Haliburton, Kawartha, Pine Ridge District Health Unit

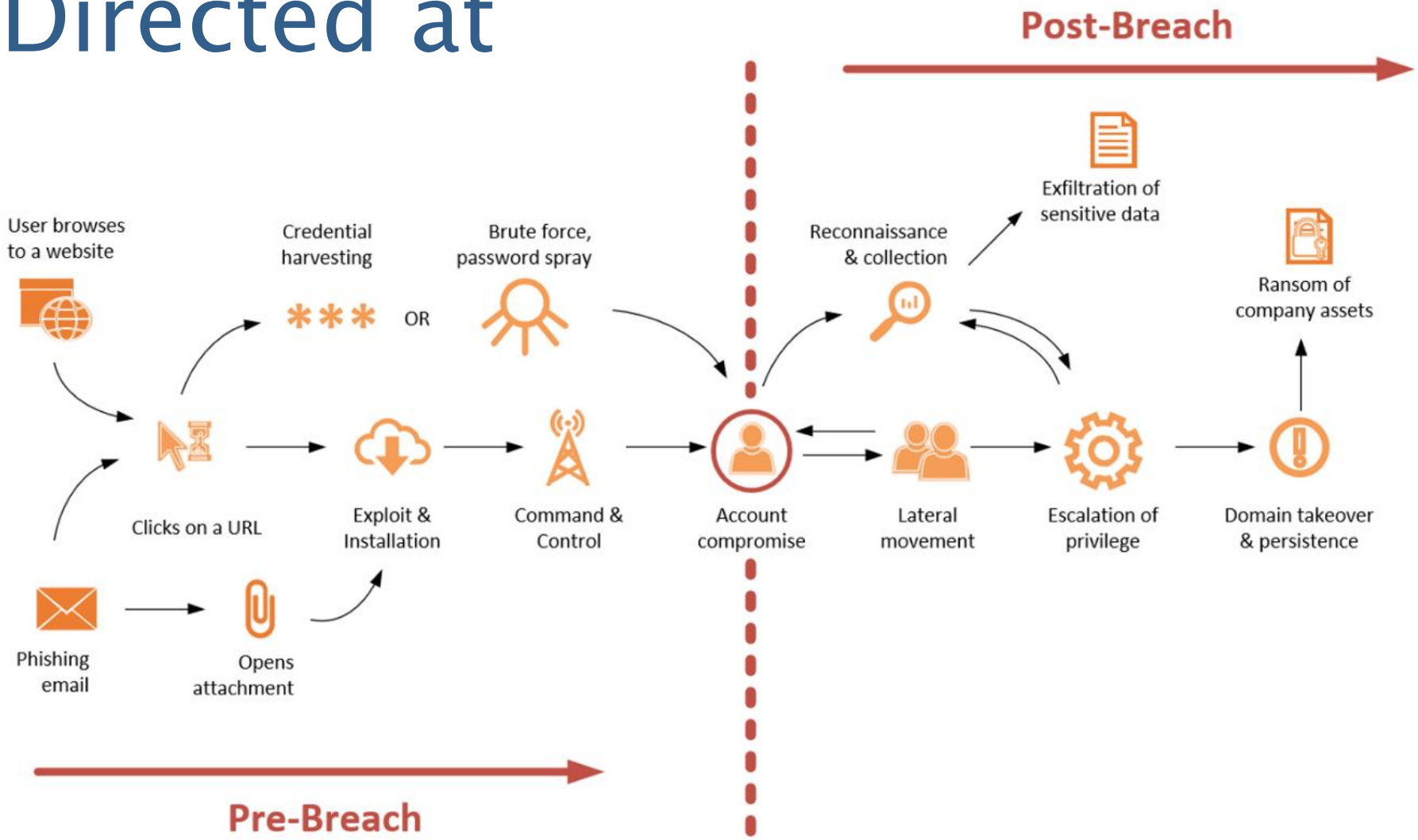
HKPR Security Posture

Matthew Vrooman

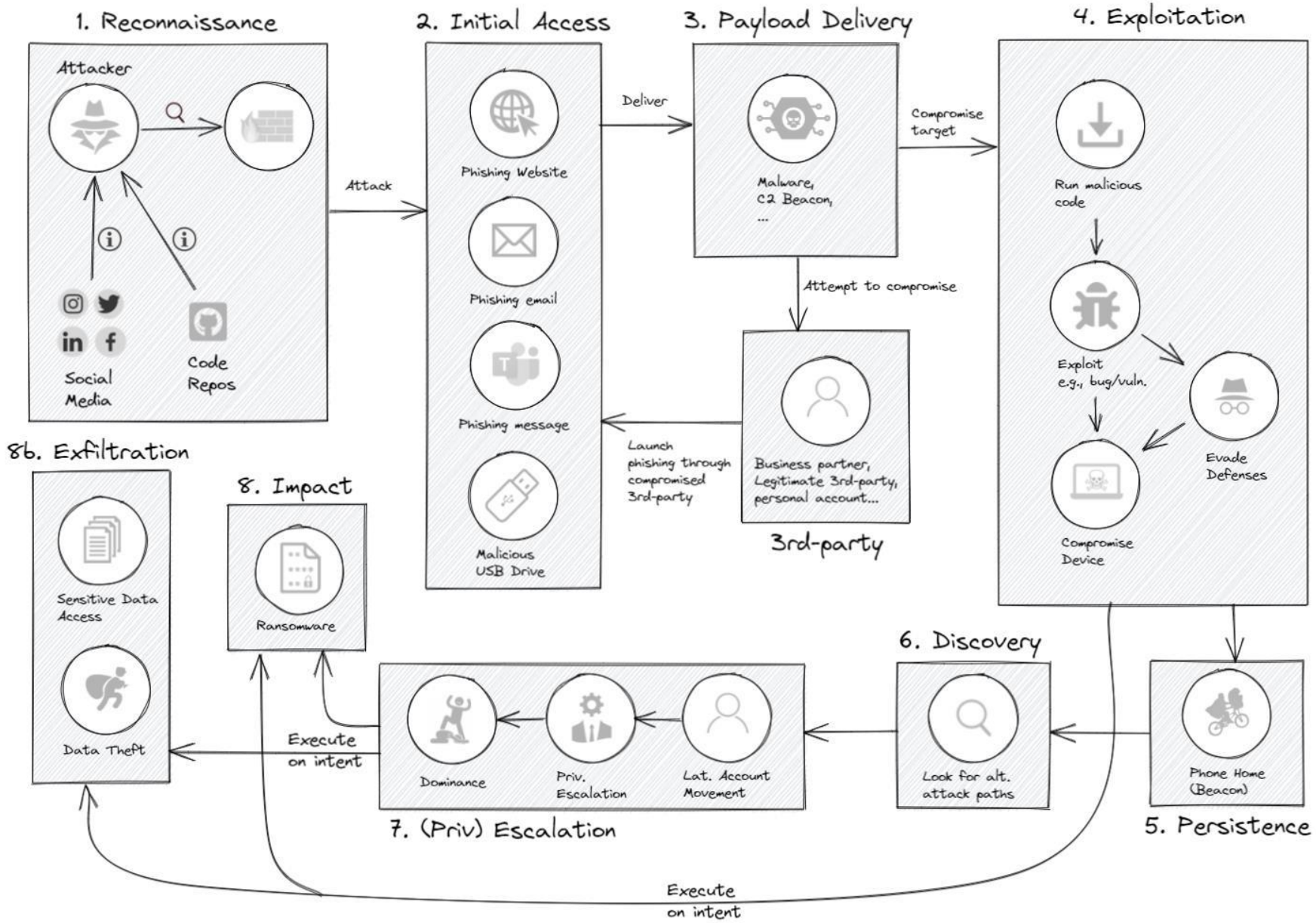
Director, Corporate Services

April 18, 2024

Anatomy of a Cyber Attack Directed at HKPR



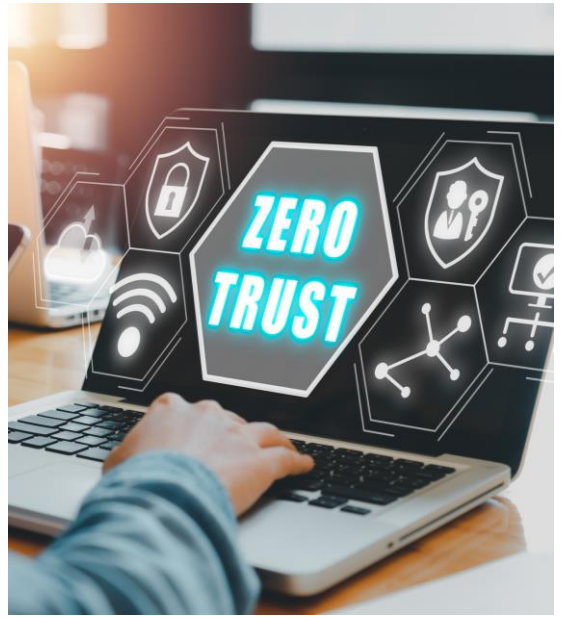
Anatomy of a Cyber Attack Planning the attack on HKPR



yourIT is Cybersecurity Centric

Zero Day Trust Model

- "Never Trust, always verify"
- A Zero Trust model is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction; asserts least-privilege access; and relies on intelligence, advanced detection, and real-time response to threats.
- The guiding principles of Zero Trust security are:
  - Verify explicitly.
  - Use the least-privilege access.
  - Assume breach.



yourIT is Cybersecurity Centric

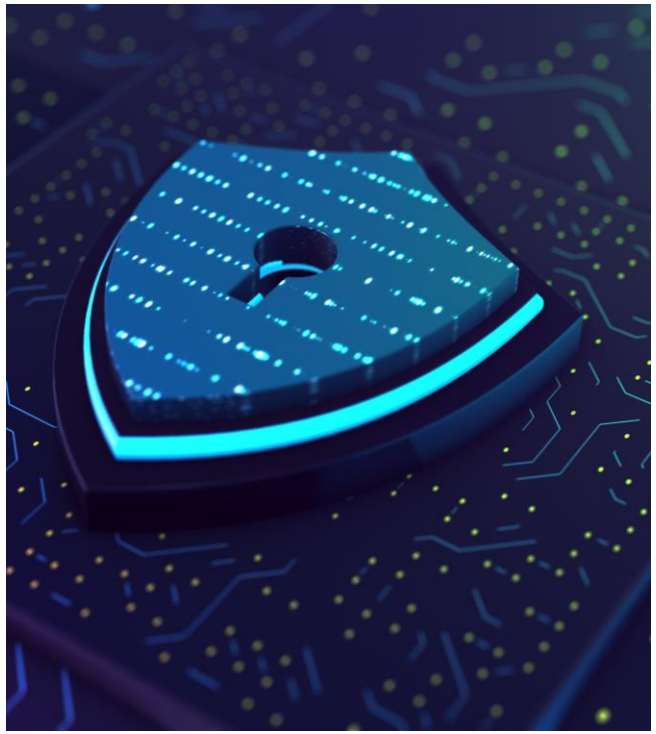
NIST Cybersecurity Framework (The National Institute of Standards and Technology)

- NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of industry, agencies, and the broader public.

yourIT is Cybersecurity Centric

The CIS Controls (Center for Internet Security)

- The CIS Controls™ is a set of security best practices that help businesses mitigate and protect themselves against the most common Cyber-Attacks and Threats out there.
- They were developed and are maintained by IT and Security Experts at the Center for Internet Security (CIS) and are recognized by Businesses and Governments globally.

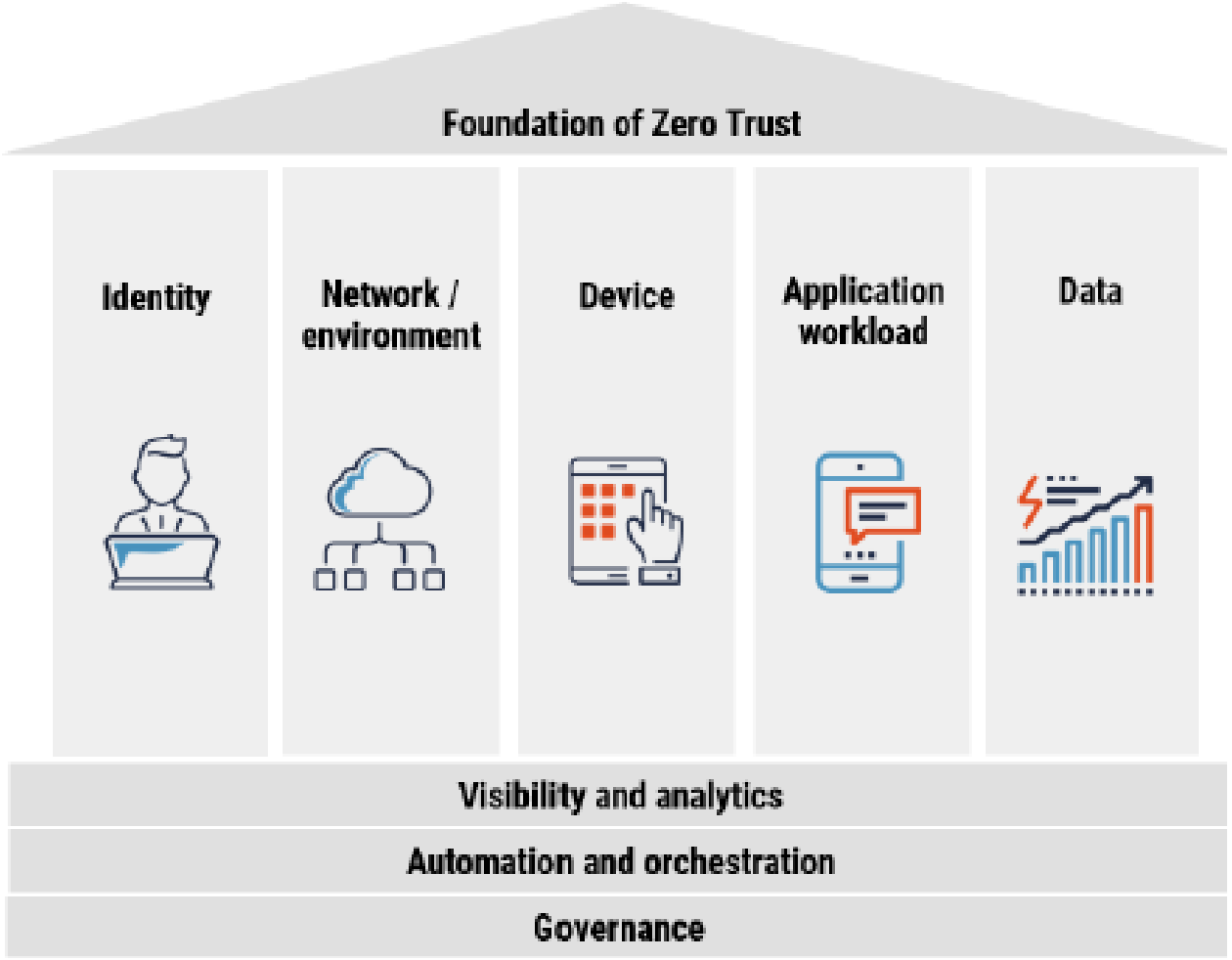


yourIT is Cybersecurity Centric

Canadian Centre for Cyber Security

- Canadian Government led Cybersecurity Guidance and Posture
- Part of the international Cybersecurity Groups that work on and develop the Model, Framework and Controls above.

Zero Trust Security Model (ZTSM)



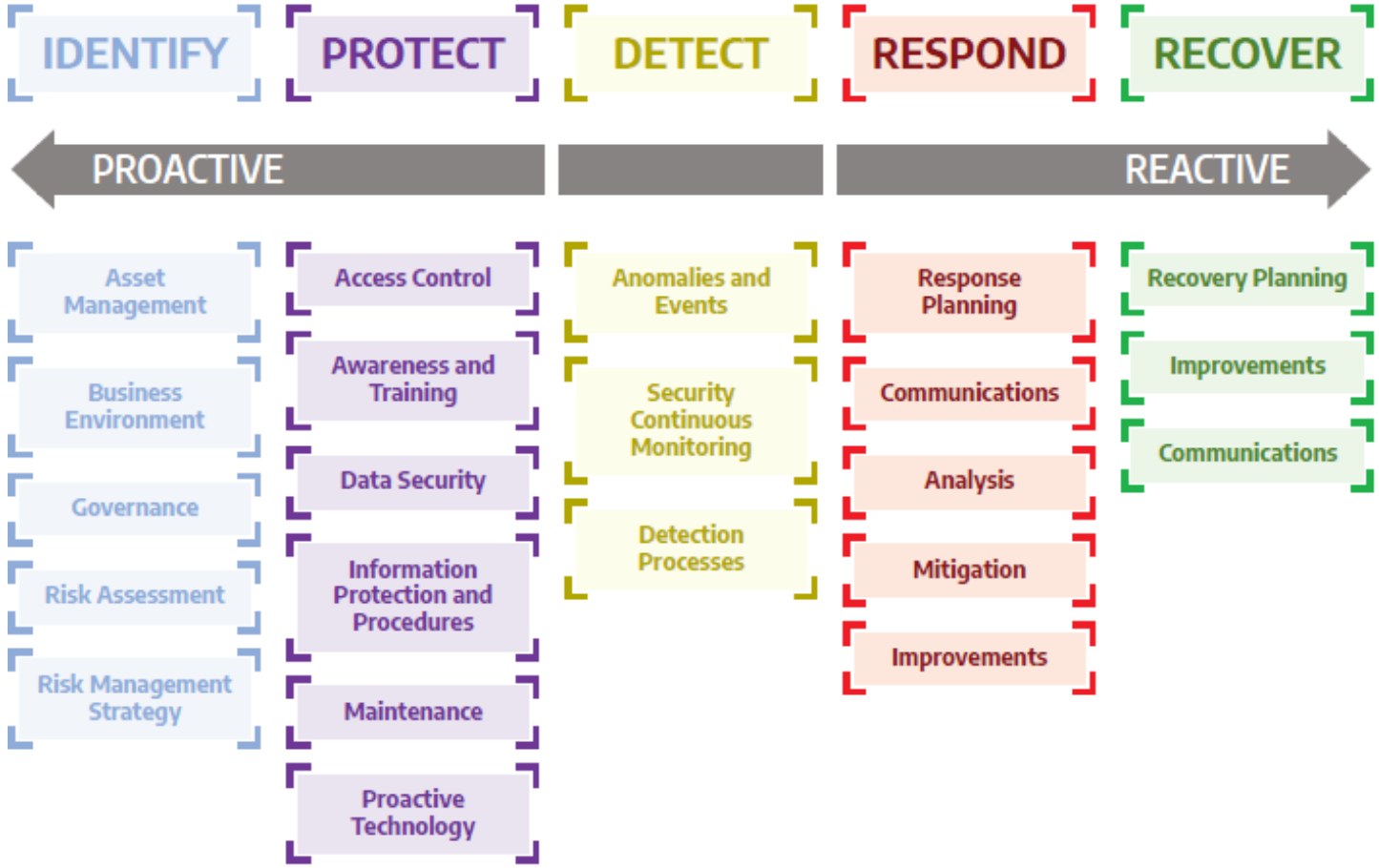
- Identity
- Network/Environment
- Device
- Application workload
- Data
- Visibility and analytics
- Automation and orchestration
- Governance

NIST Cybersecurity Framework

The NIST Cybersecurity Framework enables businesses and enterprises to evaluate the risks they encounter. The framework consists of three parts.

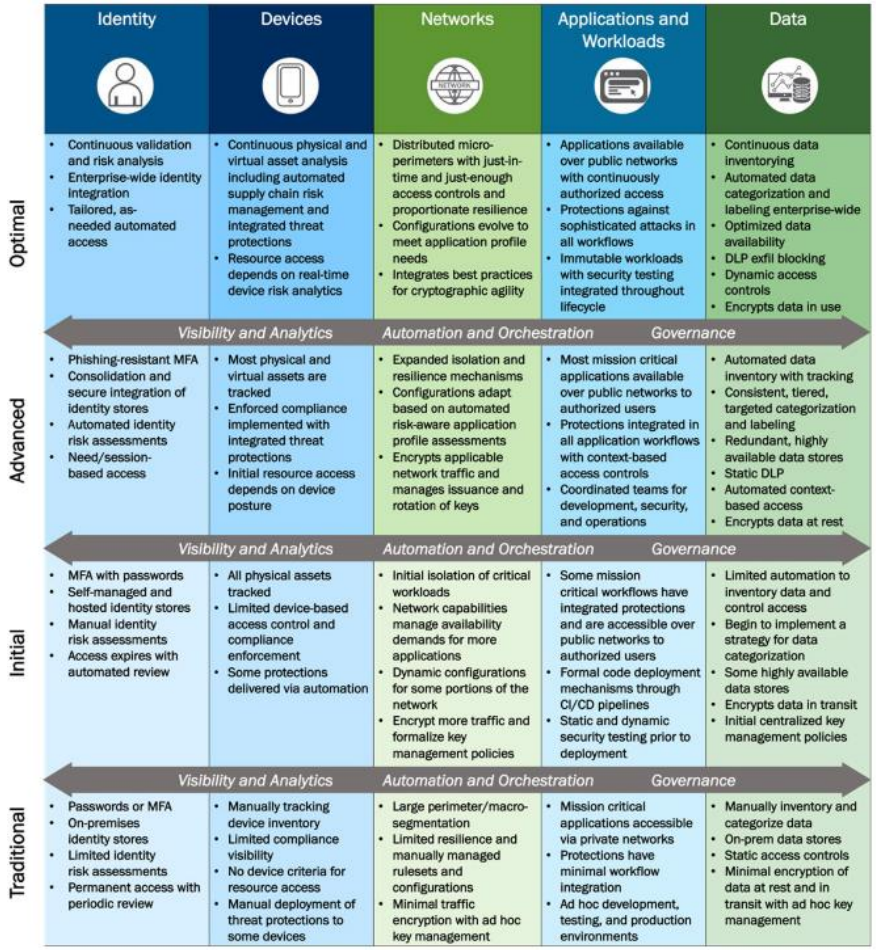
The Framework Core presents a range of references, outcomes, and activities associated with aspects and approaches to cyber defense. The Framework Implementation Tiers help organizations establish their approach to cybersecurity and clarify their stance to all stakeholders. The tier also portrays the degree of sophistication of the management approach. The Framework Profile contains a collection of outcomes the enterprise picked from the categories and subcategories based on its risk evaluation and requirements.

Organizations can create a "Current Profile" based on the framework that includes the cybersecurity activities and goals the company aims for. Then it can develop a "Target Profile" or go for a baseline profile that meets the organization's specific industry needs. Ultimately, the organization can craft actionable steps to achieve the target profile.



CIS Controls 18 Controls Observed

High-Level Zero Trust Maturity Model Overview



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

The Pillars

- Identity, Devices, Networks, Applications and Workloads, and Data.

Each pillar also includes general details

- Visibility and Analytics, Automation and Orchestration, and Governance

Visibility and Analytics:

- Observe & Analyze what is happening within each of the Pillars. The focus on cyber-related data analysis helps inform and build a risk profile to develop proactive security measures before an incident occurs.

Automation and Orchestration:

- Automated tools and workflows
- Maintaining oversight, security, and interaction of the development process for such functions, products, and services.

Governance:

- Enforcement of Cybersecurity policies, procedures, and processes, within and across pillars

The Basics

HKPR.ON.CA is Authoritative Identity Source (Identity Management)

- Microsoft 365 is where that identity source resides
- Onboarding & Offboarding & Access Control Centralized in M365

Only HKPR.ON.CA Users have access to

- Microsoft 365 Services (Email, SharePoint, Teams, M365 Apps, M365 housed data)

Only HKPR.ON.CA Registered Devices are allowed to access Microsoft 365 Services (Laptops & Mobile Devices)

The Basics

- HKPR.ON.CA Users and Devices only authorized access to HKPR Office Private Networks
- MFA with Passwords is mandatory
- All HKPR.ON.CA Data and Network Communications are Encrypted
  - At Rest, In Transit & In Use

The Basics

HKPR.ON.CA Security Services

- All Devices are encrypted.
- Location based: Canada & United States only allowed Countries to use HKPR Identity & Devices and access Microsoft 365 Services.
- No Unauthorized Devices are allowed to connect to HKPR Devices
  - USB/External Drives, Personal Printers
- All Wired and WIFI traffic is encrypted
- Each Network an HKPR.ON.CA Device connects to (Outside of HKPR Offices) is automatically “scanning” for active threats and alerts on that network.

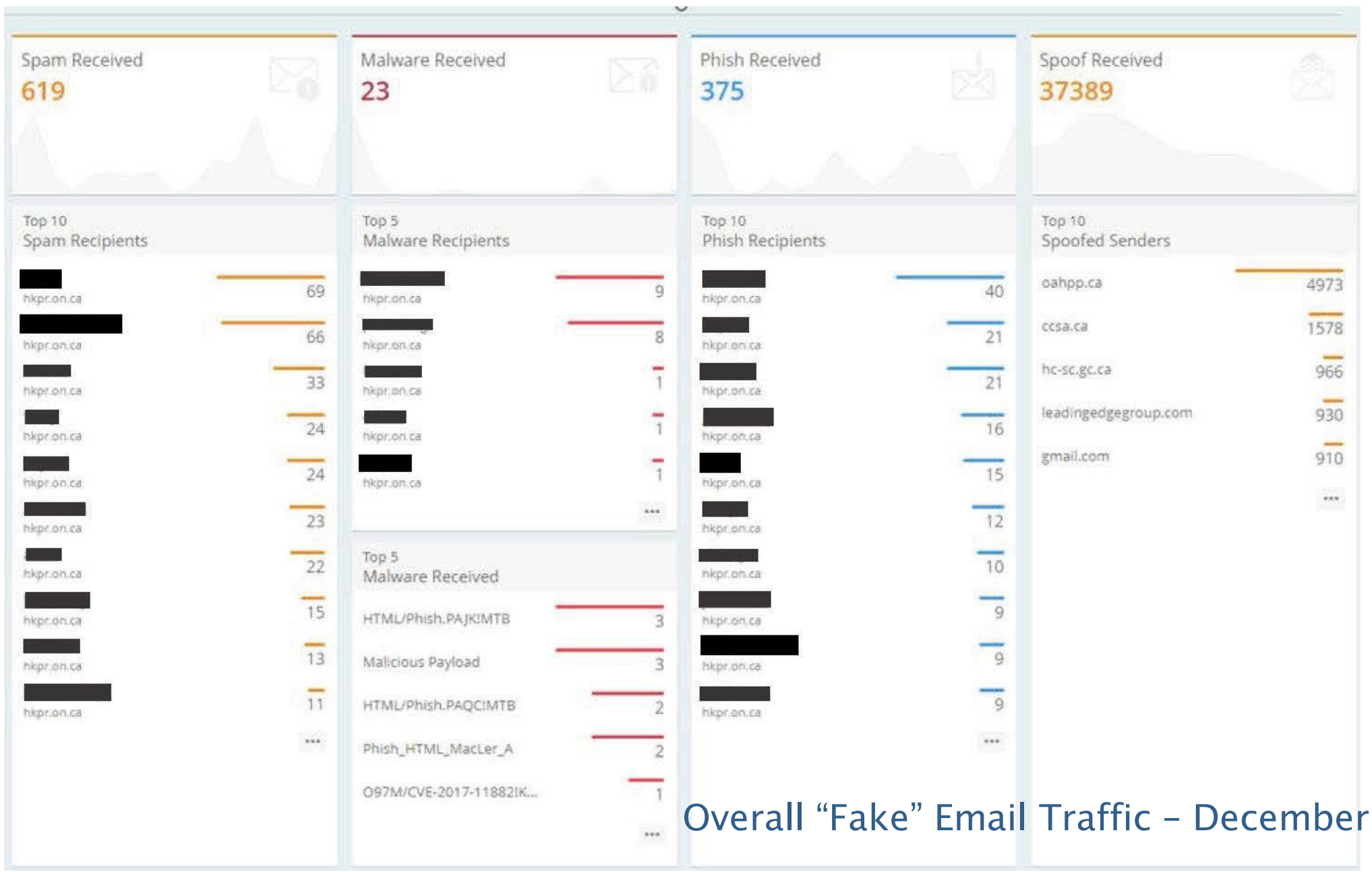
The Basics

HKPR.ON.CA Security Services

- "Nothing is deleted until verified by backup"
  - 90 days earliest purge of deleted items
    - Users see it's deleted but it is still there for 90 days to ensure it is backed up.
- Microsoft 365 Services Data Backed Up every 4 hours
- SharePoint, OneDrive & Teams Document "Revision History" for a minimum of 500 revisions, each backed up separately.

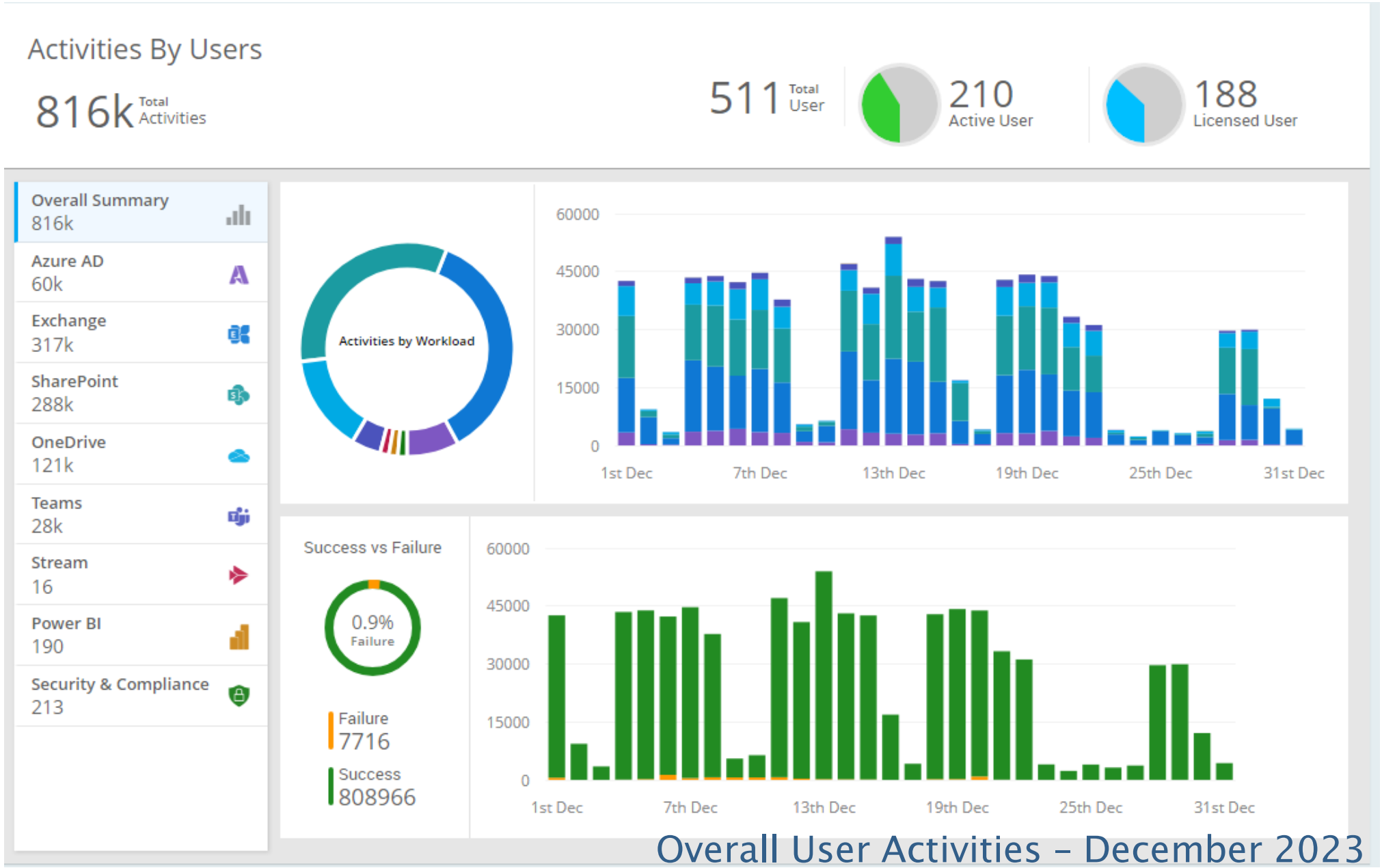
3rd Party Services brought into ZTM

- 3rd Party Services setup with SSO and Auto Provisioning with HKPR Microsoft 365
  - Require M365 HKPR.ON.CA User Identity & Devices
  - RingCentral
    - Need HKPR.ON.CA User Identity & Device (Access Control)
    - If not member of RINGCENTRAL USERS group can't access (Access Control / Onboarding & Offboarding)
  - Online Microsoft Training
    - Need HKPR.ON.CA User Identity & Device (Access Control)
    - All HKPR Users have access by default (Onboarding & Offboarding)
  - HKPR.ON.CA Website
    - Need HKPR.ON.CA User Identity & Device (Access Control)
    - HKPR Users Onboarding & Offboarding managed by Communications Department

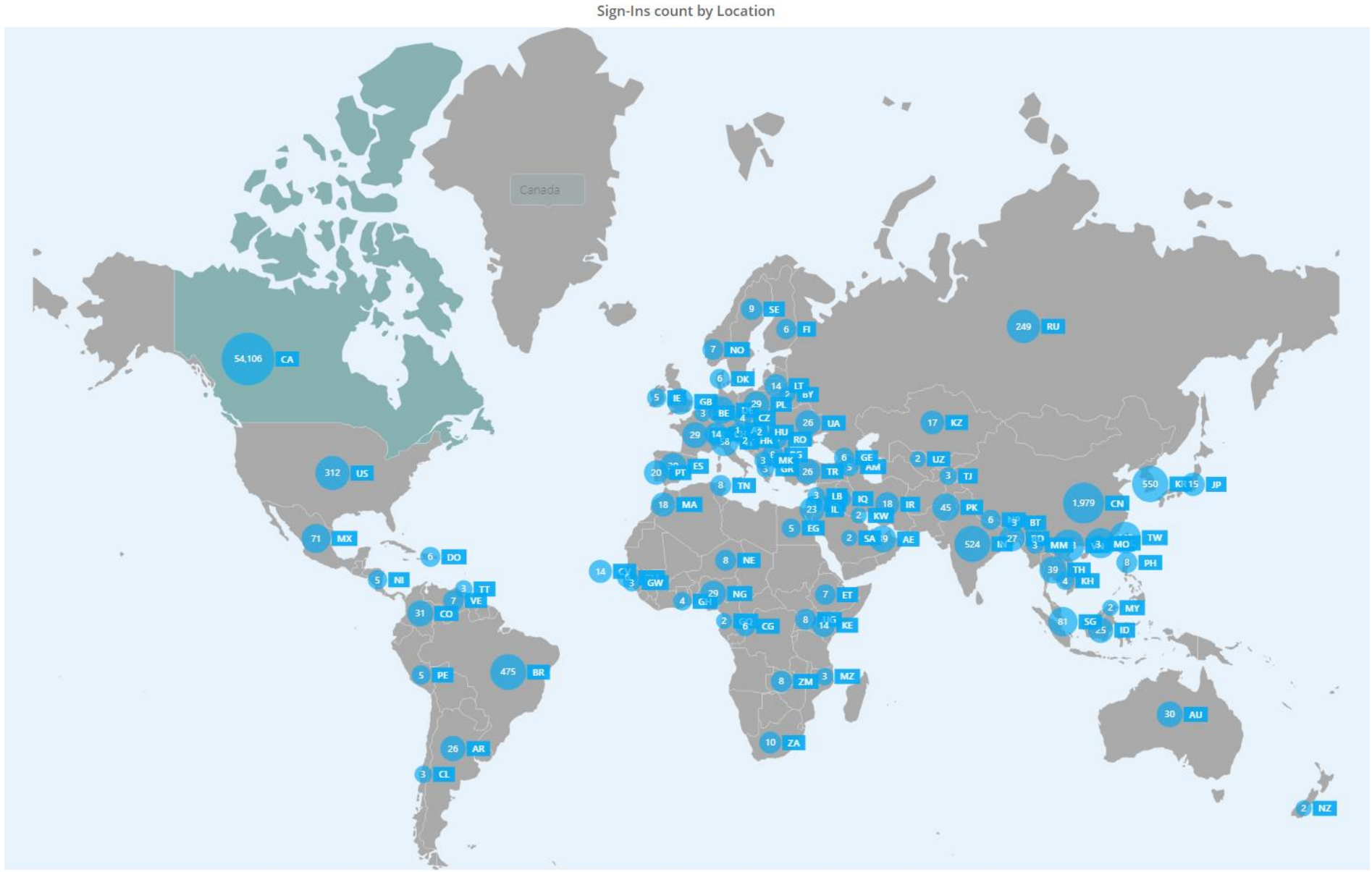


Overall “Fake” Email Traffic – December 2023

User Email Activity – December 2023



Overall User Activities – December 2023



HKPR Sign-Ins by Country – December 2023

Haliburton, Kawartha, Pine Ridge District Health Unit

Healthy People - Healthy Communities

Reach Out to Us

1-866-888-4577

info@hkpr.on.ca

hkpr.on.ca

Lead Partner Deliver

OUR VALUES • TRUST • ENGAGEMENT • ACCOUNTABILITY • LEADERSHIP