Written Testimony

Bennett L. Gaines
Senior Vice President, Corporate Services, and Chief Information Officer
FirstEnergy

Before the

Joint Subcommittees on Energy & Research and Technology
Committee on Science, Space, and Technology

United States House of Representatives

On

Cybersecurity for Power Systems

October 21, 2015

Summary

Information-sharing between the electric industry and the federal government is essential to maintaining a strong, effective and proactive approach to protecting our nation's vital communications networks from potential cyber-attacks.

Cyber-attacks to the electric sector are becoming more sophisticated and are constantly evolving as defensive security measures become increasingly predictable. According to *Under Cyber Attack – Ernst & Young's Global Information Security Survey, 2013*, 59 percent of respondents saw an increase in external threats in the previous 12 months. Despite a target's firewall, antivirus protection, email and passwords, determined and malicious actors will stop at nothing to compromise or attack an organization's cyber assets. It has been said that compromising a system is not a question of *if*, but *when*. Moreover, sophisticated cyber-attacks can evade detection, potentially for weeks or even months at a time.

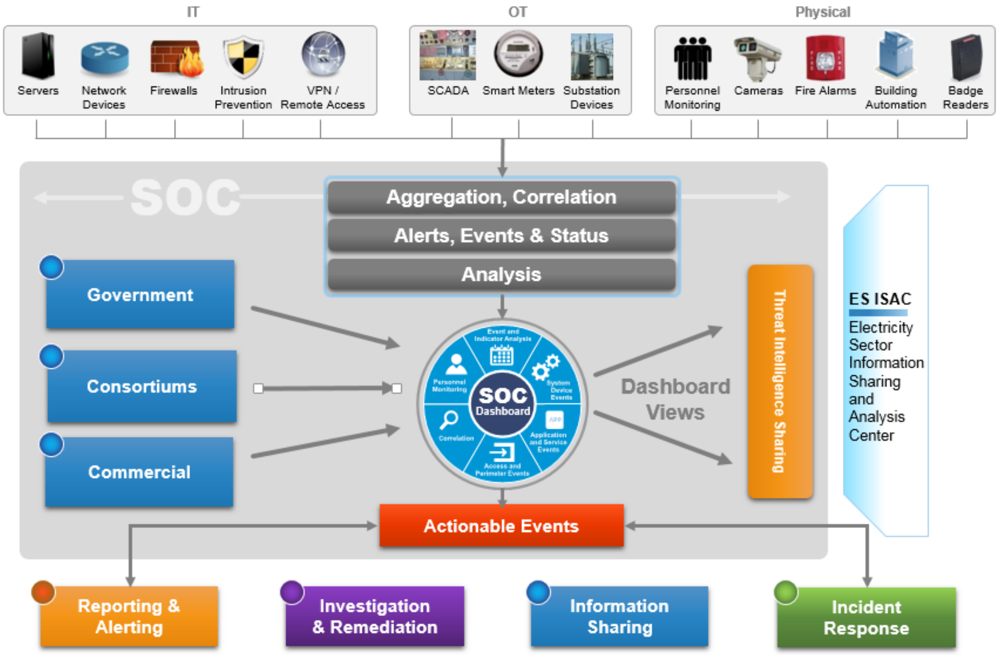
With every operational and technical advance that is made to improve productivity – including remote access, mobility and "bring your own device" policies – organizations also are broadening their attack surface and exposure. Additionally, electric utilities operate a complex, interconnected network of power plants, transmission lines and distribution facilities, and their management is distributed across each enterprise. High-value targets – such as Supervisory Control and Data Acquisition (SCADA) systems – further entice attackers to take advantage of an organization.

In response, many organizations are doing an excellent job with prevention through layered defenses, real-time alerting, operational monitoring and security awareness training and other proven tactics. In light of today's threats and vulnerabilities, however, we need to focus more of our attention on anticipating attacks rather than reacting to them. Leading organizations are expanding their efforts – and taking bolder steps – to combat cyber threats. Rather than waiting for the threats to come to them, they are prioritizing efforts that enhance visibility and enable a proactive response through monitoring and prompt detection.

Organizations may not be able to control when information security incidents occur, but they can control how they respond. The best way to reduce the adverse impact of an attack is to identify it and intervene as quickly as possible. To do this, we must increase our awareness of indicators, detect threats, and respond to incidents quickly and efficiently. We have an abundance of data to achieve this goal; however, this information often is acquired using diverse tools, stored in disconnected and isolated systems, and monitored by unrelated groups.

Solution

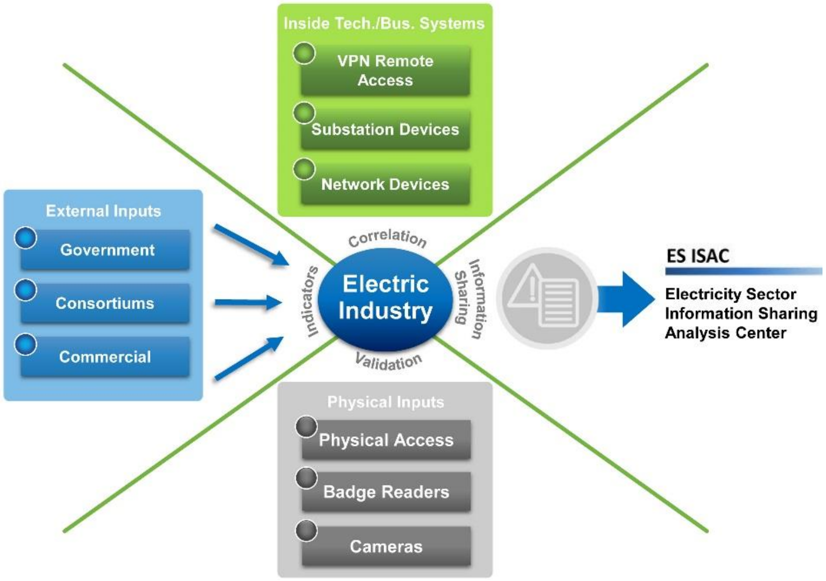
To combat cybersecurity attacks, a Threat Intelligence Management (TIM) program provides enhanced visibility of the enterprise's overall security plan by monitoring cybersecurity, physical security, information technology and operations technology. Advanced analysis of these functions is performed to provide an early-warning system for security incidents and rapid mitigation of vulnerabilities.



Analysis of the correlated data is conducted by security teams that augment real-time information from the Security Information and Event Management (SIEM) system and related tools. Teams develop requirements and identify indicators while designing the logic for additional use cases (a methodology used in system analysis to identify, clarify, and organize system requirements) to identify trends and emerging threats. The output is validated to ensure the use cases accurately identified threats and to determine the overall security posture of the organization, and this information can be shared with internal business units and external partners. It also could be shared with the federal government or sector-specific, information-sharing organizations as part of an overall threat intelligence collaborative. The benefits of this collaborative would include: identifying and communicating previously undetected Advanced Persistent Threats (APT); communicating precursors of upcoming attacks; providing indications of zero-day vulnerabilities (a gap in the software that is unknown to the vendor and exploited by a hacker); and developing and sharing mitigation strategies, use cases, firewalls and Intrusion Prevention System (IPS) rulesets.

Framework

As a practical matter, organizations can achieve the benefits of a TIM program by integrating global intelligence into their established security technologies and practices, and including these elements:



Planning: Organizations must decide the amount of protection they need to apply to their information assets on a granular level, department by department. This enables them to prioritize intelligence requirements, establish a strategic blueprint for protection, and outline intelligence workflows with both internal and external roles and responsibilities.

Collection: Typically, spending on internal intelligence collection and intrusion detection solutions is already significant. Augmenting it with external global intelligence networks and third-party data feeds such as botnets, Darknet, and peer-to-peer alternatives extends protection to cover emerging threats and preserves the value of legacy security investments. The intelligence infrastructure often includes a console or portal to make collected information available inside the organization.

Analysis: Intelligence analysis includes integration across multiple information sources, correlation to identify potential threats, and evaluation to determine the degree of risk each threat represents. This culminates in the identification of root causes and bad actors, with recommendations for defenses or countermeasures.

Dissemination: Dissemination typically involves cooperation among organizations and their external intelligence partners and includes early warning communications, customized action reports, and personal contact between internal security specialists and external intelligence analysts.

Adaptation and Enhancement: "Closing the loop" also is a shared responsibility in which intelligence partners develop event metrics and use cases to identify protection, detection, infrastructure and analysis.

A new generation of security data-mining tools uses innovative techniques to collect and analyze massive amounts of information: data from PCs, mobile devices and servers; data from internal networks, including the composition and content of network packets; and threat intelligence about attacks on other organizations and the tools and methods used. In addition to analyzing these traditional information sources, big data security tools also can obtain information from non-traditional sources such as building key card scanners, personnel records and even Microsoft Outlook calendars. This data may be used, for instance, to assess the legitimacy of remote log-ins by employees.

The heightened visibility provided by the big data capabilities of new security analytics platforms creates unprecedented opportunities to identify anomalies, uncover evidence of hidden threats or even predict specific, imminent attacks. More data creates a richer, more granular view as it presents the threat landscape in high definition. Security-related details can be seen in sharper focus, and irregularities can be found faster.

Security Indicators

Information from external sources, including governments, consortiums and commercial providers, is critical to threat intelligence. Established sources used today include Cyber Information Sharing and Collaboration Program (CISCP), which is a threat-awareness cooperative between the Department of Homeland Security (DHS), the United States Computer Emergency Readiness Team (US-CERT), and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Private organizations include the Electricity Information Sharing and Analysis Center (E-ISAC), which represents the electric sector; commercial services that inform customers of vulnerabilities and patches via alerts; and most recently, CRISP, the cybersecurity risk information sharing program that uses automated sensors to detect malicious activity attempting to compromise networks.

Data from these sources is important to overall cybersecurity, as it provides additional alarms and events that the organization is experiencing now. Knowledge gained from other organizations witnessing these attacks and events enables them to quickly identify when such events occur on their system.

Department of Energy, Cybersecurity Risk Information Sharing Program (CRISP)

CRISP is a public-private partnership that permits the sharing of cyber threat information and production of situational awareness tools to identify, prioritize and coordinate the protection of the electrical sector's critical infrastructure. CRISP enables critical infrastructure owners and operators to voluntarily share, in near real-time, cyber threat data and analysis and receive mitigation measures from other participants.

CRISP began as a partnership between the Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE/OE), the North American Electric Reliability Corporation (NERC) Electricity Sector Information Sharing and Analysis Center (ES-ISAC), Pacific Northwest National Laboratory (PNNL), Argonne National Laboratory (ANL), and participating companies. FirstEnergy is a participant, and more companies are being added.

Department of Homeland Security Enhanced Cybersecurity Services (ECS)

As the federal government’s lead agency for coordinating the protection, prevention, mitigation and recovery from cyber incidents, DHS works with business owners and operators to strengthen their facilities and communities. To accomplish this, the DHS Enhanced Cybersecurity Services (ECS) program was expanded in February 2013 by Executive Order (Improving Critical Infrastructure Cybersecurity).

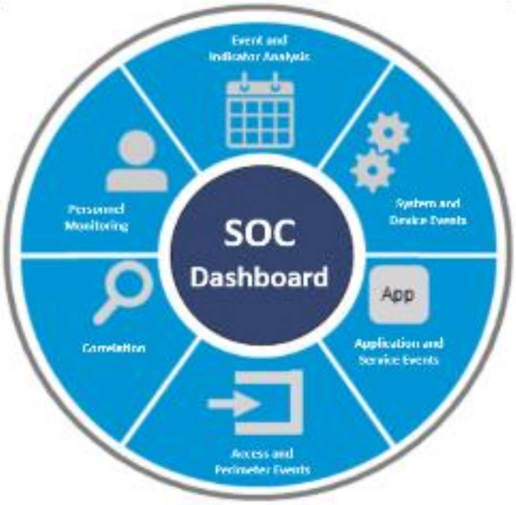
ECS is a voluntary information sharing program that assists critical infrastructure owners and operators as they improve the protection of their systems from unauthorized access, exploitation or data exfiltration. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops indicators based on this information and shares them with qualified Commercial Service Providers (CSP), enabling them to better protect their customers who are critical infrastructure entities. ECS augments, but does not replace, existing cybersecurity capabilities.

North American Electric Reliability Corporation (NERC)

NERC was founded in 1968 by representatives of the electric utility industry for the purpose of developing and promoting voluntary compliance with rules and protocols for the reliable operation of the bulk power electric transmission systems of North America. NERC’s mission is to improve the reliability and security of the bulk power system in the United States, Canada and part of Mexico. The organization aims to accomplish this not only by enforcing compliance with mandatory reliability standards, but also by acting as a catalyst for positive change – including shedding light on system weaknesses, helping industry participants operate and plan to the highest possible level, and communicating lessons learned throughout the industry.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The ICS-CERT partners with members of the control systems community to help develop and vet recommended practices, provide guidance in support of ICS-CERT incident response capability, and participate in leadership working groups to ensure the community's cyber security concerns are considered in our products and deliverables. The ICS-CERT facilitates discussions between the federal government and the control systems vendor community, establishing relationships that foster a collaborative environment in which to address common control systems cyber security issues. The ICS-CERT also is developing a suite of tools that will provide asset owners and operators with the ability to measure the security posture of their control systems environments and to identify the appropriate cyber security mitigation measures they should implement.



Security Operations Center

The Security Operations Center (SOC) is a concentrated set of sophisticated technologies and processes that provide enhanced visibility, correlation, real-time analysis and incident awareness of security events in the electric sector. The goal of the SOC is to provide a single pane of information spanning IT, OT, Physical and Cyber security. The SOC monitors and handles investigations with high efficiency and greater effectiveness than previously experienced in most organizations.

Building a well-informed Threat Intelligence Management program will result in more threat indicators, improved security, greater critical infrastructure resilience, and ultimately more industry and government collaboration. These efforts also support one of our nation’s highest priorities: Presidential Policy Directive 21 identifies “critical infrastructure security and resilience” as the shared responsibility of “Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure.”

Further, in Executive Order 13636 (“Improving Critical Infrastructure Cybersecurity”), the Obama Administration emphasized the need for robust information-sharing among all critical infrastructure stakeholders. The Threat Information Management program brings us to the closest point to not only our own identification and analysis of threats and attacks, but also to a more functional and effective information-sharing process – and the knowledge-sharing output of this process will help foster greater collaboration among all stakeholders.

Finally, while any information can be shared, it must be aggregated, correlated, analyzed and distilled to be relevant and actionable. The goal is to ensure a secure critical infrastructure that is as resilient as it is protected from threats and attacks.

Bibliography:

- Under Cyber Attack: EY's Global Information Security Survey, 2013
- EMC – Storage Report, 2013
- Cybersecurity Risk Information Sharing Program (CRISP)
- Department of Homeland Security – Enhanced Cybersecurity Services (ECS)
- North American Electric Reliability Corporation (NERC)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Department of Homeland Security – CRADA - Cyber Information Sharing Collaboration Program (CISCP)
- Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
- Presidential Policy Directive 21
- Executive Order 13636 "Improving Critical Infrastructure Cybersecurity"