Cyber Risk Management for Municipalities

Presented by:
Gerard Dunphy, Senior Director
Ruchir Kumar, Senior Director

ISA Cybersecurity
October 23, 2024

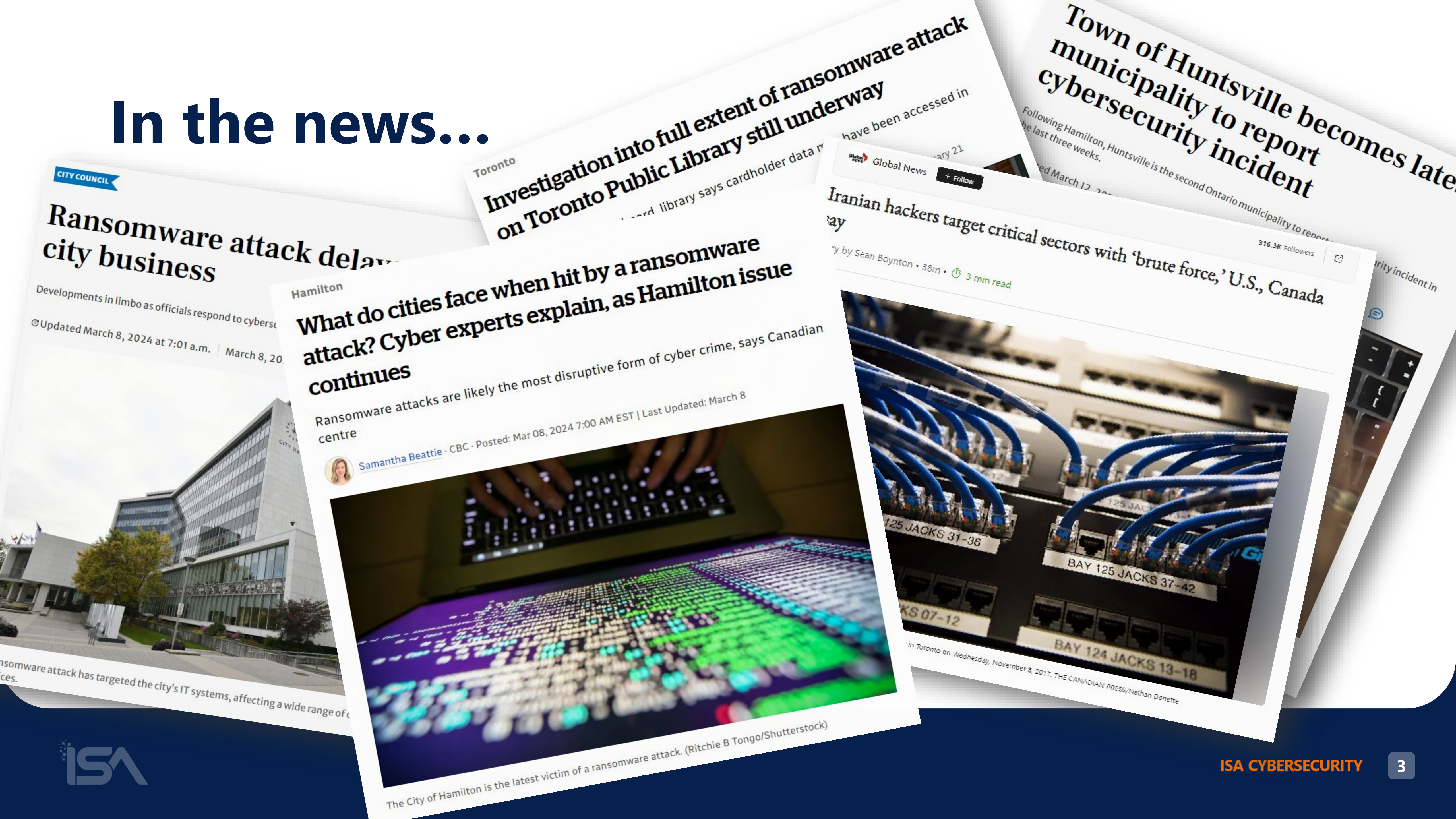
isacybersecurity.com

ISA CYBERSECURITY

Agenda

- Current Events
- Threat Landscape
- Threat Actors
- Attack Vectors
- National Cyber Threat Assessment
- Artificial Intelligence
- Cybersecurity Frameworks
- Top 15 Cybersecurity Best Practices

In the news…



CITY COUNCIL

Ransomware attack delay city business

Developments in limbo as officials respond to cyberse

Updated March 8, 2024 at 7:01 a.m. | March 8, 20

nsomware attack has targeted the city's IT systems, affecting a wide range of c ices.

Toronto

Investigation into full extent of ransomware attack on Toronto Public Library still underway

ard, library says cardholder data m have been accessed in ary 21

Town of Huntsville becomes late municipality to report cybersecurity incident

Following Hamilton, Huntsville is the second Ontario municipality to report he last three weeks.

ed March 12, 20

rity incident in

Global News + Follow 316.3K Followers

Iranian hackers target critical sectors with 'brute force,' U.S., Canada ay

y by Sean Boynton • 38m • 3 min read

in Toronto on Wednesday, November 8, 2017. THE CANADIAN PRESS/Nathan Denette

Hamilton

What do cities face when hit by a ransomware attack? Cyber experts explain, as Hamilton issue continues

Ransomware attacks are likely the most disruptive form of cyber crime, says Canadian centre

Samantha Beattie · CBC · Posted: Mar 08, 2024 7:00 AM EST | Last Updated: March 8

The City of Hamilton is the latest victim of a ransomware attack. (Ritchie B Tongo/Shutterstock)

Cyber Attacks on Canadian Organizations

Government

- **City of Cold Lake, AB** (July 23, 2024) – Ransomware
- **Municipality of La Guadeloupe, QC** (April 23, 2024) – Ransomware
- **Province of BC** (April 10, 2024) – Email access
- **Town of Huntsville, ON** (March 10, 2024) – Ransomware
- **City of Hamilton, ON** (February 26, 2024) – Ransomware
- **Town of Ponoka, AB** (February 20, 2024) – Data breach
- **Town of Greater Napanee, ON** (January 11, 2024) – Ransomware
- **Yukon, Prince Edward Island, Nunavut, and Manitoba** (September 2023) - DDoS attack

Other

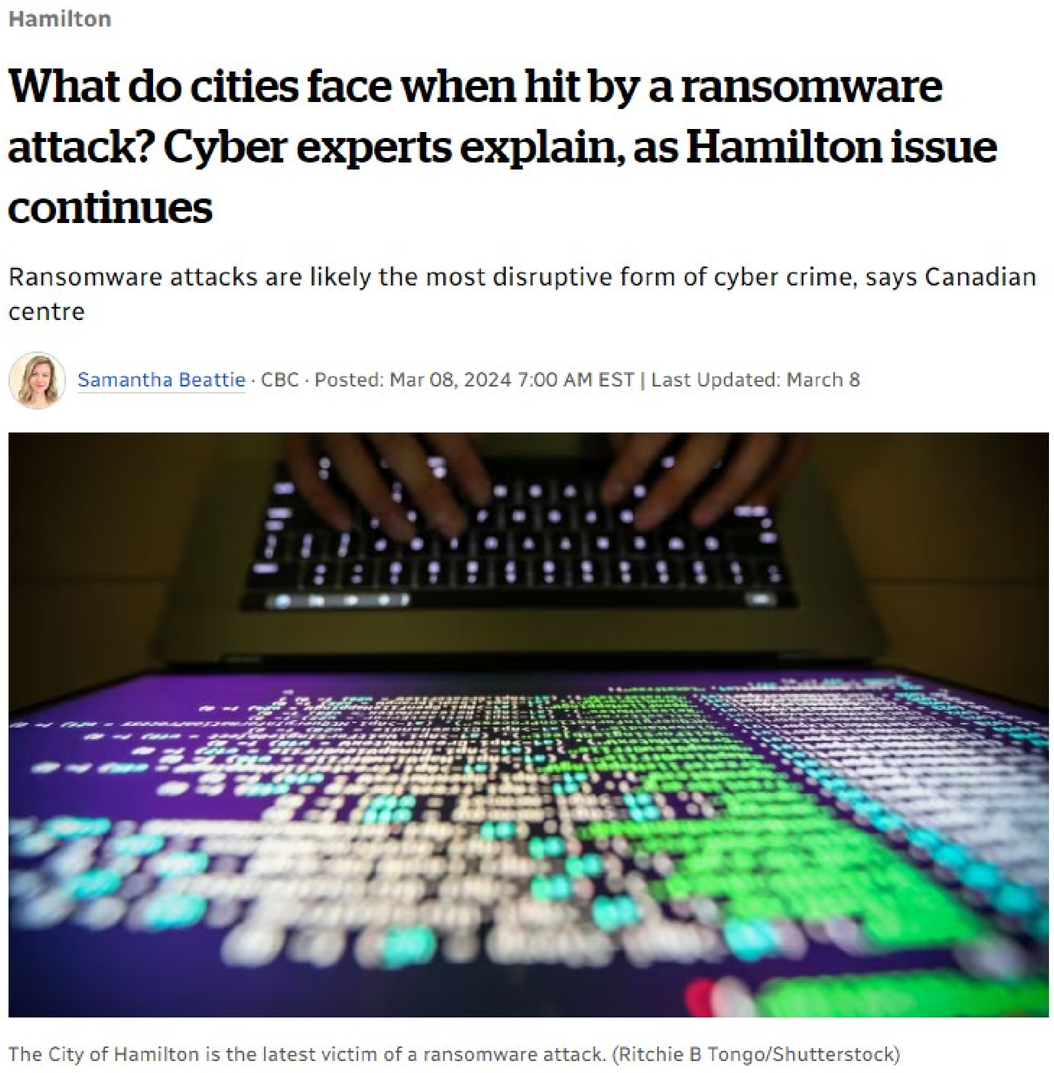
- **Calgary Public Library** (Oct 11, 2024) – unknown
- **NTV Broadcasting** (May 2024) – Data breach
- **FINTRAC** (March 2, 2024) – Unauthorized access
- **RCMP** (February 23, 2024) – RCMP/Military/Public Servant personnel data stolen
- **Global Affairs Canada** (January 30, 2024) – Sensitive data stolen
- **Toronto Zoo** (January 2024) – Ransomware attack
- **Toronto Public Library** (October 2023) – Ransomware attack
- **LCBO** (August 2023) – Data breach of customer information
- **Alberta Dental Service Corp** (July 2023) – Ransomware attack

Current Events

Cyber Attack on Municipalities

City of Hamilton

- February 2024
- Ransomware (Medusa)
- Multiple systems down:
  - Phone lines, public transit, libraries, building permits, payroll
- Will take months to rebuild and restore network
- $7.4M in costs (Aug 2024)



Hamilton

What do cities face when hit by a ransomware attack? Cyber experts explain, as Hamilton issue continues

Ransomware attacks are likely the most disruptive form of cyber crime, says Canadian centre

Samantha Beattie · CBC · Posted: Mar 08, 2024 7:00 AM EST | Last Updated: March 8

The City of Hamilton is the latest victim of a ransomware attack. (Ritchie B Tongo/Shutterstock)

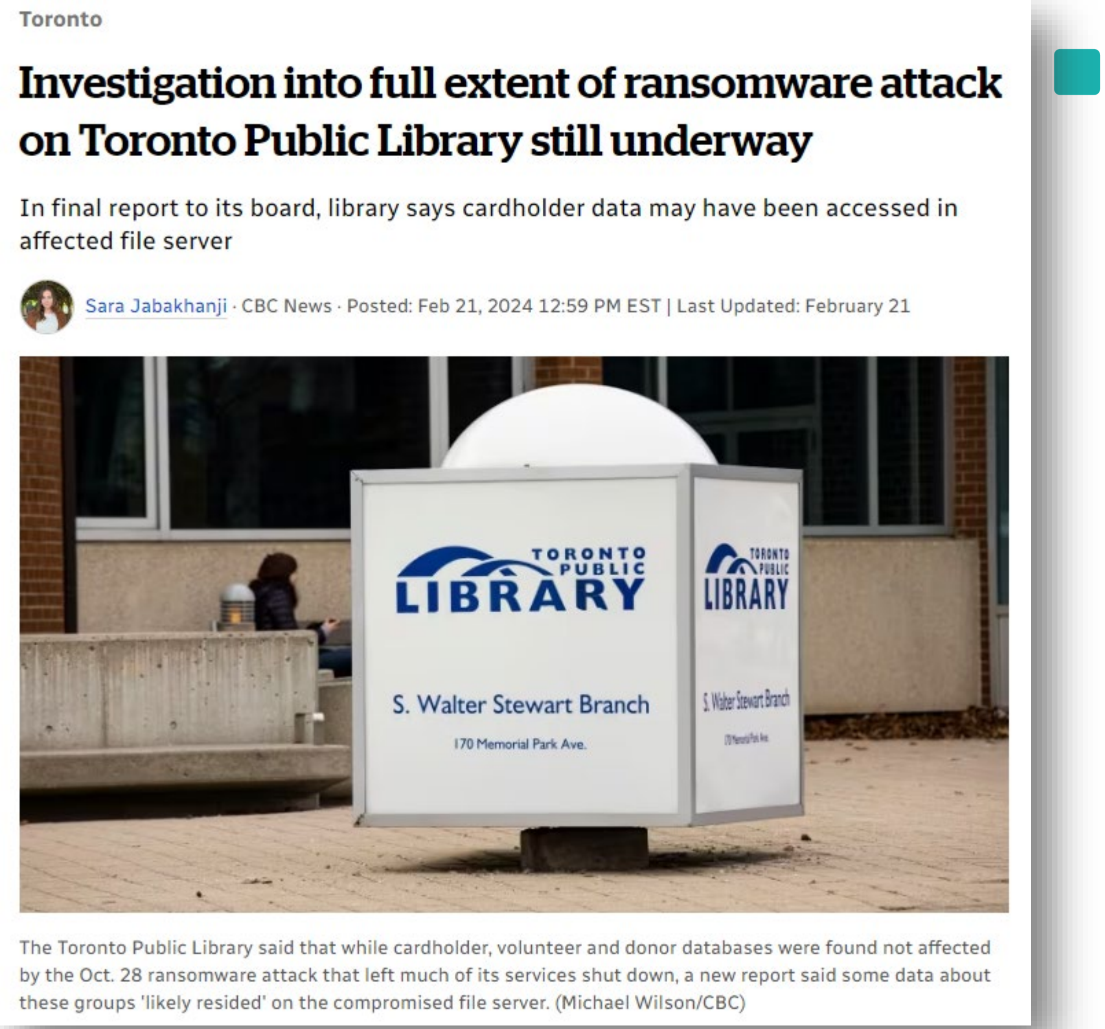
References:
https://www.thespec.com/news/council/ransomware-attack-delays-pile-of-city-business/article_e1a5893f-98f3-57a7-bb56-bc7bfef40b90.html
https://www.hamilton.ca/city-council/news-notices/news-releases/cybersecurity-update-release-incident-impact-report

Current Events

Cyber Attack on Municipalities

Toronto Public Library

- October 2023
- Ransomware (Black Basta)
- Employee PII data stolen
- 5000 computers affected
  - TPL.ca, online account, public computers, printing, cataloguing all offline
- +4 months down time
- $1M in costs (*estimated*)



Toronto

Investigation into full extent of ransomware attack on Toronto Public Library still underway

In final report to its board, library says cardholder data may have been accessed in affected file server

Sara Jabakhanji · CBC News · Posted: Feb 21, 2024 12:59 PM EST | Last Updated: February 21

The Toronto Public Library said that while cardholder, volunteer and donor databases were found not affected by the Oct. 28 ransomware attack that left much of its services shut down, a new report said some data about these groups 'likely resided' on the compromised file server. (Michael Wilson/CBC)

References:
https://www.cbc.ca/news/canada/toronto/toronto-public-library-cyberattack-1.7120921
https://www.bleepingcomputer.com/news/security/toronto-public-library-outages-caused-by-black-basta-ransomware-attack/

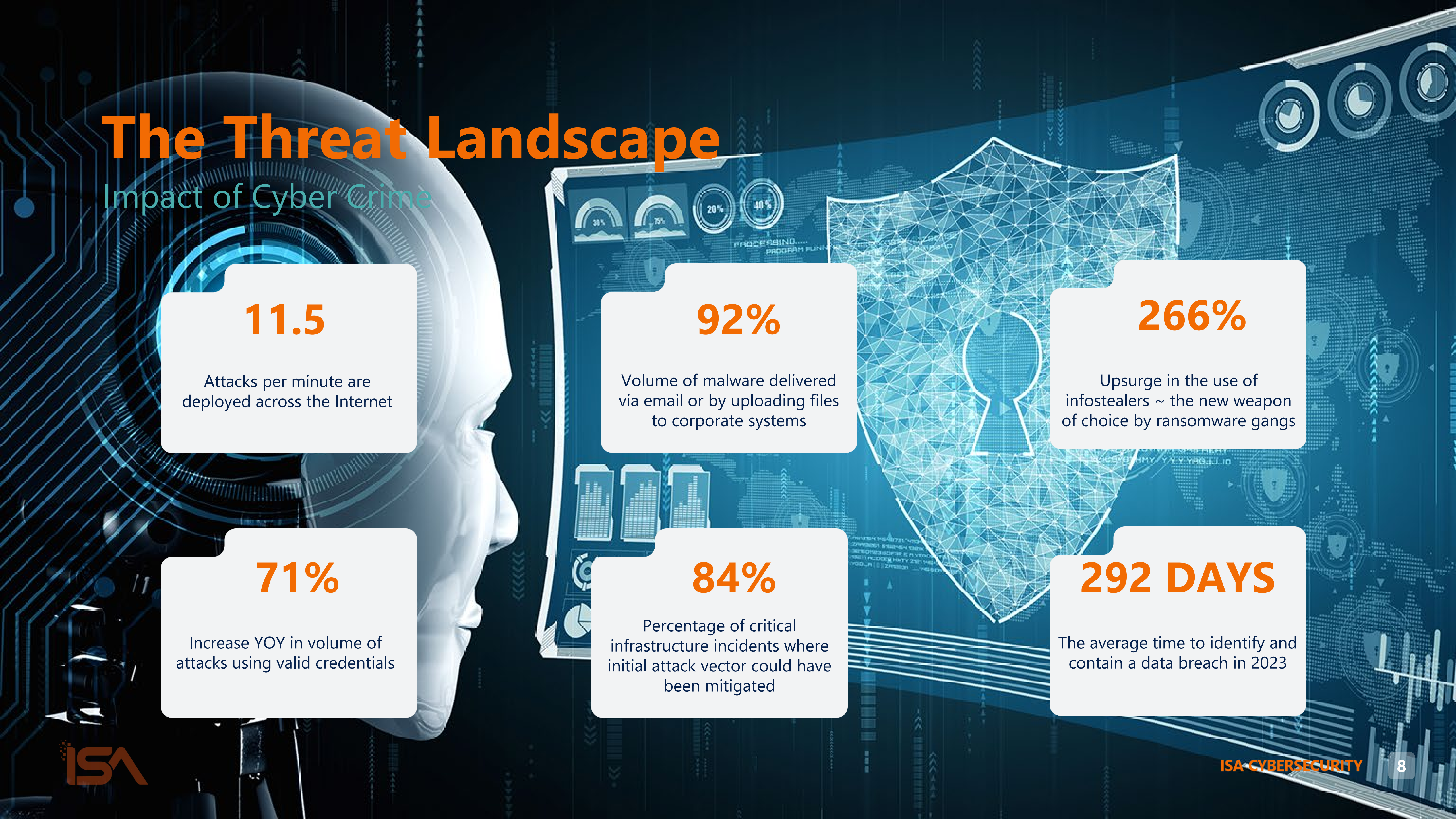
The Threat Landscape

isacybersecurity.com

ISA CYBERSECURITY

The Threat Landscape

Impact of Cyber Crime



11.5

Attacks per minute are deployed across the Internet

92%

Volume of malware delivered via email or by uploading files to corporate systems

266%

Upsurge in the use of infostealers ~ the new weapon of choice by ransomware gangs

71%

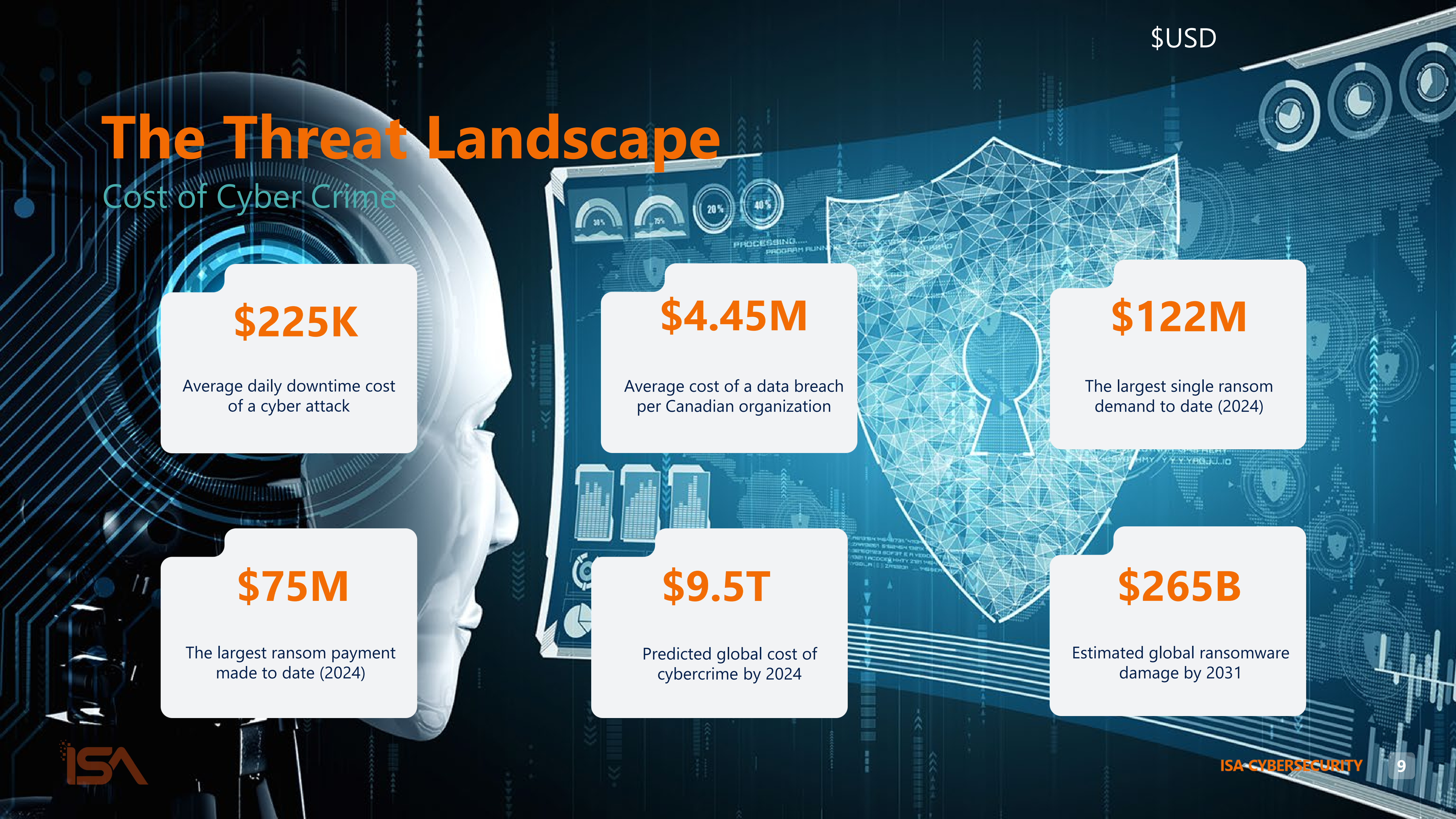
Increase YOY in volume of attacks using valid credentials

84%

Percentage of critical infrastructure incidents where initial attack vector could have been mitigated

292 DAYS

The average time to identify and contain a data breach in 2023



$USD

The Threat Landscape

Cost of Cyber Crime

$225K

Average daily downtime cost of a cyber attack

$4.45M

Average cost of a data breach per Canadian organization

$122M

The largest single ransom demand to date (2024)

$75M

The largest ransom payment made to date (2024)

$9.5T

Predicted global cost of cybercrime by 2024

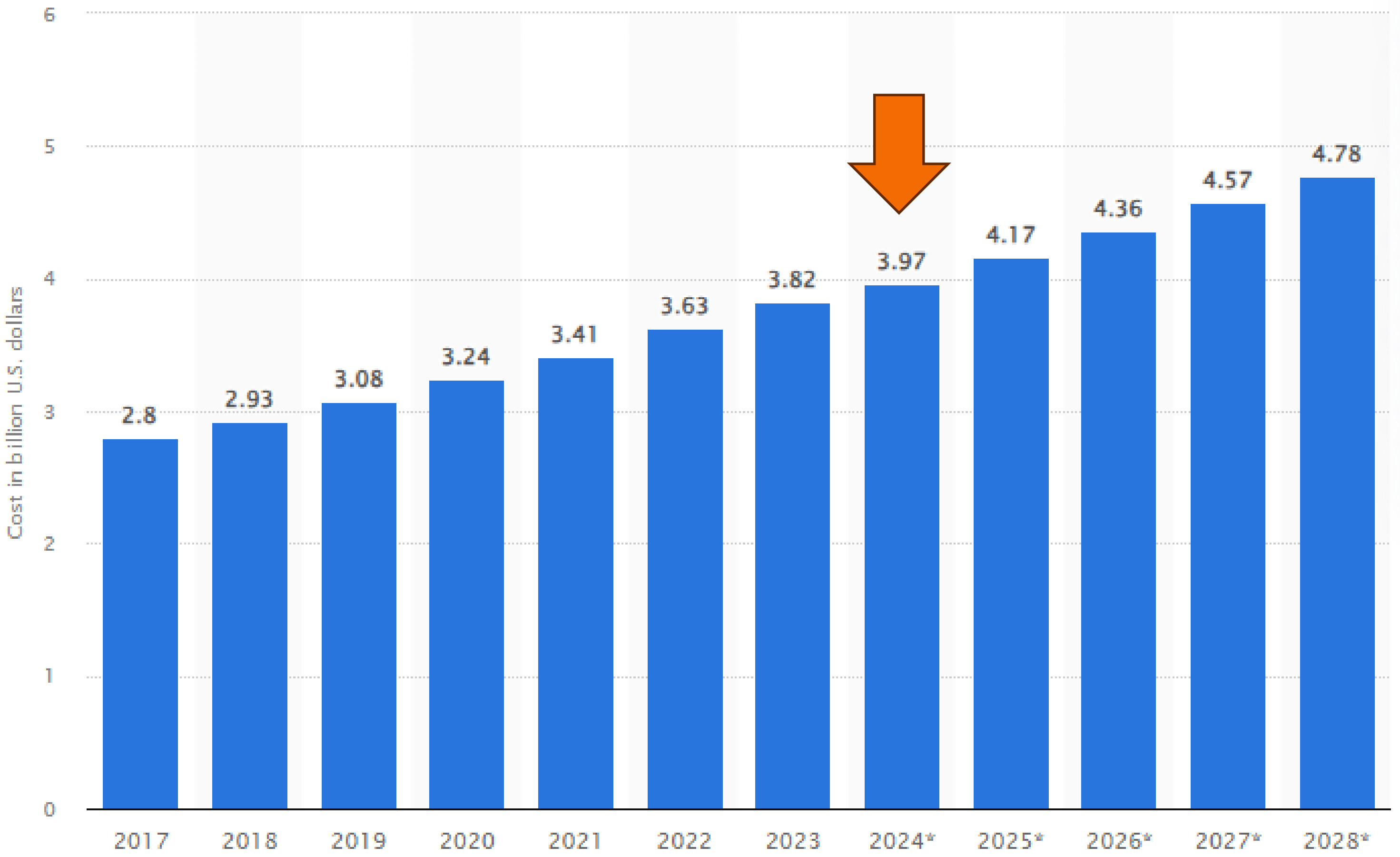
$265B

Estimated global ransomware damage by 2031

The Threat Landscape

Estimated Annual Cost of Cybercrime in Canada 2017-2025

- $3.97 Billion (USD) in 2024
- $4.78 Billion (USD) by 2028



Reference: https://www.statista.com/forecasts/1457244/canada-cybercrime-cost-annual

Threat Actors

About Threat Actors

Threat Actors

Cyber Criminal
Nation State (APT)
Hacktivist
Cyber Warrior
Accidental
Stalker

Motives

Profit
Government Sanctioned
Industrial Espionage
Hactivism
Privacy
Politics
Fame
Revenge
Curiosity

Tactics

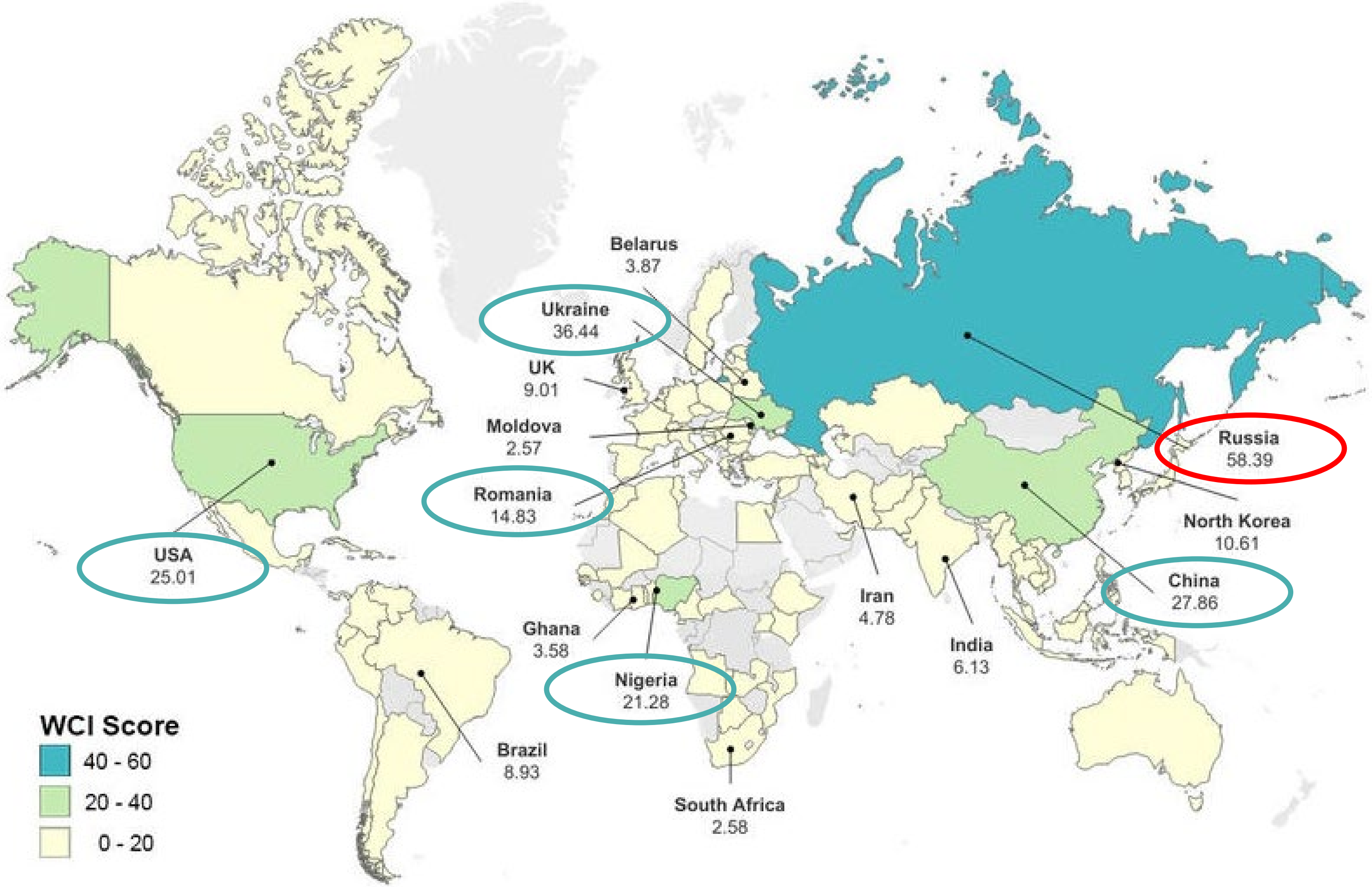
Reconnaissance
Social Engineering
Network Exploitation
Spoofing
Scripts
Malware
Password Cracking
Keylogging
Backdoors

Attacks

Phishing/Spear Phishing
Ransomware
Malware
DDoS
Data Exfiltration
Session Hijacking
SQL Injection
Brute Force

Cybercrime Map

Major Cybercrime Hotspots

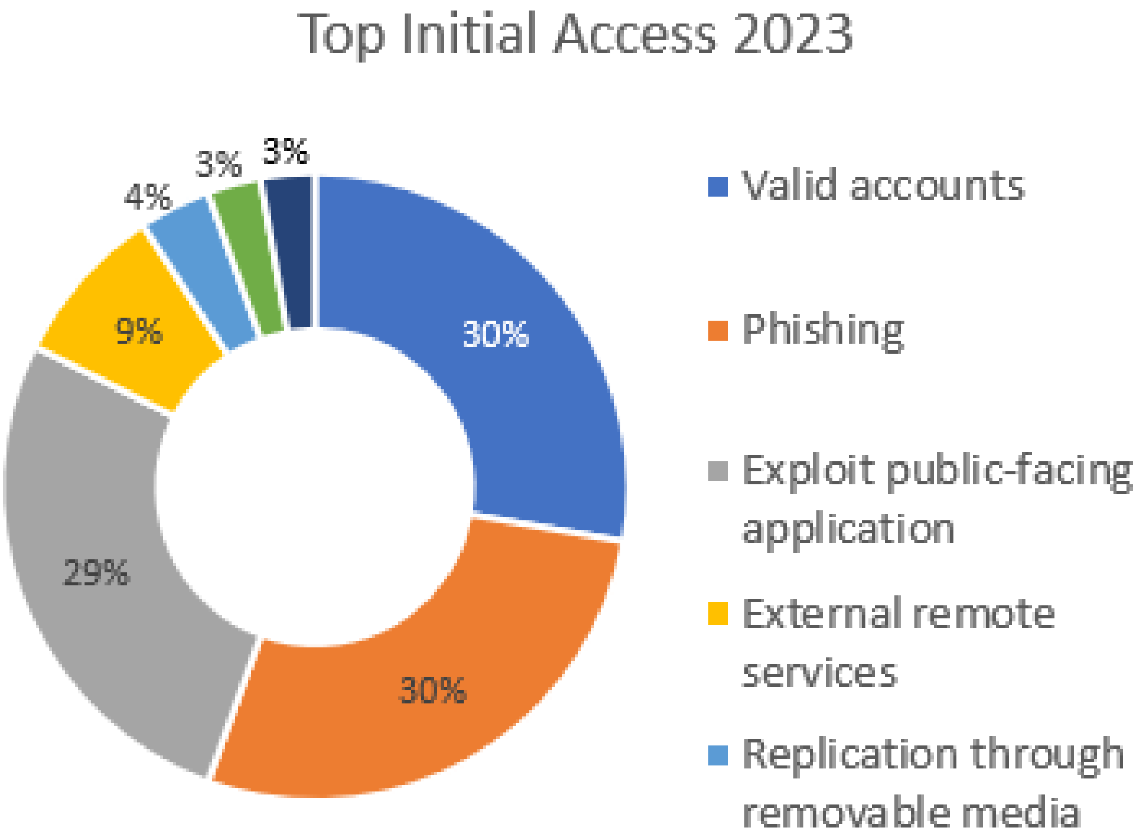


Countries with the greatest cybercrime threat

Reference: https://www.sociology.ox.ac.uk/article/world-first-cybercrime-index-ranks-countries-by-cybercrime-threat-level

Top Initial Access Vectors

- **Valid accounts 30%** ↑
- **Phishing 30%** ↓
- Exploit Public Application **29%**
- External Remote Services **9%**
- Replication through removable media **4%**
- Drive-by Compromise **3%**
- Trusted Relationship **3%**



Reference: IBM X-Force Threat Intelligence Index 2024

CANADIAN CENTRE FOR
CYBER SECURITY

National **Cyber Threat** Assessment

2023
2024

Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canada

Key Judgements

1

Ransomware is a persistent threat to Canadian organizations

2

Critical infrastructure is increasingly at risk from cyber threat activity

3

State-sponsored cyber threat activity is impacting Canadians

4

Cyber threat actors are attempting to influence Canadians, degrading trust in online spaces

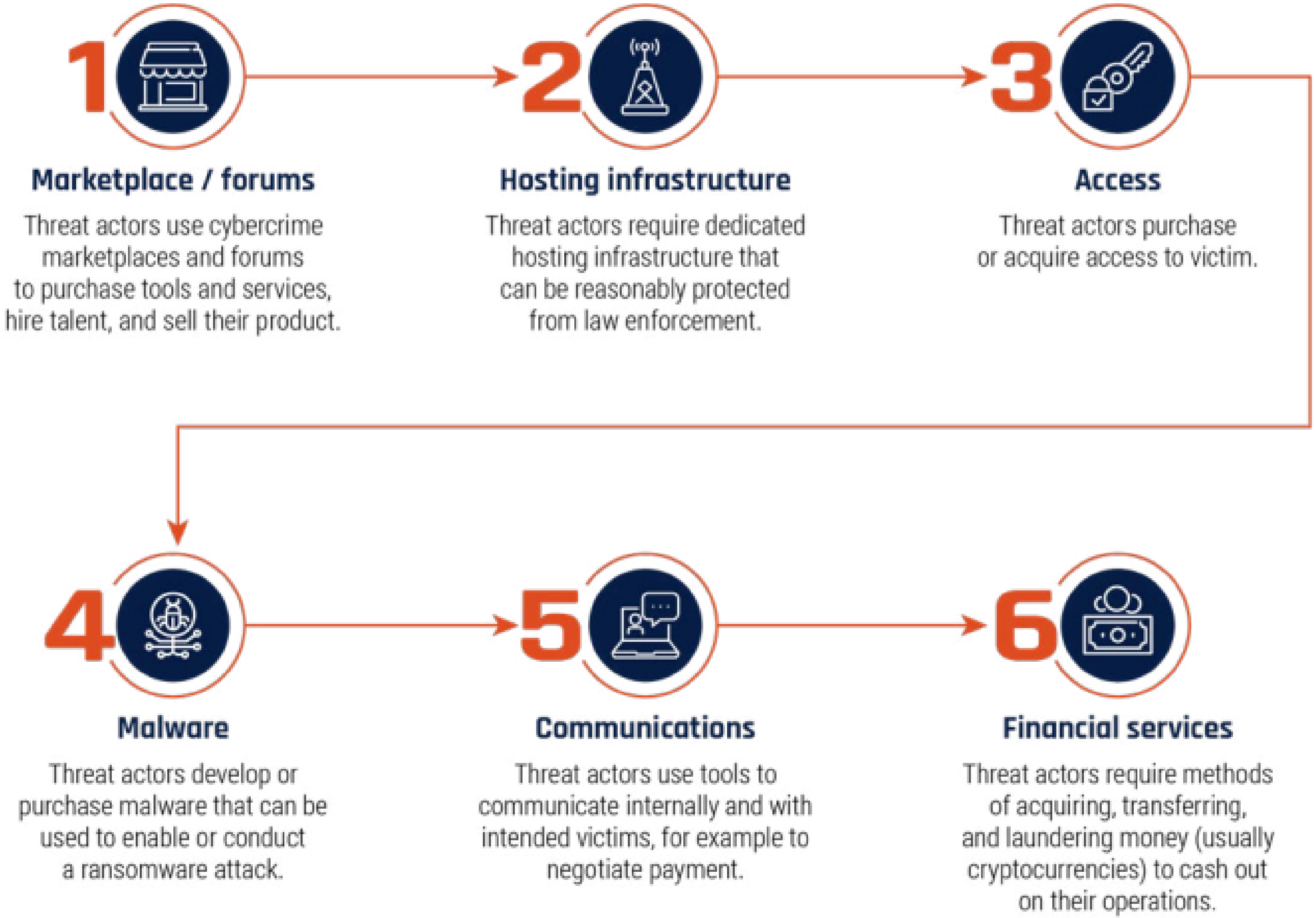
5

Disruptive technologies bring new opportunities and new threats

Reference: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

Ransomware

Ransomware-as-a-Service supply chain



1 **Marketplace / forums**

Threat actors use cybercrime marketplaces and forums to purchase tools and services, hire talent, and sell their product.

2 **Hosting infrastructure**

Threat actors require dedicated hosting infrastructure that can be reasonably protected from law enforcement.

3 **Access**

Threat actors purchase or acquire access to victim.

4 **Malware**

Threat actors develop or purchase malware that can be used to enable or conduct a ransomware attack.

5 **Communications**

Threat actors use tools to communicate internally and with intended victims, for example to negotiate payment.

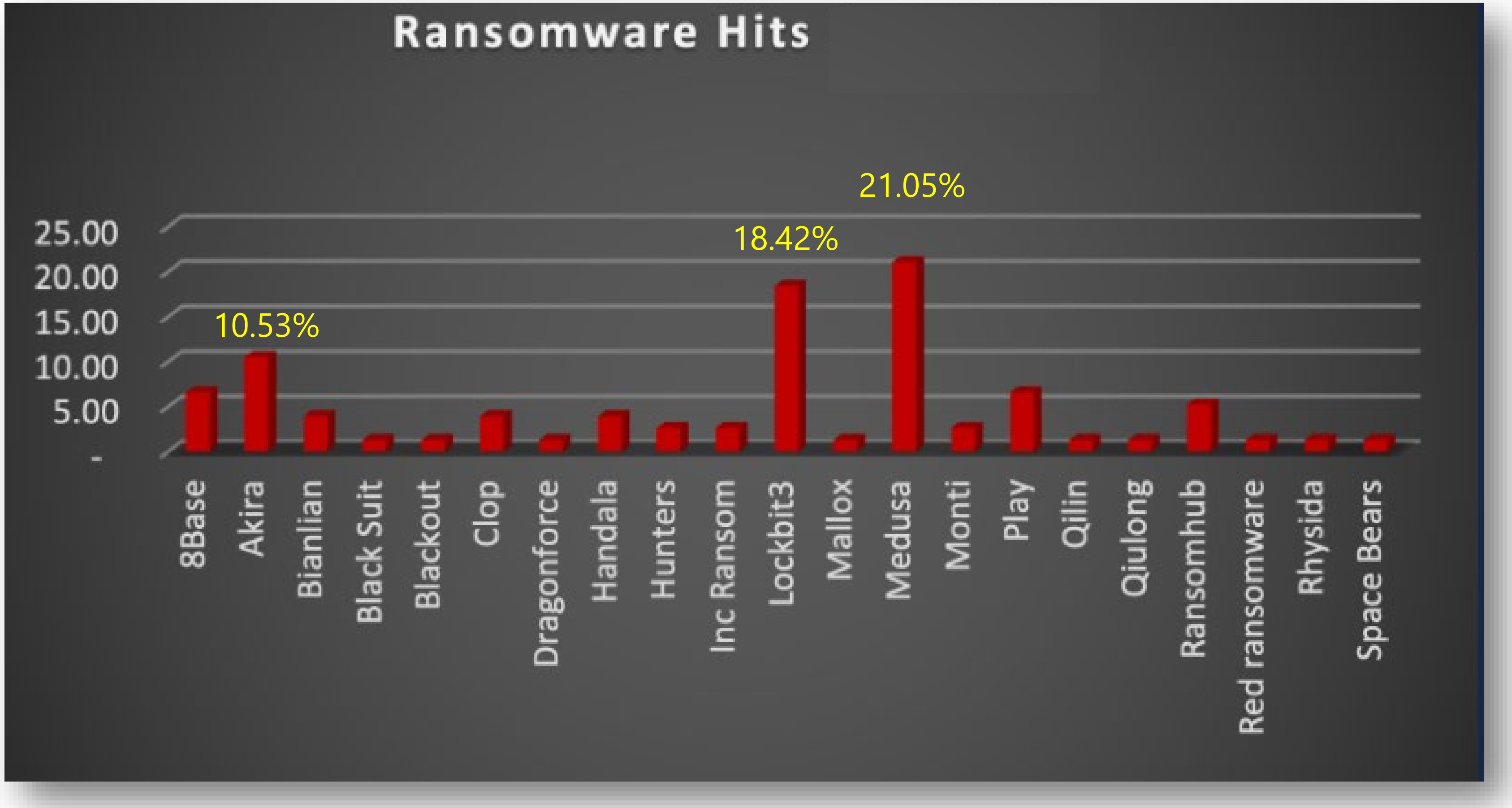
6 **Financial services**

Threat actors require methods of acquiring, transferring, and laundering money (usually cryptocurrencies) to cash out on their operations.

Reference: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

Ransomware

Ransomware groups - Global rankings
June 3, 2024



Reference: https://redpiranha.net/news/threat-intelligence-report-may-28-june-3-2024

Artificial Intelligence

How AI is Changing the Game

For Threat Actors

- Increase the efficacy of cyberattacks (DDoS)
- Enhancements to social engineering (phishing, voice, audio, etc.)
- Deepfake images trick biometric facial recognition systems
- Automating rudimentary processes, sending more realistic phishing emails
- Synthesize and execute complex malware
- Exponential scaling of attacks
- Corrupt existing AI tools, data poisoning

For Cybersecurity

- Accelerate threat detection and mitigation
- Expedite responses
- Identify vulnerabilities faster
- Protect user identities and datasets
- Provide cyber threat analysis and insights
- Enhanced threat intelligence and automation
- Simplifies reporting
- Helps fill the cybersecurity skills gap
- Reduce SOC burnout

References: https://www.ibm.com/ai-cybersecurity
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-design-ai-threat-report-v2.pdf
https://www.microsoft.com/en-ca/security/business/security-101/what-is-ai-for-cybersecurity

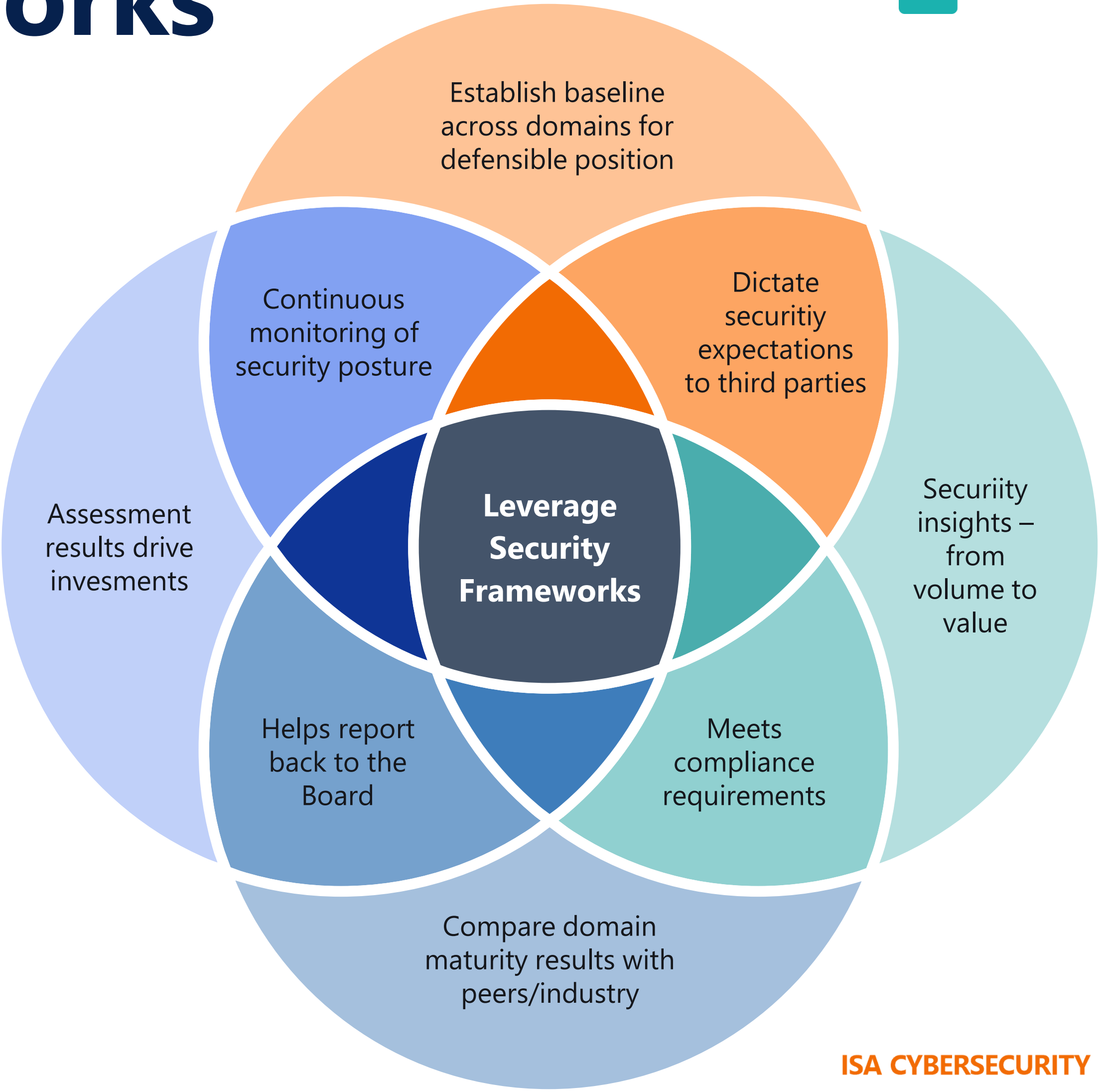
Cybersecurity Frameworks

isacybersecurity.com

ISA CYBERSECURITY

Cybersecurity Frameworks

- Choose a framework suitable to your needs. *One size doesn't fit all!*
- Cybersecurity framework is the backbone of enterprise security strategy and program
- Assessing controls:
  - Key controls are defined
  - Control owners are assigned
  - Control automation
  - Performance KPIs monitoring
  - Control coverage
  - People, process and technology alignment
- Drive remediation to closure – run as a program



Leverage Security Frameworks

Establish baseline across domains for defensible position

Continuous monitoring of security posture

Dictate securitiy expectations to third parties

Assessment results drive invesments

Securiity insights – from volume to value

Helps report back to the Board

Meets compliance requirements

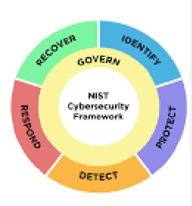
Compare domain maturity results with peers/industry

Cybersecurity Frameworks

The top three cybersecurity frameworks for building resilience against cyber threats.

CIS 18 Controls

CIS provides cybersecurity best practices and benchmarks.
Ideal for companies seeking to implement specific security controls in the short term.



NIST CSF 2.0

Provides tailored security measures based on risk tolerance.
Ideal for mature organizations seeking clear guidance on actionable steps to improve cybersecurity readiness.

ISO 27001

Designed as a compliance standard.
Used by organizations with more mature security and advanced risk.

Best Practices

isacybersecurity.com

ISA CYBERSECURITY

Top 15 Cybersecurity Best Practices

- Cybersecurity Assessment
- Endpoint Protection
- Password Policy
- Multi-factor Authentication (MFA)
- Email Security
- Cloud Security
- Virtual Private Network (VPN)
- Patch Management
- Data Encryption
- Backup & Test Critical Data
- Threat Monitoring (SOC)
- Security Awareness Training
- IR Plan & IR Retainer
- Risk Assessments
- Penetration Testing

Thank You!

Stay Safe!

ISA CYBERSECURITY