Cybersecurity: A framework for system evaluation

Ever-Green Energy shares how it developed its cybersecurity program – and lessons learned.

Tom Thomalla Jr., Senior Information Technology Manager, Ever-Green Energy

Courtesy Ever-Green Energy.

District Energy St. Paul, on the Mississippi River, operated and managed by Ever-Green Energy.

Cybersecurity is dominating the news in 2018. Data breaches reported by retailers and other companies that manage personal data have raised public concern and have individuals and corporations completely rethinking their security strategies. But what does this mean for district energy and other utility providers? Multinational companies likely already have systems in place, while smaller companies try to prioritize risk to essential services. Deciding whether your system is robust enough can be difficult to conclude as risks both increase and become more complex.

Ever-Green Energy has been navigating this territory, creating and implementing a cybersecurity program for its diverse operations, including municipally owned, private urban and medical campus district energy systems. The lessons it has learned in its decade or so of cybersecurity development may help other system owners and managers build evaluation tools and set priorities for their own operations.

SHAPING YOUR APPROACH

Cybersecurity can be a vast topic with critical implications for the businesses it affects. To narrow it down for this industry, it is important to start with a look at the essential components of cybersecurity programs serving district energy systems: program authorization, policies and procedures.

A very basic first step for system managers is determining who within their organizations is authorized to establish, manage and audit their cybersecurity programs. This includes deciding who is responsible for responding to issues, including major security breaches, if and when they arise. From the beginning, the support of organizational leadership is essential to ensure that proper investments can be made and that the protocols will be followed throughout the organization. This consistency is critical to the success of a cybersecurity program.

THE SUPPORT OF ORGANIZATIONAL LEADERSHIP IS ESSENTIAL TO ENSURE THAT PROPER INVESTMENTS CAN BE MADE AND PROTOCOLS FOLLOWED.

Policies and procedures are often thought of together, or even treated interchangeably, but they are different. A policy dictates that you must do something, and a procedure explains how to do it. In the context of district energy operations, for example, a policy might dictate delivering 42 degree F chilled water; a procedure would explain the steps to deploy chillers to deliver that service. With regard to cybersecurity, a policy example would be requiring strong passwords to combat the threat of common password decrypting methodologies; and the corresponding procedure would provide guidance for setting passwords with specific characters and complexity.

Once a cybersecurity program is established, policies should not need to be changed very frequently, whereas procedures will need to be more dynamic as threats and technology change.

With these basics in mind, and leadership support in place, development of a cybersecurity program can begin. First, a risk assessment should be initiated. This will look at what you have in place (computers, servers, network equipment, as well as physical security, data and processes) and see how threats may be able to leverage any vulnerabilities that may exist, while reviewing any protection mechanisms that are in place. Conducting a risk assessment can be an entirely overwhelming experience, producing a long list of actions that need to be prioritized to protect critical system functions. Risk assessments are essential, however, as they will help create your cybersecurity policies and procedures.

From there, the cybersecurity program will need to be implemented, with the expectation that not everything can be mobilized in year one. Management of staff time, budgets and scope is critical to success. Alongside protocol changes, it is essential to establish tools and metrics to track and assess the program as it evolves: Are users following procedures? Is training improving awareness and alignment with best practices? Is the district energy system safer?

In addition, it is important to consider how security measures can benefit the business, such as by making processes more efficient. Showing security benefits to the business is part of an ongoing discussion within the security field, as exemplified by "single sign-on" function-

ality. This allows users to spend less time signing in to applications and reduces the number of passwords they need. From the security perspective, it can also enable better audit logging and control of those applications.

In shaping an approach to cybersecurity, decision makers will also need to consider the unique challenges of managing security for a district energy system versus another type of utility or business. In addition, within the industry, there is a wide range of ownership and operational models that affect cybersecurity planning. For example, systems that serve a college or university campus are likely to function under the hierarchy of that organization's security policies; yet operators of those systems must also identify and advocate for customized protocols for the plant and controls that may not be applicable elsewhere in campus functions.

CAMPUS SYSTEM OPERATORS MUST ADVOCATE FOR CUSTOMIZED SECURITY PROTOCOLS THAT MAY NOT BE APPLICABLE ELSEWHERE IN CAMPUS FUNCTIONS.

Not all district energy systems are managing private or public customer data, but those that do may find widely varying expectations among their customers about how their data is handled – which could create challenges with metering or providing greater access to energy usage information. This is particularly relevant as demand for information and connectivity is significantly increasing.

Regulatory governance may also come into play as a variable affecting any given system's cybersecurity program, with differing expectations in each state for regulated or unregulated utilities. The scale of a district energy system's operations is another factor: A system with five buildings versus 500 needs to be able to minimize risk without making cybersecurity its number one budget line item. This will obviously depend on the complexity of the system and campus building programming. The demands of a hospital or research facility carry different risks than a standard urban center with multifamily residential and office buildings.

The District Energy St. Paul control room. Cybersecurity should not stop at the plant floor. Industrial control systems are often more vulnerable than IT systems once a physical or virtual barrier is passed. The plant staff plays an important role in helping to enforce policy and report potential issues.

OT VERSUS IT

It is all too common to focus on the information technology side of cybersecurity efforts (email, Internet, business systems) and miss the opportunity to shore up operational technology, including industrial control systems (ICS). There are a number of reasons for this. First, many companies believe that their ICS networks are separate from the Internet. They are likely not: A recent report from CyberX (*Global ICS & IIoT Risk Report*) indicated that 30 percent of ICS systems it audited had Internet access. Even if there is no Internet access to those critical ICS systems, there are likely valid business needs to get data in and out of the control systems, like utilizing real-time pricing information or sending performance data to an enterprise historian. Second, the IT staff is usually focused on protecting confidentiality, which can result in reduced access. The OT staff, such as your ICS staff and vendors, usually want more system access and availability, often at the expense of keeping things more secure.

It is also common for the IT and OT staff to be different personnel, to have limited interaction and to lack full understanding of each other's functional systems. It is critically important to consider the differing requirements of your ICS system when developing a cybersecurity program. You may need to involve your vendors in that process and conduct security cross-training for IT and OT staff, which will be a necessity as things become more connected.

BUILDING EVER-GREEN'S PROGRAM

Building a cybersecurity program for Ever-Green Energy systems has required careful consideration of all the program components noted above. Those components have changed over the years as cybersecurity threats have evolved and the business has grown. Ten years ago, Ever-Green was managing two systems of quite different scale – the nonprofit utility District Energy St. Paul with 200 customer buildings, plus the system serving the St. Paul Port Authority's Energy Park development with 28 connected buildings. At that time, the company's cybersecurity focus was primarily on such IT security basics as network permissions, antivirus software and firewalls.

Around four years ago, however, lacking a formal cybersecurity program, and with cyberattacks becoming more challenging for all businesses, Ever-Green recognized the need to institute a broader cybersecurity framework. An IT security audit had been completed, which returned a laundry list of measures that could be taken to protect the company's


Courtesy Ever-Green Energy. Photo Dean Riggott Photography.

Advanced controls systems are increasing efficiency and opportunities to manage production systems and data. They also require additional consideration and collaboration between IT and OT staff to maintain security.

IT systems. But without that broader program, it was difficult to make progress on implementing this list. The audit vendor was not capable of addressing OT security, so the results were not comprehensive.

In addition to District Energy St. Paul and Energy Park, the company had already begun operating, maintaining and managing Duluth Energy Systems, the city-owned steam and hot water system serving downtown Duluth, Minn., and Canal Park. As it was in the process of designing a broader cybersecurity program that would apply to these district energy systems, the company was also chosen in 2015 to form, operate, maintain and manage a new utility: Milwaukee Regional Medical Center Thermal. This system provides steam and chilled-water service to a consortium of six health care institutions in Milwaukee, Wis.

Ever-Green's cybersecurity efforts would now have to address the mandates of this medical campus customer as well. After securing executive support, company IT administrators developed a program based on the National Institute of Standards and Technology (NIST) 800-53 cybersecurity framework. This framework outlines standards, guidelines and best practices that organizations can adopt to help manage their cybersecurity risk. Next, Ever-Green IT administrators evaluated two different IT consulting companies as potential partners to assist in turning framework policies into action. This led to development of a multiyear approach with a phased policy rollout and continuous updating and change management. The work to define and roll out this program may be the least visible aspect to the IT work inside the organization, but it is both a critical and dynamic function of the IT team and the supporting systems.

LESSONS LEARNED

From the past decade of both cybersecurity implementation and growth of the Ever-Green operations portfolio, the company has learned several lessons:

- With its chosen approach, Ever-Green developed more general "umbrella" cybersecurity policy statements based on NIST 800-53 and deployed those in the organization. In retrospect, it would have been better for the common IT users to be provided with more concrete, specific policies and procedures so they would clearly know what was expected of them rather than have to wade through a sea of policies.
- Although the program was developed around NIST 800-53, the newer NIST Cybersecurity Framework (CSF) is gaining popularity due to having clearer language and a higher-level approach. While the overall body of work is certainly compatible with the information in NIST 800-53, it would have been easier for Ever-Green to have started with the CSF.
- As indicated above, an organization's first security assessment can be overwhelming. Instead of trying to make a little progress on many action items that an assessment will specify, pick the top 10, and do those really well. The sense of accomplishment will be greater, and you might ultimately make more progress with this focus and prioritization.
- Finally, the major lesson learned is that everything in IT comes back to risk and security. All IT decisions should have some consideration of risk and security no matter how insignificant an organization's need for those things may seem. Take, for example, core network devices. A standard security audit may identify that the firmware is out of date or the configurations may need some adjustment; but it may fail to identify that the hardware is near the end of its useful life or that the network architecture itself presents a risk from being overly complex or not resilient enough. When assessing risk, be sure to take everything into consideration, including an external security audit. Patching your network devices may be irrelevant if they are prone to general failure.

Managing cybersecurity for district energy systems is both a critical and increasingly complex challenge for system operators and managers. Below are the recommendations that Ever-Green Energy shares with project and operations partners. They are based on the company's breadth of experience and should certainly not substitute for a thorough evaluation of your system and consideration of a cybersecurity framework. Hopefully, they offer insight into the company's experience to date and what to consider when deciding your own priorities and investments.

- **Find an outside firm to provide a cybersecurity audit or assessment.** This could be an IT security consultant, a service offered through an existing IT vendor, or IT security expertise within a

District Energy St. Paul provides heating and cooling to 200 buildings in downtown St. Paul, Minn., and to a secondary area of development across the Mississippi River. The largest hot water district energy system in North America, it incorporates thermal storage, solar thermal and a wood residue-fired combined heat and power plant.

financial auditing firm. OT security expertise can be harder to find. Your ICS vendor may provide services or be able to point you in the right direction or seek leads in the IDEA forums.

- **Perform phishing tests.** This will show whether employees know how to identify and properly handle malicious email links and attachments. You may be surprised at the results. There are many free and low-cost options to do this without a major investment, such as PhishMe or KnowBe4. Your existing IT staff or IT vendor should be able to run one of these tests with minimal effort.
- **Consider a penetration test, or simulated cyberattack, to check your company's security vulnerabilities and defenses. But first assess the value to your organization in the context of everything else that can be implemented.** If you know you have large security gaps to fix and are just getting started on a cybersecurity program, the test may be a better fit for later in your protocol development. In other words: It may make most sense to be sure your front door is locked before paying a professional to try to break in.
- **Keep in mind that your risk assessment and security procedures need to take into account the multiplicity of factors at play in your particular district energy system.** The system as a whole must be considered in the development of cybersecurity plans, as different areas of security concern can be interdependent. Measures taken to mitigate risk may have tradeoffs. Closing a security gap in one area could create unforeseen challenges in another. For example, increasing password requirements may prove to be difficult for some IT systems or undesirable in OT systems. Security patching may reduce vulnerabilities but increase risk of downtime due to the patching or complications from patching.
- **Have a security-focused employee join the InfraGard.** InfraGard is a program partnership between the FBI and the private sector that is focused on protection of critical infrastructure. It can be a very informative exchange.
- **Train your users on cybersecurity.** People are an important first line of defense. Find online or in-person training methods that fit your culture and can be supported consistently by management. Create a culture where employees want to help guard your systems.
- **Talk to your IT/OT staff to better understand the "IoT/IIoT" in your environment.** While beyond the scope of this article, be aware of technology that creeps into your environment. Vendors are offering technology services that can bypass IT and put the organization at risk. This includes Internet of Things (IoT) devices like smart thermostats, smart speakers, smart meters or security cameras and Industrial Internet of Things (IIoT) like networked vending machines, water treatment monitoring systems, and systems that send plant performance data to the cloud for analysis. If it has an "app" or uses "the cloud," you should be paying attention.
- **Push your system integrators to embed security in the design of your industrial control systems.** If that's a limiting factor for the vendor's expertise, find a third party to help.
- **Just as for other operations protocols, you need to have a plan for recovery from – and not just prevention of – a security breach.**

In conclusion, as district energy system providers, we understand that our customers and users depend on us to provide reliable energy services. We have plans to deal with outages and system recovery. We have plans to deal with leaks in our distribution networks. Cybersecurity should also become an integrated part of our operations and management approach. It takes some work at the onset and ongoing diligence, but with the right framework and prioritization, it will prove immensely valuable to your system.

Tom Thomalla Jr., CISSP, *is the senior information technology manager for Ever-Green Energy in St. Paul, Minn. He holds a Bachelor of Applied Science degree in information technology infrastructure from the University of Minnesota and has a background in building and data center HVAC automation. In addition to overseeing the company's IT operations, he works closely with Ever-Green's industrial control experts to guide system architecture and security. Thomalla can be reached at tom.thomalla@ever-greenenergy.com.*