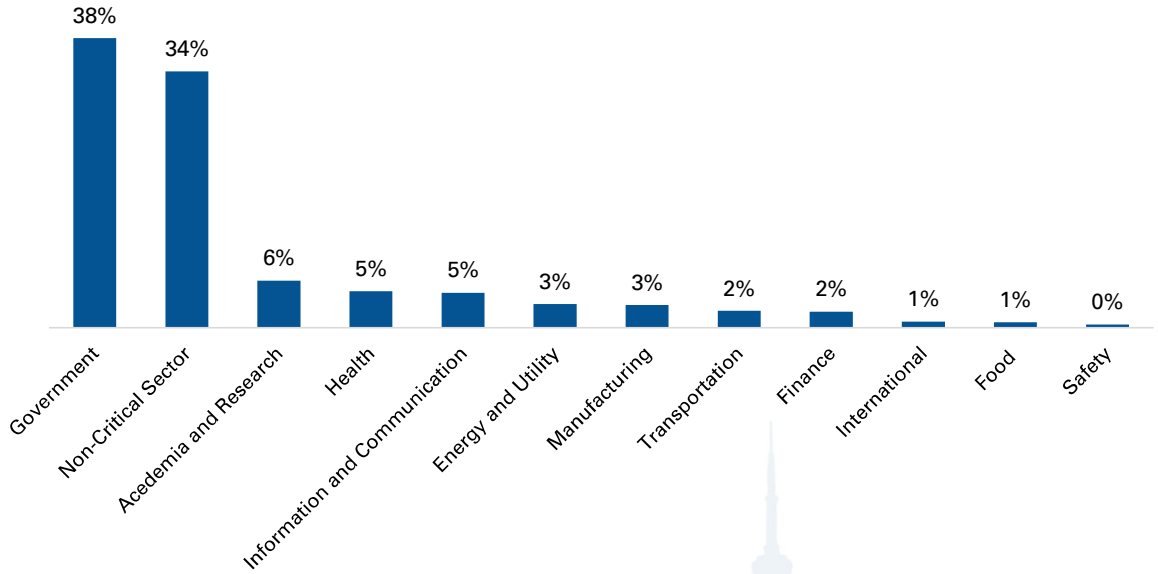
Focuses on cyber service delivery and strategic transformation to ensure operation excellence

Cyber Advisory

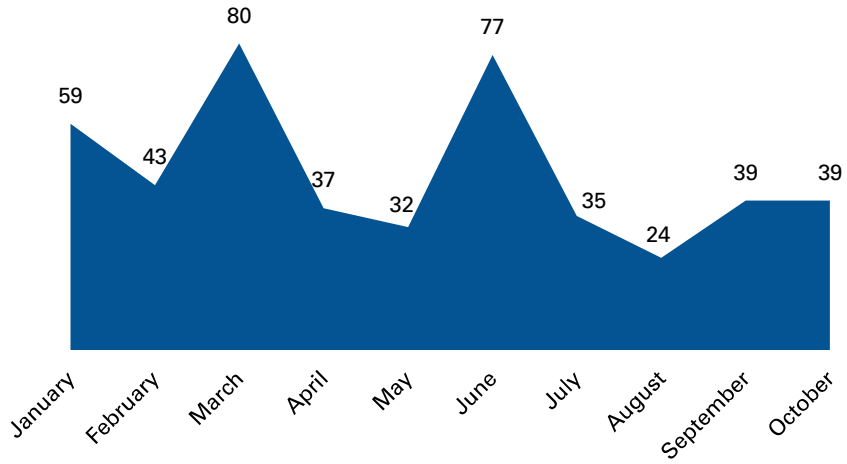
Supports cyber awareness, vulnerability management, and cyber strategic advisory, encompassing both information technology (IT) and operational technology (OT)

OC | 2024 Canadian Threat Landscape

Targeted Sectors



Number of Ransomware Attack in 2024

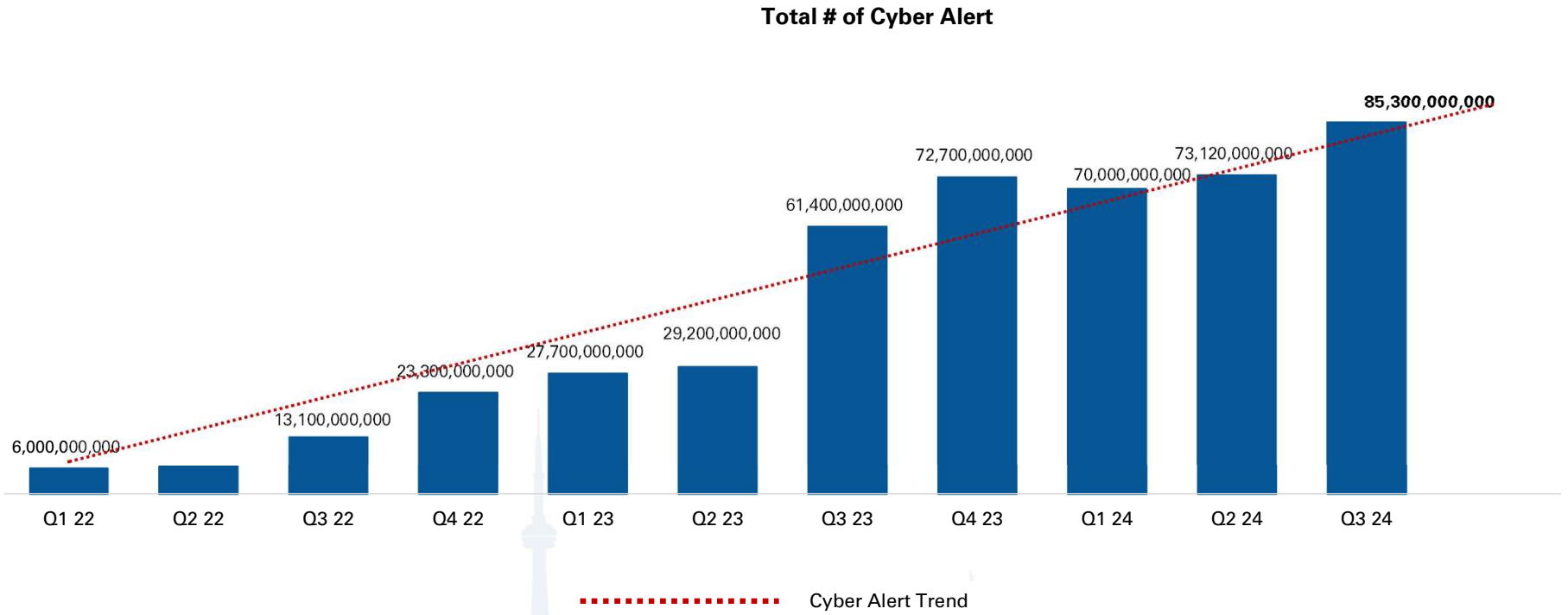


- The top 5 targeted sectors were Government, Non-Critical sectors, Academia and Research, Health and Information / Communication.
- Government sector has continued to be one of the most targeted sectors in Canada and is more likely to be attacked in comparison to other sectors and 13 times more likely to be targeted in comparison to other critical sectors on the average.
- The number of ransomware attacks against Canadian entities continued to fluctuate every month with peaks observed in January, March and June.

TORONTO

Data refreshed date: 29 October 2024

OC | Threat Management Overview



Since Q1 2022, the number of cyber alerts have increased by 1706% to 85.3 Billion in Q3 2024.

TORONTO

Data refreshed date: 25 October 2024

OC | Threat Management Monitoring Highlights

Phishing Emails Received

Over

200

emails examined daily

The team examines reported emails, promptly detecting and **mitigating any malicious threats** to the City of Toronto.

Devices Monitored

Over

4 billion

records investigated monthly

The team monitors data from over 60K devices across the City against predefined threat use cases to **promptly identify and flag malicious activities**.

Network Threats Prevented

About

22K

threats yearly

The team prevents network threats. Without proper network security, these **threats can infiltrate interconnected City systems**.

OC | Performance Highlights

Cyber Services Delivery

An increase of
270%
completed cyber risk assessments compared to the year before

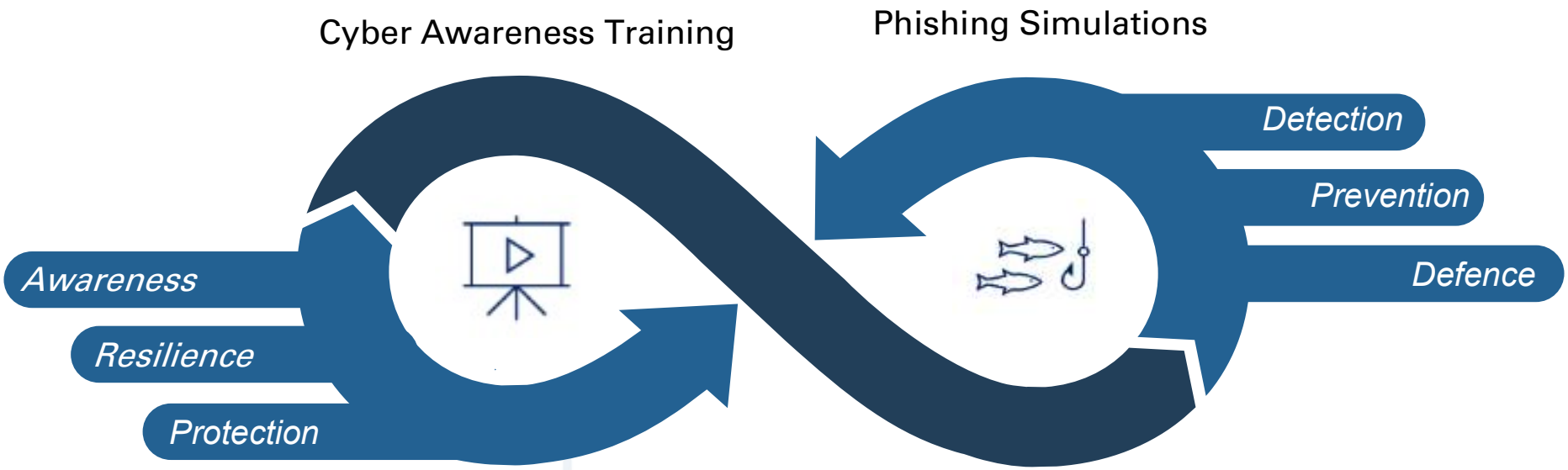
Cyber Governance & Awareness

More than
28,000
hours of cyber training and led multiple cyber awareness activities

Cyber Resilience & Maturity

An increase of
70%
in the City's cyber maturity rating since its initial rating in 2019

OC | Cyber Services Available to Toronto Investment Board Members



OFFICE OF THE
CHIEF INFORMATION SECURITY OFFICER

inside.toronto.ca/ciso

ciso@toronto.ca