Cybersecurity at CCTG and Queen’s University

Canada Foundation for Innovation
2021 Major Science Initiatives Workshop
March 18, 2021

Lam Pho
Chief Information Officer
Mission

To Develop and Conduct Clinical Trials Aimed at Improving the Treatment and Prevention of Cancer, with the Ultimate Goal of Reducing Morbidity and Mortality from this Disease
EXTENSIVE NETWORK | LEADING ACADEMIC CENTERS

- Operations and statistical centre at Queen’s University
- >85 Canadian institutions
- >600 international centres | 40 countries | 6 continents
- Only Ex-US Recognized group member of the NIH-NCI National Cancer Clinical Trial Network

IMPACT

- > 80,000 patients enrolled | 1,500-3,000 patients/year
- >508 trials ongoing or completed
- >2000 publications
- New standards of care, diagnostics, drug approvals, methods

CAPACITY

- > 150 trials running concurrently

CORRELATIVE RESEARCH / BIO-BANKING FACILITIES

- >400,000 specimens
- From 120 trials and >24,000 trial patients
- Blood, plasma, serum + buffy coat, RBC pellets, DNA, RNA
Canadian Cancer Trials Group

National Network linked to international partners

Scientific Leadership

Network Centres and Partners

Scientific Programs to support phase 1-3 trials

Oversight, scientific and supportive committees

Operations & Statistics Centre at Queen’s U

Faculty Clinicians, Statisticians, Epidemiologists

Trial Coordination & Conduct

Compliance & Oversight

Information Technology

Admin & Finance

Strategy & Partnerships

Tumour Banking
CCTG ORGANIZATION

1. Breast
2. GI
3. GU
4. Gyne
5. Hematology
6. Lung
7. Symptom Control

Scientific Committees
- Disease Sites
- Rare Cancers
- IND Program
- Endpoints

Oversight Committees
- Clinical Trials
- Data Safety Monitoring
- Strategic Executive Advisory

Support Committees
- CRA
- Pharmacy
- Auditing Monitoring
- Lay/Patient
- Centre Representative
- RTQA

> 85 member sites and 1500 Canadian Investigators
Operations and Statistics Centre at Queen’s (130 Staff & 12 Faculty)
All Canadian adult and pediatric hospitals able to conduct trials (Cancer). All have 5 year multistudy agreements (not cancer trial specific).
Since 1980 International collaboration with >40 countries with academic groups and sites
Since 2010, 50% of trials involve one or more international group or site
2010 – 2016 collaborating with > 25 countries across trials and > 700 sites
Considerations for Implementing Cybersecurity Programs

- Cybersecurity program focuses on foundational decisions about organizational mission alignment, governance, resources, and controls

- Does my organization need its own Cybersecurity Program?
  - Stand-alone
  - Unit of larger organization (i.e. CCTG is an unit of a large organization which is Queen’s University)
    - Very large and complex on its own?
    - Face cyber threats that are different from the larger organization?
    - Have stakeholders and cybersecurity obligations that are distinctive from the larger organization?
    - Have a distinct set of users or suppliers significantly different than the larger organization?
    - Have leadership roles with significant autonomy or discretion in terms of risk taking, budget, hiring, business development, and/or procurement?
    - Does the larger organization’s baseline control set and implementation clash with the unit’s mission?
    - Is the unit’s mission highly distinctive in some other way that warrants special attention and may be outside the standard operations for the majority of the rest of the business?
  - For more details - Appendix A of Trusted CI Framework Implementation Guide

- If your organization is part of larger organization:
  - “Get to know” large organization’s CIO, CISO, CTO, Strategy & Architecture Director
  - Be part of the larger organization’s cybersecurity committees/initiatives:
    - Member of Queen’s University Enterprise Information Technology Advisory Committee (EITAC) and Change Advocate Group
The Path to Cybersecurity for small and medium organizations

• Recommended path for

  1. Baseline Cybersecurity Controls for Small and Medium Organizations

  2. Canadian Centre for Cyber Security (CCCS) Top 10 IT Security Actions
     • https://cyber.gc.ca/en/top-10-it-security-actions

• Other comprehensive Enterprise Cybersecurity Frameworks – large organizations

  3. NIST CSF (National Institute of Standards and Technology Cybersecurity Framework)
  4. ISO/IEC 27001 (International Organization for Standardization/International Electrotechnical Commission)
  5. NIST 800-53, ITSG-33

• Highly recommend to look at the Trusted CI Framework Implementation Guide
  • https://www.trustedci.org/framework
Baseline Controls for Small and Medium Organizations

- Have an incident response plan
- Securely configure devices
- Enable security software
- Use strong user authentication
- Provide employee awareness and training
- Backup and encrypt data
- Secure mobility
- Establish perimeter defenses
- Secure outsourced IT services
- Secure websites
- Have access control & authorization
- Secure portable media
CCCS Top 10 IT Security Actions

PROTECT YOUR NETWORK, PROTECT CANADA’S INFORMATION.

The Top 10 IT Security Actions were selected and prioritized based on CSE’s analysis of cyber threat trends affecting Government of Canada (GC) Internet-connected networks. When implemented as a set, the Top 10 helps minimize intrusions or the impact to a network if a successful cyber intrusion occurs.

cyber.gc.ca

THREAT SURFACE BEFORE THE TOP 10

1. USE SHARED SERVICES CANADA INTERNET GATEWAYS
2. PATCH OPERATING SYSTEMS AND APPLICATIONS
3. ENFORCE THE MANAGEMENT OF ADMINISTRATIVE PRIVILEGES
4. HARDEN OPERATING SYSTEMS
5. SEGMENT AND SEPARATE INFORMATION
6. PROVIDE TAILORED AWARENESS AND TRAINING
7. MANAGE DEVICES AT THE ENTERPRISE LEVEL
8. APPLY PROTECTION AT THE HOST LEVEL
9. ISOLATE WEB-FACING APPLICATIONS
10. IMPLEMENT APPLICATION ALLOW LISTS

THREAT SURFACE AFTER THE TOP 10
Implementing Cybersecurity at Queen’s and CCTG

- Cybersecurity Education & Awareness Training
- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Endpoint Protection Platform (EPP)
- Vulnerability Scanner
- Network Intrusion Detection System
- Data Protection (@CCTG): Encryption-at-Rest, Encryption-in-Flight
- Firewalls (Palo Alto, Wildfire)
Real-Time Monitoring

Queen’s U - Azure Cloud

CCTG Network

Queen’s U - On Prem Data Center

Specifications and Notes

Azure Resources
- Qdradon Container: 50/100 - $42/85 per month
- 14 4CPUs
- 13 8GB RAM
- 1 TB SSD drive
- 1 TB HDD drive
- Azure Event Flow Processor: S4E4: $3.49 per month
- 14 4CPU
- 13 8GB RAM
- 1 TB SSD drive
- Upgrade existing VMs from 4GB steps to 1.5GB
- Azure Event Hub
- 1 - 2S5 in ingress and throughput usage per month

On Prem Resources
- Log/Event Collectors: Large
  - 1x 4CPU
  - 13 8GB RAM
  - 1TB SSD drive
  - Additional 1TB SSD drive or logs - 1St-25K EPS
- Log/Event Collectors: Medium
  - 1x 4CPU
  - 13 8GB RAM
  - 1TB SSD drive
  - 1TB HDD drive
  - Additional 1TB SSD drive or logs - 5k EPS
- Log/Event Collectors: Small
  - 2x 4CPU
  - 13 8GB RAM
  - 1TB HDD drive
  - 1TB SSD drive
  - Additional 1TB SSD drive or logs - 1k EPS

Solution Notes
- EC to EP connections are encrypted and compressed and data limits can be placed on traffic connections
- EC’s can be added as needed for additional collection or for more restricted environments.
- WIN-64 GB for storage and no retention policies should be able to hold 6 months worth of data compressed
- Additional 1TB SSD can be added to the EPs OS, VM or via external managed mode operating on Data factory or EDRs

On premise is Azure bandwidth for logs estimated to be 10GB max. Realize compression. If not, it’s proposed to upgrade Azure Site to Site VPN.

Connects to the main GUI interface, isolation API endpoint, and add on app location.
- EDRs offline data is stored and searched as well as real-time and historical connection records.
- EC’s usage or collection data, normalized storage and stripping can be monitored.
- ECs can buffer logs to local storage where VMs booted down or EP down - local disk capacity the only limit
The Cybersecurity Incident Response Plan

IT Services is launching a revised Cybersecurity Incident Response Plan (CIRP) to improve its effectiveness, alignment, and cohesiveness. The CIRP describes the process Queen’s follows to prepare for and respond to a cybersecurity event. The CIRP defines the roles, responsibilities, authorities, and tasks associated with each phase of a security incident to ensure a coordinated and effective response. The CIRP is intended to be referenced by all stakeholders identified as having a role in cybersecurity incident response.

The CIRP
Provides the foundation for responding to security incidents and the playbook development

Workshops
Conducted with three targeted groups to leverage their input to develop and fine-tune the playbooks

Playbooks
Developed by reviewing existing incident response documents and leveraging workshop outputs

ServiceNow
Implementation of playbooks into ServiceNow to enable relevant stakeholders to take necessary action

Tabletop Exercises
To simulate the incident response plan and playbooks

Benefits
- Increase visibility and awareness of security incidents by offering a common University-wide platform (ServiceNow)
- Improve response to incidents by developing standardised and actionable steps to contain an incident and appropriately escalate and delegate incident response actions
- Enhance communication by developing templates to notify the appropriate internal and external stakeholders in the event of a security incident
A series of workshops will be conducted with three targeted stakeholder groups, and their input will be leveraged to develop the seven playbooks implemented in ServiceNow.

### The Workshops

**Core**  
*Key group of stakeholders*

- Understand Queen’s current state; how security incidents are categorized and escalated, and the notification process for internal and external stakeholders
- Outputs used to build the playbooks

**Action**  
*Departmental IT units*

- Socialize the playbooks with a wider audience of incident responders, ensuring the playbooks cater to the needs of the campus community
- Outputs used to modify the playbooks

**Awareness**  
*Business and IT areas*

- Inform individuals at a high level of the streamlined approach to incident response and playbook execution at Queen’s
- Town hall-style touchpoint with open Q&A
The Playbooks

The playbook scenarios are being designed and developed in two waves. The playbooks will outline the appropriate roles, responsibilities, and actions required when responding to seven types of threat scenarios. The implementation of these playbooks in ServiceNow will enable departments to get hands on access to the playbooks and escalation tools.

<table>
<thead>
<tr>
<th>Wave 1</th>
<th>Wave 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spear Phishing</strong></td>
<td><strong>Unauthorized Access</strong></td>
</tr>
<tr>
<td>In the event that a threat actor sends an email specifically targeting a Queen’s employee to acquire sensitive data from the individual.</td>
<td>In the event that an individual (internal or external) has gained access without permission to sensitive Queen’s systems.</td>
</tr>
<tr>
<td></td>
<td><strong>Web Application Compromise</strong></td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>In the event that a threat actor has compromised/is attempting to compromise a flaw or weakness in a web-based application that belongs to Queen’s or is hosted on Queen’s infrastructure.</td>
</tr>
<tr>
<td>In the event that a malicious program is inserted into a Queen’s system with the intent of compromising the confidentiality, integrity, or availability of data and applications.</td>
<td></td>
</tr>
<tr>
<td><strong>Ransomware</strong></td>
<td><strong>Data Breach</strong></td>
</tr>
<tr>
<td>In the event that a computer system at Queen’s is infected by a ransomware. Ransomware is a type of malware that encrypts files on a computer and makes them inaccessible to the user, unless a ransom is paid to the threat actor.</td>
<td>In the event that a threat actor has compromised and potentially exfiltrated sensitive data from Queen’s systems.</td>
</tr>
<tr>
<td></td>
<td><strong>Distributed Denial of Service (DDoS)</strong></td>
</tr>
<tr>
<td></td>
<td>In the event that a threat actor prevents authorized access to Queen’s resources and delays time-critical operations through the coordinated disruption of services by various attacking systems.</td>
</tr>
</tbody>
</table>
Thank You