BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

How to Skillfully Improve Your Security Posture with Existing Microsoft 365 Resources & Internal Staff

Selkirk College

STEEVES AND ASSOCIATES

Our Presenters

MARCO BIERMANN
IT Manager
Selkirk College

ED HARGRAVE
Security Practice Leader
Steeves and Associates

CRYSTAL LEBLANC
Infrastructure Development and Support Tier II
Selkirk College

BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

About Selkirk College

- Founded in 1966
- 9 geographically distanced campus (30 min – 4 hours drive)
- Over 2,000 student FTE 2023/2024
- High speed WAN campus interconnect
- Complex legacy infrastructure
- Thriving research department
- Programs ranging from Digital Fabrication to Blacksmithing

BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

Challenges

- Small IT team
- Ever-expanding infrastructure needs
- New technology, new unknown challenges
- Covid!

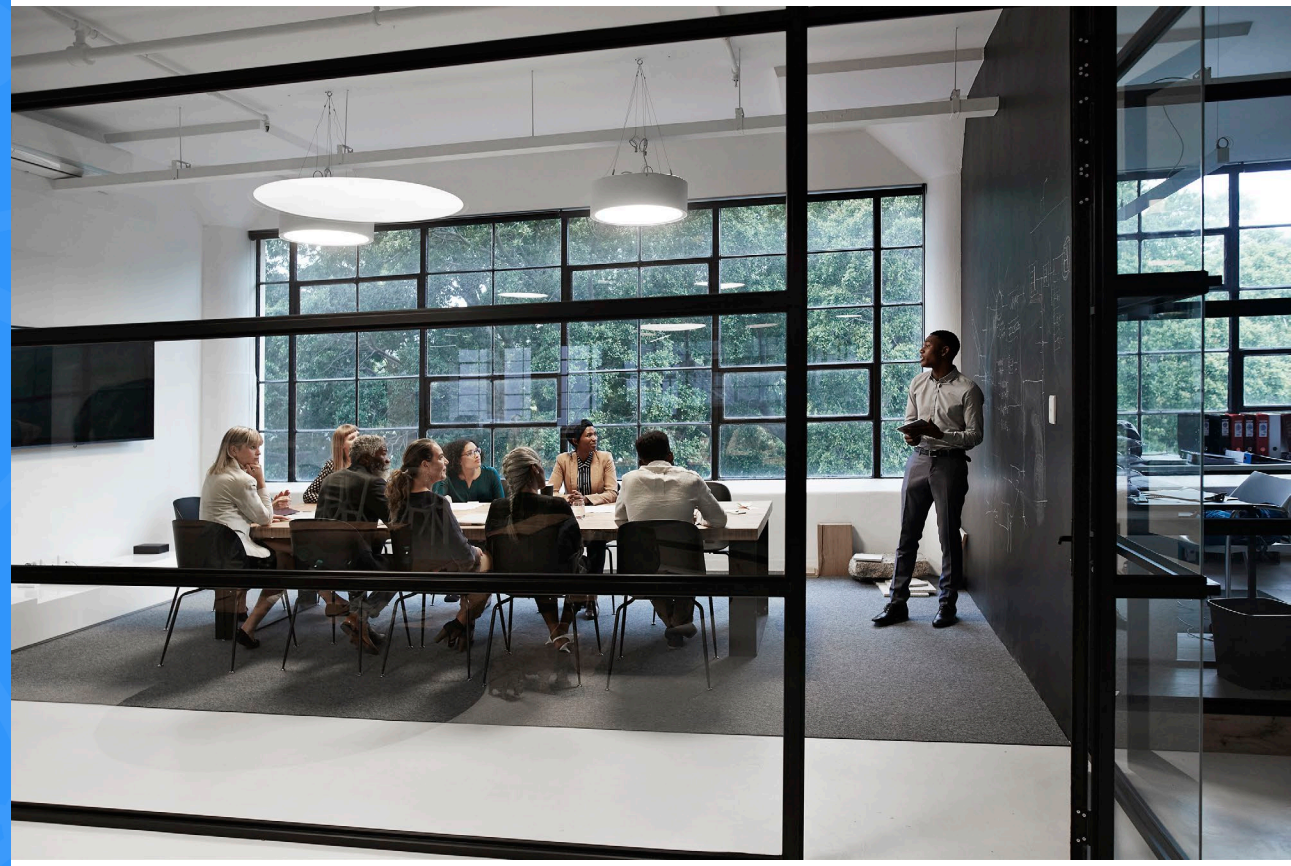
BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

Our approach

- Formally assess your current state
- Train staff to fill in skill gaps
- Practice good operational hygiene
- Set aside time for security activities
- Know what to do if something bad happens
- Don't try to do it all yourself



BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

Formal Assessment

- Takes “opinion” out of the equation
- Allows you to track progress
- Informed exceptions are OK
- Revisit exceptions on a regular basis

Microsoft Funded Workshops

- Endpoint Management and Security
- Microsoft Secure Identities & Access
- Defend Against Threats with Security Incident & Event Management (SIEM) Plus XDR
- Investigate & Respond to Risky Behavior
- Microsoft 365 Protect & Govern Sensitive Data
- Mitigate Compliance & Privacy Risks
- Microsoft Purview Portfolio

Microsoft Security

Threat Protection Workshop

Findings and Recommendations

Ed Hargrave
Steeves and Associates
December 9th 2021

BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

CIS Control and Benchmarks

CIS Critical Controls® Version 8

18 top-level best practices containing 153 prioritized safeguards

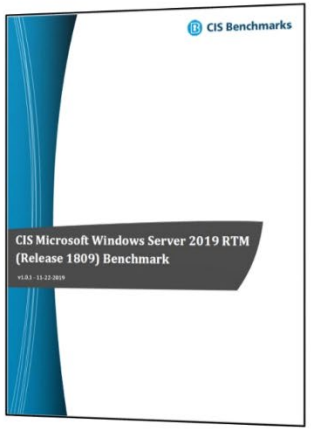
CONTROL 01 Inventory and Control of Enterprise Assets	CONTROL 02 Inventory and Control of Software Assets	CONTROL 03 Data Protection
CONTROL 04 Secure Configuration of Enterprise Assets and Software	CONTROL 05 Account Management	CONTROL 06 Access Control Management
CONTROL 07 Continuous Vulnerability Management	CONTROL 08 Audit Log Management	CONTROL 09 Email and Web Browser Protections
CONTROL 10 Malware Defenses	CONTROL 11 Data Recovery	CONTROL 12 Network Infrastructure Management
CONTROL 13 Network Monitoring and Defense	CONTROL 14 Security Awareness and Skills Training	CONTROL 15 Service Provider Management
CONTROL 16 Applications Software Security	CONTROL 17 Incident Response Management	CONTROL 18 Penetration Testing

CIS Benchmarks

Consensus-developed secure configuration guidelines

- **100+ CIS Benchmarks**
- **Covering 25+ vendor product families**
  - Operating Systems, Server Software, Cloud Providers, Network Devices, Desktop Software
- **Recognized by industry frameworks**
  - FISMA, FedRAMP, PCI
- **Community developed**
  - CIS members, subject matter experts, security community experts, and technology vendors
- **Map to CIS Critical Controls**

CIS Benchmarks™



BCNET CONNECT

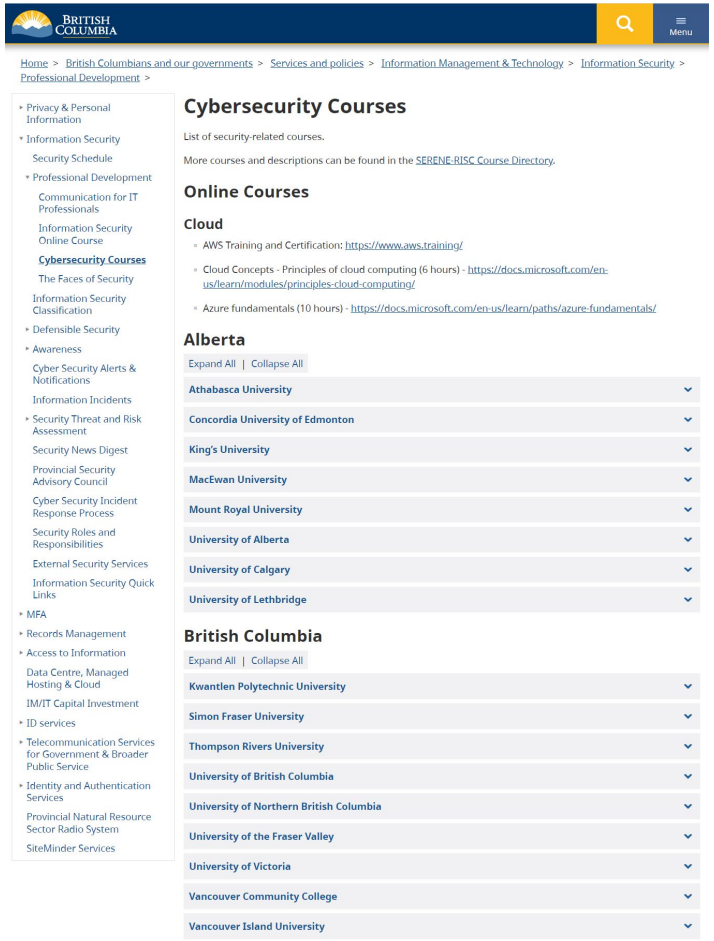
Selkirk College

STEEVES AND ASSOCIATES

Train your staff to fill in skills gaps

- There are training resources available for every learning style.
- In addition to general awareness training, make sure you include role specific training for ***IT staff*** and ***developers***
- Continue to mentor IT staff on an ongoing basis

Province of BC Cyber Security Courses



BCNET CONNECT

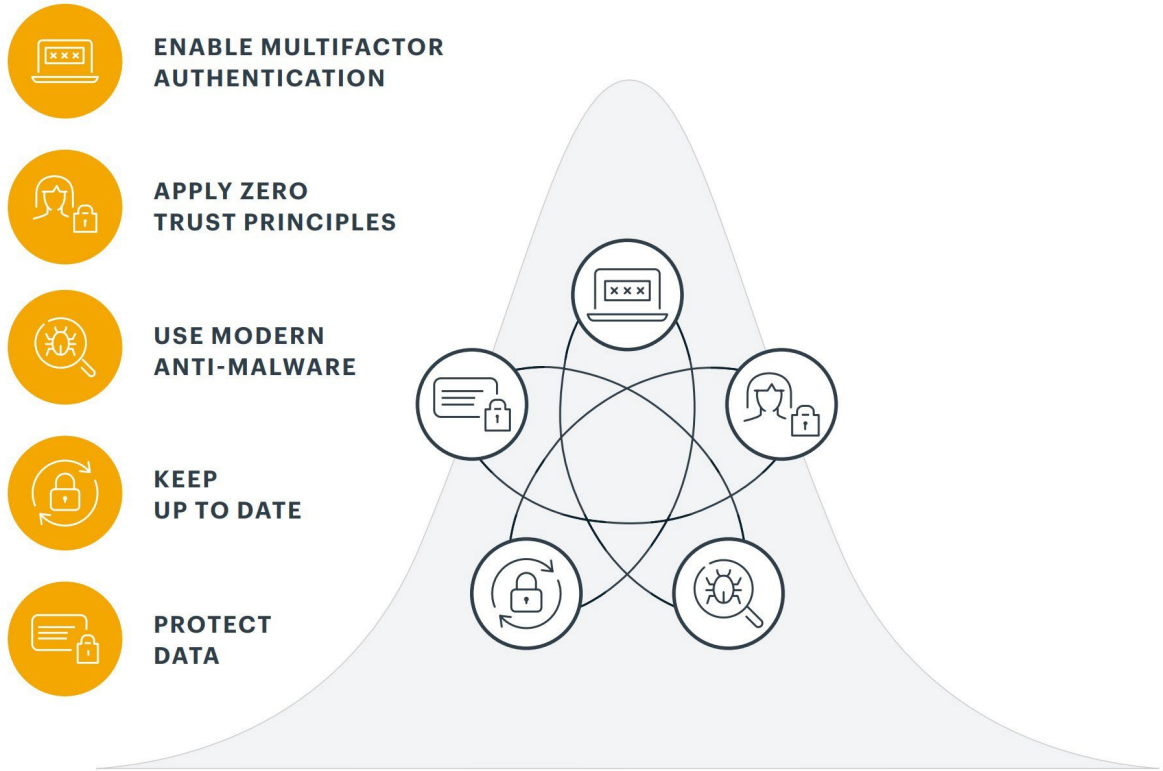
Selkirk College

cira

STEEVES AND ASSOCIATES

Practice good operational hygiene

- Know what you have
- Keep it up to date
- Configure it appropriately
- Control access to it
- Perform regular backups
- Know what normal looks like
- Know what to do if something bad happens
- Rinse and Repeat



Basic security hygiene still protects against 98% of attacks

Microsoft, Microsoft Digital Defense Report 2022.

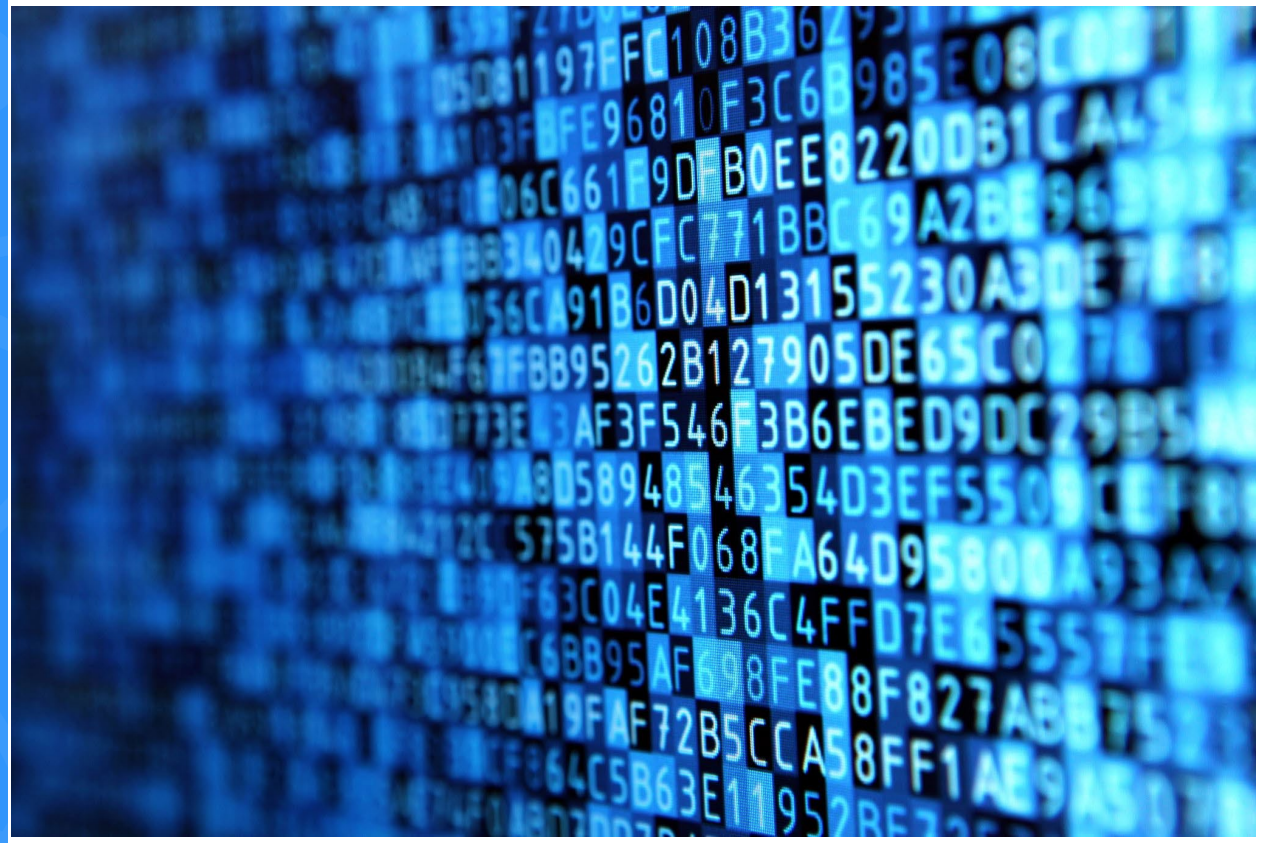
BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

Carve out time for security activities

- We all have day jobs but…..
- Regularly review output from tools
- Resolve events
- Provide management useful data
- Bring the team together weekly to review



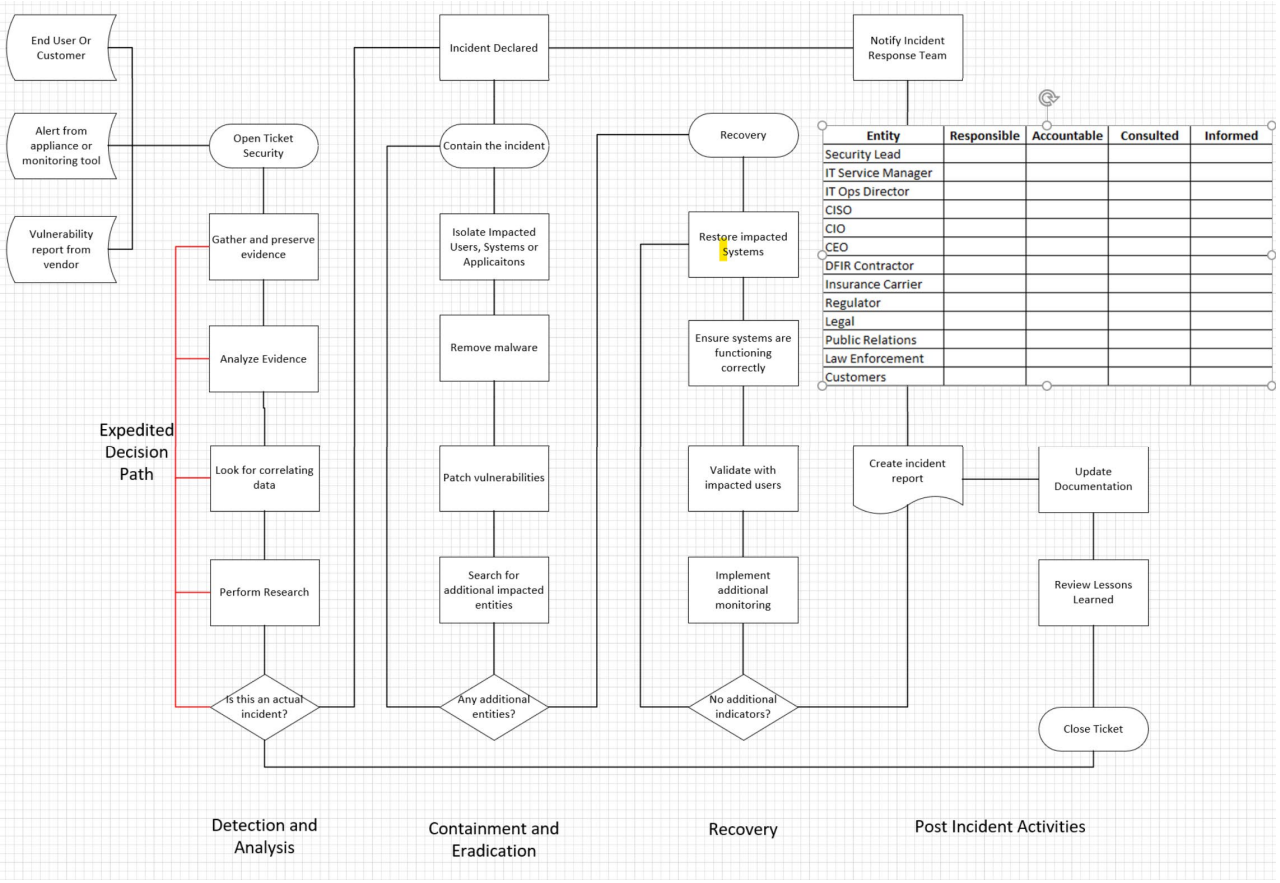
BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

If something bad happens….

- Have an incident response plan
- Preserve evidence as you go
- Get help, particularly around forensics
- An incident is a business event
- Don’t reinvent the wheel



BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

You’re not alone

- Very few organizations can afford to can effectively deal with security completely in house
- Effectively leverage your existing resources, ***INCLUDING HUMANS***

BCNET CONNECT

Selkirk College

STEEVES AND ASSOCIATES

BCNET CONNECT

Comments and Questions

Selkirk College

STEEVES AND ASSOCIATES