Cyber Harmony: Orchestrating Peopleware and Centralized Situational Awareness

By Georgianna Shea and Randi Tomasek

Introduction

In 2015, Russian cyber operators launched a coordinated cyberattack on civilian energy infrastructure across Ukraine. The attack was unprecedented in scale. Over 100 cities and towns, comprising hundreds of thousands of residents, lost power for one to six hours.[1] The hackers first gained access through the information networks of several regional power companies by using spear-phishing emails to target individuals with administrative credentials. Then the intruders used remote-access tools to seize control of power distribution systems. Next, they used the communications lines and operator workstations they now controlled to send commands to field equipment, all the while locking the actual operators out of the system.[2]

At the request of the Ukrainian government, U.S. investigators helped pinpoint the cause of the disruption and identify vulnerabilities Kyiv could fix to prevent further attacks. The investigation concluded that a series of cascading problems caused the breach. Poor security hygiene in the power companies' business networks made them easy prey for the hackers' phishing campaign. Once inside, dilapidated operational infrastructure and a lack of monitoring for anomalous activity let the attackers run rampant through the system, destroying what they wished.

While the lights may have gone out across Ukraine, the attack (and the follow-on forensics) rang alarm bells throughout the U.S. government and the American energy sector. U.S. electricity providers were vulnerable to the same sort of devastating attack that struck their Ukrainian counterparts.

After reflecting on its own susceptibility, one U.S. energy company (hereafter referred to as "the Company") concluded that although it was meeting all its industry's cybersecurity requirements, it was still vulnerable. The Company was not centrally monitoring the operation and security of its systems. This rendered it unable to detect signs that malicious actors were poking around until after the launch of disruptive or destructive malware. Early detection could have kept the lights on in Ukraine. With that in mind, the Company determined it would need to do better if it hoped to thwart an attack before systems started shutting down.

The following report outlines how the Company set up a new security operations center (SOC), with supporting technologies and processes across all its business lines to better detect indicators of risk and emerging problems before hackers could launch devastating attacks. In particular, because attackers traverse business networks to degrade the operations of the physical equipment that makes up critical infrastructure, the Company determined it needed a unified view of all of its systems.

The implementation process was not easy. In fact, it was hard, costly, and time-consuming. But the Company knew it had to prepare for threats from bolder, more skilled attackers.

While the Company's specific technical solutions may not be applicable to other organizations, the broader lessons are. Organizations of all stripes can benefit from a centralized security monitoring system that differentiates between normal and abnormal operation and alerts them to potential threats. Other organizations should also take note of how the Company's cybersecurity team gained buy-in from decision-makers, engineers, operators, human resources, and many others. In other words, the Company did not just have the right hardware and software. It also devoted attention to what this report will call "peopleware."

1. Evan Perez, "Vermont utility finds alleged Russian malware on computer," *CNN*, December 31, 2016. (https://www.cnn.com/2016/12/30/us/grizzly-steppe-malware-burlington-electric/index.html); Blake Sobczak and Peter Behr, "Inside the Ukrainian hack that put U.S. grid on high alert," *E&E News*, July 18, 2016. (https://www.eenews.net/articles/inside-the-ukrainian-hack-that-put-u-s-grid-on-high-alert)

2. U.S. Department of Homeland of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure," July 20, 2021. (https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01); "Power grid cyberattack in Ukraine (2015)," *CyberLaw*, last updated June 4, 2021. (https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015))

Cyber Harmony: Orchestrating Peopleware and Centralized Situational Awareness

Starting the Process

The equipment, technology, and processes that make up information technology (IT) and operational technology (OT) are very different. Separate tools and expertise are necessary to monitor the two. Thus, organizations usually have distinct IT and OT SOCs managed by separate teams.

An IT SOC protects an organization's information systems, such as computer networks, servers, and applications. It typically uses tools — like firewalls, intrusion detection systems, and antivirus software — to protect the systems detect anomalous activity and respond to security incidents. In addition, an IT SOC usually works on logging, correlation, incident detection, response, and continuous monitoring to identify, mitigate, and contain a security incident. IT SOCs typically handle incident response, vulnerability management, and compliance with IT-focused regulations.

OT SOCs, meanwhile, monitor and protect industrial processes, such as industrial control systems, supervisory control and data acquisition systems, programmable logic controllers, and distributed control systems. OT equipment is often highly interconnected, with specialized devices that communicate with each other using unique protocols. Like the IT SOC, the OT SOC handles incident response, vulnerability management, and compliance with regulations for operational technology. In addition, OT SOCs also monitor the performance and maintain the availability of the OT assets.

IT and OT systems typically connect at a demilitarized zone (DMZ) that allows limited communication between the two. But as the underlying technology of both OT and IT grows more complex, the DMZ has become an entirely new cyber threat vector, where an attack on one side could cross into the other. Indeed, this happened in Ukraine in 2015: The hackers compromised the business IT network and then traversed IT systems to cause operational issues within the OT environment. Given this reality, the Company realized that keeping the SOCs separate was no longer tenable.

Instead of merely meeting cybersecurity standards, the Company determined it needed to completely restructure its operations. The program lead for this new effort understood that the Company needed changes to its hardware, software, and processes. But he also learned that peopleware deserves equal attention. For this new type of cybersecurity system to function well, the program lead had to work closely with and address concerns from Company decision-makers, engineers, operators, and administrators as well as the personnel in finance, human resources, and procurement. Peopleware can be just as important as hardware and software.

The team began by developing four high-level objectives that the Company's current technologies and processes were failing to achieve:

- "Know Good" – Enable automated, centralized collection, and monitoring of OT networks to provide visibility and establish a baseline for "normal" communication. At the beginning of the process, the Company had some automated IT monitoring but lacked automated OT monitoring, and neither was centralized.
- "See Bad" – Implement uniform monitoring of networks across all aspects of the Company to detect anomalies and possible intrusions in a timely manner.
- "Take Action" – Ensure coordinated action by the cybersecurity team, operators, and enterprise partners in response to alerts of anomalous activity.
- "Do No Harm" – Minimize operational impact across the organization while enabling a safe and injury-free workspace.

To achieve these objectives, the team determined it needed a combined IT-OT SOC with the necessary supporting technology and processes embedded throughout the Company to provide a single overarching, correlated view. Execution of this vision required a three-phase approach. First, the team would secure senior management support and buy-in. Second, it would establish the infrastructure capable of providing a centralized view of the monitored IT and OT. Finally, the team would hone and advance the operations.

Phase 1: Plan and Socialize

Phase 1 consisted of research, business awareness, and analysis to develop a detailed plan and gain management buy-in. The program lead recognized early on that not everyone would be comfortable with such radical change. To succeed, the team would need thoughtful, proactive socialization with those who could be affected by the project. Continuous engagement, explanation, handholding, and lab site tours for managers and operators across the Company's business lines helped ease anxiety about the change.

Throughout the process, the program lead never lost sight of the importance of peopleware. Armed with clear expectations of timelines, milestones, and budget estimates, all stakeholders were able to understand the project's scope and could strategically plan and allocate resources for the project.

Internal Assessments

The team needed to conduct cybersecurity assessments across the Company's six business areas — generation, transmission, distribution, natural gas, renewables, and nuclear. To provide a systematic approach, it adopted the National Institute of Standards and Technology's Cybersecurity Framework (CSF). The CSF's core functions are: identify, protect, detect, respond, and recover.

Using the CSF, the team determined the security and risk posture for the six business areas and developed a plan to improve. The team also used the CSF to create an enterprise-level view of the policies and regulations relevant to each business area and then harmonized the requirements.

External Assessments

The team also assessed the Company's risk and security posture against known cyberattacks and emerging threats. In addition to the due diligence and due care expected of an energy company at the time,[3] the team carefully analyzed the 2015 Ukraine hack to identify similarities between their systems and assess where the Company might have vulnerabilities.

Peer Utility Socialization

Next, the team sought expertise from other companies within the energy sector to leverage a community understanding of cyber defense practices for IT and OT systems. By establishing a relationship with similar organizations, the Company embraced a culture of learning from peer organizations' actions and receiving early indications, warnings, and threat-sharing information.

Intra-Company Communication

The program lead engaged with the managers of each business area to understand their operations. This effort ensured that a wide variety of stakeholders felt included in the process and understood the current cyber risk and potential advantages. It was critical for the program lead to convince the OT operators that the implementation of IT-OT SOC monitoring tools would not break or disrupt their systems or current operations.

3. Due care in cybersecurity includes implementing security protocols, such as network segmentation, access controls, and incident response plans; providing employee training on cybersecurity best practices; conducting regular software and firmware updates; and ensuring compliance with regulations. Due diligence in cybersecurity includes conducting regular risk assessments, implementing a security information and event management system, developing incident response plans, finding and managing third-party vendor risks, and building a security culture.

Cyber Harmony: Orchestrating Peopleware and Centralized Situational Awareness

Throughout, the program lead translated the plan's cyber jargon to explain the real-world risk to each business area's operations. This effort helped assuage people's egos, budget concerns, pride of ownership, and general fear of change, all of which can undermine new initiatives.

Mapping the Current State and Planning the Desired End-State

The program lead and his team next identified seven workstreams to assess existing visibility and determine how to achieve the desired end-state of "knowing good," "seeing bad," and "taking action" all while ensuring they "did no harm."

1. Asset and Network Awareness: The first step in being able to "know good" is to identify all assets. It is a truism in cybersecurity that you cannot protect what you cannot see. By identifying and monitoring assets, an organization can establish a baseline for what normal operations look like. This workstream identified how the Company was currently monitoring OT devices and network activity.
2. Surveys and Controls: In this workstream, the team evaluated OT cybersecurity maturity across business lines, including existing levels of compliance. The team used these evaluations to plan (and later to measure and track) OT cybersecurity improvements.
3. Advanced OT Lab: The team created an OT lab to exercise proofs of concept for innovative technologies, initial deployments, and upgrades to existing technologies in a near-production environment spanning all business areas. This workstream was critical to meet the objective of "do no harm" because it minimized operational impact across the organization while enabling a safe and injury-free workspace. It also demonstrated to other stakeholders that the planned deployments would indeed do no harm.
4. OT Security Information & Event Management (SIEM): SIEM systems monitor networks for malicious cybersecurity activity and provide visibility into the performance of digital equipment. The Company had IT SIEM as part of its IT SOC but did not have an OT SIEM system. This workstream involved planning how to create a centralized monitoring capability to be able to "see bad" across all business areas.
5. Deployment: This workstream identified desired cybersecurity tools for the automated collection of information about, and monitoring of, relevant OT assets. In the execution phase, the team also centrally prepared, configured, and tested the selected tools and devices before field deployment. This minimized outage requirements and time spent on site and ensured the tools would do no harm.
6. Change Management and Transfer to Operations: This workstream focused on helping stakeholders smoothly transition to the new system. In addition to continuing to build program buy-in, this workstream focused on establishing an operational model for the future to ensure the appropriate players would know how to act in the event of an incident.
7. OT SOC: The last workstream developed a plan to stand up and operationalize an OT SOC co-located with the IT SOC to centralize the capability to monitor all traffic from deployed cybersecurity tools. The team aimed to use the greater visibility provided by the new joint IT-OT SOC to enable the business areas to identify vulnerabilities and anomalous activities requiring a response.

Estimate-Based Funding

Next, the program lead secured CIO and CFO buy-in by developing a clear, detailed business and financial case that communicated the project's benefits regarding risk reduction and increased efficiency. These benefits included improved incident response times and enhanced compliance with current and anticipated future industry regulations.

As part of this, the team prepared a cost-benefit analysis for all aspects of the project lifecycle so that the CFO could understand the initial and projected operational and maintenance costs and reallocate funding from other departments' budgets. This process involved developing creative solutions to budgetary and personnel constraints. For example, the Company contracted out some initial tasks to avoid having to hire full-time workers who would be laid off after the initial surge of assignments was completed.

Cyber Harmony: Orchestrating Peopleware and Centralized Situational Awareness

Oversight and Governance Committees

After securing buy-in from the C-suite, the program lead set up oversight and governance committees to operate across the three-phased execution to ensure continued buy-in and support. Each committee, identified below, addressed milestones, risks, and issues. They discussed potential solutions to challenges, convened a change configuration board to examine impact, make decisions, and escalate issues to a higher-level forum as necessary.

Business Area Working Sessions
Attendees: Business area leads and corresponding program leads
Frequency: Weekly
Purpose: Address business area-specific milestones, risks, and issues; discuss potential solutions to challenges; make decisions; and escalate to the weekly Program Status Meetings as appropriate.

Program Status Meetings
Attendees: Program lead, workstream/business area leads, and key enterprise partners
Frequency: Weekly
Purpose: Review and discuss the progress of the program; address milestones, risks, and issues; discuss potential solutions; make decisions; and escalate to the Leads Forum as appropriate.

Leads Forum
Attendees: Program sponsor, program lead, workstream/business area leads, and key enterprise partners
Frequency: Monthly
Purpose: Review and discuss the progress of the program; address milestones, risks, and issues; discuss potential solutions to challenges; make recommendations for the successful execution of the program; and review recommendations and address concerns from any of the Working Sessions or Status Meetings.

Enterprise Security Oversight Committee
Attendees: CSO, CISO, customer delivery, business area executive, IT, finance, supply chain, global risk, administrative services, legal, audit, and corporate compliance
Frequency: Quarterly or as needed
Purpose: Set up an enterprise-level governance and oversight body of security programs and functions; manage risks; and make informed decisions on value, costs, and risk as needed.

Operating Council
Attendees: COO (Chair), CSO, operational SVPs, and program sponsors
Frequency: Quarterly
Purpose: Review and discuss the progress of the program against key program performance metrics.

Phase 2: Execute Program

Phase 2 established the required infrastructure to meet the objectives and support cybersecurity compliance requirements for all business areas. The Company deployed the IT-OT SOC architecture, which included security measures such as firewalls, intrusion detection and prevention systems, endpoint protection software, a SIEM system, threat intelligence platforms, and incident response tools. The architecture also included sensors to capture the network and system data and other tools that send and receive a digital heartbeat of the sensors to ensure they are working. Data from all these sensors and tools fed into the SOC's SIEM system to establish normal baseline activity so it could detect abnormal activity indicative of a cyber threat. The IT-OT SOC also included disaster recovery and business continuity plans as well as backup and recovery software.

Cyber Harmony: Orchestrating Peopleware and Centralized Situational Awareness

Establishing the new security measures meant deploying tools and technologies at more than 700 remote sites. Before a system-wide rollout, the team designated a pilot site to receive the new or updated technologies. After this site received the technology, the team — in partnership with the operators on the ground — administered, tested, and tailored the training, upskilling, and support model. The team also outlined the changes to ongoing maintenance responsibilities. Only after resolving issues identified in the pilot rollout did the team distribute the equipment to all the other sites.

To centralize equipment assembly and configuration for the sites, the Company augmented the IT-OT SOC with a cyber laboratory, the Advanced OT Lab. This enabled the team to develop plug-and-play tools. At the lab, the team configured each tool for the systems and environments in which it was being deployed; ensured each site had appropriate rack space, power, and backup capacity for the new equipment; and ensured the sites had configuration management. Then, when each remote site received a rack, the operators on the ground installed it and proceeded seamlessly with normal operations without additional onsite assistance.

Secondly, as noted above, the lab provided an environment to test and perform proofs of concept for new security technologies deployed into various OT environments. The team conducted this testing not only before the establishment of the IT-OT SOC but also through phases 2 and 3, when the team assessed additional protective tools were needed. Before the remote sites received any changes or upgrades, including new configurations and software modifications, the team conducted tests in the lab in a near-real-world environment replicating all OT business areas. Since OT systems are known for being fragile, these tests alleviated the operators' fears and ensured that changes would not impact critical communications, safety, or reliability.

After deploying the protective technologies, the team implemented updated processes for OT asset management, patch management, vulnerability management, governance and compliance, risk management, and supply chain risk management. The Company also created, updated, and tested disaster recovery and business continuity plans to recover from cyberattacks and restore normal operations. These plans included procedures for backing up and restoring data and recovering critical systems and applications.

Throughout the process, the implementation team worked with stakeholders across all business areas to transition all monitoring to the IT-OT SOC. Prior to the transition, each of the 700 sites had its own monitoring and response capabilities and responsibilities. This transition also harmonized SOC operations to meet cybersecurity regulatory compliance across the business areas.

Phase 3: Mature and Enhance

Phase 3 focused on maturing cybersecurity practices to increase operational resilience. After establishing the infrastructure in Phase 2, the SOC fine-tuned the sensor configurations and honed the standard operating procedures to detect anomalies and respond appropriately.

During Phase 3, the Advanced OT Lab served as a test and evaluation platform to simulate cyberattacks against the systems to see how they would respond. The IT-OT SOC systematically tested the OT protections and detection capabilities against known and potential hacker tactics, techniques, and procedures.

Cyber threats are dynamic. As such, efforts to mature the Company's cybersecurity capabilities continue to this day. Based on an evolving threat landscape, the Company regularly reviews its current and desired security posture. As necessary, the Company develops plans to close the gap by addressing security policies, procedures, and standards. These cover all aspects of operations, including people, processes, and technology.

As part of the maturing process, the Company also regularly conducts cyber tabletop exercises to evaluate its incident response plans. These exercises help identify gaps in the roles and responsibilities of each team member, gauge the effectiveness of the communication protocols, and determine the steps necessary to contain and remediate an

incident. Cyber tabletop exercises also help identify potential risks when deploying new technologies and capabilities. The Company also uses penetration testing and vulnerability assessments to identify and fix problems in its networks and systems.

Finally, the Company has continued to focus on peopleware. It provides employees with regular security awareness training that covers the Company's security policies, social engineering tactics, and individual response procedures. Regular training helps reduce the risk of human error and improves the Company's overall security posture.

Conclusion

Standing up a centralized IT-OT SOC across all business areas enabled the Company to "know good," "see bad," and "take action" while "doing no harm." The Company gained an enterprise-wide view of cyber events and can now more easily demonstrate regulatory compliance to auditors. Additionally, by prioritizing peopleware throughout the planning, implementation, and maturation phases, the Company created a business culture focused on cybersecurity. Because it included so many stakeholders outside the traditional cybersecurity sphere, the process (in combination with other, regular security training) helped raise awareness across the Company regarding cybersecurity risks and how to mitigate them. Across its multiple business areas, OT operators have become outspoken advocates for improving the Company's cybersecurity posture. Business leads are now knowledgeable about cybersecurity operations and receptive to operational changes that improve cybersecurity.

The Company has integrated the cybersecurity program into its overall business strategy. It is scalable, sustainable, and cost-effective. With an initial robust investment of time, money, and effort, the Company took significant steps to safeguard its systems, data, and reputation. This proactive approach is critical for all businesses operating in today's digital landscape, where cyber threats are increasingly complex and sophisticated. Of course, cyber threats will continue to evolve. There will be new attacks and new challenges. But by investing in the people critical to cybersecurity, the Company has better positioned itself to continue providing reliable and secure energy services to its customers.

Cyber Harmony: Orchestrating Peopleware and Centralized Situational Awareness

About the Authors

Dr. Georgianna "George" Shea serves as chief technologist for FDD's Center on Cyber and Technology Innovation and its Transformative Cyber Innovation Lab (TCIL). In that role, she identifies cyber vulnerabilities in the U.S. government and private sector, devising pilot projects to demonstrate feasible technology and non-tech solutions that, if scaled, could move the needle in defending U.S. prosperity, security, and innovation. Prior to coming to FDD, Dr. Shea spent 20 years spearheading cyber initiatives throughout the Department of Defense and other government organizations.

Randi Tomasek works as a cybersecurity operations analyst in the electrical industry, where she works with operational technology (OT) and industrial control system (ICS) security. In this role, she ensures compliance with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and Federal Energy Regulatory Commission (FERC) cybersecurity regulations. Randi Tomasek has obtained a Master of Science degree in cybersecurity and is currently a student at Colorado Technical University to obtain a doctorate in computer science with a concentration in cybersecurity and information assurance.

About the Foundation for Defense of Democracies

FDD is a Washington, DC-based, nonpartisan 501(c)(3) research institute focusing on national security and foreign policy.

About FDD's Transformative Cyber Innovation Lab

TCIL finds and nurtures technologically feasible, testable pilot projects which begin to solve some of the hardest cyber problems afflicting the national security industrial base and the United States. TCIL's mission is to help shorten the lag between idea and piloting and between piloting and the adoption of potential solutions to the thorniest of cyber problems. TCIL seeks to drive revolutionary, society-wide improvement in cyber resilience through the innovative synthesis of technology, policy, and governance.

For more information, visit: https://www.fdd.org/projects/transformative-cyber-innovation-lab

---