Leveraging Intelligence for Proactive Security

Philip Propes
Chief Information Security Officer
October 2017
Leveraging Intelligence

• The Approaching Storm
  • What is Intelligence?
  • Intelligence Sources
  • Applying Intelligence
The Global Threat – Frequency and Impact

- Equifax: 143 Million Customers
- Yahoo: Up to 3 Billion Accounts
- United States Office of Personnel Management: 21.5 Million Personnel
- Chipotle: Up to 2,250 Stores
- National Security Agency: Numerous Files and Tools
- Verizon: 6 Million Customers
- PlayStation: 2.5 Million Accounts
The Global Threat – Trends

Current Cyber Attack Trends

Motivations Behind Attacks
August 2017

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
The Global Threat – The Bad Guys and Their Intent

<table>
<thead>
<tr>
<th>Criminals</th>
<th>Insiders</th>
<th>Hacktivists</th>
<th>Terrorists</th>
<th>Nation States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intent on monetary gain</td>
<td>Ideology or monetary gain</td>
<td>Attention to their cause</td>
<td>Disruption of critical infrastructure</td>
<td>Support foreign nation’s strategic objectives</td>
</tr>
</tbody>
</table>

**Impacts**

- System Disruptions / Outages
- Economic impacts
- Impacts to national security
- Financial loss
- Loss of Customer Information
- Reputational Impact
- Regulatory Impacts
- 3rd Party Impacts
The Global Threat – The Rise of the Nation-State

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

A gloomy forecast

Cyber Predictions – Financial Resource Impacts

- Cyber crime damage to reach $6 trillion annually by 2021.
- Cybersecurity spending to exceed $1 trillion annually by 2021.
  - Unfilled cybersecurity jobs will triple by 2021.
- The number of people online will exceed 4 billion by 2020.
- Ransomware damage will exceed $5 billion by the end of 2017 (15 times larger than 2015 - $325 million).

"Cyber crime is the greatest threat to every company in the world."
– Ginni Rometty, President and CEO, IBM
Global Cyber Threat

Feeling Overwhelmed?
Leveraging Intelligence

• The Approaching Storm
• **What is Intelligence?**
• Intelligence Sources
• Applying Intelligence
What is Cyber Intelligence?

Intelligence is Multi-Faceted

• Cyber intelligence is information used to better anticipate a potential issue.
• Intelligence can be gained and subsequently used in multiple ways.
• It can be found in the news, from specific sources, or from things you learn about your own environment.
  • Articles
  • Intelligence Feeds
  • Self-Assessments
  • Penetration Tests
What is Cyber Intelligence?

Intelligence in Many Forms

• Articles, news reports, and simple current events can yield all manner of intelligence.

• Intelligence can be gained through a variety of commercial and free sources.

• It includes awareness of the people, processes, and technology in your company.

• Asset lists, assessments, and penetration testing results are great resources.

• Vendors, suppliers, and contracting agencies are also valuable sources.
Intelligence as a Tool

- Once gathered, intelligence can be used to advance security.
  - Implement patching processes
  - Tune or implement monitoring
  - Modify or isolate networks and systems
  - Drive system retirement
  - Drive investment
  - Identify at-risk staff or contractors
  - Insider Threats

- It is used to accelerate detection of an incident, or ultimately, to prevent an incident from occurring.
Why is Intelligence Important?

As predictive abilities advance, cyber groups can identify and remediate issues before an event occurs.

Proactive is getting ahead of cyber incidents.

As reactive abilities advance, cyber groups can more quickly detect and respond to cyber events, reducing reaction time.

Reactive is responding to cyber incidents.

Intelligence to Drive Maturity
Leveraging Intelligence

- The Approaching Storm
- What is Intelligence?
- **Intelligence Sources**
- Applying Intelligence
Intelligence Feeds

Common Intelligence Sources

• Public / Open Sources:
  • Government: FBI, DHS, ISACs, US-CERT, Defense Cyber Crime Center (DC3)
  • Open: SANS Internet Storm Center, ThreatBrief

• Commercial Sources:
  • CrowdStrike, FireEye, AlienVault, RecordedFuture, many others

• Articles / Media:
  • Reports: Mandiant M-Trends, Checkpoint, Verizon Data Breach, Cisco Security, Symantec, PWC Global State
  • Blogs: Krebs on Security, MandiantBlog, Recorded Future, Cyveillance, OODAloop
External Trends

Cyber Predictions – Technical
Most Likely Attacks in 2018

1. Socially Engineered Malware

2. Password Phishing Attacks

3. Unpatched Software

4. Social Media Attacks

5. Advanced Persistent Threats (aka, Nation-State)
Internal Trends

Information Derived from Events

Filtered Events

322,152,556,180 Total Events
55,039,609,535 Security Events
922,839 Correlated Events
484 Total Escalations

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

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

Security Event Types

Denial of Service
Exploit Attempt
Host Infection, Trojan, or Malware
Reconnaissance

1,954,689
10,826
158,329
3,885,911
Awareness and Assessments – Know Yourself

Information Derived from Tools and Processes
Leveraging Intelligence

• The Approaching Storm
• What is Intelligence?
• Intelligence Sources
• Applying Intelligence
Applying Intelligence – Know the Attacker

The Attack Process, Simplified

1. Research and Reconnaissance
   - Learn about target
2. Scan and Probe
   - Develop a blueprint
3. Exploit
   - Leverage discoveries
4. Elevate and Expand
   - Increase presence
5. Establish a Point of Return
   - Create a discrete door
6. Steal or Disrupt
   - Steal, disrupt, or disable
7. Cover and Conceal
   - Wipe and distract

Intelligence can be leveraged to prevent or detect an attack at each step.
Applying Intelligence

Threat Intelligence Methodology

- Threat / Targets Intel
- Prioritize Data
- Analysis and Synthesis
- Apply Mitigation
- Feed into Intel Loop

- Identify Attacker Types
- Identify Associated Threats
- Identify Potential Targets
- Associate with Recent Events
- Use Risk-Based Scoring to Rank
- Apply Mitigation Based on Rank
- Incorporate Mitigation
- Continuous Improvement Loop
Applying Intelligence

Continuous Improvement Loop

1. Define Intel Needs Within Organization
2. Configure Collection Systems and Processes
3. Review and Fine Tune Processes
4. Sort, Filter, and Prioritize Data
5. Analyze and Package Relevant Data
6. Vetting/Exploitation
7. Production
8. Analysis
9. Dissemination
10. Take Action
11. Assess and Implement Changes as Identified
12. Collect Data
13. Review and Fine Tune Processes
14. Convey Intel Package to Operational Teams
15. Review Accuracy and Value of Intel Package
16. Information Requirements
Applying Intelligence

Fusing Intelligence

• A cyber defender must combine known threats, existing vulnerabilities, and system criticality to properly prepare and integrate intelligence.

• This integration is realized through improved protective measures, tailored monitoring, and accelerated detection and response.
A Collaborative Defense
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
  - TVA’s unique intelligence sources

Training Opportunities

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