CYBERSECURITY OVERVIEW

Douglas A. Gernat, Deputy Director, Sr. Strategy & Cybersecurity
Department of Information Technology

Governmental Operations Standing Committee
December 10, 2025

DEPARTMENT OF
INFORMATION
TECHNOLOGY

OVERVIEW

1. All About Cybersecurity
2. What Makes Cybersecurity so Complicated
3. ThreatScape
4. Top Threats Observed within the City
5. Cybersecurity Trends
6. Top Recommendation / Top Focus

ABOUT CYBERSECURITY

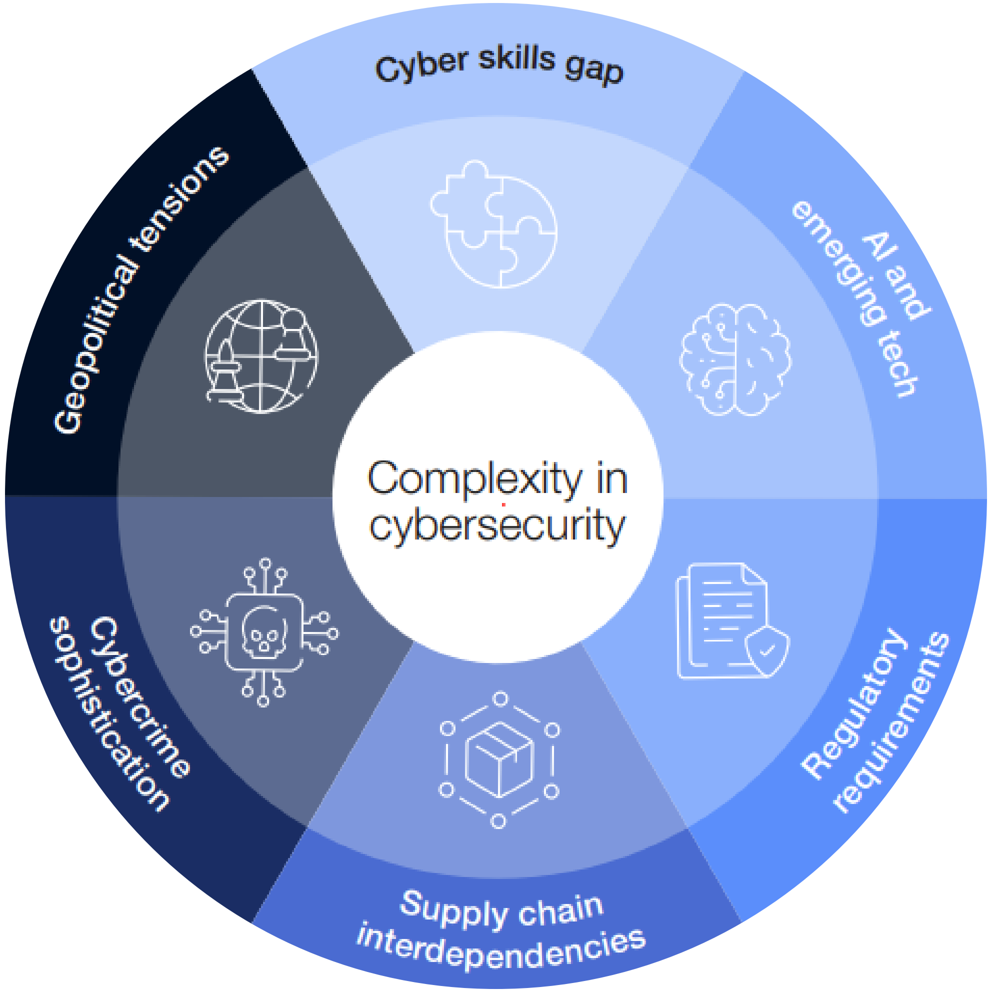
Cybersecurity is an essential foundation that supports nearly every aspect of the City’s work.

It is not just a technology concern but a comprehensive discipline that safeguards systems, data, and operations, ensuring the integrity, availability, and confidentiality of information across all functions. Over the past several years, technology based cybersecurity professionals have moved towards the role of Security Risk Management for an organization.

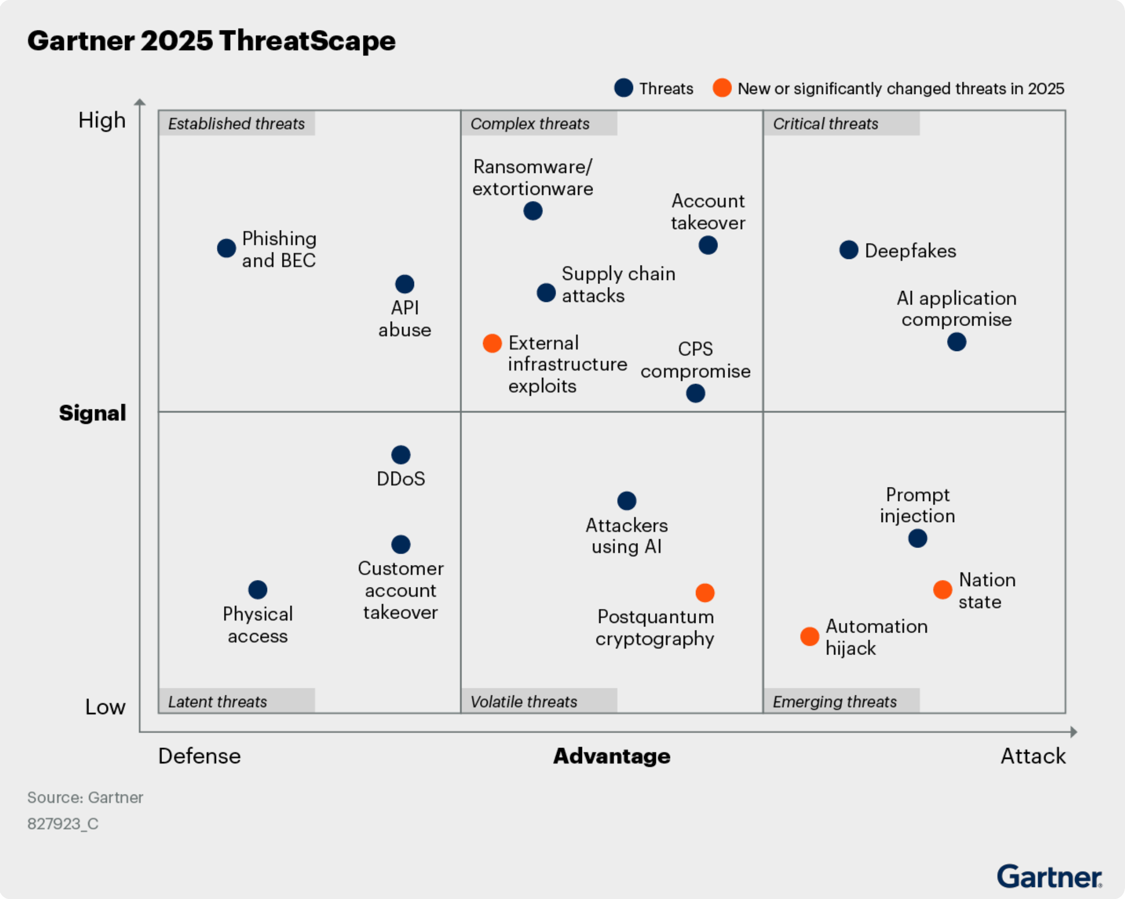
Benefits

1. Risk Management of daily processes
2. Protection of Sensitive Data
3. Regulatory Compliance
4. Continuity of Services and Operations
5. Collaboration and Efficiency
6. Safeguarding Public Funds

What makes cybersecurity so complicated?


Complexity in cybersecurity
Cyber skills gap
AI and emerging tech
Regulatory requirements
Supply chain interdependencies
Cybercrime sophistication
Geopolitical tensions

THREATSCAPE



Gartner 2025 ThreatScape

Source: Gartner
827923_C

Signal

Frequency seen

Advantage

Who has the upper-hand:
The defender or the attacker?

TOP THREATS OBSERVED WITHIN THE CITY

- **Nation state sponsored exploitation:** Targeted for both financial gain through criminal networks as well as disruptive measures
- **Ransomware & Extortion:** Use of targeted attacks, typically spearphishing at key individuals to exploit social tactics which have proven effective
- **Traditional phishing:** Extremely common entry vector or precursor of more complex attacks
- **Account Takeover:** Lockout of key staff, exploit a “position of trust” in today's digital ecosystem, perform insider threat activities
- **Complex Deepfakes and AI driven tactics**
- **API abuses**

Source: Gartner.com “Update your Cybersecurity Policies in a shifting threat landscape

CYBERSECURITY TRENDS

Personnel

- 55% of organizations are facing understaffed Cybersecurity Teams
- 65% have unfilled vacancies
- 50% struggle to retain cyber talent

Cyber Strategy

- Globally, only 47% of Cybersecurity teams are involved in AI governance, 40% are involved in AI implementation
- With Social Engineering as the leading entry to cyber attacks, upskilling the workforce with training and awareness remains a priority
- Moving towards the updated Cybersecurity framework (CSF 2.0) and proactive defenses are within our FY25 and FY26 plan

According to the 2025-2026 ISACA Report on the State of Cybersecurity:

TOP RECOMMENDATIONS (TOP FOCUS)

Balance innovation with vigilance

Embed resilience to cyber threats to allow a "fearless" improvement in our technology stack, but keep that innovation moving forward

Awareness

Continue to keep cybersecurity in all conversations in Council Chambers, executive meetings, and design or business decision sessions

Source: Microsoft 2025 Digital Defense Report, Gartner.com

AUDIT FINDING STATUS

Audit #	Audit Report Name	Recommendation	Status
2023-08	DIT Chargebacks for Constitutional Officers	(#01) We recommend that the Director of the Department of Information Technology bill Constitutional Officers for information technology services provided that are reimbursable, such as monthly telephone and internet access costs.	Closure requested 12/1/2025. We have been advised that while the Compensation Board can by law reimburse for IT and office expenses, it has not budgeted for such for several years.
2023-13	DIT Disaster Recovery	(#01) Confidential – FOIA exempt	Documentation submitted to Audit for review/closure on 11/20/2025
2023-13	DIT Disaster Recovery	(#02) Confidential – FOIA exempt	Documentation submitted to Audit for review/closure on 11/20/2025

Source: Microsoft 2025 Digital Defense Report, Gartner.com

QUESTIONS