

**CANCELLED**



# **Town of Newmarket Agenda Council Workshop**

Date: Tuesday, February 12, 2019  
Time: 1:00 PM  
Location: Council Chambers  
Municipal Offices  
395 Mulock Drive  
Newmarket, ON L3Y 4X7

**Pages**

**1. Notice**

In accordance with the Town's Procedure By-law, no decisions are to be made but rather this meeting is an opportunity for Council to have informal discussion regarding various matters.

**2. Additions & Corrections to the Agenda**

**3. Declarations of Pecuniary Interest**

**4. Items**

**4.1 Introduction**

**Note:** Mary-Anne Wigmore, Director, IT, will be attendance to provide an introduction to the presentations.

**4.2 Cyber Security Overview**

**1**

**Note:** Eric Parent, EVA Technologies will be in attendance to present on this matter.

**4.3 Newmarket Council Orientation on Cyber Security**

**19**

**Note:** Paul Ferguson, President, Newmarket-Tay Power Distribution Ltd., Scott Bradley, IT Manager, Newmarket-Tay Power Distribution Ltd., and Wayne Ronhaar, CEO, Snowy River will be in attendance to present on this matter.

**4.4 Cyber Liability and Privacy Breach Insurance Benefits**

**47**

**Note:** Sara Runnalls, Public Sector Risk Advisor, BFL Canada will

# **CANCELLED**

be in attendance to present on this matter.

## **5. Closed Session**

That the Council will resolve into Closed Session to discuss the following matter:

- 5.1 Educational/training session under Section 239(3.1) of the Municipal Act, 2001 (cyber security update)

## **6. Adjournment**

**CANCELLED**



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

# Cybersecurity Overview

# CANCELLED



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

## ERIC PARENT



**ERIC PARENT, IMITI CISSP-ISSAP CRISC CGEIT CISM CCSE MCSE CNE CCDA**

30+ years experience security veteran. Holds multiple prestigious security certifications and has worked as security advisor for numerous large national and international corporations at the CxO level. Recognized in 2009 for outstanding industry contributions by the International Information Systems Security Certification Consortium. Teaches a Cyber Security course at École Poly Technique de Montréal & HEC.

- Ex-Military (1980) – SigInt & Countermeasures
- Security consultant since 1990
- Specialized in senior executive coaching
- Teach cybersecurity at École Polytechnique & HEC
- CSO of Sonepar Canada
  - Advisory CSO for a dozen Enterprises (50m - 500m)

**CANCELLED**



# AGENDA

- INTRODUCTION
- COMMON THREATS
- COMMON REASONS ATTACKS SUCCEED
- Q & A

**CANCELLED**



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

# Common threats

# CANCELLED



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

## Enterprises MUST

- Protect against all possible threat scenarios (not possible)

## Criminals NEED

- To find one single threat scenario that works (possible)

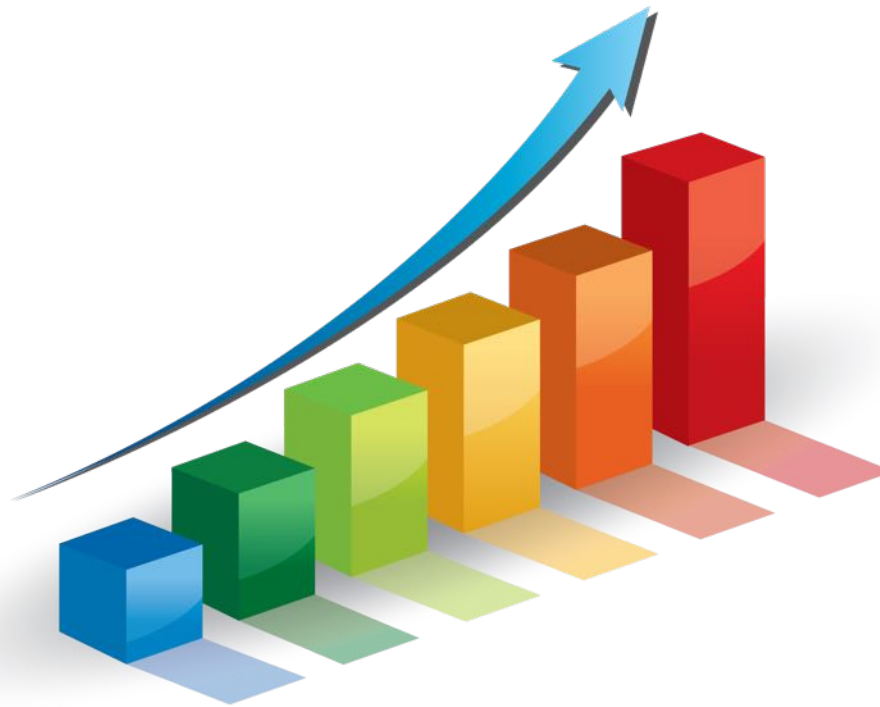
# CANCELLED



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

Breaking security used to be a sport

It is now a **mature** business model generating billions in revenue





# CANCELLED



- Enterprise security is currently reactive
- Criminals are not reactive (they plan, and they invest)
- Enterprises think they have tested their security because they invested 5 or 10 days of security testing (restricted testing)
- Criminals build teams of 10 to 80 qualified individuals, develop specific attack vectors over months of research and testing, then unleash against a series of “victims” that fit a certain profile

**CANCELLED**



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

# Most common threats

- Random attacks
  - Ransomware
  - Virus or other malware
- Targeted vulnerability attack
  - Looking for a specific technology flaw
- Overly confident IT
  - Lack of expertise
  - Lack of competence
- They all have the same (or very similar) chain of events

# CANCELLED



When RANSOMWARE hits and hurts an enterprise, something is wrong

Why pay the ransom ? (The ones you hear about paid)

Clear indication that SEVERAL things have gone wrong

- Exploitable technical vulnerabilities
- Exploitable humans
- Poor backup ecosystem
- Absent or poor DR (Disaster Recovery) plan

# CANCELLED



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY



QUIT X

[FAQ](#) ■ [Contact Us](#)

## INTERNET BANKING SOLUTIONS - BUSINESSES

Authentication with password

Authentication with SecurID passkey

User code:

Password:

[Forgotten password?](#)



### *Important security reminder!*

If someone contacts you by phone, email or text asking you to confirm or enter your login information (password, SecurID key number or PIN), or if you believe you might have been a victim of fraud, immediately contact your account manager or National Bank Business Central® at 1-844-394-4494.

Never share your password, SecurID key number or PIN. A National Bank employee will never ask for this information.

To learn more about our policies and best practices in fraud prevention, refer to our "ABCs of Security" section at [nbc.ca/security](http://nbc.ca/security).

[Legal information](#) - [Confidentiality policy](#) - [ABC's of security](#)

© NATIONAL BANK OF CANADA.

<sup>11</sup>  
**CANCELLED**



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

# Why attacks succeed





ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

# Most common threats

- Security Debt versus technology debt
- Lack of integrated security combined with weak security testing
- Weak or absent security awareness
- Absence of advanced AI driven security technologies

<sup>13</sup>  
**CANCELLED**



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

In 2019

- Still have users with passwords like Winter2019
- Still have senior executives with accounts that do not expire, because that is inconvenient
- Still have a belief that security shouldn't impact business processes at all
- Still prefer comforting lies versus the truth (Equifax)
- Still cross our fingers that it will not happen to us



## The problem

- Most enterprises think they are a 3/5, they are mostly 1/5
- IT staff is not Security aware (this is not their primary responsibility)
- Security professionals are rare and costly (\$130k)
- On going training is expensive (\$25k / year)
- Tools to gauge security are complex and expensive (\$25k/ year)
- Overall single person **team** is well above \$180k / year
- Lack of understanding between Security and SecOps

### Result

- Best effort, fingers crossed
- Technology debt = security debt (and every IT group has a debt)





## Missing piece

IT Operations versus IT Security are two different things

A qualified third party should be:

- Evaluating your maturity using an acceptable framework
- Performing ongoing security testing that gets progressively more aggressive
- Providing security opinions and coaching your IT teams to ask questions
- Addressing root causes, not focused on found issues

Adhering to a healthy self-criticism approach to security is the only logical way to address security

16  
**CANCELLED**



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

**Q & A**

**CANCELLED**



ENTERPRISE  
VULNERABILITY  
ASSESSMENT &  
AVOIDANCE TECHNOLOGY

**ERIC PARENT**

eparent @ eva-technologies.com

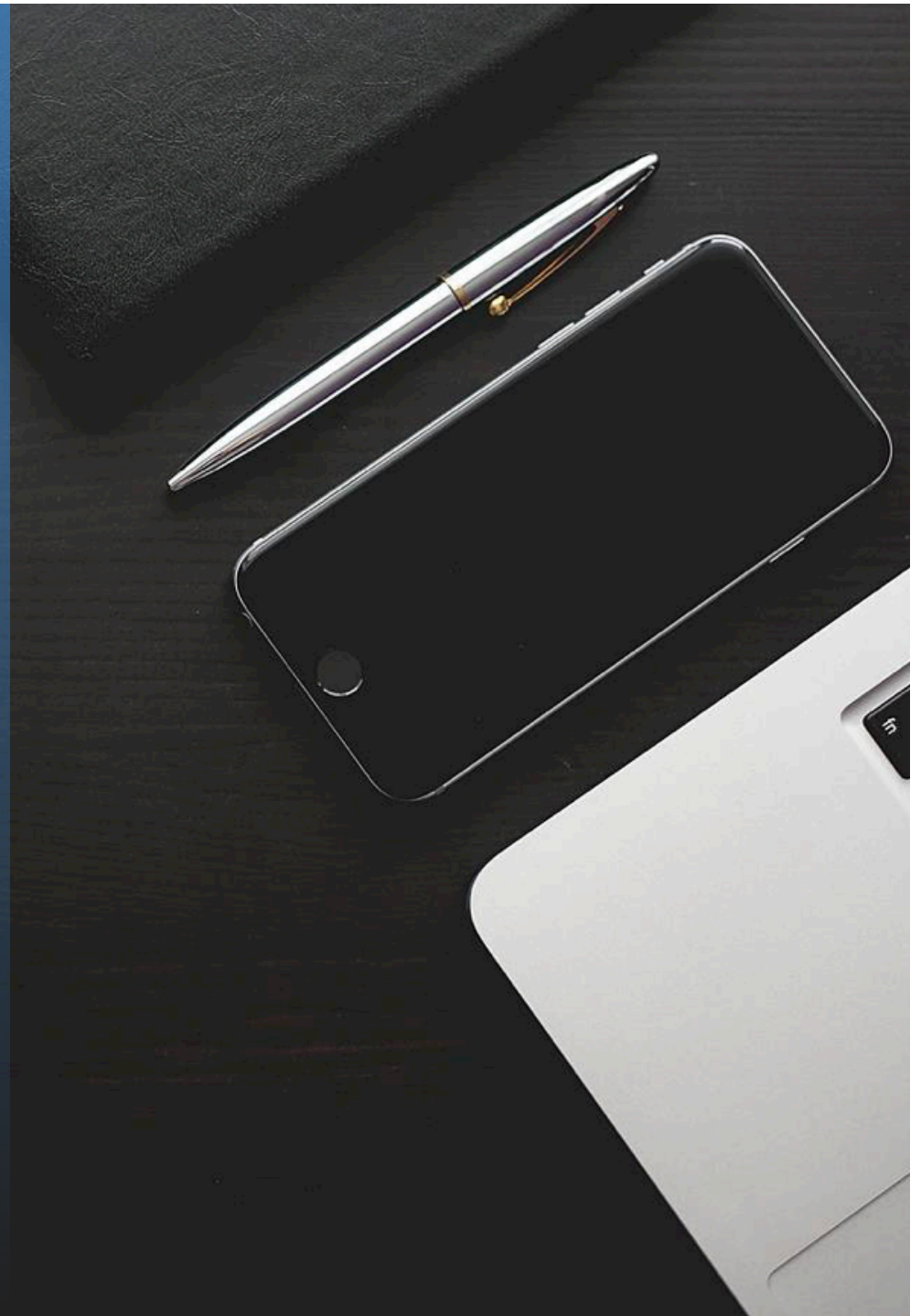
www.eva-technologies.com

blog.ericparent.com

514-973-8501 (cell)

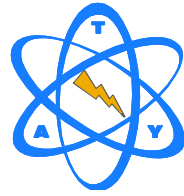
514-907-5488 (office)

EVA-Technologies – 2019



**CANCELLED**

18



**CANCELLED**

Newmarket-Tay Power Distribution Ltd.



## Newmarket Council Orientation on Cyber Security

February 12, 2019

Paul Ferguson, President

Scott Bradley, IT Manager

Wayne Ronhaar, CEO Snowy River

# Agenda

- **Introduction and Overview – Paul Ferguson**
- **The Cyber Risk Challenge – Wayne Ronhaar**
- **Our Actions – now and in preparation for the future – Scott Bradley**
- **Discussion**



**CANCELLED**

# NDPDL in Context



# Our Vision

**An independent, industry-leading LDC committed to our customers' changing needs**







# Our Customers

**We serve:**

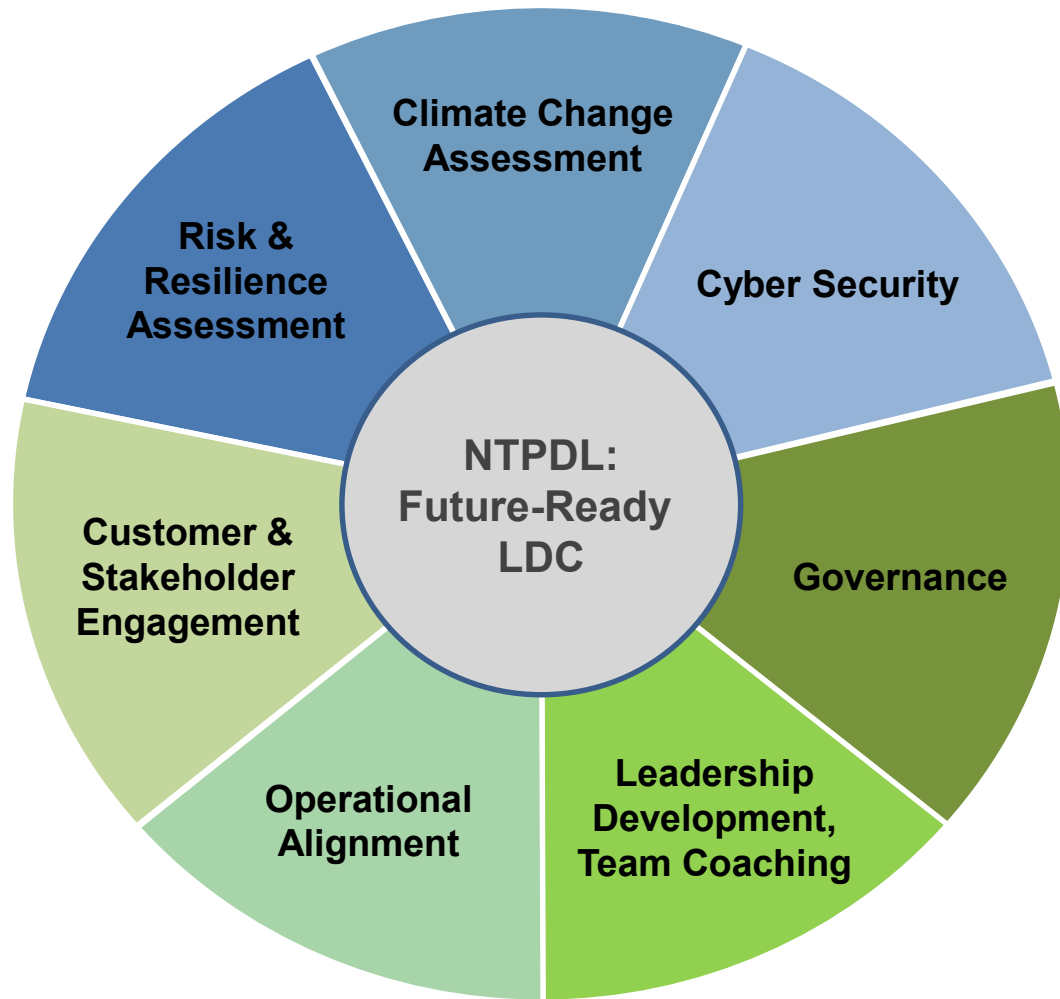
- **The Town of Newmarket**
- **Northern portion of Tay Township  
(Port McNicoll, Victoria Harbor and Waubauskene)**
- **Town of Midland (as of September, 2018)**

**45,000 customers**

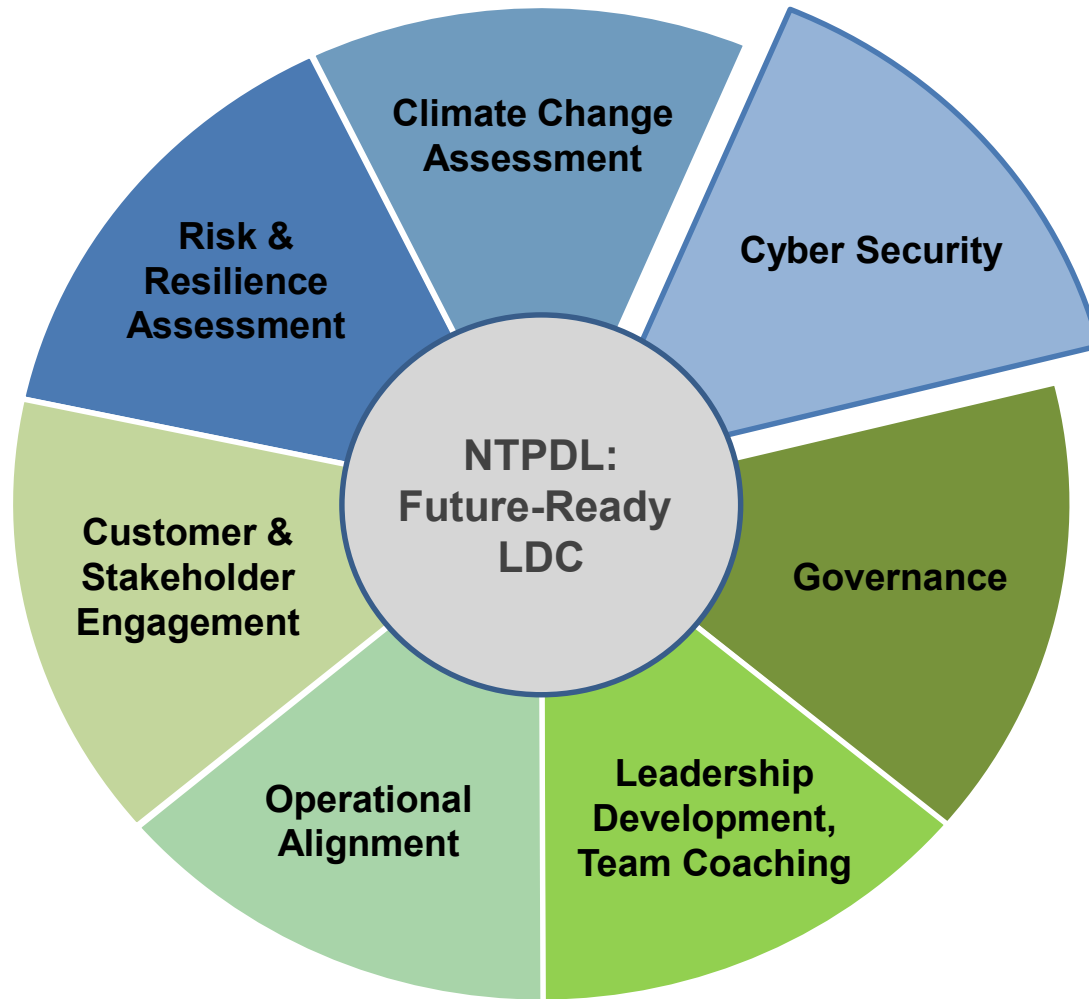
**2017 electricity sales of \$77,747,796.00**

**2017 distribution revenue \$12,805,980.00**

# Holistic, Comprehensive Strategic Risk Assessment



# Holistic, Comprehensive Strategic Risk Assessment

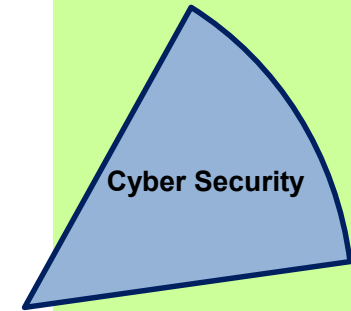


# Addressing Cyber Security Challenges

Since 2017 we've been:

- **Upgrading Information Technology (IT) Control Systems to ensure data safety and security**
- **Integrating Midland PUC IT Systems**
- **Planning for Technological Change**
- **Addressing Changing Regulatory Requirements**
- **Preparing for Changing Customer Requirements – Safe and Secure Operational Technology (OT) Systems**
- **Updating Policies and Procedures – Team Training**

# Why is cyber security important to LDCs?

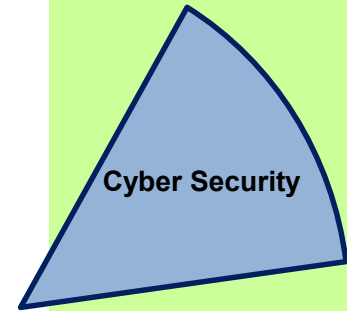


- Utilities evolving fast through digitization
- More assets connected today than ever as LDCs become more agile, customer focused and innovative
- Result: Sector increasingly vulnerable to cyber attacks



# Why cyber security is important to LDCs

- Two distinct styles of utility in the future



## Utility Environment

### Characteristics

- Asset intensive
- Regulated
- Enabler of new grid technology

### Traditional

### Business Drivers

- Sweat asset safety
- Cost reduction
- Careful investment

### Technology

- Asset maintenance
- Big data
- Field mobility

### Characteristics

- Customer-facing
- Exploit grid
- Product / offer innovation

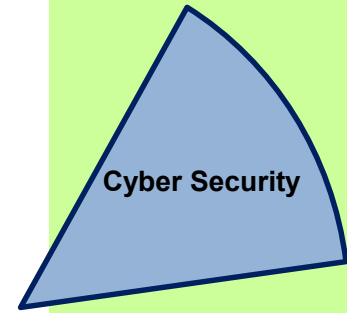
### New

### Business Drivers

- Innovative culture
- Excellence in customer experience
- Rapid new product development

### Technology

- Ideation
- Big data
- Process automation



# LDC Vulnerability

**Two types of cyber attacks – driven by convergence of OT/IT infrastructure via digitization:**

- **IT Systems:**
  - Corporate breaches -- networks attacked, office computers compromised, and/or business information stolen
- **OT Systems:**
  - System breaches -- Sensors, Supervisory Control and Data Acquisition (SCADA) systems, software and other controls that facilitate power plants and Transmission & Distribution (T&D) grids

## Putting our best people on the job

**Scott Bradley is our IT Manager. He and the IT Team play an integral role in realizing the corporate mission and vision by leading the design, delivery and implementation of technology at the LDC.**

**Scott has more than 16 years experience in the Ontario utility industry. He has participated in numerous working groups responsible for implementing time-of-use pricing, smart meters/advanced metering infrastructure, customer presentment technologies and conservation & demand management pilot projects.**





## Putting our best people on the job

**Wayne Ronhaar is founder and CEO of Snowy River International Inc.**

**Snowy River is a Global Cyber Security and Cyber Resiliency company that helps redefine how organizations think about resiliency, cyber security and cyber resiliency.**

**Wayne has been supporting our team at NTPDL since 2017.**



# What is cyber risk? – Impact on cities and LDCs

**Cyber security is a business issue – not just a technical matter:**

- » Must be looked at from a holistic standpoint – a critical risk issue
- » Cyber capabilities are the weakest point that can elevate risks and increase the impact of malicious incursion in any organization

**Cyber security requires Board oversight:**

- » Cyber risk management
- » Compliance with various national and international government requirements and standards

**Utility assets are critical to the economic well-being of the jurisdictions in which they operate**

- » Any failure can cause catastrophic impacts on people and the economy

**Cyber risk will only increase over time unless appropriate risk management techniques are put in place**

# Building Cyber Resilience

- **Context** – build the operational competencies that enable leaders to protect their businesses
  - » We focus on building security-driven systems and cultures, powered by adaptive strategy and operational agility.
- **Definition:**

Our solutions address the realities of today's security environment:



## A MUTATING THREAT

Risks are changing at a viral pace, driving the need for adaptive and agile cyber security.



## DATA DRIVES REGULATION

Regulators are looking for holistic compliance that goes beyond technical fixes.



## INTERNET OF (BAD) THINGS

Blending distributed, automated technology with aged infrastructure is exposing major security vulnerabilities.



## REPUTATION UNDER ATTACK

Corporate brand can be ruined by the compromise of customer data or internal leaks.



## PRESSURE TO PERFORM

To protect years of security investments, reaction times must be seconds.



## SECURITY TALENT

Security talent is the single largest expenditure and defining asset of a high-performing security organization.

# Cyber security risks, threats

## – Today and in the future

- **Good cyber risk management involves the following:**
  - » A cyber security risk management program to identify analyze and mitigate cyber security risks across the organization and its supply chain
  - » A program covering both operational technology (OT) and information technology (IT) assets
  - » An ability to manage threats and vulnerabilities with appropriate plans and procedures
  - » The capability to be situationally aware, and constantly scan potential future threats
  - » A culture that views cyber security risk management in the same way as other core functions
  - » Collaboration with other utilities – sharing critical information, strategy development and operational activities

# The threat is real

## Recent cyber attacks:

- **Unnamed Ontario LDC**
  - » 2018, Ransomware, \$150k
- **Unnamed Ontario LDC**
  - » 2017, Spear-phishing, \$100k+
- **Town of Midland**
  - » 2018, Ransomware
- **Town of Wasaga Beach**
  - » 2018, Ransomware, \$30k + \$250k
- **Utilismart, Meter Service Provider vendor**
  - » 2018, Details undisclosed



## Why is this important?

- The utility sector is a valuable target for bad actors
- Impacts of essential service disruption
- Not if, but when
- Trust is hard to build and easy to lose in a breach
- Many organizations never fully recover from incidents



## NTPDL Recent cyber attacks

- **Logged attempts of spear-phishing**
- **Increasing sophistication and knowledge**
- **Identified 0-day ransomware and proven kill chain implementation**



# Holistic Approach to Cyber Security

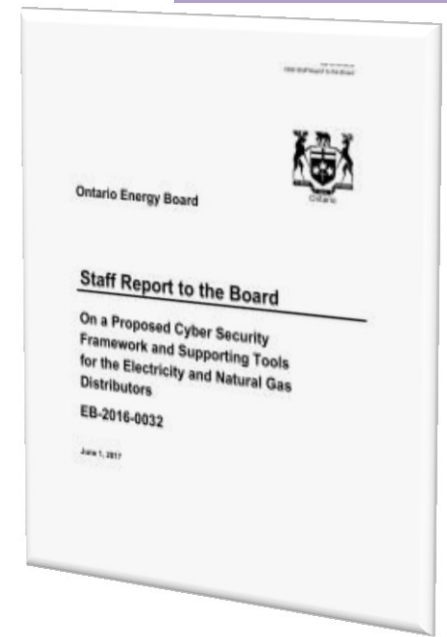
- Elevated focus on the importance of IT
- Cross-functional teams engaged, covering all aspects of NTPDL business
- Soft target hardening
- Capitalizing on the integration of MPUC
- Exploring new ways to leverage our existing infrastructure





## Taking Action

- **Ontario Energy Board Cyber Security Framework (CSF)**
  - » National Institute of Standards and Technology (NIST) based supplemented with privacy components
- **IT General Controls Audit**
  - » Completed annually, unified with financials
- **IT /Cyber Security Policy**
  - » Corporate policy refresh
  - » Aligning with CSF



# OEB Cyber Security Framework



## OEB CSF – Identify

- Asset inventory
- System diagrams
- Business plans
- Security Policy
- Risk strategy/assessment
- Identify vulnerabilities using asset inventory
- Disaster Recovery /Business Continuity Plan
- Contractual agreements and Service Level Agreements

### IDENTIFY

- ▶ Asset management
- ▶ Business environment
- ▶ Governance
- ▶ Risk assessment
- ▶ Risk management strategy

# OEB CSF – Protect

- Physical access control
- Network segmentation
- System metrics
- Backup procedures
- Awareness training
- Logical access control Role Based Access Control.  
Attribute Based Asset Control
- Remote device access control
- Response plan
- Change and configuration management  
formalization

## PROTECT

- ▶ Access control
- ▶ Awareness and training
- ▶ Data security
- ▶ Information protection and procedures
- ▶ Maintenance
- ▶ Protective technology

## OEB CSF – Detect

- Anomalous behavior scanning, physical assets and operations
- Malicious code detection
- Mobile code
- Risk and vulnerability management program
- Third party access point monitoring
- Security Information & Event Monitoring tooling

### DETECT

- ▶ Anomalies and events
- ▶ Security continuous monitoring
- ▶ Detection process

## **OEB CSF – Respond**

- Reporting criteria
- Procedures for investigating notifications
- Impact assessment
- Communication and customer & community engagement plan
- Thresholds/Categorization
- Response plan testing

### **RESPOND**

- ▶ Response planning
- ▶ Communications
- ▶ Analysis
- ▶ Mitigation
- ▶ Improvements

## OEB CSF – Recover

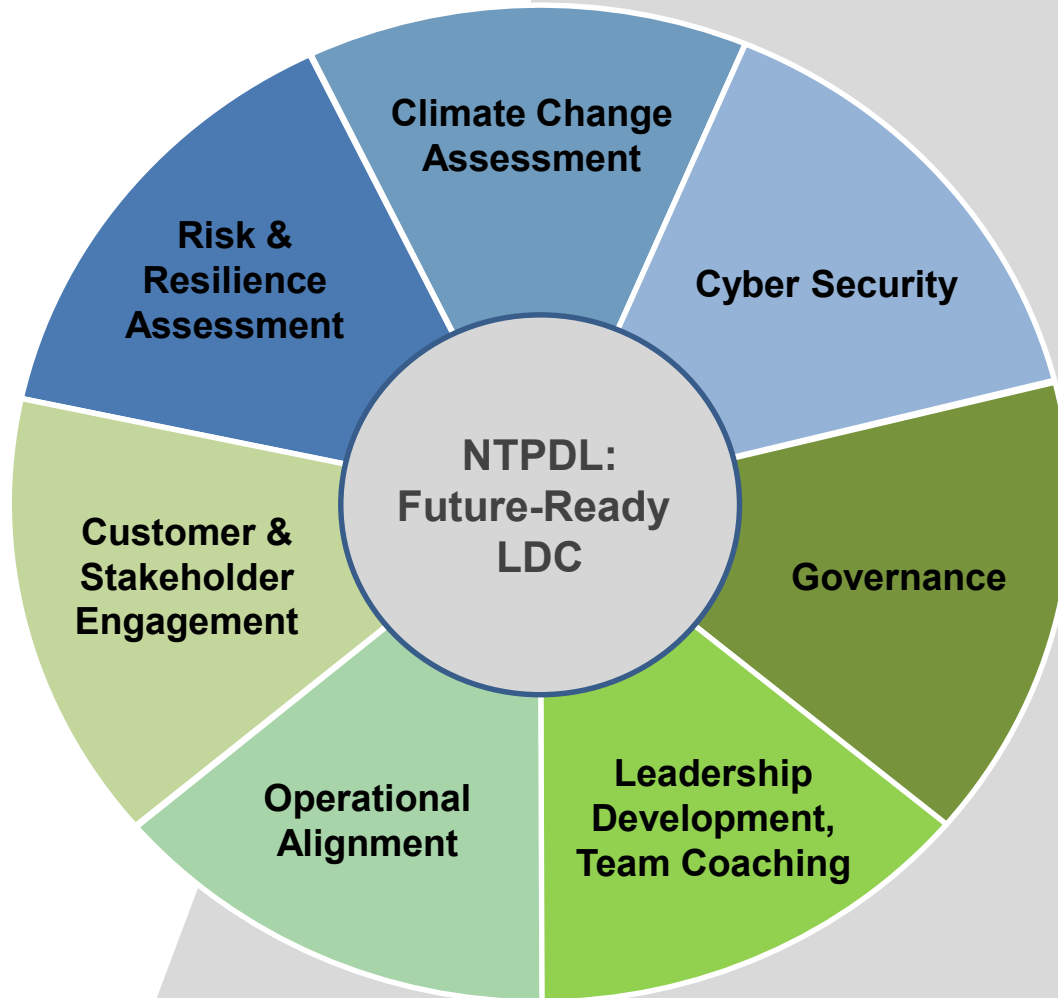
- Capacity and performance planning
- Professional public relations, implement customer & community engagement plan
- Incident response operations
- Feedback process for improvements
- Recovery plan review

### RECOVER

- ▶ Recover planning
- ▶ Improvements
- ▶ Communications

**CANCELLED**

# Comment and Questions







**CANCELLED**

# **CYBER LIABILITY AND PRIVACY BREACH INSURANCE BENEFITS**

Town of Newmarket  
February 12, 2019

# INTRODUCTION

## Why does Cyber Insurance exist?

- Insurance is an industry of evolution - as risks develop, so do insurance products
- General Liability and Property policies were not designed to handle the specific exposures brought about by the digital age
- Y2K is a perfect example
- Firewalls and other security measures are not foolproof

# CYBER INSURANCE

**Cyber Risk** has two main elements:

1. **First Party Losses** – direct loss suffered by you as a result of a hacking event
2. **Third Party Losses** – actions brought against you, either by victims or by regulatory bodies, as a result of alleged negligence that may have caused an unauthorized release of confidential information



**CANCELLED**

# FIRST PARTY LOSSES

BFL MAKES A DIFFERENCE



## FIRST PARTY LOSSES

### CYBER EXTORTION

# **CANCELLED** CYBER EXTORTION

- Pays loss you incur as a result of a Security Threat or Privacy Threat
- Loss means monies you pay:
  - ✓ To terminate the threat, including the obtaining of Bitcoin or other cryptocurrency to be surrendered as payment
  - ✓ To conduct an investigation to determine cause of the threat



## FIRST PARTY LOSSES

### NETWORK INTERRUPTION

# ~~CANCELLED~~ 52 NETWORK INTERRUPTION

- Pays 'loss' you incur as a result of a Security Failure
- 'Loss' means costs you incur for a defined period (usually 120 days) following the date of first interruption, that you would not have incurred if not for the interruption
- Costs include:
  - ✓ Net income that would have been earned
  - ✓ Continuing normal operating expenses incurred, including payroll



## FIRST PARTY LOSSES

### EVENT MANAGEMENT

# ~~CANCELLED~~ EVENT MANAGEMENT

- Pays loss you incur as a result of an alleged or actual Security Failure or Privacy Event
- Loss means reasonable and necessary expenses and costs within one year of the discovery of the Security Failure or Privacy Event:
  - ✓ To conduct investigation as to cause
  - ✓ To retain advice from Public Relations, Crisis Management or Law Firms to mitigate damages, including reputational damage



## FIRST PARTY LOSSES

### EVENT MANAGEMENT

**CANCELLED**

# EVENT MANAGEMENT

- ✓ To notify victims of the breach
- ✓ For identity theft education and assistance, including call centre services, credit monitoring, victim reimbursement
- ✓ To restore, recreate or recollect Electronic Data





**CANCELLED**



**THIRD PARTY LOSSES**



## THIRD PARTY LOSSES

SECURITY & PRIVACY  
LIABILITY

# ~~CANCELLED~~ SECURITY & PRIVACY LIABILITY

- Pays loss you incur as a result of a Security Failure or Privacy Event (failure to protect Confidential Information of others)
- Loss means compensatory damages, judgments, settlements, pre-judgment and post-judgment interest and defence costs, including:
  - ✓ Punitive damages (where permissible by law)



## THIRD PARTY LOSSES

SECURITY & PRIVACY  
LIABILITY

# **CANCELLED** **SECURITY & PRIVACY LIABILITY**

- ✓ Civil fines or penalties resulting from a Regulatory Action (where permitted by law)
- ✓ Monetary amounts you are required by law or agreed to by settlement to deposit into a consumer redress fund
- ✓ Amounts payable in connection with a PCI-DSS Assessment (payment card fines or penalties associated with your non-compliance of PCI Data Security Standards)



**CANCELLED**

# WHAT DOES IT ALL MEAN?



## CLAIM EXAMPLE



## CLAIM EXAMPLE

# ~~CANCELLED~~ THE SITUATION:

- Hackers gained entry to an insured's point of sale system and were able to access over 5 million customer credit and debit card numbers (before they were detected)



## CLAIM EXAMPLE

### ~~CANCELLED~~ THE REMEDY:

- Retained Breach Counsel, Forensic Investigator and Payment Card Industry (PCI) Forensic Investigator
- Based on preliminary investigation, selected and retained vendors to manage the public relations messaging and notification to regulators and consumers
- Offered consumers access to credit monitoring protection
- Established call centre to handle inquiries and registration for the credit monitoring protection
- Breach counsel defended a dozen class action lawsuits as well as regulatory investigations



## CLAIM EXAMPLE

# ~~CANCELLED~~ THE COSTS:

- \$50,000 for public relations
- \$750,000 forensics
- \$3 million for credit monitoring, notification and call centre
- \$1.5 million for breach counsel
- \$1.2 million in regulatory fines
- \$2 million in PCI fines
- **TOTAL \$8.2 MILLION**





**CANCELLED**

# POTENTIAL ISSUES FOR MUNICIPALITIES

## WHERE CAN THINGS GO WRONG?

BFL MAKES A DIFFERENCE





## MUNICIPAL EXAMPLES

CYBER EXTORTION /  
NETWORK INTERRUPTION

# **CANCELLED** SCENARIO #1

Ransomware is introduced and successfully installed onto your SCADA (Supervisory Control and Data Acquisition) software:

- Extortionist completely disables your water distribution system
- No water delivery available
- Encryption key will be handed over once ransom is paid in Bitcoin



## MUNICIPAL EXAMPLES

CYBER EXTORTION /  
NETWORK INTERRUPTION

**CANCELLED**

Are you prepared with the financial and human resources to:

- Carry out forensics to investigate the situation, solve the problem, and ensure it doesn't repeat?
- Procure the appropriate ransom in the form of cryptocurrency?
- Ship in water for your most vulnerable customers?
- Recover lost revenues because there was no product available to distribute?
- Handle the public relations nightmare?

**Do you want your reputation to be tarnished because residents are worried their water isn't safe?**



## MUNICIPAL EXAMPLES

PRIVACY BREACH  
LIABILITY

# **CANCELLED** **SCENARIO #2**

On the first day of summer camp, the Camp Supervisor puts down her laptop to assist a crying child. The unlocked laptop is stolen. It contains a file with a complete list of day camp attendees, including names, addresses, phone numbers, birthdates and health card numbers, now open and accessible to the thief:

- Laptop cannot be recovered and you have reason to believe it was taken for inappropriate means
- Notification of release of confidential information, including health information, must be sent to families



## MUNICIPAL EXAMPLES

PRIVACY BREACH  
LIABILITY

**CANCELLED**

Are you prepared with the financial and human resources to:

- Provide notifications to regulators and authorities?
- Draft and send notifications of potential breach to victims?
- Hire breach counsel?
- Provide post-breach services to victims as appropriate?
- Handle the public relations nightmare?

**Do you want parents to stop using municipal recreation services because they believe it is not safe?**



## MUNICIPAL EXAMPLES

SECURITY LIABILITY /  
EVENT MANAGEMENT

# **CANCELLED** **SCENARIO #3**

The municipal website is hacked and a notice is put up advising residents that if they sign up now, swimming lessons are offered free to all family members for one full year:

- Over 500 families sign up before the notice can be taken down
- Credit card information was collected to “reserve” the lessons, and has been compromised



## MUNICIPAL EXAMPLES

SECURITY LIABILITY /  
EVENT MANAGEMENT

**CANCELLED**

Are you prepared with the financial and human resources to:

- Carry out forensics to investigate the situation, solve the problem, and ensure it doesn't repeat?
- Follow the protocols dictated by your Payment Card agreement and industry standards?
- Notify the victims of the breach?
- Provide credit monitoring services to victims?
- Pay for the expenses needed to provide services without the revenue to support?

**Do you want your residents to be worried they can't trust your municipal website?**



**CANCELLED**

# SERVICES AVAILABLE TO HELP



SERVICES  
AUTOMATICALLY  
INCLUDED

## **CANCELLED** **Employee eLearning**

Awareness, training, and compliance. Customizable, web-based training and compliance to help reduce the single largest risk to an organization: human error.

## **Blacklist IP Blocking**

Powered by global threat intelligence. Helps prevent criminal activity on your network by blocking bad IP traffic – inbound or outbound.





**SERVICES  
AUTOMATICALLY  
INCLUDED**

## **CANCELLED** **Domain Protection**

Identify and block typo squatting domains. Protects your organization by identifying and blocking knockoff domains used by criminals. Their social engineering attacks trick employees into clicking on malware.

## **Infrastructure Vulnerability Scan**

Identification of high risk infrastructure vulnerabilities. Select parts of your internet-facing infrastructure to have experts examine and identify vulnerabilities that are open to potential exploits by cyber criminals.



**SERVICES  
AUTOMATICALLY  
INCLUDED**

## **CANCELLED** **Legal Risk Consultation**

Review and strengthen incident response capabilities. Two hours with an expert on incident response planning, regulatory compliance, security awareness, or privacy training.

## **Forensic Risk Consultation**

Organizational preparedness for different threat scenarios. One hour with a forensic expert on what an organization needs to think about and prepare for different threat scenarios.



**SERVICES  
AUTOMATICALLY  
INCLUDED**

**CANCELLED**

## **Public Relations Risk Consultation**

Crisis communication plan best practices and preparation. One hour with an expert to prepare and plan for your organization to handle potential scenarios if one should occur.

## **Insurance Portfolio Diagnostic**

Cyber as a peril analysis against insurance portfolio. Experts review your entire property and casualty portfolio to determine how it is anticipated to respond to the spectrum of cyber predicated financial and tangible losses.



**SERVICES  
AUTOMATICALLY  
INCLUDED**

## **CANCELLED** **CyberEdge Hotline and Information Portal**

Online access to cybersecurity information and cyber hotline 24/7/365.

Our CyberEdge Claims Hotline is available 24/7/365 at 1-800-CYBR-345 (1-800-292-7345). Once a call is made to the hotline, the CyberEdge Claims Team will coordinate with the client to implement their response plan, engage any necessary vendors including breach counsel and forensics firms to identify immediate threats (such as a hacker inside a network), and start the restoration and recovery processes.



SERVICES  
AUTOMATICALLY  
INCLUDED

**CANCELLED**

# Get Started Today

Take advantage of these services and improve your organization's protection against a cyber attack.

Visit [www.aig.ca/CyberRiskConsulting](http://www.aig.ca/CyberRiskConsulting) and complete the contact form, or

Email [CyberRiskConsulting@aig.com](mailto:CyberRiskConsulting@aig.com)



**For more information on how your policy transfers the risk of Cyber Attack through insurance, please contact:**

**Sara Runnalls FCIP CRM – Public Sector Risk Advisor**

**TF 1-800-668-5901 ext. 3067 E [srunnalls@bflcanada.ca](mailto:srunnalls@bflcanada.ca)**