Brown AND Caldwell

PNWS AWWA

Cybersecurity in the "Utility of the Future"

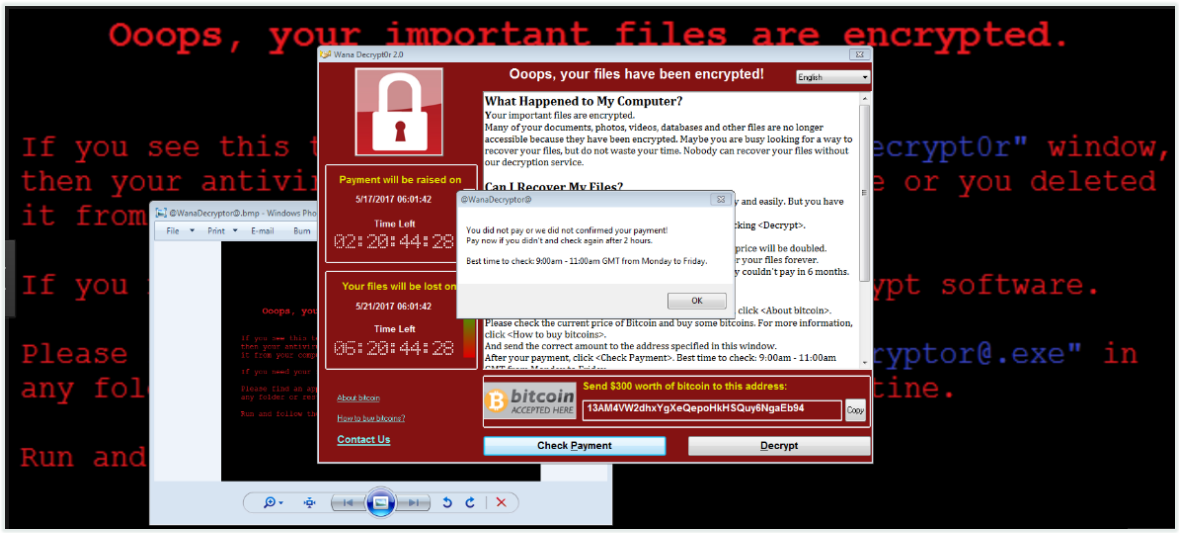
Mark Castagneri, PE, CISSP | Michael Karl, Project Manager

Cybersecurity Agenda

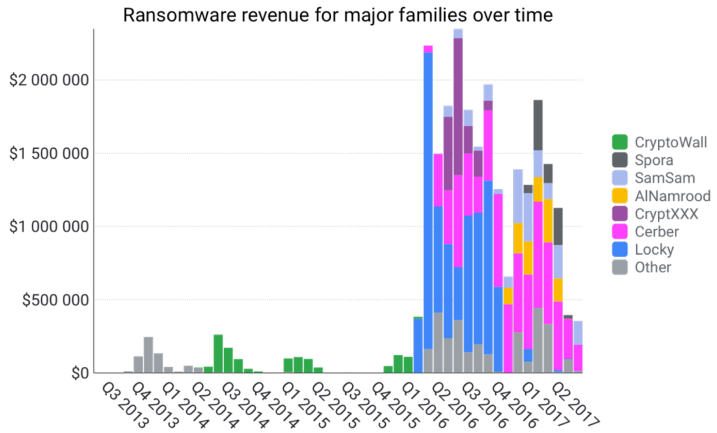
1. Understand Current Risks, Trends
2. Cut Through the maze of Due Care Standards
3. Cybersecurity and Physical Security
4. Risk & Priority – The AWWA Tool
5. How can I influence budgets to implement risk reduction?

Industry examples of risk

Drivers: Ransomware



Drivers: Ransomware as a Service



Notable 2018 Events

- Boeing Jet Factory
- City of Atlanta
- Colorado DoT

Estimated Annual Revenue

- 2015 - $315M
- 2017 - $5B
- 2019 - $11B

RaaS

- Provide bitcoin wallet
- Purchase Ransomware App
- Rent bulletproof proxy
- In business!

Sources: CIS, Cybersecurity Ventures

Drivers: Belligerent Nation State APT

FBI and Department of Homeland Security Issue Alert

"Since at least March 2016, Russian government cyber actors…targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors," according to a joint alert issued by the Department of Homeland Security and the FBI.

— Rick Perry during a House Appropriations Subcommittee hearing in Washington on March 15.

Drivers: Cyberwarfare

Nation States: Advanced Persistent Threat, March 2017

- Ukrainian power transmission tower relays tripped
- Grid blackout

CYBER RISK | Thu May 11, 2017 | 10:59am EDT

Suspected Russia-backed hackers target Baltic energy networks

FILE PHOTO: A man types on a computer keyboard in front of the displayed cyber code in this illustration picture taken March 1, 2017. REUTERS/Kacper Pempel/Illustration/File Photo 1/2

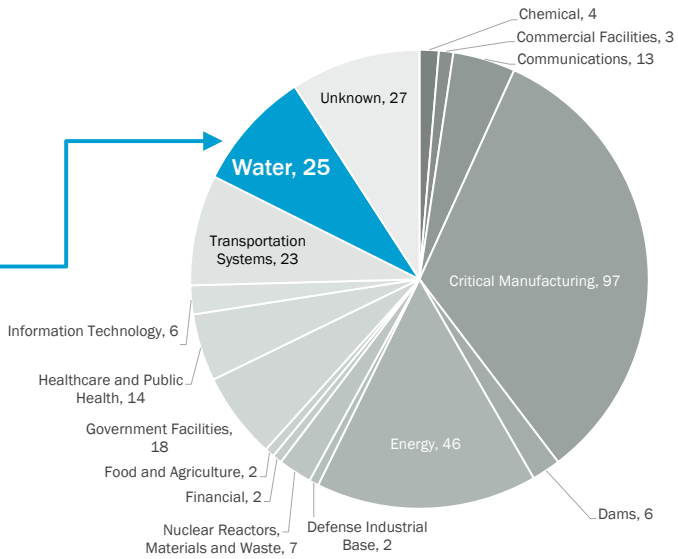
By **Stephen Jewkes** and **Oleg Vukmanovic** | MILAN/LONDON

Suspected Russia-backed hackers have launched exploratory cyber attacks against the energy networks of the Baltic states, sources said, raising security concerns inside the West's main military alliance, NATO.

Is Water impacted?

Department of Homeland Security incident analysis data

Water a significant slice of the pie....



Verizon 2017 Data Breach Digest

2018 Cyber Threat Outlook

Threat Vectors // Ransomware, Electronic Theft

Threat /Action	Target / Prevalence
Ransomware Encrypts computer preventing any function, Bitcoin ransom to decrypt, restoring function.	Municipalities and water treatment plants of any size. Rapid growth in 2018 expected. City of Atlanta notable recent victim (March 2018), Lansing, MI Board of Water and Light, many others.
Zeus Cyber Theft Ring / Invoice Theft Steals banking credentials, moves money out of victim accounts. Invoice Scams targeting Accounts Payable Staff	2007 malware still prevalent in 2017, now targeting smaller orgs with older systems

2018 Cyber Threat Outlook

Threat Vectors // Cryptomining, cyberwarfare, IIoT

Threat /Action	Target / Prevalence
Cryptomining Uses bandwidth and CPU of unprotected servers to mine cryptocurrencies	Any unmonitored or unprotected network (nearly all Water, Wastewater networks are unmonitored). Monero cryptocurrency can be mined with any computer.
Cyberwarfare Stolen Weapons / Terror & Disruption goals	Critical Infrastructure including W/WW. Secretary of Energy, FBI, DHS issued warning March, 2018.
Industrial Internet of Things, Digital Transformation More connections = more risk.	Widespread technology expansion, suppliers providing secure solutions if integrated properly.

Cybersecurity Law and Standards

State Cybersecurity Initiatives

- New York, New Jersey require cybersecurity program compliance for critical infrastructure, including water and wastewater
- Utah has voluntary outreach – Governor's program
- Additional State Legislatures considering regulated cybersecurity
- State efforts align with Executive Orders
- All reference NIST as common requirements framework

Due Care Cyber Security Standards

ISA/IEC 62443
ISO 27001/2
NIST SP 800-w82
NIST SP 800-171
NIST SP800-53
....

Which to Use?

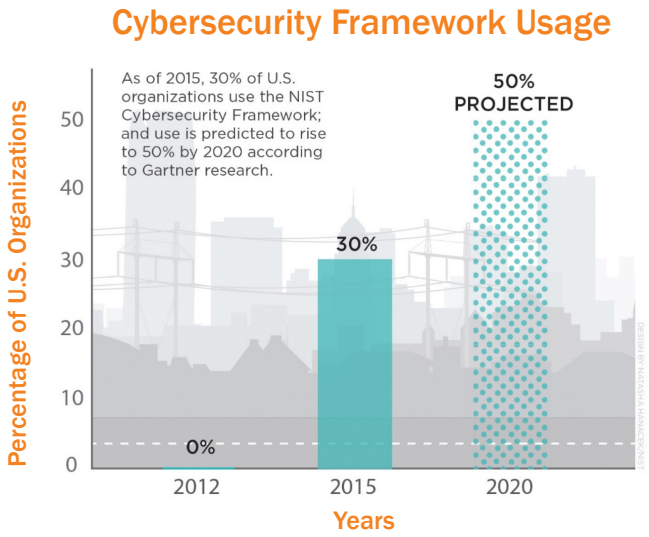
NIST, ISO, ISA/IEC, and ***more....***

- Any can provide effective cybersecurity programs
- Significant overlap, highly equivalent
- Some standards apply to an industry or data class
- Discipline jargon make them hard to understand

Due Care Cyber Security Standards – choose NIST

NIST SP800-82	Maps to NIST Common Security Framework (CSF)	Supported by Executive Order	Broad Adoption	Industry tools map to NIST CSF
Focus on Industrial Control Systems	Translated into Common English, Understandable	EO February 2013 – required NIST to develop a risk reduction framework	48% of ICS Managers map internal polices, standards and practices to NIST CSF (SANS 2017)	DHS ICS-CERT Risk Assessment Tool
References underlying NIST SP800-53 Controls, "The Bible"	Maps equivalency to many standards			
Provides interpretations for ICS	Provides a maturity model for phased implementation	EO May 2017 requires Federal Agencies to use the NIST Framework for risk reduction	More than 50% of private sector organizations will be using this framework by 2020 (Gartner, 2018)	Many commercial tool providers: Microsoft, Tripwire, Alienvault
Graded approach to controls application (H,M,L)	Adaptable to industry and Corporate Risk Appetite			

NIST CSF Adoption



Cybersecurity and Physical Security

Brown AND Caldwell

Physical and Cybersecurity Comparisons

Cartoon credits: The Economist 2009

VS

Equivalent Cyber and Physical Security Controls

Physical Security Control	Equivalent Cybersecurity control
Critical equipment secured by fenced area, locked cabinets within fenced area,	Intrusion Prevention System (IPS), defense in depth zone control
Break glass alarms; motion, IR sensors; video cams	Network monitoring and Intrusion Detection System (IDS)
Locked doors	Firewalls, blacklisting
Key management	Role-based access control (RBAC) (e.g. active directory)
Guard patrol, emergency radio, response team	Network monitoring and incident response
Strong fences, reinforced walls and ceilings	Hardware and software hardening
Control room badge access	RBAC, whitelisting

These controls have the same objective » **Safeguard mission-critical equipment**

So what is the State of Industrial Cybersecurity?

Cartoon credits: The Economist 2009

Defense in Depth

VS

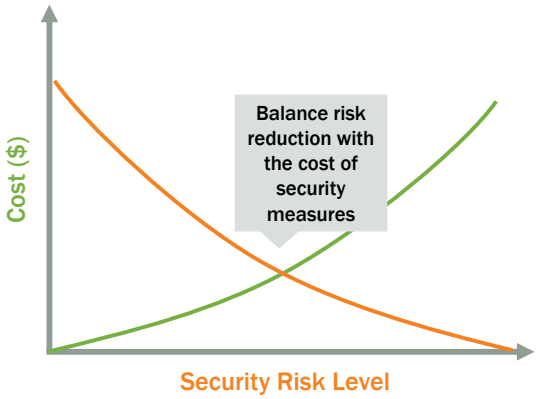
Too little too late?

Risk and Priority
The AWWA Use Case Tool

Brown AND Caldwell

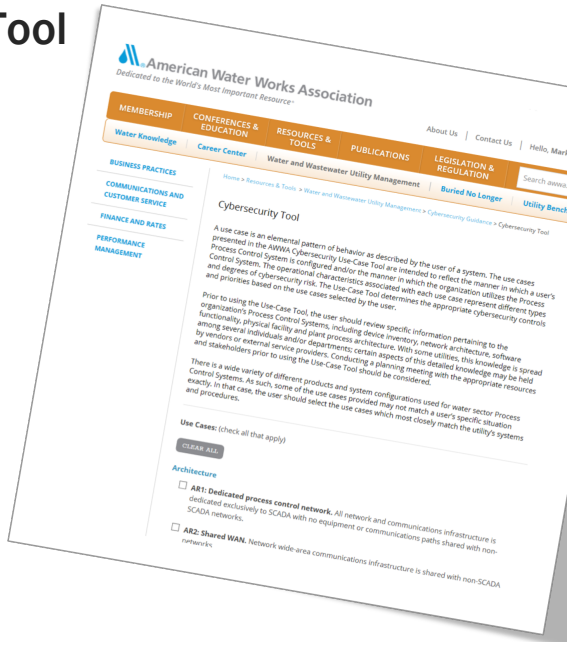
We can Improve Security and Reliability!

- Good security reduces inadvertent error, improves reliability
- AWWA Use Case Tool provides clarity on what controls apply
- Prioritized controls reduce exposure to threats
- Provides a consistent, repeatable, course of action



AWWA Cybersecurity Use Case Tool

- Incorporates NIST security controls
- Approved by EPA
- Supports Executive Orders for Critical Infrastructure signed by Presidents Obama and Trump
- Provides a process to define operations and determine security controls applicable to them
- Implements Department of Homeland Security Requirements
- Focused on the Water and Wastewater sector



Recommended Controls Priorities

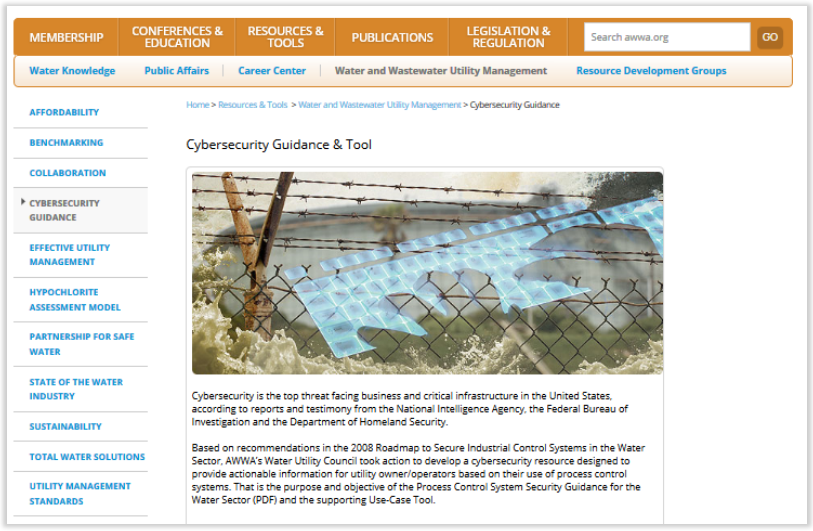
The Tool provides a prioritized list of recommended controls as follows:

- **Priority 1 controls** – minimum level of acceptable risk reduction
- **Priority 2 controls** – baseline level of functioning cybersecurity program
- **Priority 3 controls** – more mature program, managed with performance metrics
- **Priority 4 controls** – mature implemented program, can provide protection against advanced persistent threats.

Introducing the AWWA Use Case tool

Brown AND Caldwell

Selecting Use Cases



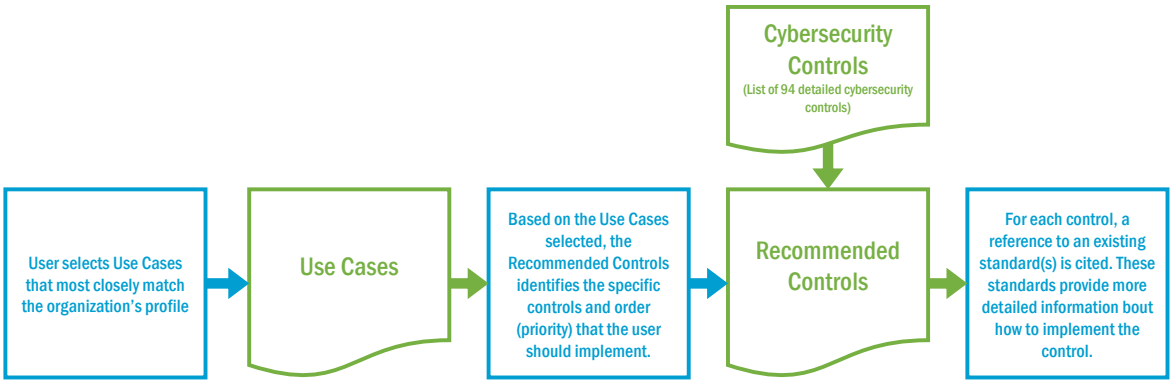
What is a Use Case?

Elemental pattern of user behavior

Basic descriptions of important processes within PCS

Control system elements that define system configuration

How are Controls Selected by the Cybersecurity Guidance Tool?



Architecture

- ☐ **AR1: Dedicated process control network.** All network and communications infrastructure is dedicated exclusively to SCADA with no equipment or communications paths shared with non-SCADA networks.
- ☐ **AR2: Shared WAN.** Network wide-area communications infrastructure is shared with non-SCADA networks.
- ☐ **AR3: Shared LAN.** Network local-area communications (within control system) is shared with non-SCADA networks.
- ☐ **AR4: Unlicensed wireless Wide-Area (site-to-site) Network.** Network wide-area communications fully or partially comprised of wireless links using unlicensed (ISM 900 MHz, 2.4 or 5 GHz) spectrum.
- ☐ **AR5: Licensed wireless Wide-Area (site-to-site) Network.** Network wide-area communications fully or partially comprised of wireless links using licensed spectrum.
- ☐ **AR6: Communications via Internet.** Network wide-area communications fully or partially comprised of links over Internet services using public address space.
- ☐ **AR7: Communications via 3rd party carrier.** Network wide-area communications fully or partially comprised of links over 3rd party carrier services (e.g. cellular, Metro-E/Ethernet/LAN).
- ☐ **AR8: Dedicated process control server virtualization.** Virtualized server infrastucture dedicated to SCADA/Process Control with no equipment shared with non-SCADA/Process Control systems.

Information needed for the tool and results

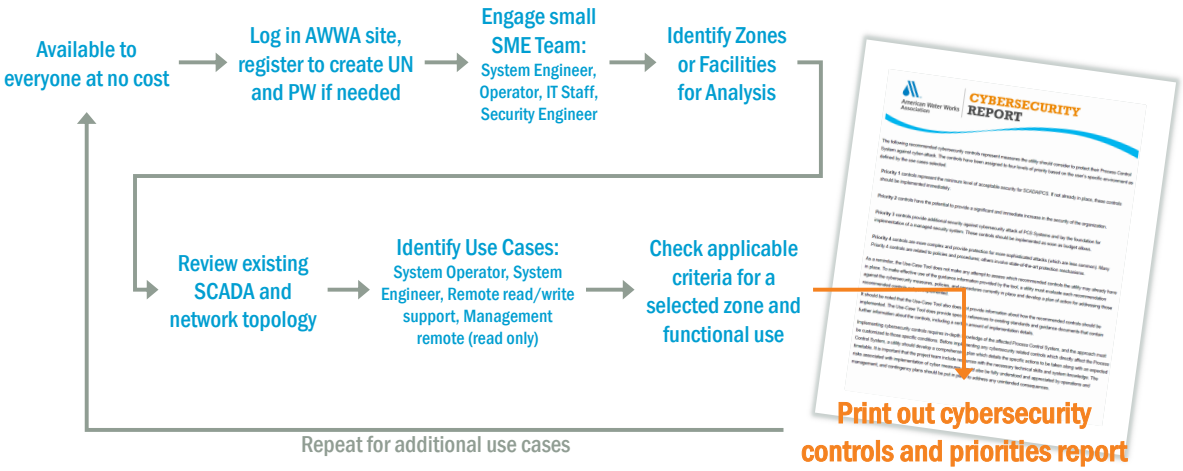
How are Use Cases evaluated against the Existing Control System?

- Users with appropriate subject matter expertise and system knowledge read each use case and determine if it applies to their system
- Use cases that most closely match the utility's PCS configuration and practices are selected
- Use cases that do not match the current state of the PCS are removed from further consideration

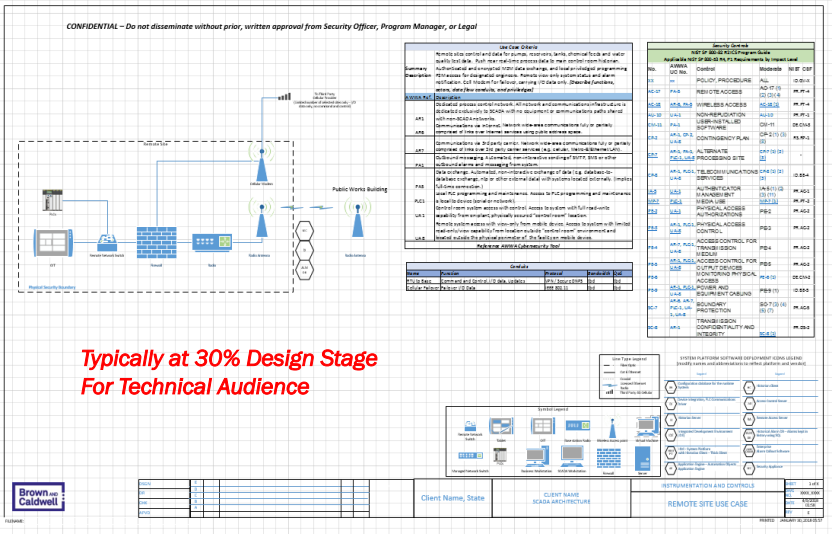
What should a well designed Use Case Provide?

- ☑ Logical functional and security architecture
- ☑ Description of communication channels, protocols, ports and services
- ☑ Identification of key applications that are a part of the Trusted Computing Base
- ☑ Description of functional actors and their privileges: Engineer, Operator, Manager,
- ☑ AWWA Use Case tool criteria descriptors
- ☑ NIST cross reference
- ☑ Demonstrated compliance to relevant executive order and NY, NJ cybersecurity mandates for cybersecurity

Executing the Tool



Cybersecurity Use Case Example – Remote Site



Features:

- AWWA Use Case Descriptors
- Security Requirements Shown
- Trusted Computing Base Shown
- H, M, L impact level Shown

Cybersecurity Use Case Example – Remote Site NIST CSF

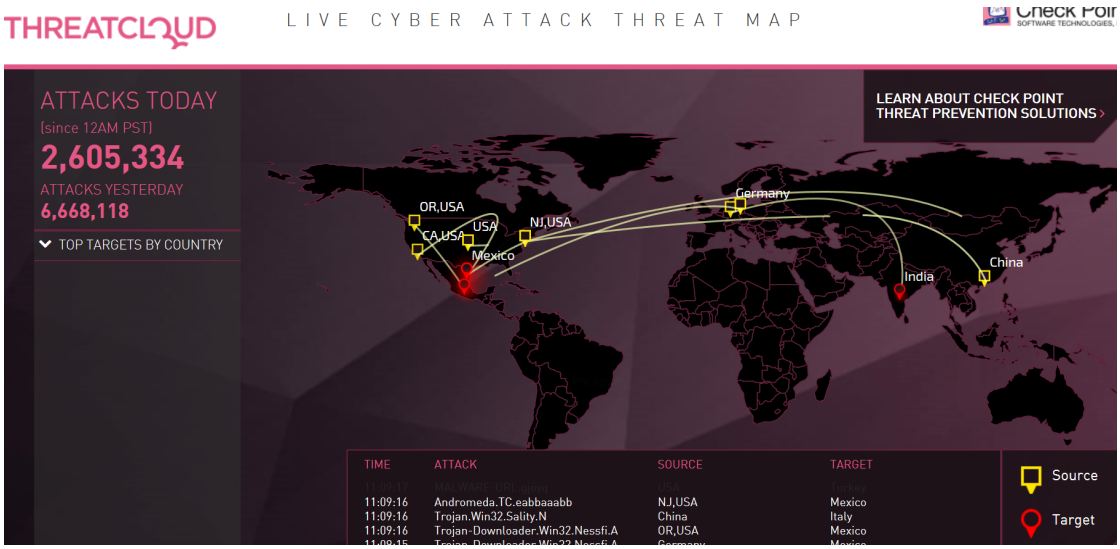
Security Control Families

IDENTIFY (ID)	ID.BE-4: Dependencies and critical functions for delivery of critical services are established
	ID.GV-1: Organizational information security policy is established
PROTECT (PR)	PR.AC-1: Identities and credentials are managed for authorized devices and users
	PR.AC-2: Physical access to assets is managed and protected
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate
	PR.DS-2: Data-in-transit is protected
	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
	PR.PT-2: Removable media is protected and its use restricted according to policy
	PR.PT-4: Communications and control networks are protected
DETECT (DE)	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
RESPOND (RS)	RS.RP-1: Response plan is executed during or after an event

How to bring awareness of this critical need to my utility

Brown AND Caldwell

Cyber Attack Map



Return on Investment

ROI = ((ALE)(RM) – SC)/ SC

ALE (Annual Loss Expectancy) = Annual probability of occurrence x Loss Estimate in dollars

SC = Solution Cost; RM = % of Risk Mitigated by Solution

Let's use Atlanta's Ransomware example

Loss Estimate = $2.7M

Annual Probability: Assume once every five years (.2)

Solution cost: $100K to segment network, firewalls, critical backups, will mitigate 75% of ransomware risk

ROI = (($2,700,000)(.2)(.75) - $100,000)/ $100,000

= 305%

Cybersecurity Need Awareness – Sources of Information

- Industrial Control System Threat Feeds and analysis
  - Department of Homeland Security - ICS Threat Feed
  - New Jersey Cybersecurity Threat Feed
- National Vulnerability Database
  - https://nvd.nist.gov/vuln/search
  - Test this out – search on a critical switch, router, server, application in your system!
- State Legislation – current and outlook
  - NY Department of Health Water Vulnerability Assessment and Emergency Response
  - NJ Board of Public Utilities – Cyber Security Program Requirements
  - National Governor's Association – Resource Center for State Cybersecurity
- Sources of costs
  - Council of Economic Advisors: The Cost of Malicious Cyber Activity to the U.S. Economy
  - IBM Breach Calculator
- Real-Time Attack Maps
  - https://threatmap.checkpoint.com/ThreatPortal/livemap.html
  - https://threatmap.fortiguard.com/

Mark Castagneri, PE, CISSP

mcastagneri@brwncald.com

T 303.968.2010

C 303.802.7961

Michael Karl, Project Manager

mkarl@brwncald.com

T 206.749.2236

C 425.749.2020

Brown AND Caldwell