Cyber Risk: Risk Management Progress So Far

The Threat Landscape

Phishing and Identity Theft

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss.

SANS Institute

95%

of all cyberattacks began with spear-phishing

Ponemon Institute

86%

of all phishing attacks contain ransomware

Anti Phishing World Group

65%

increase in phishing attacks compared to the previous year

https://gdpr.report/news/2017/06/08/new-trend-report-shows-email-phishing-attacks-hook-organizations/

AESI

The Threat Landscape

Simulated Ransomware Attack Shows Vulnerability of Industrial Controls

+DETAILS ⊕DOWNLOAD IMAGE +MORE PHOTOS

Posted February 13, 2017 • Atlanta, GA

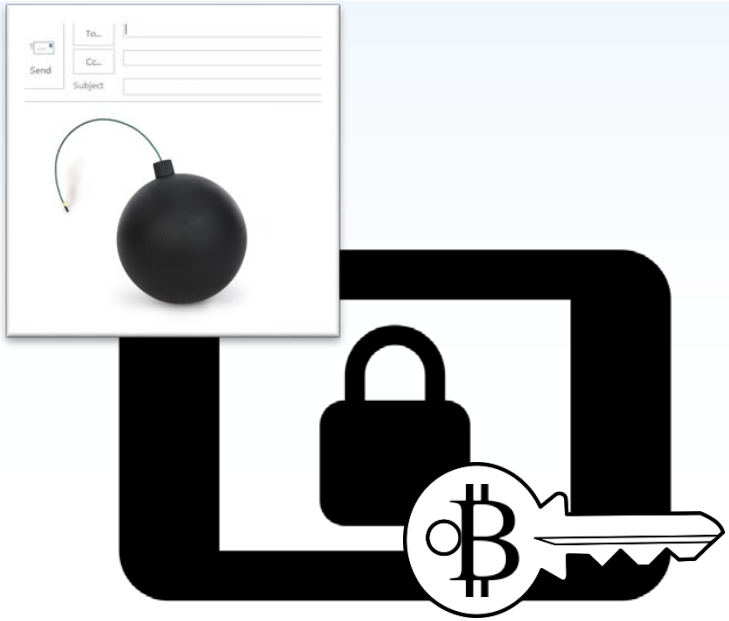
Cybersecurity researchers at the Georgia Institute of Technology have developed a new form of ransomware that was able to take over control of a simulated water treatment plant. After gaining access, the researchers were able to command programmable logic controllers (PLCs) to shut valves, increase the amount of chlorine added to water, and display false readings.

http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls

Cyber Attacks on Utilities

How a U.S. Utility Got Hacked

Michigan utility paid $25,000 ransom to get back into its systems after hackers from overseas took over its computers



"The ransomware was delivered via a phishing attack and malicious attachments that locked them out of all their systems. The Lansing Board of Water & Light chose to pay $25,000 in bitcoin because it was cheaper than replacing all the infected computers and software, which would have cost up to $10 million. As it is, the incident cost them $2.5 million to wipe the infected computers and beef up their security controls, much of which was covered by insurance."

https://www.linkedin.com/pulse/wsj-how-michigan-utility-got-hacked-ransomware-phil-neray

Cyber Attacks on Utilities

Jan 09, 2017 | Vote 0 0

St. Catharines Hydro's cyber fraud investigation continues

Board votes to have KPMG take audit to second phase

Niagara This Week - St. Catharines
By Melinda Cheevers

ST. CATHARINES — St. Catharines Hydro is proceeding to the second phase of a forensic audit as part of its investigation into an apparent phishing fraud that resulted in the theft of more than $655,000 from corporate coffers.

RELATED STORIES

Cyber thieves steal $655,000 from...

The company's board voted to proceed to the next phase on Jan. 6, following a presentation from professional service company KPMG who were hired to investigate the incident in late

NRP cruiser
NRP photo

Compromised Hydro One computer shows difficulty of tracking hackers

CTVNews.ca Staff
Published Tuesday, January 3, 2017 8:07PM EST
Last Updated Tuesday, January 3, 2017 9:17PM EST

The discovery that Ontario's main electricity distributor allegedly had an IP address compromised by Russian hackers is "a wake-up call" and should put Canadians on high alert for their personal cyber security, according to a technology analyst.

U.S. Homeland Security and the FBI found an IP address from Hydro One during an investigation into malicious cyber-activity allegedly linked to the hacking of the Democratic National Committee. Six other Canadian computer addresses were swept up in the digital search – including an IP address from an Alberta-based internet provider.

AESI

The Equifax Breach

After the breach, Equifax now faces the lawsuits

(Dado Ruvic/Reuters)

"Equifax has said its breach exposed sensitive information about 143 million consumers, including Social Security and driver's license numbers. This kind of data could be used for identity theft and to create fake accounts, cybersecurity experts have said."

https://www.washingtonpost.com/news/business/wp/2017/09/22/after-the-breach-equifax-now-faces-the-lawsuits/?utm_term=.7e7aedac895b

AESI

State Sponsored Activity

Official website of the Department of Homeland Security

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Description

Since at least March 2016, Russian government cyber actors—hereafter referred to as "threat actors"—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.

Analysis by DHS and FBI, resulted in the identification of distinct indicators and behaviors related to this activity. Of note, the report Dragonfly: Western energy sector targeted by sophisticated attack group, released by Symantec on September 6, 2017, provides additional information about this ongoing campaign. [1]

This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as "staging targets" throughout this alert. The threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims. NCCIC and FBI judge the ultimate objective of the actors is to compromise organizational networks, also referred to as the "intended target."

Technical Details

The threat actors in this campaign employed a variety of TTPs, including

- spear-phishing emails (from compromised legitimate account),
- watering-hole domains,
- credential gathering,
- open-source and network reconnaissance,
- host-based exploitation, and
- targeting industrial control system (ICS) infrastructure.

AESI

The Ontario Cyber Security Framework

Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a ***consistent and iterative approach*** *to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today".*

AESI

The Ontario Cyber Security Framework

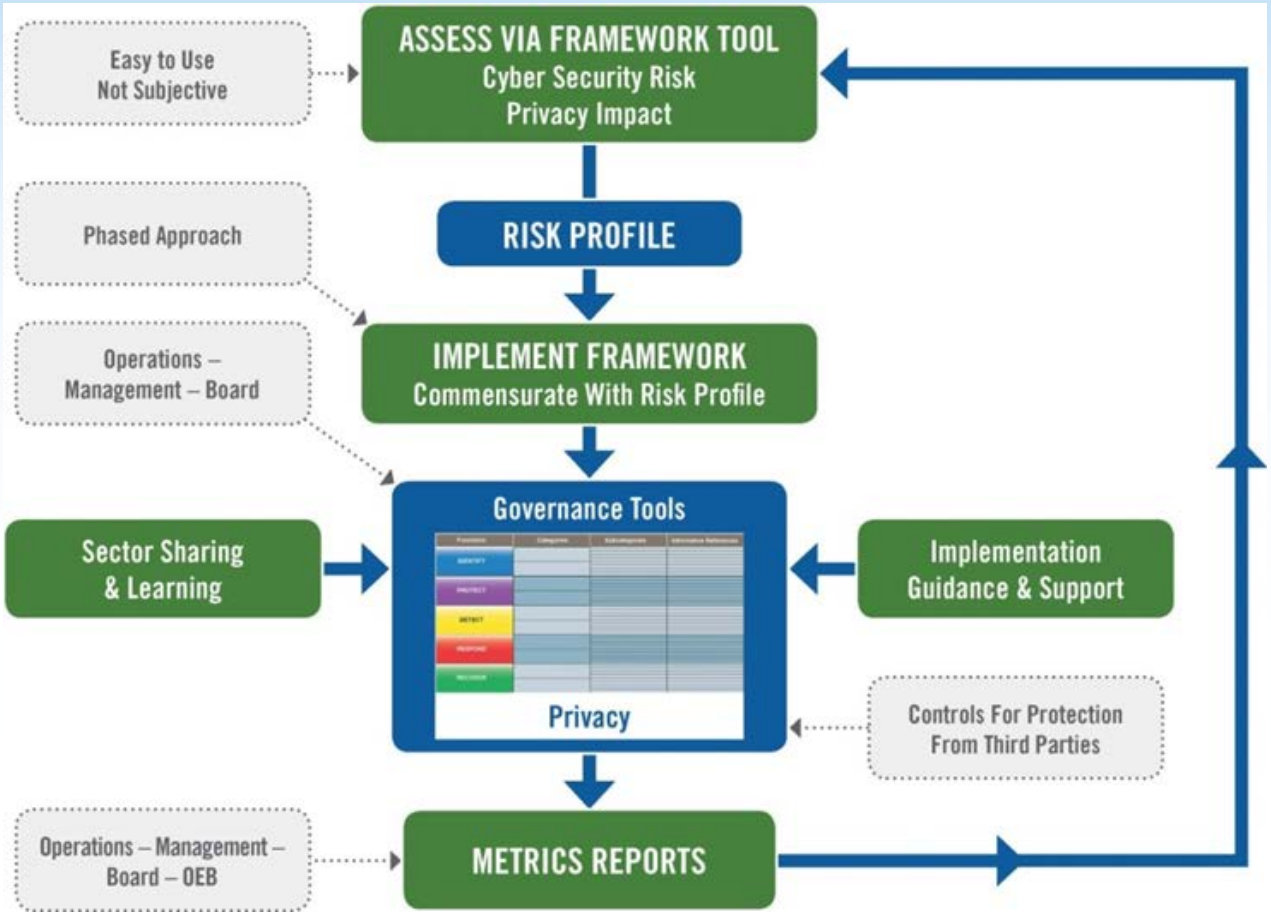
"Ontario is breaking new ground in developing a Framework that is focused on the distribution sector."

- Propose a set of benchmark control objectives for different risk levels
- Be scalable so that the Cyber maturity aligns with LDC risk
- Provide guidance on an evaluation method that can be used by the LDC
- Augment the Framework with training, tools and mechanisms to support assessment & implementation
- Encourage more sector sharing of Cyber Security Information
- Engage third parties (Phase 2) that interact with the distribution system to meet LDC's Cyber preparedness expectations

Source: Developing a Cyber Security Framework, EDIST 2017, Andres Mand (OEB) and Doug Westlund (AESI)

AESI

The Ontario Framework



Source: Staff Report to the Board, On a Proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors, Ontario Energy Board, June 1, 2017

NIST Framework – Structure

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

AESI

Privacy Integrated into the Framework

Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
	ID.GV-P1: A policy is established for collection, use and disclosure of customer personal and proprietary information, including requirements for consent and notification
	ID.GV-P2: A policy is established for retention and disposal of customer personal or proprietary information
	ID.GV-P3: Governance and risk management processes address privacy risks
	ID.GV-4: Governance and risk management processes address cybersecurity risks. The Executive Team and Board are actively involved and supportive of the Cyber Security Program.

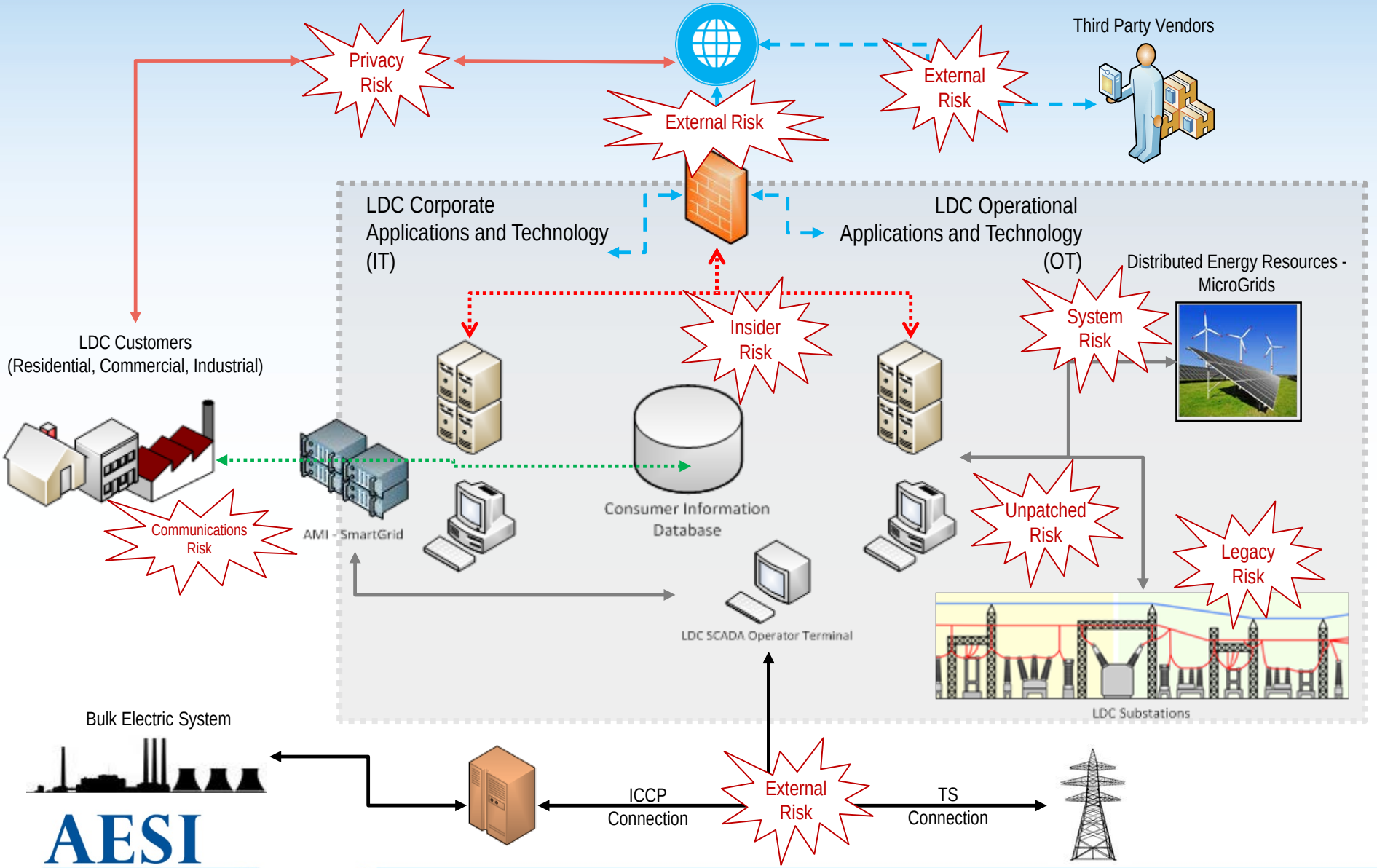
AESI

Implementing the Framework

- Executive and Board Support
- Team Effort
  - Representatives of Business and IT/OT
- Understanding of Accountabilities
- On-going awareness and continuous improvement
  - Not a one-and-done effort
  - Continuous reporting
  - Advancement in Maturity

Inherent Risk Profile Tool

LDC Attack Surface – Core to the OEB Framework



AESI

Inherent Risk Profile Tool

Question	Response	Risk Factor
Q1. Do you have a SCADA System ?	Response	RF1
Q2. How many customers do you serve ?	Response	RF2
Q3. Do you process credit card transactions or pre-authorized bank payments ?	Response	RF3
.		
.		
.		
Qn.	Response	RFn
		Total Risk Factor

Specifies

High Risk Profile

Medium Risk Profile

Low Risk Profile

AESI

Cyber Risk Management Techniques

Inherent Risk:

- Risk associated with business, operations, attack surface
- Security controls to be applied to address inherent risks and to improve risk posture

Residual Risk:

- Risks that remain after security controls have been applied
- Residual risks can be:
  - Addressed via additional security controls
  - Mitigated or partially mitigated through others means such as insurance
  - Intentionally not addressed

Risk Profile Tool Defines Security Controls

Function	Category	Subcategory	High	Med	Low
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	✓	✓	✓

Function	Category	Subcategory	High	Med	Low
DETECT (DE)	**Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.**	**DE.CM-4: Malicious code is detected**	✓	✓	

Function	Category	Subcategory	High	Med	Low
RESPOND (RS)	**Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.**	**RS.AN-3: Forensics are performed**	✓		

AESI

Self Assessment Questionnaire (SAQ) Tool

Function	Category	Subcategory	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Self Assessment	Self Assessment Notes
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	1	1	1	C2M2 ACM-1a: There is an inventory of OT and IT assets that are important to the delivery of the function	Select Status	
		ID.AM-2: Software platforms and applications within the organization are inventoried	1	1	1	C2M2 ACM-1a: There is an inventory of OT and IT assets that are important to the delivery of the function	Select Status	

AESI

SAQ Tool

Response	Definition
Yes	The expected testing has been performed and all elements of the requirement have been met
Yes with CCW[1]	The expected testing has been performed and the requirement has been met with the assistance of a compensating control.
No	Some or all of elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be know if they are in place
N/A	The requirement does not apply to the organization's environment.
Not Tested	The requirement was not included for consideration in the assessment, and was not tested in any way

[1] CCW compensating control worksheet – this is a document that has additional controls outlined that were required to ensure compliance with the tests performed.

Action Plan Process