The Utility Cybersecurity Challenge: Converging Information and Operational Technologies

Philip Propes

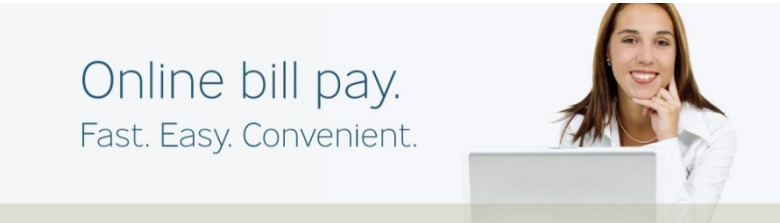
October 2016

The Cybersecurity Challenge

- **The Global Threat**
- Utility Cyber Perspective
- TVA Cyber Perspective
- Establishing a Defense

Global Cyber Threat

Increased Connectivity is a Global Demand

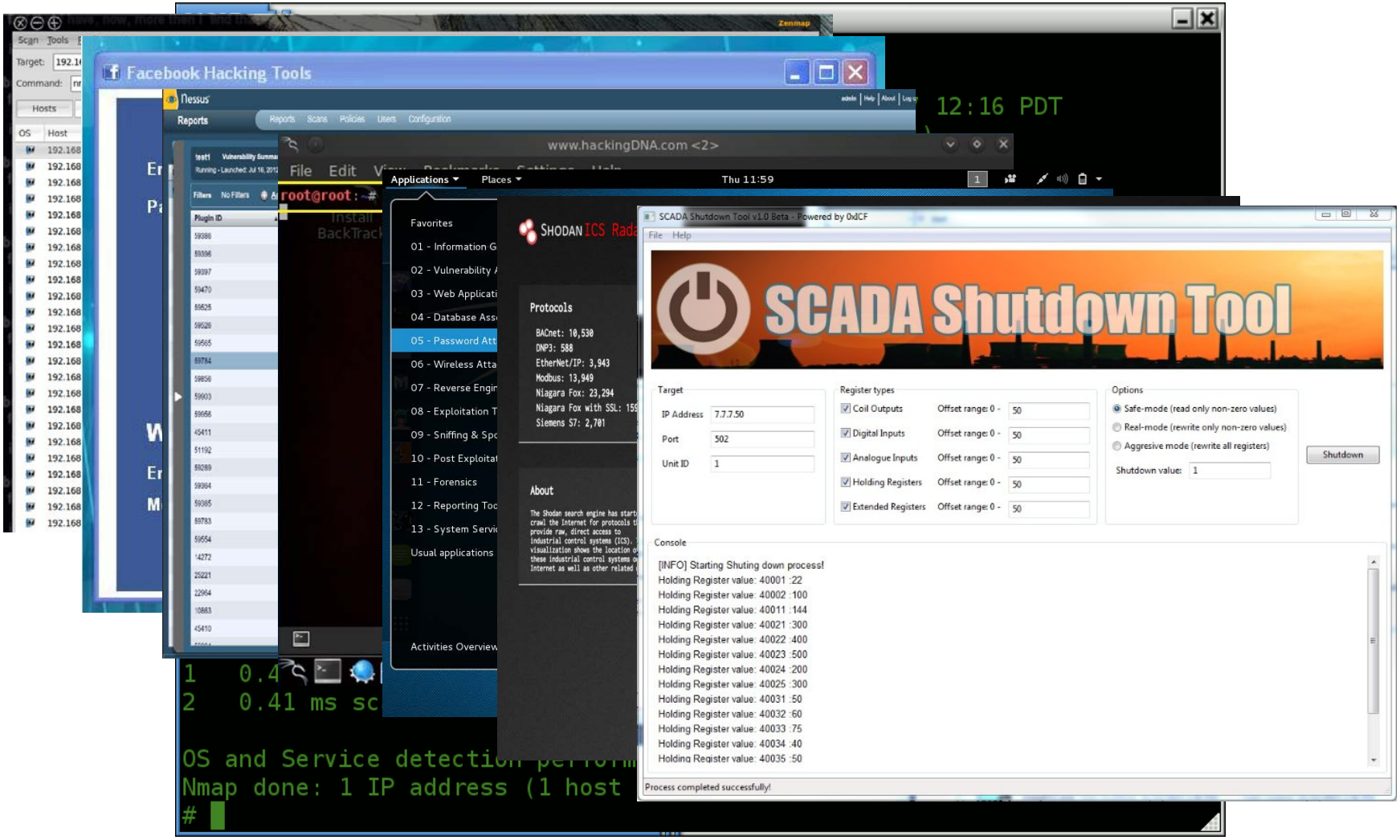


Global Cyber Threat

Increased Internet Speed is a Global Reality

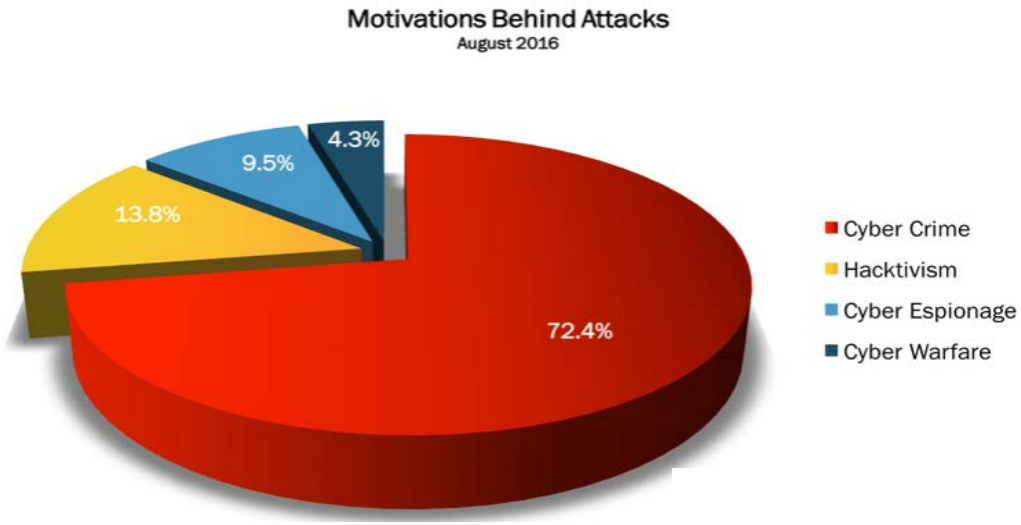
Global Cyber Threat

Increased Simplicity is a Global Threat

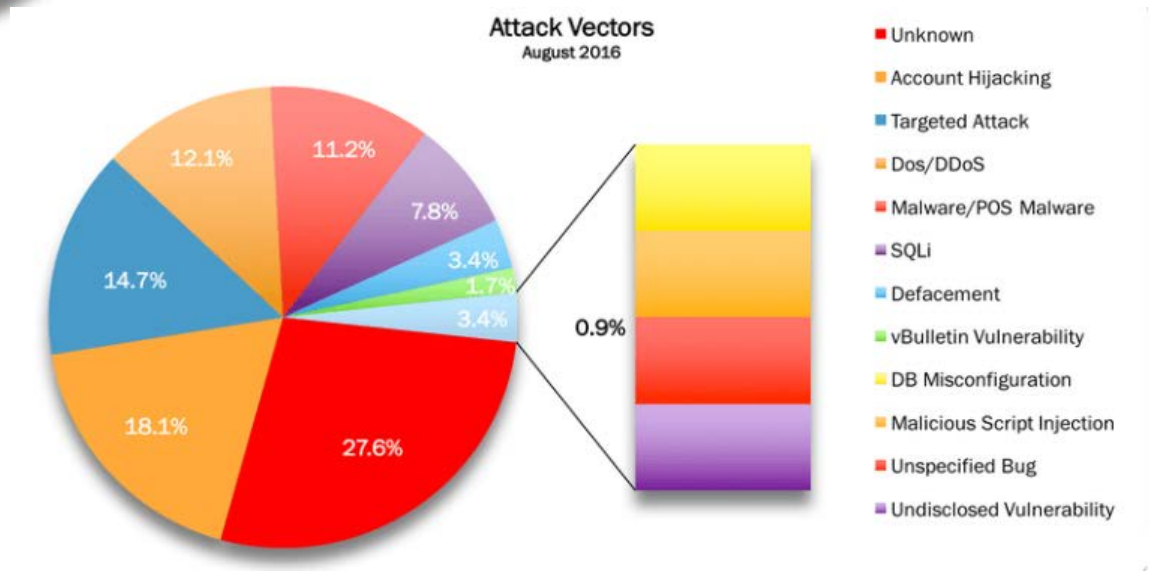


The Global Threat – Trends

Current Cyber Attack Trends



Nation-State activities such as cyber espionage and cyber warfare are increasing.



Over half of successful cyber attacks target people and computer-related behaviors.

Source: Hackmageddon.com

Global Cyber Threat

The Perfect Storm for Cyber Attacks

- More connected devices
- Internet speeds increasing exponentially
- Simple and more powerful hacking tools
- Online training and videos on tool use
- Increasing activity of nation-states

The world is becoming a dangerous place.

Global Cyber Threat

Cyber Breaches are a Global Issue

NBC NEWS HOME TOP VIDEOS DECISION 2016

Russians Hacked Two U.S. Voter Databases, Officials Say

FORTUNE

Oracle's Data Breach May Explain Spate of Retail Hacks

POPULAR SCIENCE

WHO HACKED THE NSA?

THE MYSTERY BEHIND THE IDENTITY OF THE SHADOW BROKERS, AN EIGHT-FOOT-TALL ALIEN, AND THE DIPLOMATIC CHESS GAME SURROUNDING A 234 MB LEAK

CNN politics Election 2016 Nation World

First on CNN: FBI investigating Russian hack of New York Times reporters, others

NETWORKWORLD FROM IDG

Dyn attack: US Senator wants to know why IoT security is so anemic

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

Yahoo says half a billion accounts breached by nation-sponsored hackers

The Washington Times HOME NEWS

IRS computer hack was worse than agency admitted

FORTUNE

LinkedIn Lost 167 Million Account Credentials in Data Breach

COMPUTERWORLD FROM IDG

NEWS

Hackers breach DOJ, dump details of 9,000 DHS employees, plan to leak 20,000 from FBI

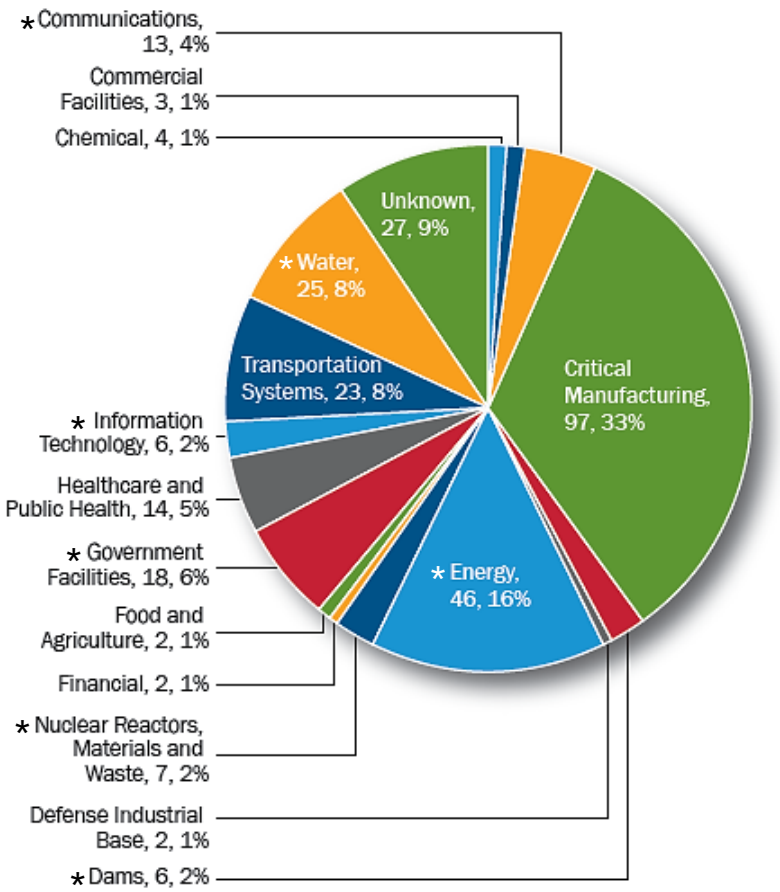
The Cybersecurity Challenge

- The Global Threat
- **Utility Cyber Perspective**
- TVA Cyber Perspective
- Establishing a Defense

Utility Cyber Perspective – Sectors

Critical Cyber Event Response by Sector, 2015

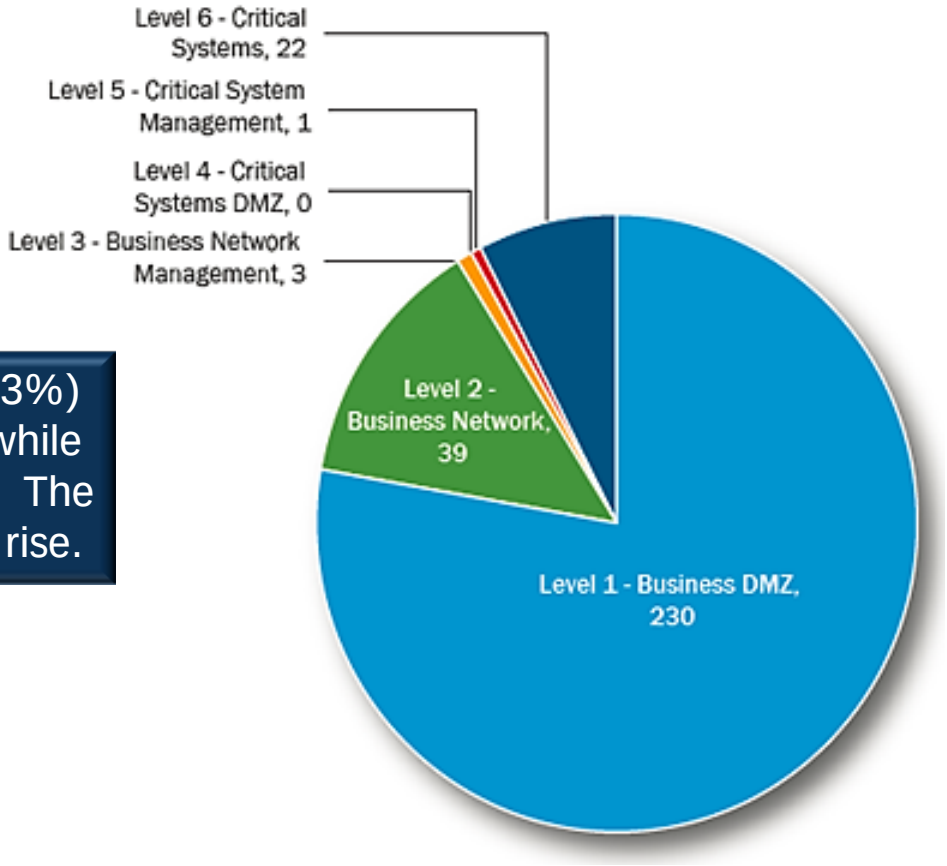
TVA is active in sectors encompassing 40% of total cyber events in 2015.



As reported by the US Computer Emergency Readiness Team (US CERT)

Utility Cyber Perspective – Intrusions

Observed Depth of Intrusion, 2015



Of 295 reported intrusions, 39 (13%) reached the corporate network, while 22 (7%) reached critical systems. The frequency and impact are on the rise.

Utility Cyber Perspective – Types of Attack

Attackers Target People as Often as Systems

"...spear phishing represented 37 percent of the total incidents. Being relatively easy to execute and demonstrably effective, spear phishing continues to be a common method of initial access against critical infrastructure targets."
~US Computer Emergency Readiness Team (US CERT)

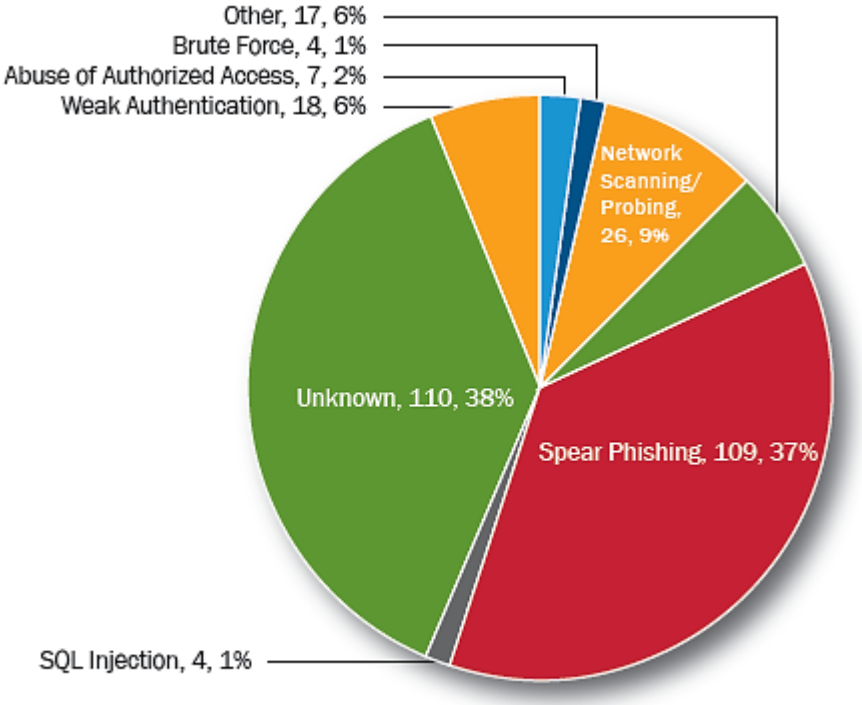


Figure 2. FY 2015 Incidents by Attempted Infection Vector, 295 total.

Utility Cyber Perspective – Threat Actors

Our Industry is Being Targeted

RUSSIA

TARGETS: Electricity, manufacturing, oil and gas
CAPABILITY: Penetrate IT, OT / ICS networks
OBJECTIVES: Geopolitically driven disruption and destruction of infrastructure
RISK: Likely to conduct attacks against US; likely to target ICS operators; unlikely to cause disruptions or destruction against US

NORTH KOREA

TARGETS: Light rail and electricity
CAPABILITY: Penetrate IT and ICS networks
OBJECTIVES: Retaliatory strikes against national adversaries
RISK: Likely to conduct disruptive or destructive attacks outside US; possible disruptive or destructive attacks against US ICS operators

IRAN

TARGETS: Electricity, water, and dams
CAPABILITY: Penetrate IT, OT / ICS networks
OBJECTIVES: Retaliatory strikes against national adversaries; establish persistent access as contingency for future conflicts
RISK: Likely to target US ICS operations; unlikely to cause disruptions or destruction

CHINA

TARGETS: Electricity, manufacturing, oil and gas, light rail, water and dams
CAPABILITY: Penetrate IT, OT / ICS networks
OBJECTIVES: Traditional espionage; support of national economic interests through intellectual property theft; establish persistent access as contingency for future conflicts
RISK: Highly likely to conduct attacks against US; highly likely to target US ICS operations; unlikely to cause disruptions or destruction

Source: "Industrial Cybersecurity Threat Briefing"; Booz, Allen, Hamilton; www.boozallen.com/ics.

Combined Attacks - The Ukraine Event

Industry Case Study – The IT/OT Converged Event

Attack Sequence

- Spear phishing to gain access
- Stole passwords
- Gained access to control network
- Erased control systems and records
- Used the network to impact backup power
- Overwhelmed and disrupted call center

Outage Data

- 225,000 customers
- 3 service territories
- Several hours

The Cybersecurity Challenge

- The Global Threat
- Utility Cyber Perspective
- **TVA Cyber Perspective**
- Establishing a Defense

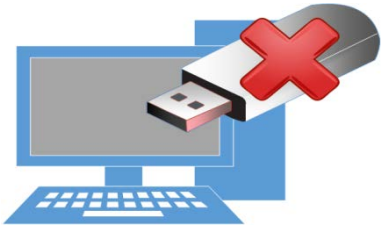
TVA Cyber Perspective – Types of Attack

TVA – Most Common Incident Sources

- **Electronic Mail**

- **Internet**

- **Removable Media**



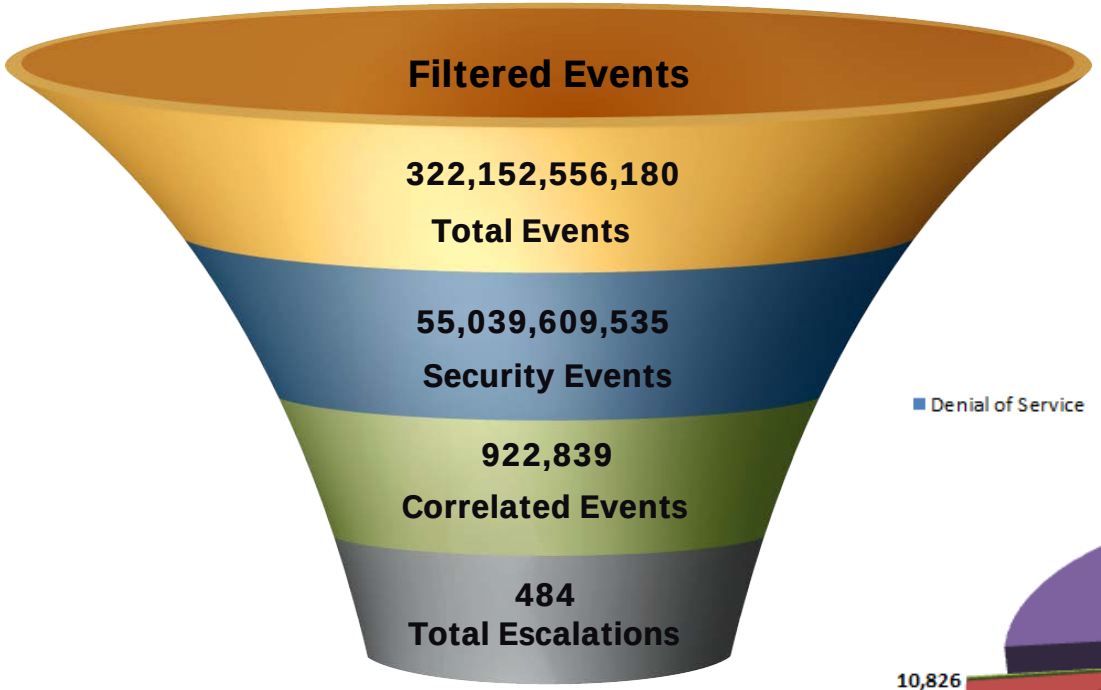
TVA Cybersecurity – Email-Based Incident Prevention

Spam and Malicious Email

- As of September 2016, TVA has received **13,021,585** spam emails (FY16).
- Of those, **17,542** were infected and blocked by TVA.
- Only **7** impacted the TVA recipient.

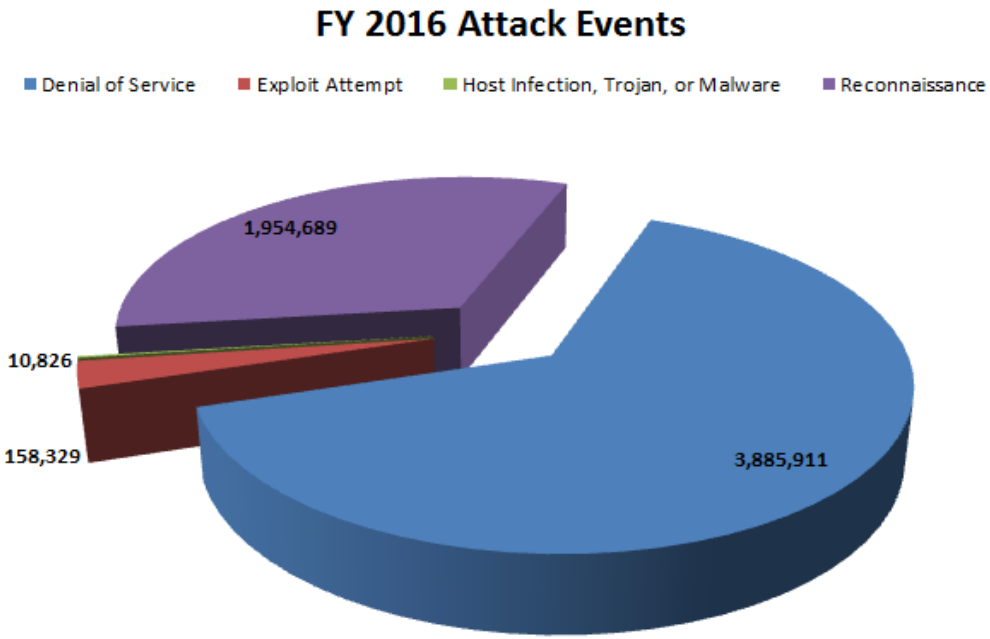
TVA Cyber Perspective – Email-Based Incidents

TVA Cybersecurity Events – FY2016



Events are processed via automation, then by security analysts as they escalate.

TVA also encounters a variety of attack types beyond email, again with analyst escalation. None have been successful to date.



The Cybersecurity Challenge

- The Global Threat
- Utility Cyber Perspective
- TVA Cyber Perspective
- **Establishing a Defense**

Establishing a Defense

What Does This All Mean?

Perimeter Defenses Are No Longer Sufficient

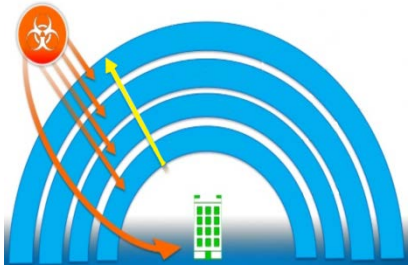
- Typical security focuses on building the “cyber castle” to keep attackers at bay
- Attackers and attack tools sought to find holes in the walls, as a single crack could be exploited and entry could be gained

Attackers Quickly Evolve; Defenders Lag Behind

- Attackers use creative ways to manipulate people into “opening windows” in the wall, allowing for easy access
- Defenders continue to buy technology as fresh “cement” to reinforce their castle walls

Information and Operational Technology (IT and OT) Convergence

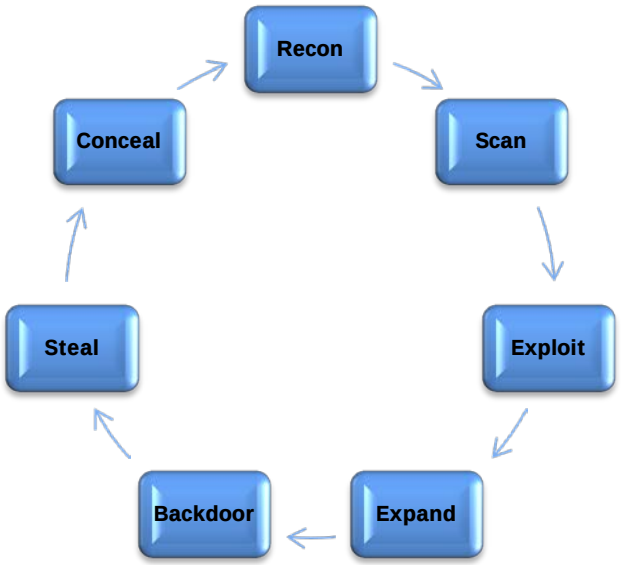
- Attackers have recognized the challenge of the IT/OT gap
- Accessing IT systems via user manipulation is now the gateway of choice to access OT networks and systems
- Outbound communications used to bypass inbound defenses



Establishing a Defense – Know the Attacker

The Attack Process, Simplified

1. **Research and Reconnaissance**
   - Learn about people, processes, and technology
2. **Scan and Probe**
   - Use gathered data to locate, map, and plan
3. **Exploit**
   - Leverage discoveries to select and implement a tool
4. **Elevate and Expand**
   - Expand access via privileges and pivoting to new systems
5. **Establish a Point of Return**
   - Create a discrete method of return (backdoor)
6. **Steal or Disrupt**
   - Steal data, disrupt services, destroy/disable systems
7. **Cover and Conceal**
   - Wipe tracks, create a false trail, and/or distract from point of return



Establishing a Defense – Thwart the Attacker

Practical Steps to a Reasonable Defense

- **Focus on Security, with Compliance as a By-product**
  - Security best practices are the focus
  - Compliant is not synonymous with secure
- **Develop a 3-Year Strategy, with Practical 1-Year Goals**
  - Predict, Protect, Detect, Respond as focal areas
  - Yearly increments to achieve balance across the four goal areas
- **Get the Basics Down**
  - Minimize information exposed publicly; do not share unnecessarily
  - Identify systems and business priorities and focus accordingly
  - Establish the essential perimeter capability
  - Use effective anti-malware tools
  - Use least privilege access model
  - Block and filter anything that isn't necessary
  - Patch with a focus on criticality and risk
  - Encrypt when possible and practical
- **Train, Train, Train**
  - General awareness training to all staff
  - Targeted messages/actions – anti-phishing, how to report, etc.
  - Train your technical staff to detect and respond more efficiently

Establishing a Defense – Thwart the Attacker

Practical Steps to a Reasonable Defense

- **Share Information and <u>Intelligence</u>**
  - Establish relationships with peer companies, industry groups, law enforcement, etc.
  - Locate and sign up for intelligence feeds/sources
- **Know the <u>Normal</u> So You Can Identify the <u>Abnormal</u>**
  - Establish baselines for systems and regular communications
  - Focusing on anomalies is the only practical way to handle volume of data
  - Don't look for the needle in the haystack; remove the haystack!
- **Do Not Simply Focus on the Front Door; Watch Doors and Windows**
  - Establish trust in your perimeter
  - Focus energies on what is <u>leaving</u> your network (data exfiltration, command and control comms, backdoor beaconing)
  - For either theft or disruption, outbound communications are necessary
- **Seek a Balanced Approach**
  - Remember, OT systems are targeted through IT systems, so you can't ignore either group
  - Avoid over-investing in specific defenses and neglecting others
  - Plan the work and work the plan; avoid distractions!

Establishing a Defense – A Collaborative Approach

TVA Can Help

TVA and Partner Information Sharing

- Establishing peer groups among cybersecurity experts
  - Event notices and updates
  - Real-time event communications

Collaborative Security Opportunities

- Direct security support
  - Emergency surge support
  - Managed security services
  - Resource sharing – people and tools
  - TVA's unique intelligence sources

Training Opportunities

- Staff Sharing/Training
  - Send staff to TVA for embedded training and experience
  - Targeted training opportunities

Establishing a Defense – A Collaborative Approach

TVA Cybersecurity Outreach Program

Cybersecurity Coordination Forums

- Recurring cybersecurity meetings
- TVA and customer cybersecurity personnel
  - Sharing of best practices
  - Current threat information sharing
    - FBI and DHS intelligence updates
  - Cybersecurity compliance support

Specialized Topical Groups

- Informal technical discussions
  - Incident response and monitoring
  - Intelligence and threat indicators
  - Hardware/software recommendations

For More Information:

Philip Propes
Chief Information Security Officer (CISO)
pdpropes@tva.gov