Cyber Security For Utilities
Risks, Trends & Standards

IEEE Toronto – March 22, 2017

Doug Westlund

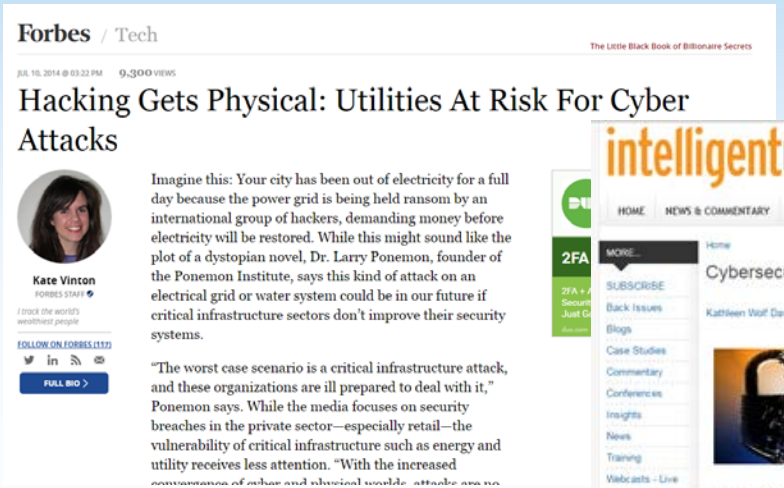
Senior VP, AESI Inc.

Agenda

- **Cyber Security Risks for Utilities**
- **Trends & Recent Incidents in the Utility Sector**
- **Standards**
- **Q & A**

Physical & Cyber Security for Utilities

The Threat Landscape


Forbes / Tech

The Little Black Book of Billionaire Secrets

JUL 10, 2014 @ 03:22 PM 9,300 VIEWS

Hacking Gets Physical: Utilities At Risk For Cyber Attacks

Kate Vinton
FORBES STAFF
I track the world's wealthiest people
FOLLOW ON FORBES (117)
FULL BIO >

Imagine this: Your city has been out of electricity for a full day because the power grid is being held ransom by an international group of hackers, demanding money before electricity will be restored. While this might sound like the plot of a dystopian novel, Dr. Larry Ponemon, founder of the Ponemon Institute, says this kind of attack on an electrical grid or water system could be in our future if critical infrastructure sectors don't improve their security systems.

"The worst case scenario is a critical infrastructure attack, and these organizations are ill prepared to deal with it," Ponemon says. While the media focuses on security breaches in the private sector—especially retail—the vulnerability of critical infrastructure such as energy and utility receives less attention. "With the increased


intelligentutility

HOME NEWS & COMMENTARY CALENDAR RESOURCES MAGAZINE SUBSCRIBE

MORE...
SUBSCRIBE
Back Issues
Blogs
Case Studies
Commentary
Conferences
Insights
News
Training
Webcasts - Live
Webcasts - On Demand
White Papers
Advertise/Media Kit/Edit. Calendar
About Us
Contact Us

Home

Cybersecurity and the electric grid

Kathleen Wolf Davis | Sep 15, 2014

By Marvin T. Griff

A computer storing operating cost data for the Midcontinent Independent System Operator Inc., power network extending from the Midwest to the Gulf Coast was compromised this summer. Within the past two years, sophisticated cyber-attacks, whose colorful names "Dragonfly" and "Energetic Bear" belie their disruptive capability, gained access to U.S. and European power networks. These and other recent cyber intrusions highlight the persistent risk confronting the U.S. electricity grid.

The source of a breach to the electricity system is often closer than one might think. A survey of global IT and IT security executives in the energy industry released by Unisys this summer reveals a majority of companies have had at least one security compromise in the past 12 months leading to the loss of confidential information or disruption of operations. Most survey respondents said the breach was likely caused by a negligent employee with privileged access and that their firms' cybersecurity


The Dallas Morning News

Home News Business Sports Entertainment Arts & Life Opinion Obits Marketplace DMNstore
Communities Crime Education Investigations State Nation/World Politics Videos Photos

News › General News

General News

Breach of power: Foreign hackers prove capable of crippling U.S. electric grid

Facebook Twitter Email Comments Print

All your Local News


San Francisco
1:57 PM PT

LIGHTS OUT
TOP OFFICIALS WARN OF APOCALYPTIC CYBERATTACK ON POWER GRID
CNN
NAS ▲ 73.40
THE LEAD


IT WORLD CANADA

CIO CSO MOBILE STORAGE CLOUD RESEARCH EVENTS NEWS VIDEO BLOGS #T

Hewlett Packard Enterprise
Push profit margins with flexible financing and on-demand capacity.*

Shocking debate: How unprepared are electrical utilities for cyber attacks?

Howard Solomon - December 3, 2015

When mischief makers and thugs want to create chaos in a country these days among their first targets are the financial system and utilities.


Entrust

Cybersecurity High on List of Energy Sector Concerns

Posted by Entrust in Authentication

August 25, 2014

As technology continues to grow more ubiquitous in everyday life, its use in the running of regular processes is becoming increasingly common. While this is true for every industry, the energy sector has adopted the use of technology especially aggressively.

The control rooms of substations and the myriad devices used to manage the energy industry's critical infrastructure are all digital now, increasing the risk that they will fall victim to cyberattacks.

Those working in the sector have acknowledged the growing danger of cybercriminals in a recent survey by construction and engineering firm Black and Veatch. The firm's study found cybersecurity to be one of the top five concerns for U.S. electrical companies this year.

In the same survey conducted in 2013, cybersecurity was the sixth on the the industry's list of biggest worries but this year has risen to fourth. Though the issue is considered such a threat to energy companies, only 32 percent of electrical utilities surveyed reported having security systems that were integrated with the appropriate segmentation, monitoring and redundancies

AESI

The Threat Landscape

Simulated Ransomware Attack Shows Vulnerability of Industrial Controls

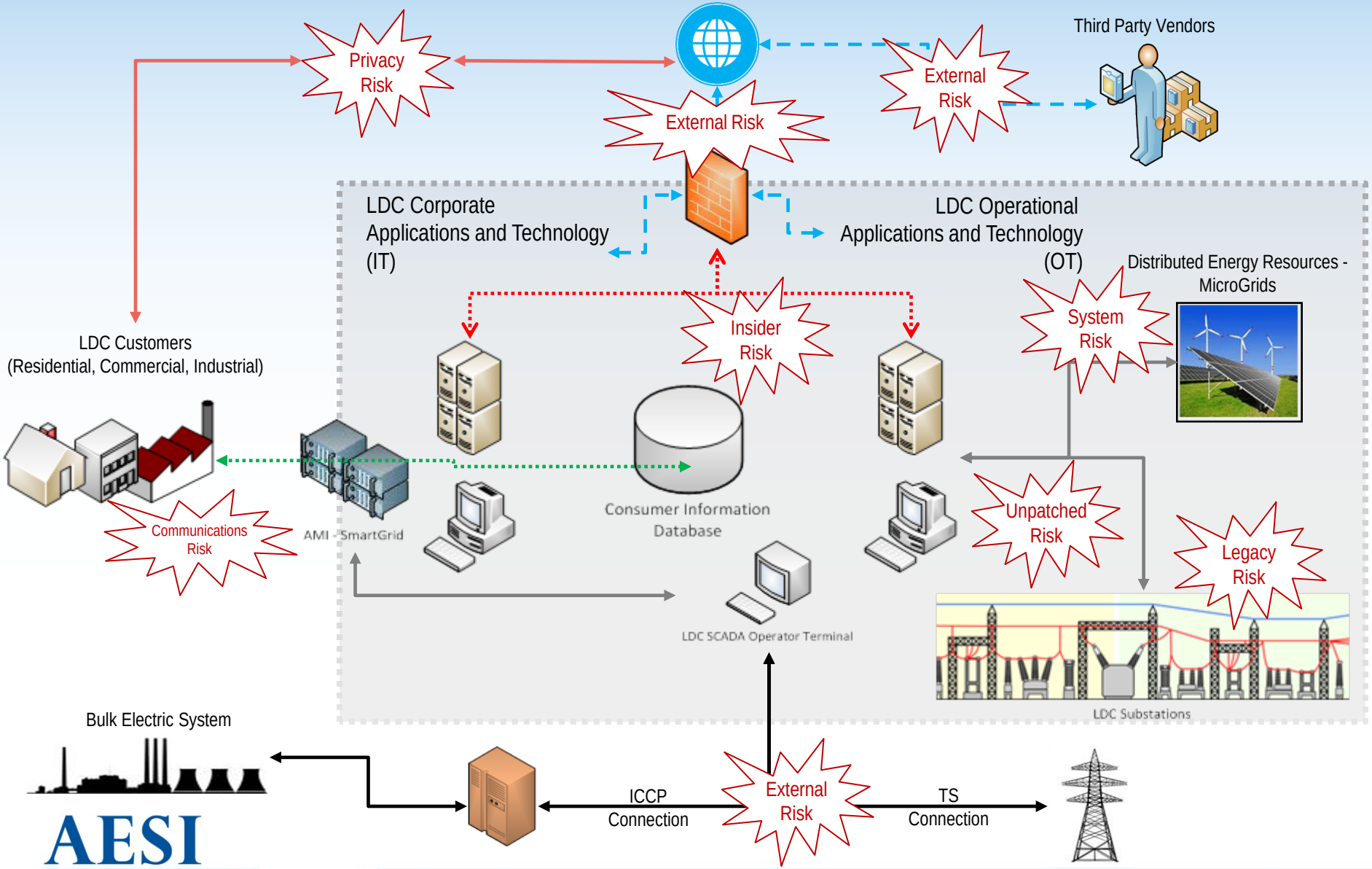
+DETAILS DOWNLOAD IMAGE +MORE PHOTOS

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

The LDC Attack Surface



AESI

Chronology of a Typical Cyber Attack

Development of Target

Gain Access with Discovery

Arm Cyber Weapons & Launch Attack

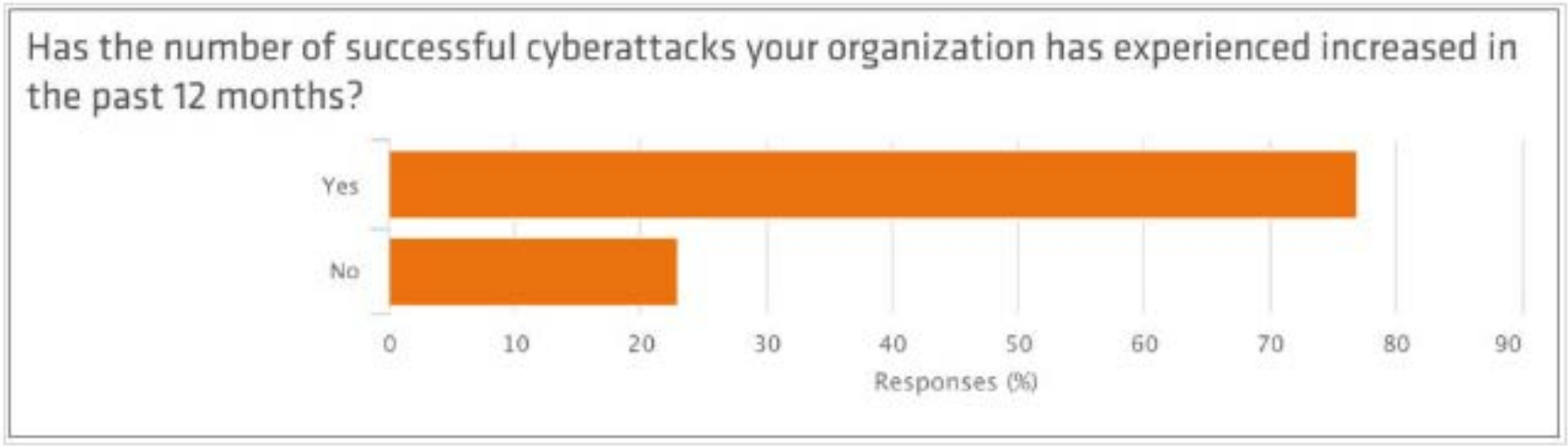
Exploit

Cover Up

Trends & Recent Incidents

In the Utility Sector

Cyber Attacks on Utilities



Electric utilities and companies in the oil, gas and other energy sectors have seen a rash of cyberattacks, information technology workers say.

COURTESY TRIPWIRE

http://www.usnews.com/news/blogs/data-mine/2016/04/08/cyberattacks-surge-on-energy-companies-electric-grid

Cyber Attacks on Utilities

JUL 07

'Dragonfly' Virus Strikes U.S. Power Plants

U.S. and European energy companies have become the target of a "Dragonfly" virus out of Eastern Europe that goes after energy grids, major electricity generation firms, petroleum pipelines operators and energy industrial equipment providers. Unearthed by the cyber security firm

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.

Cyber Security & Overall Risk Management

Top 10 risks

In every survey, respondents are asked to rank formidable risks facing their companies. We then choose the top 10 risks for detailed discussion, which is one of the perennial highlights:

1. Damage to reputation/brand
2. Economic slowdown/slow recovery
3. Regulatory/legislative changes
4. Increasing competition
5. Failure to attract or retain top talent
6. Failure to innovate/meet customer needs
7. Business interruption
8. Third-party liability
9. Computer crime/hacking/viruses/malicious codes
10. Property damage

"Computer crimes/ hacking have emerged for the first time as a top-10 risk"

"Cyber risk is fast moving, impossible to predict, and difficult to understand, but the damage can be immense"

http://www.aon.com/2015GlobalRisk/

Trends & Future Considerations

Advanced Persistent Threats

Growing Attack Surface

Liabilities

Financial Risk

Resources / Budgets

Business & Operational Risk

Philosophy & Culture of Cyber Security

- **It is a Risk Management issue, not an IT issue**
- **Executive Team / Management Team / Board support is crucial**
- **It is a continuous process requiring increasing maturity levels, not a "one and done"**

DOE C2M2 Maturity Levels
MIL0: Not Performed
MIL1: Initiated
MIL2: Repeatable
MIL3: Managed / Adaptive

- **Can emulate existing safety programs**

AESI

Standards

Bulk vs Non-Bulk Electric System Standards

	Bulk System	Non-Bulk System
Utility Types	**Generators, Transmission Entities**	**Distribution Entities**
Examples	**OPG, Hydro One**	**Toronto Hydro**
Mandatory Cyber Security Standards	**NERC CIP**	**Ontario: OEB Framework** **Rest of North America:** **None (NIST = de facto)**

NERC CIP Standards

CIP v6	Title
CIP-002-5.1	Bulk Electric System (BES) Cyber System Categorization
CIP-003-6	Security Management Control
CIP-004-6	Personnel & Training (Access Management)
CIP-005-5	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5	Cyber Security Incident Reporting and Response Planning
CIP-009-6	Recovery Plan for BES Cyber System
CIP-010-2	Configuration Change Management & Vulnerability Assessment
CIP-011-2	Information Protection
CIP-014-2	Physical Security of Transmission Stations

NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity

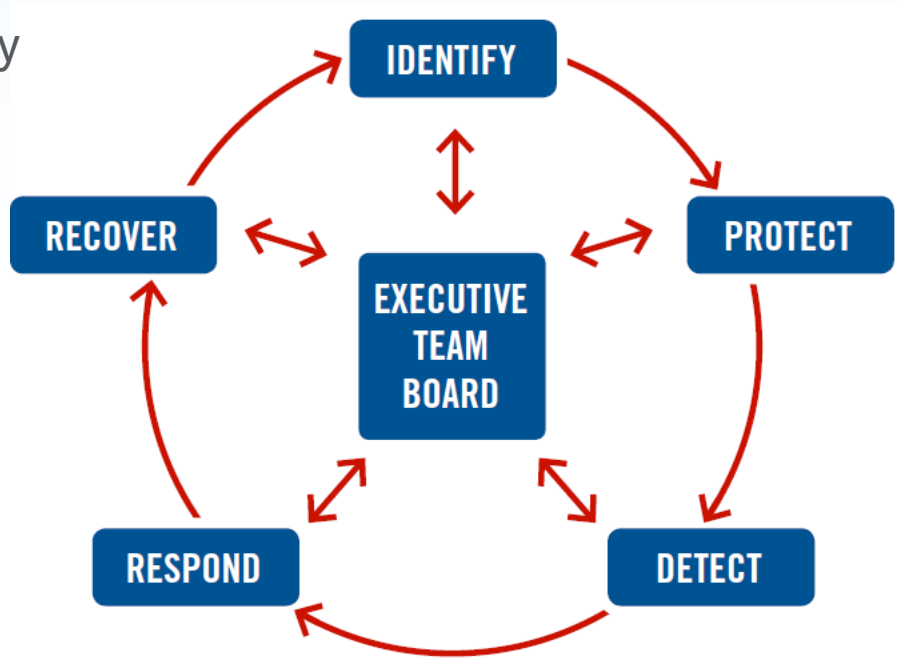
Identify:1. Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy

Protect:2. Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology

Detect:3. Anomalies and Events, Security Continuous Monitoring, Detection Processes

Respond:4. Response Planning, Communications, Analysis, Mitigation, Improvements

Recover:5. Recovery Planning, Improvements, Communications




Questions
Answers

Thank You

Doug Westlund

Senior VP

AESI Inc.

dougw@aesi-inc.com

905-875-2075 ext 278