Ontario Cyber Security Framework

Wendy Young

Director of Information Technology

June 21, 2018

Presented to MEARIE Risk Conference

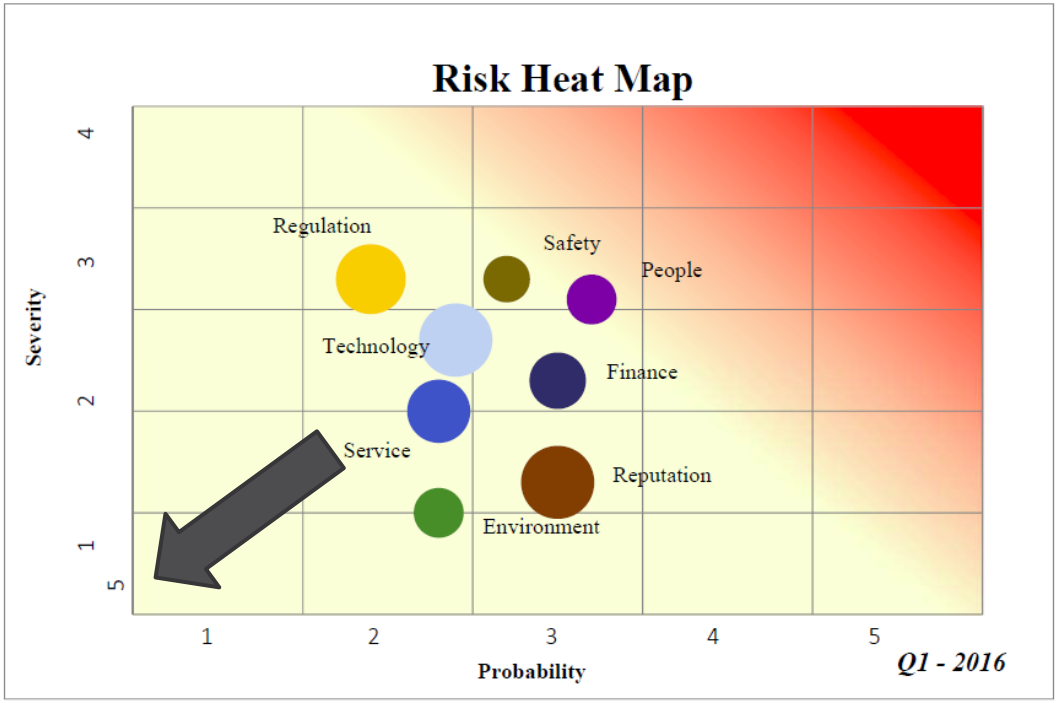
OAKVILLE HYDRO

OEC At-a-Glance

Infrastructure Services	Generation	Energy Services	Distribution
G-TEL ENGINEERING PLANVIEW Utility Services Ltd. PVS el·con UTS Huron GEOMATICS inc.	OEC GENERATION Sunny Shores LP Green Energy Solar Park OEC GEOEXCHANGE	OAKVILLE HYDRO ENERGY SERVICES Golden Horseshoe METERING SYSTEMS	OAKVILLE HYDRO

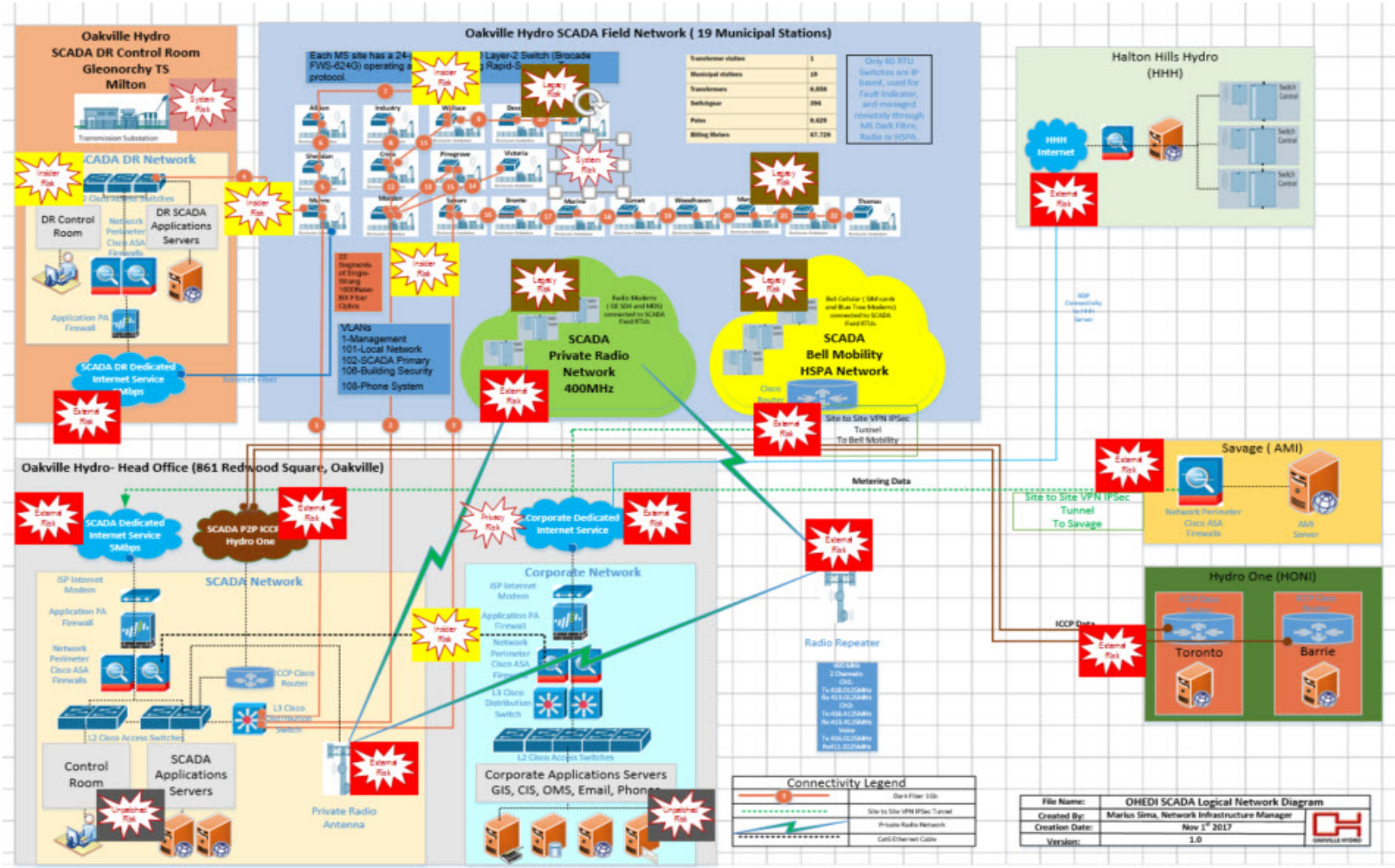
Risk Profile

Enterprise Risk Management



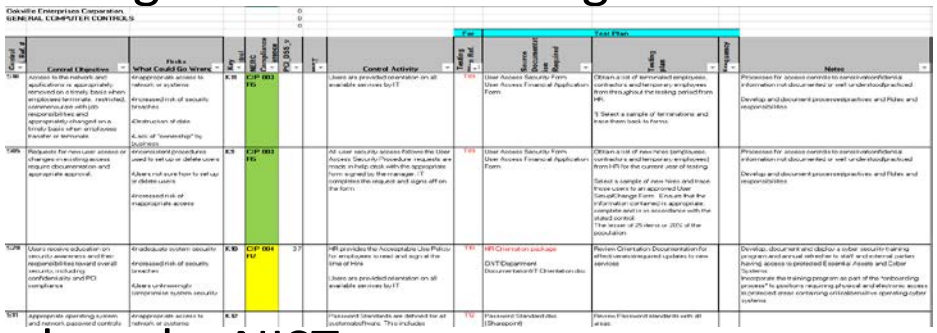
For illustrative purposes only

Oakville Hydro Attack Surface



Our Framework

- Implementing best practices through a defined set of general controls
  - Network implementation
  - Layered security
  - Segregation of Networks



- 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	**1**	**Cyber Security Plan**	**62%**				**Tue 11/1/11**	**Thu 5/14/20**
2	*1.1*	**Leadership and Governance**	75%				Tue 11/1/11	Fri 5/3/19
13	*1.2*	**Operations and Technology**	85%				Sat 9/1/12	Wed 1/30/19
45	*1.4*	**Information Risk Management**	26%				Fri 4/1/16	Wed 8/1/18
33	*1.3*	**Awareness**	15%				Sat 10/1/16	Fri 6/29/18
51	*1.5*	**Legal And Compliance**	0%				Mon 1/2/17	Thu 11/30/17
56	*1.6*	**Business Continuity and Respond Manageme**	3%				Wed 2/1/17	Thu 5/14/20

Ontario Framework

	A	D	E	F
1	Category		Notes	
2	**1 Identify**	**86%**		
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	Anomolies 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%		
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%	Stratejm Works with the IT team to mitigate issues	
21	Response Planning	25%		
22	**5 Recover**	**29%**		
23	Communications	50%	Recover plans are followed but are not formalized	
24	Improvements	0%		
25	Recovery Planning	25%		
26	**Overall Percentage**	**75%**		
27				

Notes	OEB Notes	Score 0-4	Possible Score
ocumented in visio all physical and umented on data nents listing all rvice from source		4	4
d in the service excel spreadsheet intained but will be e-Now for full ITSM.		4	4
d in the service excel spreadsheet intained but will be e-Now for full ITSM. r a full audit of all		4	4

Respond and Recover

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 Procedu
		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

Take Aways

- ✓ 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

OAKVILLE HYDRO