

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





## **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







## About Selkirk College

BCNET

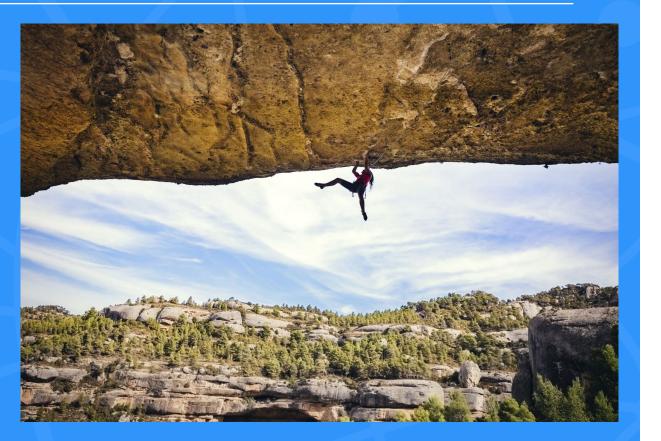


- Founded in 1966
- 9 geographically distanced campus (30 min – 4 hours drive)
- Over 2,000 student FTE 2023/2024
- High speed WAN campus
   interconnect
- Complex legacy infrastructure
- Thriving research department
- Programs ranging from Digital Fabrication to Blacksmithing





### Challenges



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







### 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









### **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 <u>2021</u>







# **CIS Control and Benchmarks**

## CIS

#### **CIS Critical Controls® Version 8**

18 top-level best practices containing 153 prioritized safeguards

Inventory and Control of Enterprise Assets	Control of Software Assets	Data Protection
Secure Configuration of Enterprise Assets and Software	Management	Access Control Management
Continuous Vulnerability Management	Audit Log Management	Email and Web Browser Protections
Malware Defenses	Data Recovery	Network Infrastructure Management
Network Monitoring and Defense	Security Awareness and Skills Training	Service Provider Management
Applications Software Security	Management	Penetration Testing

Confidential & Proprietary

### CIS. CIS Benchmarks

Consensus-developed secure configuration guidelines

100+ CIS Benchmarks

### B CIS Benchmarks<sup>™</sup>



- 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

Confidential & Proprietary







### 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





TISH JMBIA	<u> </u>	≡ Menu	
ish Columbians and Development >	d our governments > Services and policies > Information Management & Technology > Information Securit	<u>ty</u> >	
rsonal	Cybersecurity Courses		
Security	List of security-related courses.		
hedule	More courses and descriptions can be found in the SERENE-RISC Course Directory.		
al Development cation for IT	Online Courses		
nals on Security urse urity Courses of Security n Security	Cloud  AWS Training and Certification: <u>https://www.aws.training/</u> Cloud Concepts - Principles of cloud computing (6 hours) - <u>https://docs.microsoft.com/en-us/heart/modules/principles-cloud-computing/</u>		
on Security	Azure fundamentals (10 hours) - https://docs.microsoft.com/en-us/learn/paths/azure-fundamentals/ Alberta		
rity Alerts & IS	Expand All   Collapse All Athabase University		
n Incidents		*	
reat and Risk t	Concordia University of Edmonton	*	
ws Digest iecurity	King's University	*	
ouncil rity Incident	MacEwan University	~	
rocess	Mount Royal University	~	
les and lities	University of Alberta	*	
curity Services n Security Quick	University of Calgary	~	
r Security Quick	University of Lethbridge	*	
nagement	British Columbia		
ormation Managed	Expand All   Collapse All		
oud	Kwantlen Polytechnic University	~	
Investment	Simon Fraser University	*	
ication Services ent & Broader	Thompson Rivers University	*	
e Authentication	University of British Columbia	*	
atural Resource System ervices	University of Northern British Columbia		
	University of the Fraser Valley	*	
	University of Victoria	*	
	Vancouver Community College	*	
	Vancouver Island University	*	

Home > Britis Professional D Privacy & Per Information Information 9 Security Sch \* Professiona Communic Profession

> Informatio Online Cou Cybersecu The Faces o

Information Classificatio • Defensible 5 • Awareness Cyber Secur Notification

Information

Security Thr

Security Nev Provincial Se Advisory Cou

Security Rol Responsibili External Sec

Links
MFA
Records Man
Access to Infe
Data Centre,
Hosting & Clo

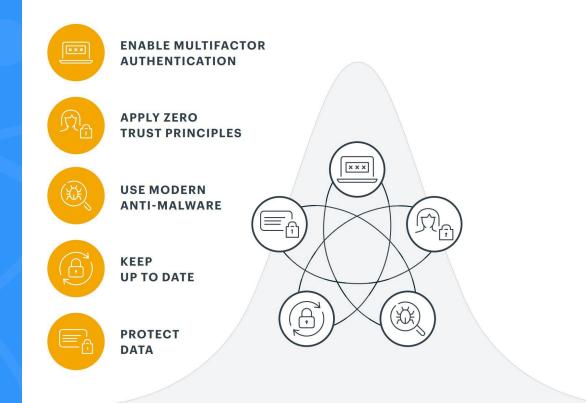
IM/IT Capital ID services Telecommun for Governm

Public Service Identity and A Services Provincial Nat Sector Radio S SiteMinder Se



## 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.





### 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



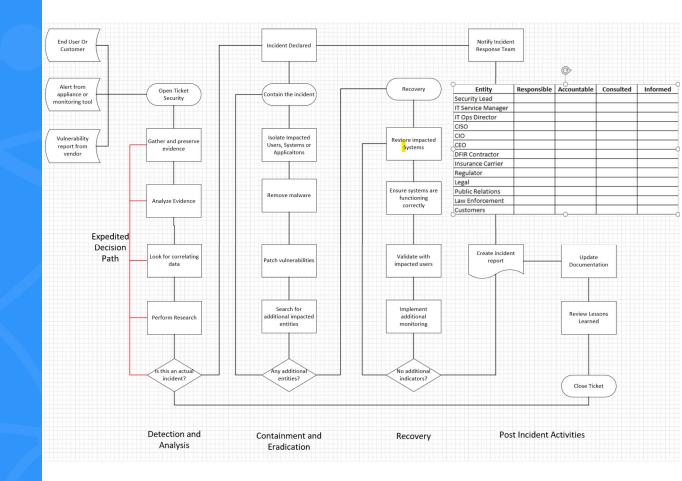






### If something bad happens....

- 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









### 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*











### **Comments and Questions**



