AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

PUBLIC POWER
Cybersecurity Information Sharing Report

Acknowledgment: This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000811.

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government to protect the interests of the more than 49 million people that public power utilities serve, and the 93,000 people they employ. Our association advocates and advises on electricity policy, technology, trends, training, and operations. Our members strengthen their communities by providing superior service, engaging citizens, and instilling pride in community-owned power.

Table of Contents

Executive Summary **4**
Introduction **6**
The Evolution of Cybersecurity **7**
Systems Evolution for applying Threat Information 7
Segmentation 8
Cybersecurity Framework Management Evolution 9
Threat Information Sharing Standards Evolution 10
The Central Role of E-ISAC 10
Cybersecurity Information **11**
Understanding Cybersecurity Information 11
How Cybersecurity Information Sharing Interrupts Attacks 11
Cybersecurity Information Sharing in Action **13**
Survey Results 13
Market Research Study Results 14
Security Patching as a Team **15**
Recommendations **16**
Conclusion **17**
Appendix A. STIX Specification **18**

Executive Summary

Cybersecurity Information Sharing Among Public Power Utilities

Sharing threat information among public power utilities is critical to prevent cyberattacks that can negatively impact each utility. To facilitate this communication, public power utilities need to establish information sharing agreements to confidentially share security threat information.

It is imperative that public power utilities have the capability to identify threats and share security information with key stakeholders. Small-to-midsized public power utilities organize operations, grid systems control, and monitoring in different ways. Some public power utilities have cybersecurity operations provided by local government information technology (IT) departments and/or third-party service providers due to limited internal resources. These operational structures may hinder a utility's ability to immediately recognize threats or may prevent the escalation of potential incidents to decision makers. Small to midsized public power utilities must be able to coordinate with local government agencies to set proper expectations among all stakeholders, monitor and detect threats, maintain situational awareness among decision makers, and quickly respond to cyber incidents. To do so requires that the utility invest in capability building, and pre-established resources.

The American Public Power Association evaluated public power utilities' understanding of and requirements for secure information sharing technologies. The evaluation addressed the effectiveness of a variety of technologies to reduce the time burden placed on the public power utilities, while ensuring interconnectivity with public and private partners in public safety, security, and community resiliency. The evaluation also identified secure information sharing tools and technologies that will improve the culture of cyber and physical resiliency as well as security within the public power community.

The Association surveyed member utilities to determine the level of awareness and use of secure information sharing technologies within public power utilities. The survey results confirmed that many utilities have insufficient resources to efficiently process the deluge of threat alerts, including how to identify and respond to important data. To address this problem, the Association explored a risk-based framework for determining priority levels for the dissemination of secure messages and notifications to public power utilities of different sizes. The exploration identified several recommendations to the Electricity Information Sharing and Analysis Center (E-ISAC) to improve service for public power utilities (see Recommendations). The survey found that it is important for the E-ISAC to categorize, assess, disclose, and disseminate secure threat information that is useful and understandable for public power utilities. Secure information should include near real-time documentation of key threat indicators and actions taken to date by the reporting entity. This report shows the key findings on how public power utilities will be able to use various levels of secure information.

Addressing Cybersecurity Threat Prevention within Public Power Utilities

To address the growing complexities associated with public power utility cybersecurity threat prevention and to increase cybersecurity information sharing among utilities, there is an opportunity to leverage economies of scale through the joint action agencies (JAAs). Many public power utilities do not have the software and hardware systems available to detect potential cyber threats. The JAAs could serve as a centralized repository for their utilities' security logs through the deployment of security event and information management (SEIM) tools. The JAAs could also broker threat information from the E-ISAC to member utilities; filtering the threat information to be more actionable for the public power utilities.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

When adopting SEIM solutions, it is critical to require the use of threat information sharing standards such as the Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). Use of these standards ensures interoperability among JAA utilities, other JAAs, mature public power utilities, the E-ISAC, and other key stakeholders.

Role of Managed Security Systems Providers (MSSPs)

Due to the limited technical human resources available to public power utilities, there is an opportunity to leverage MSSPs to host secure SEIM solutions. This approach would also provide greater access to correlated threat information across a broader set of the public power sector. The MSSPs can perform the day-to-day security event monitoring, ingest automated threat information from sources, such as the E-ISAC, and notify the JAAs when there is suspect security event information that is actionable by public power utilities. The JAAs can then provide a mechanism to share anonymized and aggregated events back to the E-ISAC.

Recommendations

To provide a robust secure information sharing program for public power utilities and integrate into the new E-ISAC automated indicatory sharing program, the Association recommends:

- Public power utilities with the capability to start gathering security event logs should install an SEIM-type solution. At a minimum, utilities should correlate security logs across the utility enterprise.
- Utility SEIMs should use STIX/TAXII specifications to establish a secure channel for exchanging threat information. This allows a utility to send only the threat information versus providing full security event log information to other parties when sharing threat events externally.
- The E-ISAC should continue to develop the capability to send/receive threat information using the STIX/TAXII protocol within its portal.
- MSSPs providing SEIM solutions to public power utilities must be able to integrate with a STIX/TAXII solution to create an end-to-end security event log management and threat information sharing process for the industry.

Introduction

Cybersecurity information sharing of threat information is critical to preventing cyberattacks. While certain systems such as individual PCs and software have automatic and standard cybersecurity threat prevention processes through automatic updates, the threat prevention process for utility information technology (IT) and operational technology (OT) network systems that need to be upgraded for cybersecurity protection is much more complex.

The United States Department of Energy (DOE) entered into a cooperative agreement with the American Public Power Association to address the growing complexities associated with cybersecurity threat prevention and to increase cybersecurity information sharing for utilities. The Association engaged Navigant Consulting to:

- Identify gaps in sharing cybersecurity threat data among utilities;
- Examine industry best practices in areas related to cybersecurity; and
- Highlight technologies that could help public power utilities with situational awareness and security.

To accomplish these tasks, Navigant conducted a sampling of how public power utilities gather and utilize cybersecurity threat intelligence. This review included an analysis of a survey of cybersecurity practices at public power utilities, onsite testing of information sharing systems at public power utilities, and market and subject matter research.

Cybersecurity threat intelligence is often provided as indicator of compromise (IOC) data (e.g., IP addresses, URL, hash files and other data points), and many public power utilities do not have the software and hardware systems available to make this threat intelligence actionable.

Navigant also identified cybersecurity concerns related to:

- Liability risks associated with sharing sensitive information with others;
- Out-of-date information;
- Information duplicated across multiple sources; and
- Deluge of irrelevant information.

This report discusses possible solutions to these concerns and provides guidance on next steps with the goal of helping utilities identify, manage, and mitigate cyber threats through better threat information sharing.

This report is part of a larger DOE initiative to make shared information more accessible and actionable for public power utilities of all sizes. The DOE Cybersecurity for Energy Delivery Systems (CEDS) initiative aims to protect the power grid against attacks by advancing cybersecurity technology in alignment with the strategic framework of the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

The Evolution of Cybersecurity

Systems Evolution for Applying Threat Information

Large utilities often have the resources to keep their defensive posture high, including dedicated staff to manage cybersecurity systems. However, many public power utilities do not have the resources to commit to this level of protection. Survey results indicate that current threat information, which is mostly IOC data, is of limited practical use to public power utilities because they lack the advanced systems that use IOCs.

A strong cybersecurity approach uses a "defense in depth" strategy with multiple layers of cybersecurity controls that provide overlapping protection. As displayed in Figure 1, these controls can fall into four categories.

- **Cybersecurity management controls:** Tools and processes to monitor systems and networks, ensure continuous compliance with cybersecurity standards, and address any potential cybersecurity threats. The center of the cybersecurity system is the security information event management (SIEM).
- **Network controls:** Measures to manage and protect data transmission across networks, including managing user access to sensitive systems, ensuring data compliance with cybersecurity standards, and addressing potential cybersecurity threats. At the edge or perimeter of the network, a unified threat management (UTM) system can deliver a host of advanced cybersecurity controls that are maintained by the vendor. UTM systems provide:
  - Network firewalling
  - Network intrusion detection/prevention
  - Gateway antivirus /gateway anti-spam
  - Virtual private network
  - Content filtering
  - Load balancing
  - Data loss prevention
  - Reporting

The SIEM is the focal point collecting IOC data and interacting with other control systems. An SIEM is required to fully utilize information sharing platforms.

Figure 1: Types of cybersecurity controls

Source Navigant

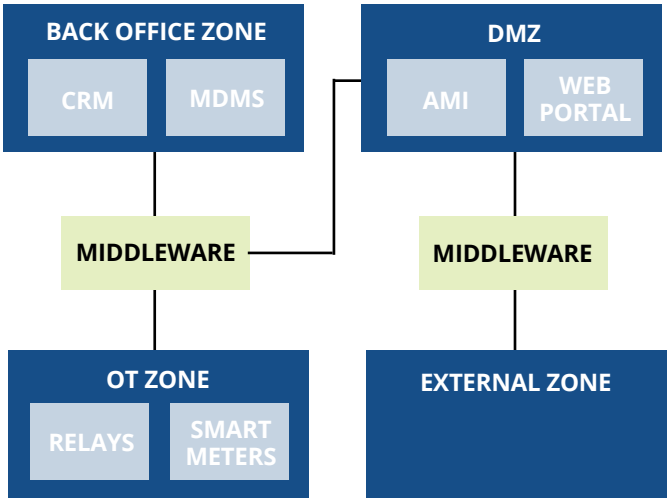
Cybersecurity Management	Network Controls	Information Controls	Asset Controls
SIEM	Firewalls	Encryption	Anti Virus
Patch Management	NIDS	• PKI	Hardening
Log Management	HIDS	• SFTP	
	UTM	• IPSec	
		• etc.	

- **Information controls:** Protections from unauthorized access, through data or communications encryption, for information at rest and in transit. Cybersecurity information (CSI) alerts provide information on tactics, techniques and procedures (TTP) that can compromise shared information as well as countermeasures and recommended upgrades.
- **Asset controls:** Measures including server and desktop hardening, antivirus, and whitelisting to improve the resiliency of systems if attacked. Antivirus vendors have systems built in to update "signatures," one type of IOC data.

Segmentation

Highly interconnected systems require segmentation into different cybersecurity zones. Assets and controls are grouped together for multiple systems with similar vulnerabilities that require similar cybersecurity controls. An example of such segmentation is illustrated in Figure 2. In this example, the back office zone contains systems that are housed on the utility's internal network, while the demilitarized zone (DMZ) contains systems that communicate with external systems and devices. The DMZ requires more stringent controls than the back office zone because its systems interface with systems outside of the utility's network and control, thus presenting greater risk for both physical security and cybersecurity. The OT zone requires the most stringent controls, as it houses the utility's most critical infrastructure.

Figure 2: Information sharing in different cybersecurity zones



Cybersecurity information sharing can automate updating complex architectures as well as collecting and sharing IOC data with the E-ISAC.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Cybersecurity Framework Management Evolution

To assist utilities in addressing growing cybersecurity threats, organizations have established frameworks to help guide them in protecting their critical infrastructure. The leading international frameworks include the following:

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a set of technical guidelines for implementing cybersecurity technology. The CSF includes specific information and guidance for implementing cybersecurity controls and practices for different industries and situations. The CSF consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. It also consists of four tiers (Partial, Risk-Informed, Repeatable, and Adaptive) to describe the degree to which an organization's cybersecurity risk management practices have matured. A utility can use the CSF to assess its current state (the "as is" profile) and identify a target state (the "to be" profile). This risk-based assessment approach provides a standardized methodology to support informed prioritization and serves as a reliable means for measuring progress toward an adaptive, or fully mature, target profile.

- The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) provides a framework for auditing a cybersecurity program to assess the effectiveness of the procedures and controls that have been employed. The ES-C2M2 helps utilities determine which security controls need to be implemented or improved. The ES-C2M2 is similar to NIST CSF profiles, but it is intended to be a comprehensive and enterprise-wide measurement tool centered around 10 competency areas. The ES-C2M2 evaluation process defines how the competencies are measured as well as how data collected during the evaluation should be analyzed and scored. The ES-C2M2 evaluation is designed to assist organizations in identifying specific areas to strengthen their cybersecurity program, prioritize cybersecurity actions as well as investments, and maintain the desired level of security throughout the IT and OT systems' lifecycle.

- The North American Electric Reliability Corporation (NERC) Critical Information Program (CIP) standards support the ongoing operation and maintenance of cybersecurity procedures and controls for the electric utility industry and the Bulk Electric System. The standards assess resource adequacy as well as provide educational and training resources to ensure power system operators remain qualified and proficient. While NERC is responsible for working with utility companies to develop and implement the NERC CIP standards and enforcing compliance with those standards, public power utilities could use the NERC CIP standards to improve their overall enterprise cybersecurity practices.

All three frameworks support a mature cybersecurity posture.

Threat Information Sharing Standards Evolution

Cybersecurity information is more than a series of data points. Threat indicators are a mainstay of cybersecurity information, and cybersecurity information models have evolved to include IOC data. IOCs need to be put into cybersecurity control systems to proactively identify the tell-tale signs of trouble. However, this level of prevention requires specific system hardware and software (as shown in Figure 2), someone to manage the system and investigate each alarm (e.g., an analyst), and a secure place to operate the system such as a security operations center.

Two new CSI specifications, or standards, have been successfully adopted by the financial industry (FS-ISAC), healthcare (NH-ISAC), and the Department of Homeland Security (DHS ICS-CERT). The standards, trusted automated exchange of indicator information (TAXII) and structured threat information expression (STIX), provide a secure way to share information between stakeholders and to make CSI actionable. The E-ISAC is also adopting these standards for use. These standards allow CSI and its applications to be much more powerful. The specifications are summarized below.

- **TAXII:** a free and open transport mechanism that standardizes the automated exchange of cyber threat information. The protocol allows different information sharing systems to communicate automatically. Hardware and software vendors that have adopted the specification can now bridge the space that used to require custom programming to move information around.
- **STIX:** a language to standardize the method used to represent cyber threat information. This language is increasingly powerful, not only because it has emerged as the de-facto standard for all CSI, but because it greatly enhances data points by connecting them with other threat intelligence objects.

The Central Role of E-ISAC

E-ISAC, in association with the Pacific Northwest National Laboratory and Argonne National Laboratory, collects CSI to provide advanced threat analytics that allow users to detect advanced persistent threats and other problems. When better data is available from utilities, not only at the external electronic perimeter, but also from within organizations, E-ISAC can recognize emerging threats in real time. Observable information from a range of cybersecurity hardware and software platforms can be made available more easily and in a secure manner. A company's network, the control center, and other OT environments can collect this information. E-ISAC can also make CSI more easily available and can be improved to include context and actionable intelligence on top of IOC data.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Cybersecurity Information

In close coordination with Association staff and designated subject matter experts from public power utilities across the country, Navigant surveyed public power utilities about how they use security threat data and how this data is incorporated into utility protection programs. Navigant held follow up web sessions with leaders at several key utilities and agencies to understand the cybersecurity challenges utilities are facing. During these meetings Navigant developed a thorough understanding of the survey participants' cybersecurity architecture. Findings from the survey and the follow-up sessions are summarized below.

Understanding Cybersecurity Information

Cybersecurity information comes in several forms. By following the series of events that occur in an attack, it is possible to get a better idea of how these information types fit in. Many cybersecurity systems use IOC data to detect threats and attackers. IOC data is typically in the form of IP addresses, URL, file hash, or other bits of information. Cybersecurity controls depend on having an up-to-date list of these indicators to be able to raise an alert when a match is found. Some indicator data, such as IP addresses and URLs, are added to firewall blacklists so that they cannot be reached. Threat actors are the enemies. They use tactics, techniques and procedures (TTP) to find ways around security controls and into systems. If a security analyst understands the TTP methodology, countermeasures can be put in place such as encrypting vulnerable information transmitted between machines, removing unnecessary ports and services, hardening servers, and otherwise reducing the number of vulnerabilities or "attack surfaces." A relatively small part of the malicious code is written by the threat actor. Almost all attacks use sets of tools that are programmed to act together to create a campaign. When the targeted recipient downloads the file or opens the email attachment, they become the exploit target. If the computer applied a security patch to prevent the exploit from working, then the security incident is avoided. The security patch is just one example of a preventive course of action. If the computer is not protected, the attack succeeds. If other control systems on the network detect this event, an incident response plan is activated. In some cases, a course of action will be available to repair the damage inflicted by an attack.

How Cybersecurity Information Sharing Interrupts Attacks

The United States leads the world in information technology innovation, yet the asymmetrical structure of cyber warfare means that government, industry, and individual technology users face significant challenges in the battle to stop cyberattacks. For example, one skilled hacker can attack hundreds of thousands of targets worldwide with the push of a button — and launch thousands of computer security professionals into action who will attempt to put out the same fire. Using the counter measures outlined in this report could help security professionals to streamline an orderly cybersecurity response.

The most potent counter measure available to the electric utility industry is to start playing as a cybersecurity team by executing according to the same playbook. Using a playbook will ensure that each player knows what to do, how to do it, and when to do it. Importantly, execution of a playbook requires cybersecurity systems to have access to the latest and most relevant threat information so that everyone can provide effective counter measures.

When cybersecurity information sharing programs are adopted and integrated into existing security control systems, defensive measures will be rapidly deployed, and cyberattacks will be far less likely to spread. The duplicative efforts of cybersecurity analysts can be redirected towards more important tasks, and a new level of collective situational awareness will be possible.

Stages of a Cyberattack

Each of the items in red represent a threat intelligence object type.

Reconnaissance – The **threat actor** uses the internet, social media, or other tools to discover likely courses of attack. Seemingly harmless activity can be flagged as malicious at the edge firewall by comparing the IP, URL or another **indicator**.

Weaponization – Public or privately developed code is designed to exploit the vulnerabilities on the target infrastructure. **Tactics, techniques and procedures** found on a forum are used to create the attack.

Delivery – The weaponized code is transmitted to the **exploit target** via spear fishing, email attachments, Java exploit, infected files, websites, or USB drives. **Indicators** detected in emails, or on the network, may signal that an attack **campaign** is underway.

Exploitation and Installation – The attacker uses the **tactics, techniques and procedures** in the delivered code to dismantle and/or work around internal cyber controls in the exploit target to avoid detection.

Command and Control – The attacker successfully installed the code without discovery and traversed the controls through an encrypted tunnel to a remote location. This may include screen capture, keyboard capture, malware execution, or spawning new virtual operating system environments. The **campaign** has succeeded.

Execution – The attacker executes the objective of the intrusion. This can include exfiltration or destruction of IT and OT assets, installation of ransomware, IP theft, or a host of other actions. This now has escalated into an **incident**.

Remediation – If the attack is detected early enough and the incident response plan is successful, a **course of action** will be put in place to correct the problem.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Cybersecurity Information Sharing in Action

Survey Results

A survey asked public power utilities to share their experiences with trying to obtain, interpret, and use CSI from various sources. Nearly all the respondents valued CSI with the following key attributes:

- **Accurate:** The information does not cause "false-positives," which indicate there is a problem when there is not.
- **Timely:** The information results in preventing an attack instead of remediating it.
- **Actionable:** The information can be used to detect, prevent, or recover from a threat.
- **Relevant:** The threat needs to have *context*.

Respondents recognize that CSI is critical for improved security posture and situational awareness. When asked about cybersecurity priorities, 95 percent of survey respondents ranked improved security posture as very important or critical and 89 percent ranked situational awareness as very important or critical. Good CSI sources provide a threat context. Organizations that filter incoming information can more easily maintain an improved security posture compared with organizations that do not filter information. By monitoring incident profiles and new exploits, a utility can see this information to set risk management priorities and improve incident response programs.

Many respondents have significant concerns about the security of sensitive cybersecurity information. Respondents universally identified a need to maintain processing control of CSI that originates from within the organization. Survey respondents also noted the importance of procedures or technical solutions that guarantee impartiality and anonymity when sharing CSI outside of the organization.

Many security professionals are overwhelmed by the amount of information received and find it difficult to hire, train, and retain qualified analysts. Most respondents noted that they use the E-ISAC along with one or more other platforms for obtaining CSI; however, respondents were also concerned about their ability to actionably use CSI obtained. For example, many small public power utilities reported that they do not have the advanced cybersecurity control systems to use IOC (indicator) threat intelligence. Instead, small utilities require information that indicates if the issue affects the hardware or software they have (exploit target) and what needs to be done to prevent the issue in a timely manner (course of action).

Market Research Study Results

To better understand existing and emerging technologies that could aid utility cybersecurity efforts, Navigant undertook a market research study on cybersecurity information sharing technology firms. Following this study, Navigant conducted onsite visits and installed information sharing systems at select public power utilities. The systems were configured and loaded with publicly available threat intelligence to provide a proof of concept. During a proof-of-concept exercise between two public power utilities, the Petya (2017) ransomware attack was simulated to assess system capabilities to detect and respond.

The two public power utilities were able to share the most current threat intelligence in a way that was accurate, timely, and actionable. A single CSI record contained all of the available information on the threat, including specific actions required to prevent the Petya ransomware attack from succeeding. As shown in Figure 3, many data points (Indicator/Observable or IOC) were associated with specific exploits (TTP), and provided a description of the threat (campaign), which systems were vulnerable (exploit target), and what had to be done to prevent the problem (course of action). This exercise demonstrated the opportunities to more collaboratively and powerfully collect, organize, and distribute CSI so that attacks can be interrupted before they occur. Moreover, this exercise demonstrates that CSI can flow in and out more easily than before, allowing utilities to interrupt each phase of the attack by playing as a team.

Figure 3: CSI record

Description

IB-17-10297-Petya Ransomware

On June 27, 2017, CISCP was notified of Petya ransomware events occurring in multiple countries and impacting multiple sectors. Based on initial reporting, this Petya campaign is exploiting a vulnerability in Microsoft Office when handling RTF documents (CVE-2017-0199) while also exploiting the SMBv1 vulnerabilities identified in Microsoft Security Bulletin MS17-010.

Technique used in Petya Attack

Preventive Course of Action is attached

Type	Title	Id
Exploit Target	Windows Server 2008 SP2	ncpa:et-d557b3b7-3467-4932-85a8-96bbca2af834
Course Of Action	Security Update for Microsoft Windows SMB Server (4013389)	ncpa:coa-c6959389-c4c7-4aee-9518-60989129ae87
Indicator	Malicious File Indicator	indicator-6f737751-5b57-11e7-87db-64006a85e1fb
Observable	(untitled)	NCCIC:Observable-50b258e0-c75b-4647-80d3-18a4ad38b0ae
Indicator	Malicious IPv4 Indicator	indicator-d364e78f-5b56-11e7-a875-64006a85e1fb
Observable	(untitled)	NCCIC:Observable-b9d9d1b2-5d51-41a8-a52c-8efdeeb785e9

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Security Patching as a Team

Hackers use security flaws in operating system and application software to release weaponized malware, worms, and other threats. As a result, there is a constant race in cyberspace between patching these flaws and exploiting these flaws. When a new threat emerges using an unknown flaw, this is known as a "zero-day" event. This is not the norm, nor was it the case with two recent major cyberattacks; both the WannaCry and the Petya attacks used an exploit that had a security patch available weeks before. However, simply automating patching security flaws is not always a straightforward solution. The patch may prevent an attack, but it may also break something else on the network.

Here is where "playing as a team" can have a significant impact. When an important security patch becomes available, the community can help determine the significance of the patch and can include caveats and other information gathered during testing to assist each other in updating cyber control systems. Leadership is required to drive these efforts forward. Accordingly, industries, including the OT hardware and software manufacturers, need to provide automated and timely threat intelligence to the utilities they serve. In addition, associations and other regional stakeholders have an opportunity to create a collaborative and accessible program that can bring unified and rational cyber threat intelligence to all members.

Recommendations

- When utilities deploy cybersecurity tools such as SIEM and antivirus products, the utility should ensure the tools can use the STIX/TAXII specification to facilitate the future success of sharing threat intelligence.
- Using TAXII, it is important to create "trust groups" that allow sensitive information to be shared between companies and associations that have a formal agreement in place to cover the activity.
- Utilities should join and participate with the E-ISAC to facilitate cybersecurity threat intelligence.
  - E-ISAC should collect and analyze STIX-compliant data. After analysis, the resulting threat intelligence should be available electronically through a secured TAXII service to member utilities.
  - The information should contain as many STIX objects as possible so that the information is actionable by smaller utilities without an SIEM platform.
  - E-ISAC could work with industrial control system vendors to develop and publish manufacturer-specific cybersecurity threat intelligence feeds. This will greatly reduce the integrity of the information provided, and will allow member utilities to access only the information that applies to them.
- Joint action agencies should provide members with access to the more advanced cybersecurity control systems SIEM platforms to increase cyber threat detection and mitigation.
- Larger utilities should proactively share threat intelligence and foster cooperation through legal intelligence sharing arrangements.
- Joint action agencies, state associations, and other collaborative entities should develop cost effective methods for collecting threat intelligence inside of smaller OT environments and securely sending that information to collective monitoring SIEM platforms to support improving the capabilities of public power utilities.

The recommendations above are, in part, the result of technical research and analysis and were confirmed through the feedback of public power utilities who generously volunteered to participate in the delivery of a proof-of-concept cybersecurity intelligence platform. Several platforms for cybersecurity information sharing were evaluated. Based on review and technical capabilities analysis, the product chosen for the proof-of-concept was NC4 Soltra Edge. This product was made available by the vendor and supported the complete STIX specification as demonstrated during the proof-of-concept. Other highly ranked products including Anomali STAXX and Eclectic IQ have also been involved in the development of the STIX/TAXII specifications; however, it was not possible to independently test and use these products. The market for cybersecurity information sharing products is rapidly evolving and there are many different models for sharing cybersecurity information.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Conclusion

Given the unique business and functional requirements as well as constraints of each public power utility, public power utilities should conduct independent critical analysis of the options available to determine which system is best for the utility. Information sharing represents a high-level objective that depends on existing cybersecurity systems being in place. Cybersecurity information sharing itself does not prevent cyber threats or provide any defense. Cybersecurity information sharing is a force multiplier that enables the software, hardware, and most importantly the dedicated security professional to work as a team. The best way to position a utility to take advantage of this powerful tool is to require any future vendors to demonstrate STIX/TAXII compliance and provide verifiable utility industry references prior to selecting the system.

APPENDIX A
STIX Specification

STIX is a language for having a standardized method for the representation of cyber threat information. The STIX language has constructs or components associated with the type of information being shared, including:

- **Observable:** A dynamic event or stateful property. In this example, the URL of a site that is being used for "phishing" has been observed.

Title	phish_url: http://varadsmilecare.com/images/Google/gduc/
Type	URIObjectType
Value	http://varadsmilecare.com/images/Google/gduc/

- **Indicator:** An observable with context. An indicator can contain a time range, information source, and intrusion detection system rules, among other items.

Date First	iType	Indicator	Country	Source	IP Address	Classification	Confidence	Source Reported Confidence	Status
2017-05-11 03:58:13	Malware C&C Domain Name	p27dokhpz2n7nvgr.1 33chr.top	GB	ISC SANS suspicious domains - High	89.238.181.75	Public	77	60	Active
2017-05-10 08:58:28	Malware C&C Domain Name	p27dokhpz2n7nvgr.1 33chr.top	GB	Lehigh Malwaredomains	89.238.181.75	Public	59	75	Active
2017-05-06 06:58:13	Malware C&C Domain Name	p27dokhpz2n7nvgr.1 33chr.top	US	ISC SANS suspicious domains - Medium	104.223.87.193	Public	56	60	Active

- **TTPs:** Tactics, Techniques and Procedures - Represents the modus operandi of the adversary. Note the assimilation of common attack pattern enumeration and classification (CAPEC) and common vulnerabilities and exposures (CVE) standards into the STIX specification. The following table provides examples:

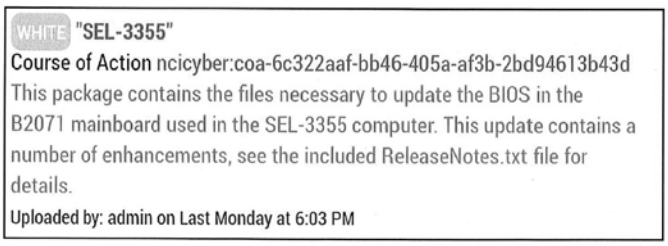
Intended Effects	Attack Pattern	Malware
Advantage - Economic Advantage - Military Advantage - Political Theft Theft - Intellectual Property Theft - Credential Theft Theft - Identity Theft Theft - Theft of Proprietary Information Account Takeover Brand Damage Competitive Advantage Degradation of Service Denial and Deception Destruction Disruption Embarrassment Exposure Extortion	CAPEC-484: XML Client-Side Attack An application does not perform sufficient validation to ensure that user-controllable data is safe for an XML parser Related Vulnerabilities: CVE-2013-0006 CVE-2013-0007 .	Automated Transfer Scripts Adware Dialer Bot Bot - Credential Theft Bot - DDoS Bot - Loader Bot - Spam DoS / DDoS DoS / DDoS - Participatory DoS / DDoS - Script DoS / DDoS - Stress Test Tools Exploit Kits POS / ATM Malware Ransomware Remote Access Trojan Rogue Antivirus Rootkit

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

- **Threat Actor:** The cyber adversary. This construct includes an associated TTP as well as the following information types:

Type	Intended Effects	Motivations	Sophistications	Planning and Ops
Cyber Espionage Operations	Advantage	Ideological	Innovator	Data Exploitation
Hacker	Advantage - Economic	Ideological - Anti-Corruption	Expert	Data Exploitation - Analytic Support
Hacker - White hat	Advantage - Military	Ideological - Anti-Establishment	Practitioner	Data Exploitation - Translation Support
Hacker - Gray hat	Advantage - Political	Ideological - Environmental	Novice	Financial Resources
Hacker - Black hat	Theft	Ideological - Ethnic / Nationalist	Aspirant	Financial Resources - Academic
Hacktivist	Theft - Intellectual Property	Ideological - Information Freedom		Financial Resources - Commercial
State Actor / Agency	Theft - Credential Theft	Ideological - Religious		Financial Resources - Government
eCrime Actor - Credential Theft Botnet Operator	Theft - Identity Theft	Ideological - Security Awareness		Financial Resources - Hacktivist or Grassroot
eCrime Actor - Credential Theft Botnet Service	Theft - Theft of Proprietary Information	Ideological - Human Rights		Financial Resources - Non-Attributable Finance
eCrime Actor - Malware Developer	Account Takeover	Ego		Skill Development / Recruitment
eCrime Actor - Money Laundering Network	Brand Damage	Financial or Economic		
eCrime Actor - Organized Crime Actor	Competitive Advantage	Military		
eCrime Actor - Spam Service	Degradation of Service	Opportunistic		
eCrime Actor - Traffic Service	Denial and Deception	Political		
eCrime Actor - Underground Call Service	Destruction			
Insider Threat	Disruption			
Disgruntled Customer / User	Embarrassment			
	Exposure			
	Extortion			

- **Exploit Target:** An asset's weakness in light of a TTP. This construct details the vulnerabilities, weaknesses and configurations. The patch update process is the ongoing effort to remediate software against specific TTP. In this construct, the STIX specification has integrated common vulnerabilities and exposures (CVE), common weakness enumeration (CWE) and common configuration enumeration (CCE) information standards.
- **Campaign:** A concerted effort by a threat actor to use one or more related TTPs that generate specific indicators when deployed against exploit targets.
- **Incident:** A set of activities associated with a campaign against an exploit target that may or may not be successful. This construct includes TTPs, observables and indicators along with several other types of information including: effects, victims, responders, discovery methods, and intended effects. This specification captures all the information that would normally be collected during the activation and execution of an Incident Response Plan.
- **Course of Action (COA):** Defensive actions against a threat (prevention, remediation, or mitigation). A COA not only specifies the procedures to be implemented, it also captures the impact, cost, efficacy and objective. An example is given below for updating SEL equipment.



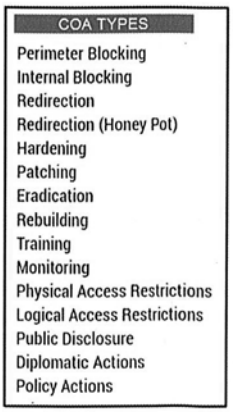
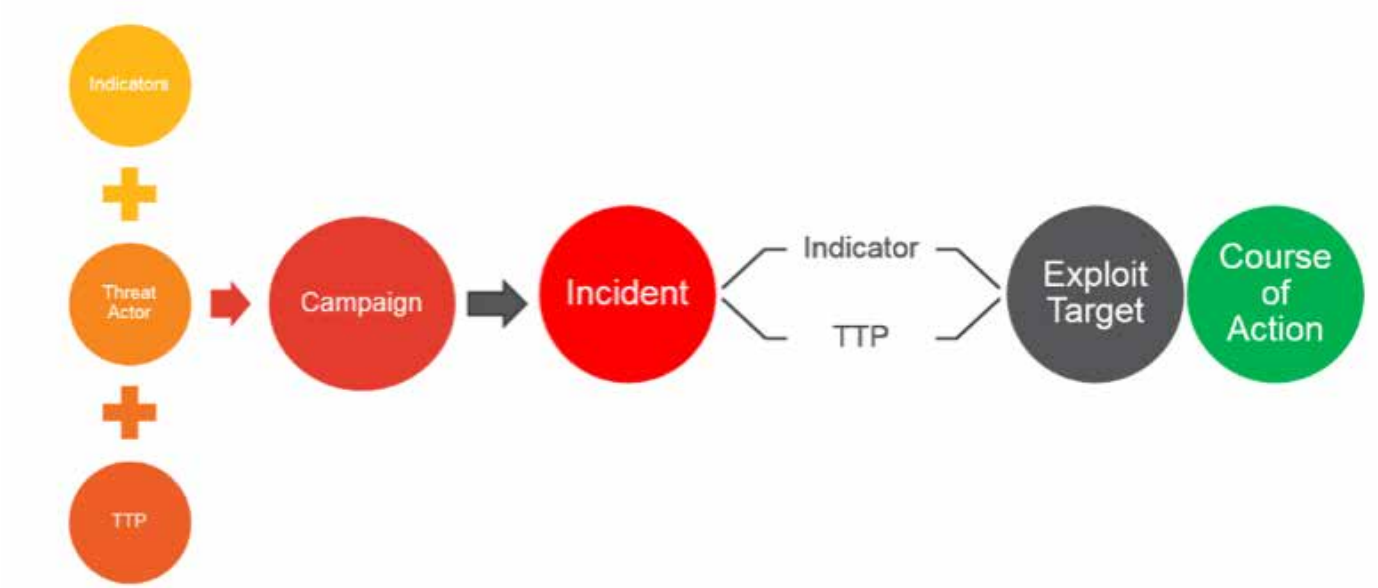


Figure 4 is a basic illustration of the relationship between these constructs. Threat actors develop TTP which can be identified by specific indicators. When directed against an exploit target, an incident may occur when the TTP is successful because a course of action was not implemented. The successful incident can be detected by associated indicators. Hopefully there is a course of action response available to remediate the problem. Depending on the situation, there may be different configurations.

Figure 4. Sample configuration of STIX constructs



2451 Crystal Drive
Suite 1000
Arlington, VA 22202-4804
PublicPower.org