Behind the Firewall: A Conversation on the Evolution of Cybersecurity for the Utility Industry

Tremendous change is transforming the utility industry. Everything – from the digitalization of critical infrastructure to the relationship between utilities and its customers – is in transition. In the past decade, sophisticated organizations have seized on the promise of data from information technology (IT) to optimize operational technology (OT), including legacy power generation assets, digitally native energy sources and distribution systems. While the push to increase connectivity has helped the utility industry achieve greater efficiency, reduce emissions, and deliver reliable and affordable power to customers, it has also exposed weaknesses in its cyber defenses.

Cyberattacks now threaten the core value proposition for energy companies. Digitized operating technologies make an attractive target for a host of actors whose objectives range from financial gain to sheer disruption; and today a cyber arms race is the new normal for utilities and its suppliers. As digital technologies spread through and add value to energy infrastructure, attacks will continue to escalate in frequency and sophistication.

To explore the cyber challenges and opportunities facing the utility industry, Leo Simonovich, the Vice President and Global Head, Industrial Cyber and Digital Security at Siemens Energy, Inc., and Phil Tonkin, the Principal Security Engineer and a Global Head of the Cybersecurity Engineering for Operational Technology at National Grid, shared their perspectives on the state of the industry.

Phil, how do you view the evolution of the industrial cyber threat and what are you seeing on the ground at National Grid today?

Phil: Over the years, we've seen utilities being targeted either for criminal purposes or other nefarious reasons with ever increasing maturity, and an ability to exploit OT systems. The increase of cyber threats to utilities has grown as attackers and adversaries have become more familiar with the technology that we use. Previously, only cybersecurity professionals working at a utility understood the end products and protocols that were vulnerable to attacks, but now we are moving to a set of threats which are executed by very talented adversaries who are capable of specifically targeting the industrial sector.

A key reason for this change is that for a long time cybersecurity for the energy sector has been built around the need to improve efficiency by increasing connectivity within organizations. As a consequence, security for utilities was constructed in a way to ensure resilient operations within a very trusted environment. However, as utilities increasingly adopted digital technologies to improve efficiency and create system-level solutions to balance the grid, companies unknowingly created new cyber threats which became very appealing to malicious actors to exploit. We've seen real movement towards attackers targeting industrial organizations with social or critical infrastructure responsibilities, like us in the energy sector, and also all those in manufacturing, critical healthcare, or municipal functions.

Leo, how has Siemens Energy viewed the threat to industrial cyber?

Leo: At Siemens Energy, we are seeing similar trends. The number of attacks has gone up exponentially. The sophistication of those attacks is going up as well. What's more is that threats are increasingly targeted towards the industrial sector, and in particular towards energy production. The impact of those attacks is what's really worsened because an attack against the OT environment can result in a shut down, or worse, a safety event.

The attacks are increasingly coming from the convergence of physical and digital worlds. The notion that someone is safe because they're air gapped, I think is largely gone because a significant share of attacks now comes from within the plant. Either the attacks are from the office environment into the OT environment – such as a phishing scam – or they are brought in by an intelligent insider carrying malware into the plant environment. This has created a new threat landscape that utilities and operators, as well as OEMs like us, must urgently address. Going forward solving this problem will require strong partnerships between utilities, like National Grid, and companies like ours at Siemens Energy who have a long legacy in both manufacturing OT and securing the IT systems that are essential in today's digital environment.

The energy industry is undergoing a lot of change at the moment. We're currently seeing an increasingly decentralized grid, new ways of working as COVID-19 has forced more employees to work remotely leaving systems more vulnerable to cyber threats, and a rise in nation state-driven cyber-attacks intentionally targeting critical infrastructure. Given all this change, how have cybersecurity strategies and tactics shifted in this landscape? And how are these new threats forcing the industry to adapt - both from the utility's perspective and OEMs like Siemens Energy?

Phil: In terms of assessing new threats, it's critical for us to prioritize security investments in compensating controls by hardening cybersecurity around physical assets while balancing improvements in operational resilience and business efficiency. As we look into the future at a decentralized grid, defense-in-depth measures become harder to implement as the industry adopts more edge connected devices, smaller distributed generation facilities, and even people's homes being part of the energy ecosystem. This is where partnerships really matter and companies like Siemens Energy who develop, deploy, and maintain hardware across the energy value chain – and the software these systems run on – becomes crucial as the utility's threat landscape expands.

Today's strategies and tactics are about having a risk-driven approach to mitigating threats. This risk-based approach requires we assess the exposure of our assets. The first thing we consider is the internal threats to our legacy or brownfield systems to better understand how they are digitally connected. This process helps us identify all possible threat vectors, and then weigh their vulnerability individually as well as against our entire system. Then, we examine external attack patterns that are being used against assets to implement an appropriate defensive strategy. As we undergo this process, we consider how threats often manipulate organizations through corporate domains, breach protected zones, and ultimately work down to the assets through various layers of defense. We also identify accidental threat actors that may look to bring data into the site through transient devices, whether that's an engineer carrying a laptop or a USB stick.

Leo: Utilities are facing the perfect storm. On the one hand, they have to secure brownfield assets that are old and that have not been maintained; on the other hand, utilities are in the midst of the energy transition towards renewables and decentralized production, so they have to secure assets that are digitally native. Therefore, utilities must have a dual focus to their industrial cyber programs.

As the sophistication of threats increases, the concept of resiliency becomes a core strategy in protecting brownfield and digitally native assets. We recently partnered with the Ponemon Institute to do a study on the cyber risk facing utilities, and we asked one question to get a sense of how many utilities were going to experience a major event this year. The majority of those surveyed said that they experience at least one major event that leads to a shutdown, or some sort of a safety event.

This statistic tells us that in a world where the probability of being attacked is 100 percent, utilities needed to focus on resiliency and their ability to withstand attacks. The concept of resiliency is really multifaceted and is especially important for organizations bringing together interoperable networks or systems. First, utilities must be proactive in detecting attacks; second, they must be capable of responding to attacks with speed; and third, utilities must be practiced in mastering resources, not just within their organization, but within their larger ecosystem. Ultimately, mastering resources is really a question of focusing on multiple risks, the complexity of responding to risks, and then balancing priorities to muster resources and to tap the relationships between organizations.

The statistic demonstrating that most utilities will face a major cyber event annually is an alarming reality. To dive deeper, now that we know attacks will happen, and companies must constantly prepare, what role does instant response play in the utility industry? And how does Siemens Energy and National Grid think through this process?

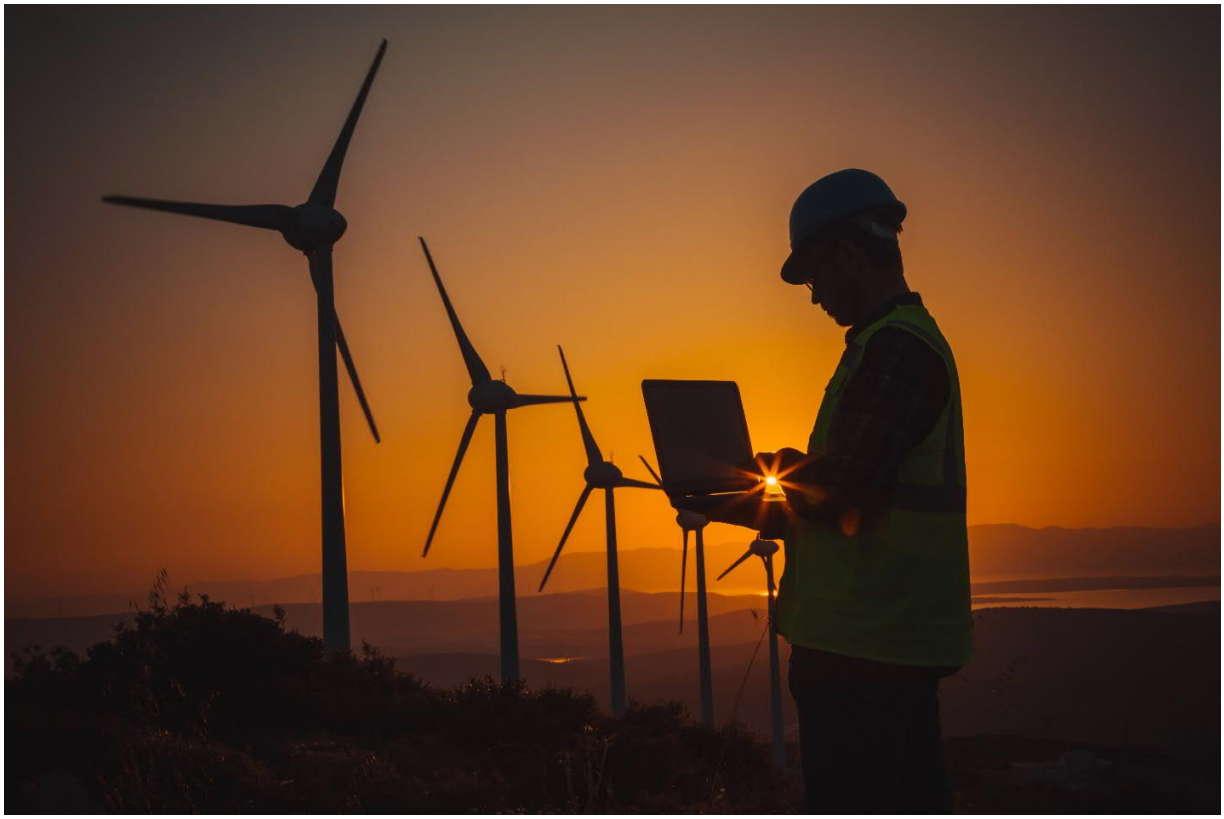
Leo: Siemens Energy recently issued a Playbook for Instant Response where we simulated multiple scenarios that might come up during an attack. Sometimes an attack will start with a physical incident or with a potential breach in the supply chain, and then very quickly manifest itself to something that's larger. What we found is that having visibility and awareness in multiple parts of the organization - not just in the security function – but rather deeply embedded within the operational control, will allow you to identify incidents early. Once you have that level of awareness, you can then diagnose and triage issues by deploying resources appropriately.

The Playbook also revealed that it's not just important to prepare internally. As operators and suppliers become increasingly interconnected, utilities often depend on external partners, therefore all aspects are crucial to the security value chain outside the plant too. It's important for people in Phil's role at National Grid to involve the OEMs, like us at Siemens Energy, in incident response planning so we have a common playbook to effectively identify, triage, and recover from attacks when they occur.

Phil, since involving OEMs and others partners in a utility's supply chain is crucial for a plant's overall security and instant response planning, how should a solutions provider – like Siemens Energy - think about the challenges that security leaders like you face on a daily basis?

Philip: I think there are two ways to look at this. On the one hand you have the OEMs and the system integrators who are partners in delivering the technology that we need to operate on business. They manufacture power generation, and transmission and distribution equipment so they have an intimate knowledge of these critical systems that utilities rely on. In that sense, we couldn't work without organizations, such as Siemens Energy, to deliver the technology necessary to deliver energy to our customers; this is especially true as companies like National Grid bring together interoperable systems to ensure reliability throughout the grid. So, it is important that cybersecurity is seen as something that is embedded in how we work with all technology suppliers.

When it comes to cyber security solutions providers, one of their biggest challenges is to understand the environment in which we operate, and the timescales in which we construct solutions. A lot of the technology providers have smart ideas that may be technically sound, but not possible or realistic given the constraints of the environment in which we operate. We're building assets that we expect to last for many years, and we start the engineering process far before anything is commissioned. Because we've probably started thinking about the next locations, we will build five or 10 years in advance, and it's not a simple case of plugging in a monitoring box on a site. It requires careful consideration and an understanding of the engineering environment in which they're operating. Cybersecurity providers need to make sure that their solutions match both the technical and business realties that utilities face on a daily, weekly, and yearly basis.



What would you say to board members, to C-suite executives in the energy industry or even in the financial and investment community, about what they need to do, what solutions you think could be brought to bear that would really make this entire ecosystem more secure? And what are some short term and long-term steps that they can take to help you do your jobs?

Phil: In order to expect any board member to really understand the threat of industrial cyberattacks in the organization that they represent, it's really important to demonstrate the critical nature of cybersecurity. You can never forget that board members are in a leadership position because they bring a wealth of experience from a variety of sectors.

In my experience, board members are very concerned today about managing risk, and about managing sustainability. Cyber is a key component of both of those things and has a clear impact on business. Not just in terms of how cybersecurity issues are managed during an incident, but how an organization recovers from an attack, manages messaging, and maintains confidence with its customer base. Given these multifaceted aspects, board members are often very well equipped with their background and experience to understand how it all fits together. So, it is our job to make sure that the threats we face become real for leadership. It's important for CISOs to bring tangible and measurable risks to board members and CEOs early and often, and bring them into the process of the challenges we face and the solutions that will address an issue – whether it be on new technologies, strategies, or expertise needed to ensure risks are managed.

Leo: For boards, cybersecurity has become a key part of their job and a way to manage risk. What's important for boards to recognize from a strategic level is that industrial cyber risk is different from other aspects of cybersecurity, both from a threat and impact point of view; industrial cybersecurity requires direct ownership from division heads and business unit CEOs, employees out in the field, and suppliers to

then be able to have visibility into their risk profile. It's absolutely crucial that communication is a two-way street so that industrial cyber professionals are in conversations early and frequently with CEOs.

At a tactical level, often boards typically get involved when an incident has already occurred, and they are forced to respond. At this stage – when an attack or crisis is underway - you lose a lot of agility, and it's often too late to minimize impacts. In my view, boards need to be in conversations just as early and often as business unit CEO. They must be asking tough questions on tradeoffs between cyber risk and business operations before any event occurs, and they must recognize the two strategies that utilities must pursue in securing the brownfield environment and securing the new digitally native industrial IoT world.

It's almost like they need to make cyber a part of their day-to-day job. In the way that they ask questions about the business itself, they need to be asking questions about industrial cyber as well on a daily basis. Moving beyond the executive level and speaking at the overall utility ecosystem, I think we need to develop a mentality that says, "we're in this together." It's going to take a community effort - a concerted effort - that really brings together different parts of the ecosystem to enhance security for critical infrastructure. And it takes a real partnership, all levels of the organizations, but also between organizations, to build trust and then to act in concert against the ever-increasing threat.

SIEMENS
energy