

Ontario Cyber Security Framework

Wendy Young

Director of Information Technology

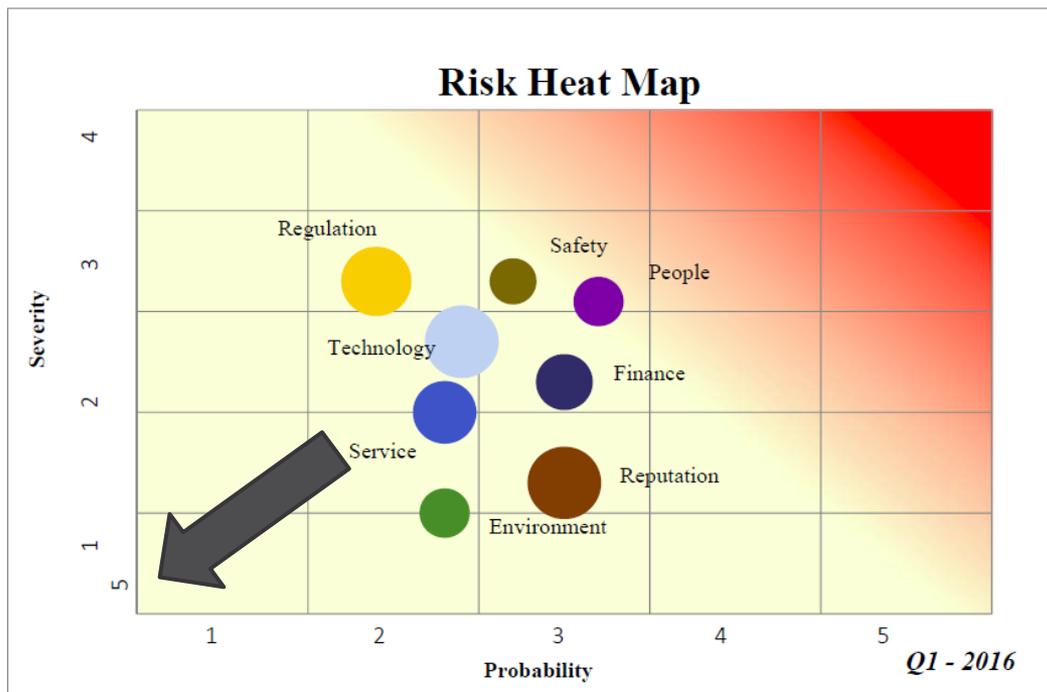
June 21, 2018

Presented to MEARIE Risk Conference



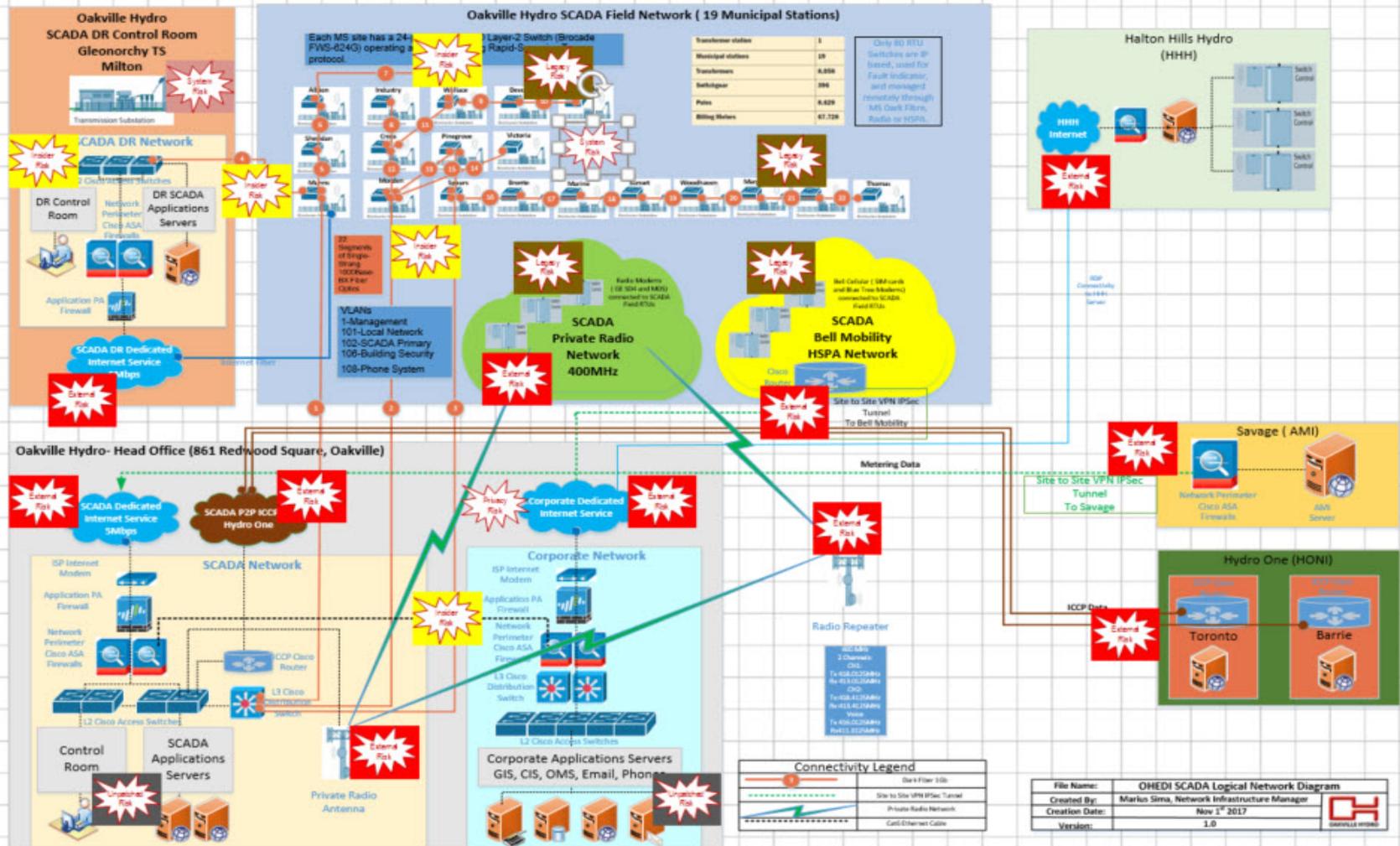
Infrastructure Services	Generation	Energy Services	Distribution
 			
 			
 			

Enterprise Risk Management



**For illustrative purposes only*

Oakville Hydro Attack Surface





Our Framework

➤ Implementing best practices through a defined set of general controls

- Network implementation
- Layered security
- Segregation of Networks

Control ID	Control Objective	Risk	Control Activity	Frequency	Test Plan	Notes
56	Access to the network and applications is appropriately restricted through least-privilege principles for roles, restricted permissions and appropriate segregation and segregation of duties based on the principle of least privilege.	Unauthorized access to network or systems Increased risk of security breaches Disclosure of data Loss of "ownership" of resources	Users are provided education on all available services for IT	100	1. Select a sample of transactions and review them for errors.	Processes for access controls to ensure confidentiality of information not documented or well understood followed Develop and document process/procedures and Roles and responsibilities
58	Requests for new user access or changes in existing access require documentation and appropriate approval.	Unauthorized access to network or systems Increased risk of security breaches Disclosure of data Loss of "ownership" of resources	All user security systems follow the User Access Security Procedure requests and review and sign-off with appropriate sign-off by the manager. IT completes the request and signs off on the form.	100	1. Obtain a list of new hires (employees) and review their access requirements from HR for the current year of testing. 2. Select a sample of new hires and trace their access to an approved User Access Change Form. Ensure that the information on the form is appropriate, complete and in accordance with the stated controls. 3. The access of 25 users or 25% of the population.	Processes for access controls to ensure confidentiality of information of documents or well understood followed Develop and document process/procedures and Roles and responsibilities
59	Users receive education on security awareness and an appropriate level of control security including confidentiality and PII compliance.	Unauthorized access to network or systems Increased risk of security breaches Disclosure of data Loss of "ownership" of resources	IT provides the appropriate User Access Security Procedure requests and review and sign-off with the manager.	100	1. Review User Access Security Procedure requests and review and sign-off with the manager. 2. The access of 25 users or 25% of the population.	Processes for access controls to ensure confidentiality of information of documents or well understood followed Develop and document process/procedures and Roles and responsibilities
60	Appropriate operating system and network password controls	Unauthorized access to network or systems Increased risk of security breaches Disclosure of data Loss of "ownership" of resources	Network standards are defined for all systems/hosts. This includes:	100	1. Review Network Standards with all areas.	Processes for access controls to ensure confidentiality of information of documents or well understood followed Develop and document process/procedures and Roles and responsibilities

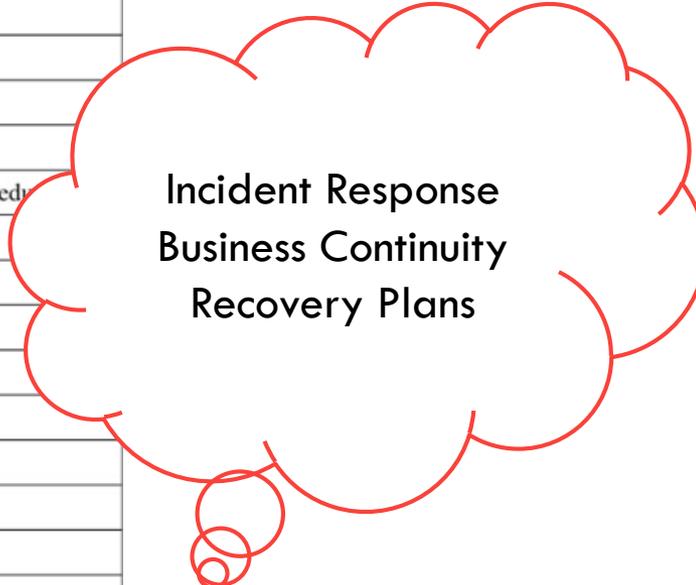
➤ Adopted framework was based on the NIST

➤ Developed a rolling Cyber security plan that adopts changes

Out Nur	Task Name	% Cor	External Resource	Internal Resource Lead	Internal Resource Support	Start	Finish
1	<input type="checkbox"/> Cyber Security Plan	62%				Tue 11/1/11	Thu 5/14/20
2	<input type="checkbox"/> Leadership and Governance	75%				Tue 11/1/11	Fri 5/3/19
13	<input type="checkbox"/> Operations and Technology	85%				Sat 9/1/12	Wed 1/30/19
45	<input type="checkbox"/> Information Risk Management	26%				Fri 4/1/16	Wed 8/1/18
33	<input type="checkbox"/> Awareness	15%				Sat 10/1/16	Fri 6/29/18
51	<input type="checkbox"/> Legal And Compliance	0%				Mon 1/2/17	Thu 11/30/17
56	<input type="checkbox"/> Business Continuity and Respond Managemen	3%				Wed 2/1/17	Thu 5/14/20

	A	D	E	F	Notes	OEB Notes	Score 0-4	Possible Score
1	Category				Notes			
2	1 Identify	● 86%					4	4
3	Asset Management	● 100%						
4	Business Environment	● 75%						
5	Governance	● 79%						
6	Risk Assessment	● 83%						
7	Risk Management Strategy	● 88%						
8	2 Detect	● 82%						
9	Anomalies and Events	● 100%						
10	Continuous Monitoring	● 88%						
11	Detection Process	● 63%	Not all assets are monitored, only critical devices					
12	3 Protect	● 94%						
13	Awareness and Training	● 75%						
14	Data Security	● 100%					4	4
15	Information Protection Processes and Procedure	● 100%						
16	Protective Technology	● 100%						
17	4 Respond	● 19%						
18	Communications	● 15%	Response plans are followed but are not formalized					
19	Improvements	● 0%						
20	Mitigation	● 75%	Stratejcm Works with the IT team to mitigate issues					
21	Response Planning	● 25%						
22	5 Recover	● 29%					4	4
23	Communications	● 50%	Recover plans are followed but are not formalized					
24	Improvements	● 0%						
25	Recovery Planning	● 25%						
26	Overall Percentage	● 75%						
27								

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



Incident Response
Business Continuity
Recovery Plans

- ✓ New Ontario Framework takes into account the best practices for an organization to follow to achieve good cyber security
- ✓ The Framework is flexible enough for any organization
- ✓ Responding and recovering from an event should be our focus

Thank
You