

Water, a Vial Resource, needs Cybersecurity too!

Basics, Tips and Tricks

September 24, 2021

Shawn Taylor / Senior Systems Engineer & Customer Evangelist

 @smtaylor12





Topics

1

In the News & Current Threats

2

Best Practices: Tips, Tricks and Recommendations

3

Atlanta Case Study

In the News...



U.S. Water Supply System Being Targeted By Cybercriminals



Israel Thwarts Major Coordinated Cyber-Attack on Its Water Infrastructure Command and Control Systems



But wait, there's more...

Two Critical U.S. Dams at High Risk From Insider Cyber Threats > A new report by the Interior Department's Inspector General highlights several basic cybersecurity issues

“Significant control weaknesses” in account management and personnel security practices left two dams open to compromise from insider attacks.

Hacker Charged in Breach of New York Dam

How have the attacks originated?

<) Watering Hole Attack

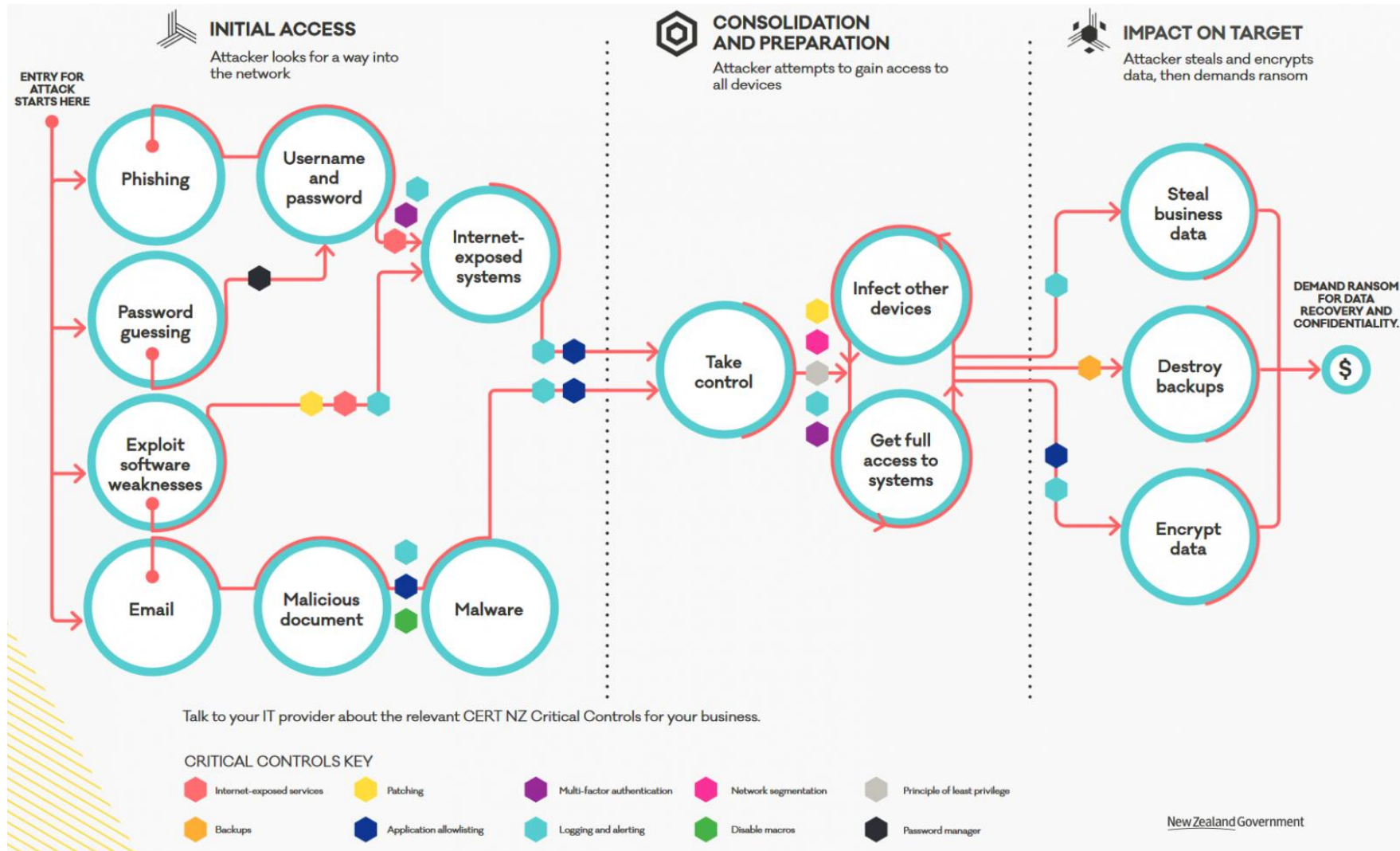
- Attacker compromises frequently-visited website; user visits website/payload is downloaded; malware is loaded and malicious activity is initiated; malware is spread/add'l damage occurs

<) Orphaned account credentials

- Especially for remote control software

<) Internet-connected components

Sample Ransomware process flow



[Researchers compile list of vulnerabilities abused by ransomware gangs \(bleepingcomputer.com\)](https://bleepingcomputer.com)

CIS Top 20 Controls – Prioritized List



V7.1

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

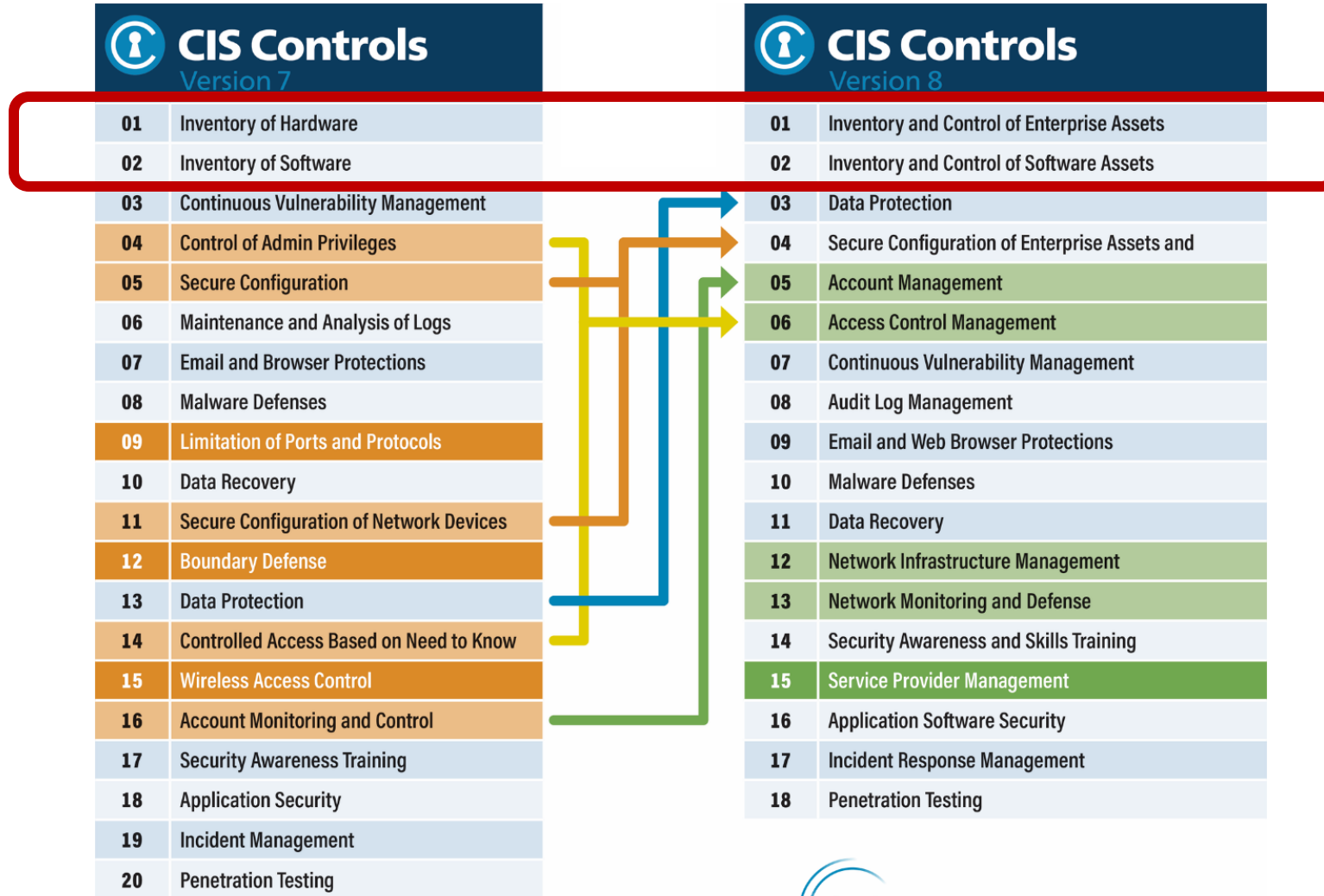
Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

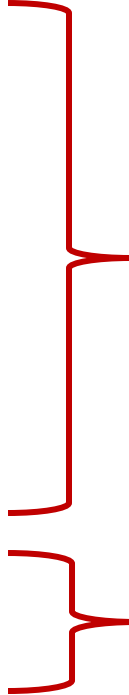
- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

CIS Top 18 Controls



Best Practices

- Keep all systems patched. Effective patching requires:
 - Know what systems are on the network.
 - Implement:
 - CIS Control 1.4: Maintain Detailed Asset Inventory
 - Know what software is running on the network.
 - Implement:
 - CIS Control 2.1: Maintain Inventory of authorized Software.
 - CIS Control 2.2: Ensure software is supported by vendor
 - CIS Control 2.6: Address unapproved software
 - Patch your systems.
 - Implement:
 - CIS Control 3.4: Deploy Automated Operating System Patch Management Tools
 - CIS Control 3.5: Deploy Automated Software Patch Management Tools
- Use anti-virus and anti-spam solutions.
 - Implement:
 - CIS Control 8.2: Ensure Anti-Malware Software and Signatures are Updated
- Protect sensitive data.
 - Implement:
 - CIS Control 13.1: Maintain an Inventory of Sensitive Information
 - CIS Control 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization
 - CIS Control 14.6: Protect Information through Access Control Lists
- Train all employees on how to identify and report suspicious activity and to not click on links or download files within any suspicious emails.
 - Implement:
 - CIS Control 17.3: Implement a Security Awareness Program
 - CIS Control 17.6: Train Workforce on Identifying Social Engineering Attacks

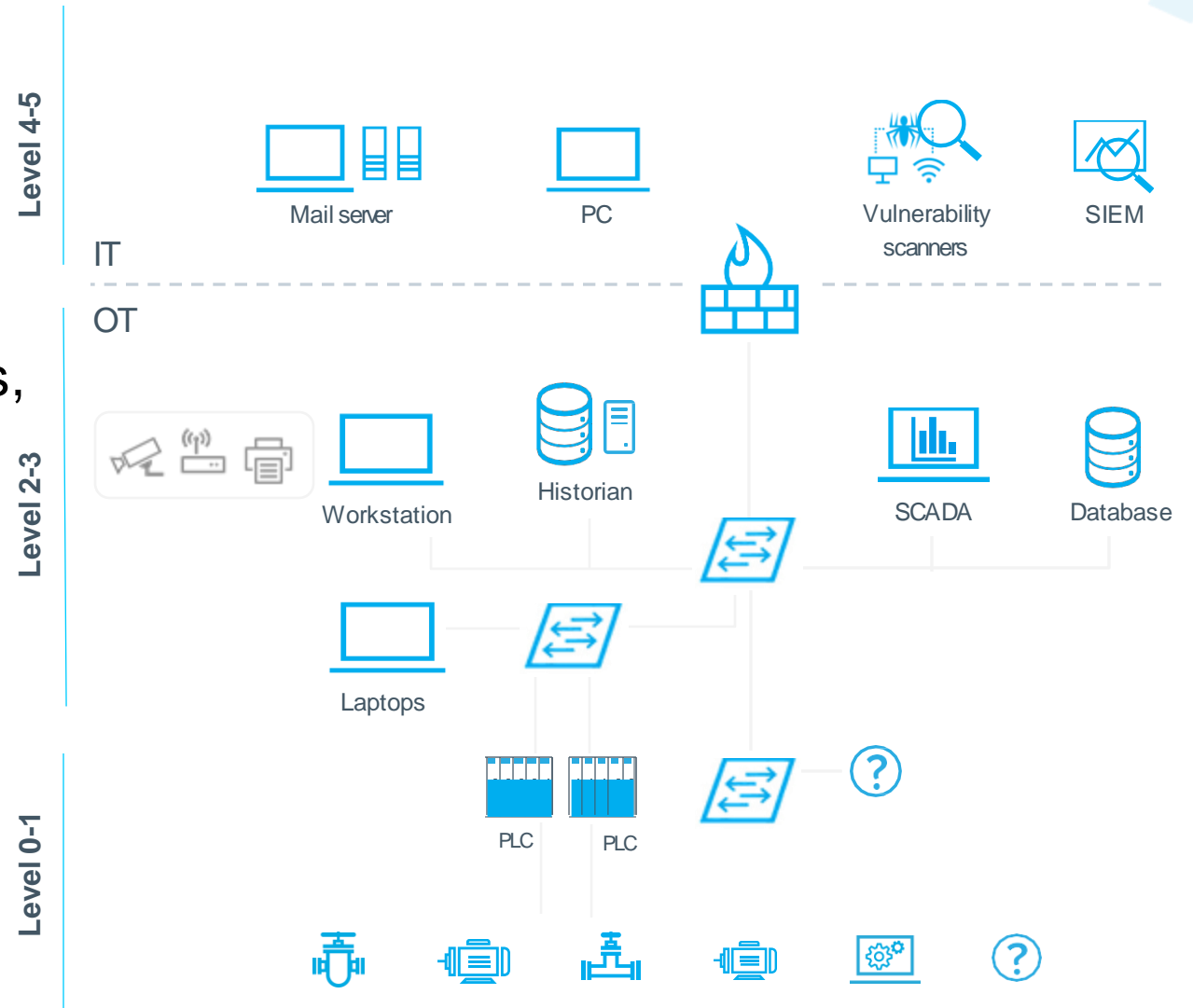


Know what you have
and keep it updated

Check the “checkers”

What's the difference between IT vs. OT?

- IT = Traditional office
 - Laptops, Desktops
- OT=Operational Technology
 - Valves, pumps, monitoring sensors, human-machine interfaces



CASE STUDY ON RANSOMWARE EVENT

COMPLETE ORIGINAL MOTION PICTURE SCORE

MUSIC COMPOSED BY JAMES HORNER



THE
PERFECT STORM

Stages of a SamSam Ransomware Outbreak

- 1) Vulnerability Exists-remediating vulnerabilities not 100% complete/effective (SamSam uses JBOSS or RDP)
- 2) Exploitation/penetration occurs via stolen/compromised credentials
- 3) Privileges elevated via Domain Controllers
- 4) Identify vulnerable systems-actor tests waters identifying those systems he can pwn, what systems are “manageable” via credentials (write a empty text file to a directory)
- 5) Deploy the Payload - executable, script
- 6) Execute Payload
- 7) Encrypt systems (e.g.-file extension changed to “.sorry”, “.imsorry”)
- 8) Demand Ransom



Spearfishing



Custom Malware



Zero-Day Exploits



Social Engineering



Physical Compromise



A Ransomware Story...

- Breach occurs due to brute force, human error, etc.
- Domain service account leveraged
 - Strategy during immediate hours following may be to deploy password change solutions
- Critical, foundational, enterprise-level systems GONE:
 - Active Directory (multiple DCs)
 - No GPO
 - Inconsistent authentications
 - SCCM
 - No patching
 - No software delivery
 - SQL Server
 - No Network Fault Management system
 - No CiscoWorks
 - Anything using SQL as DBMS

ForeScout Capabilities during Incident Response

- SYSTEM OF RECORD
 - Depending on extent of damage, ForeScout may be only system
- Damage Assessment
 - Policies to assess infection rate
 - Cross reference against analytics tools parachuted in
- Risk Assessment
 - Policies to identify un-protected devices
 - Threat Protection to help identify “holes” in armor
- Risk Mitigation
 - Agent deployment/script execution
- Keep Lights on/Rebuild Environment
 - Software/agent deployment

Publicly Known Impact to City of Atlanta

- Considering their latest victim, the City of Atlanta, the group behind SamSam had a number of available access points to choose from.
- Original ransom was ~\$50,000
- In first 60 days post-breach ~\$5.6 Million (including entire City of Atlanta agencies, not just Atlanta Information Management/AIM)
- As of June, estimates of a third of 424 applications (30% of which are mission critical) were taken offline
- Recently announced an additional \$9.5 Million needed by AIM to fully recover

<http://www.govtech.com/security/Total-Costs-Still-Unknown-Atlanta-Moves-to-Refortify-Post-Hack.html>

<https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/>

<https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/>

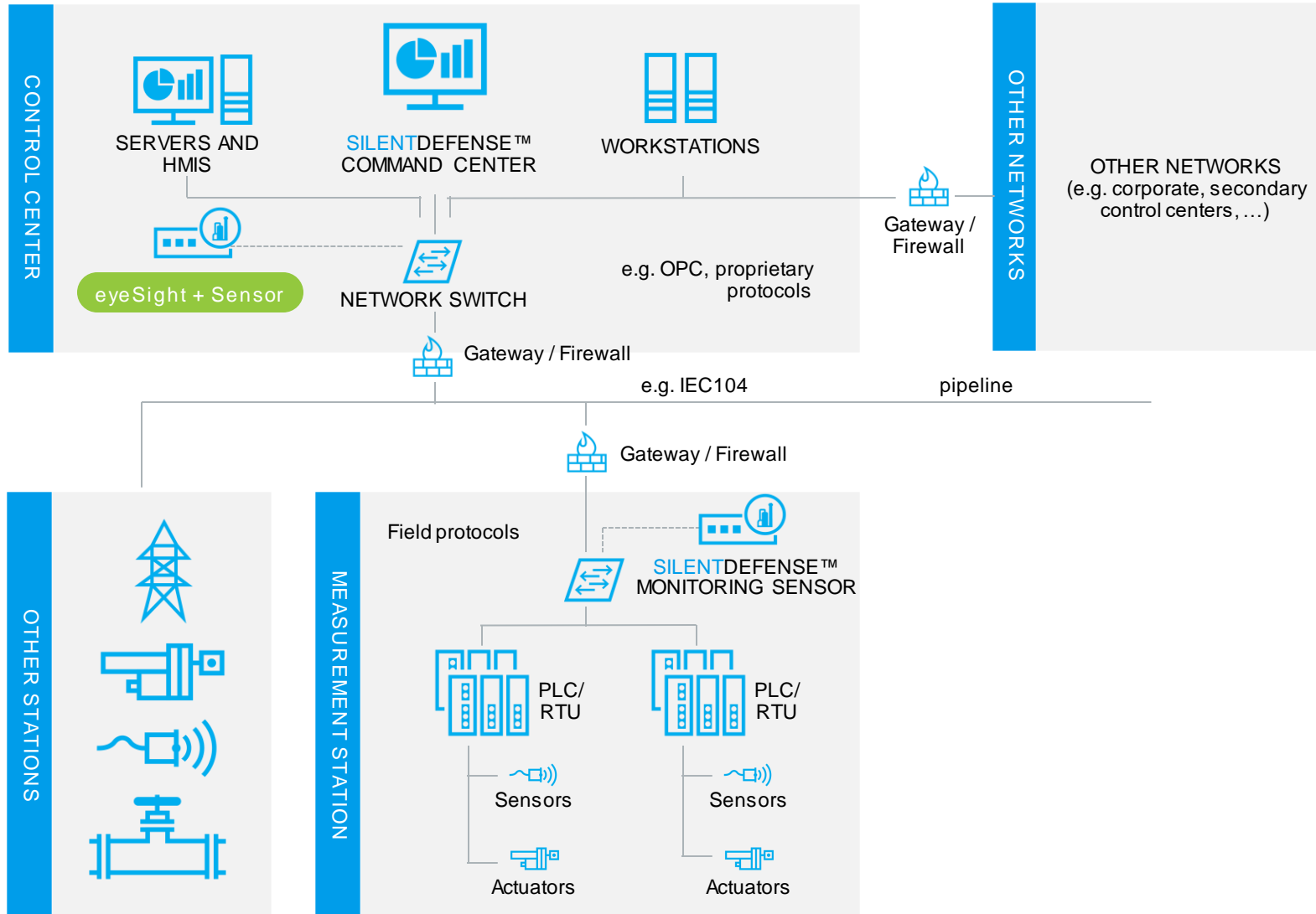
Lessons Learned

- Be prepared to be overwhelmed by Armies
 - Vendors such as Microsoft, Cisco
 - Incident Response Provider
 - Feds: FBI/DHS (US-CERT)/Secret Service
- Gain:
 - VISIBILITY as quickly as possible
 - An understanding of Damage and existing Risks
 - Ability to mitigate those risks in automated, policy-based manner

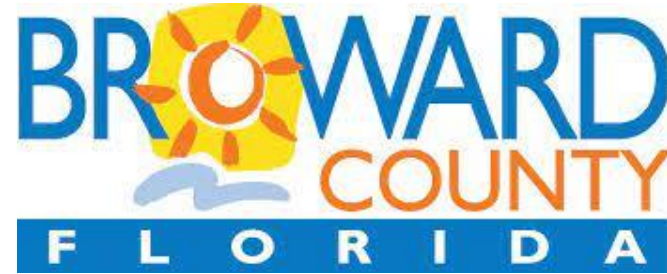
Lessons Learned

- Governance-VITAL!!!
 - Tools
 - Discovery/CMDB/ITSM
 - People
 - Process
 - **Plan for worst, hope for best** 😊
- Disaster Recovery
 - Plan
 - Complete
 - Periodically Tested
 - Verified
 - Green/Clean environment as target

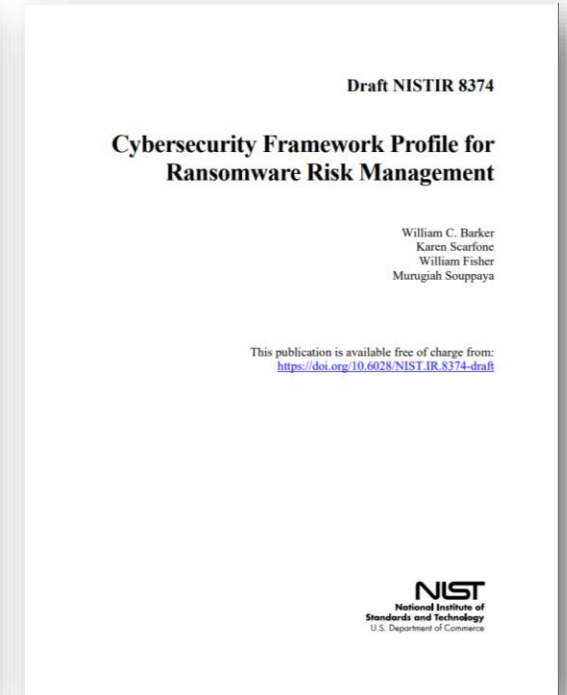
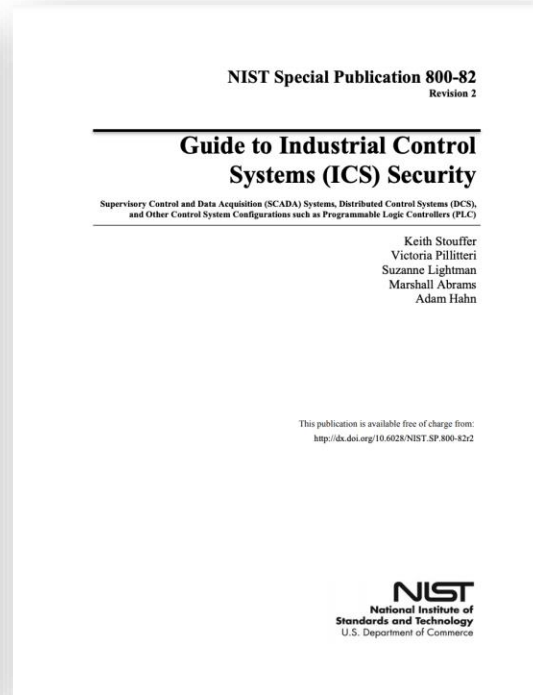
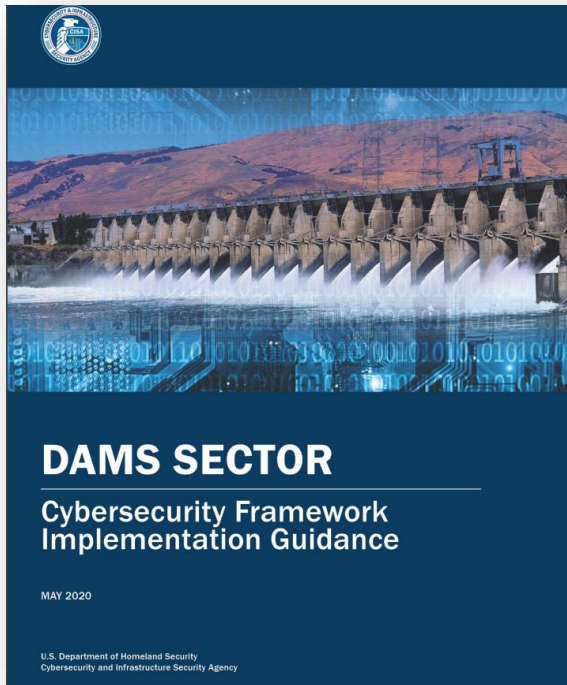
Customer Sample: Power and Utilities



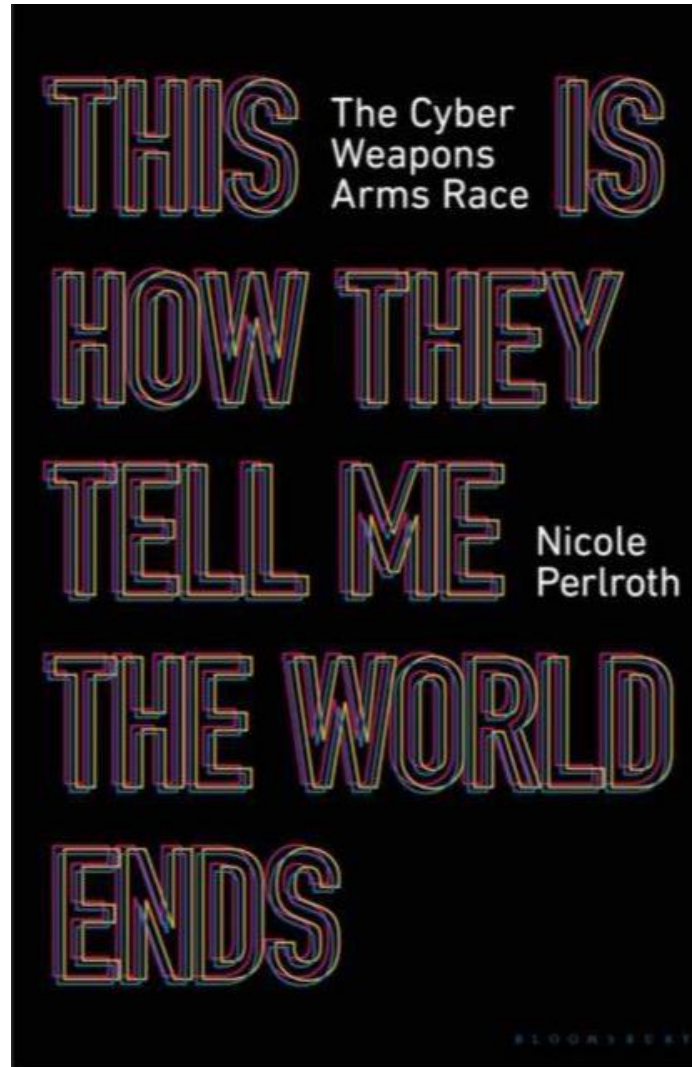
Protecting the Nation's Water



Additional Resources



And for some light late night reading...





THANK YOU

Shawn Taylor / staylor@forescout.com / [@smtaylor12](https://twitter.com/smtaylor12)