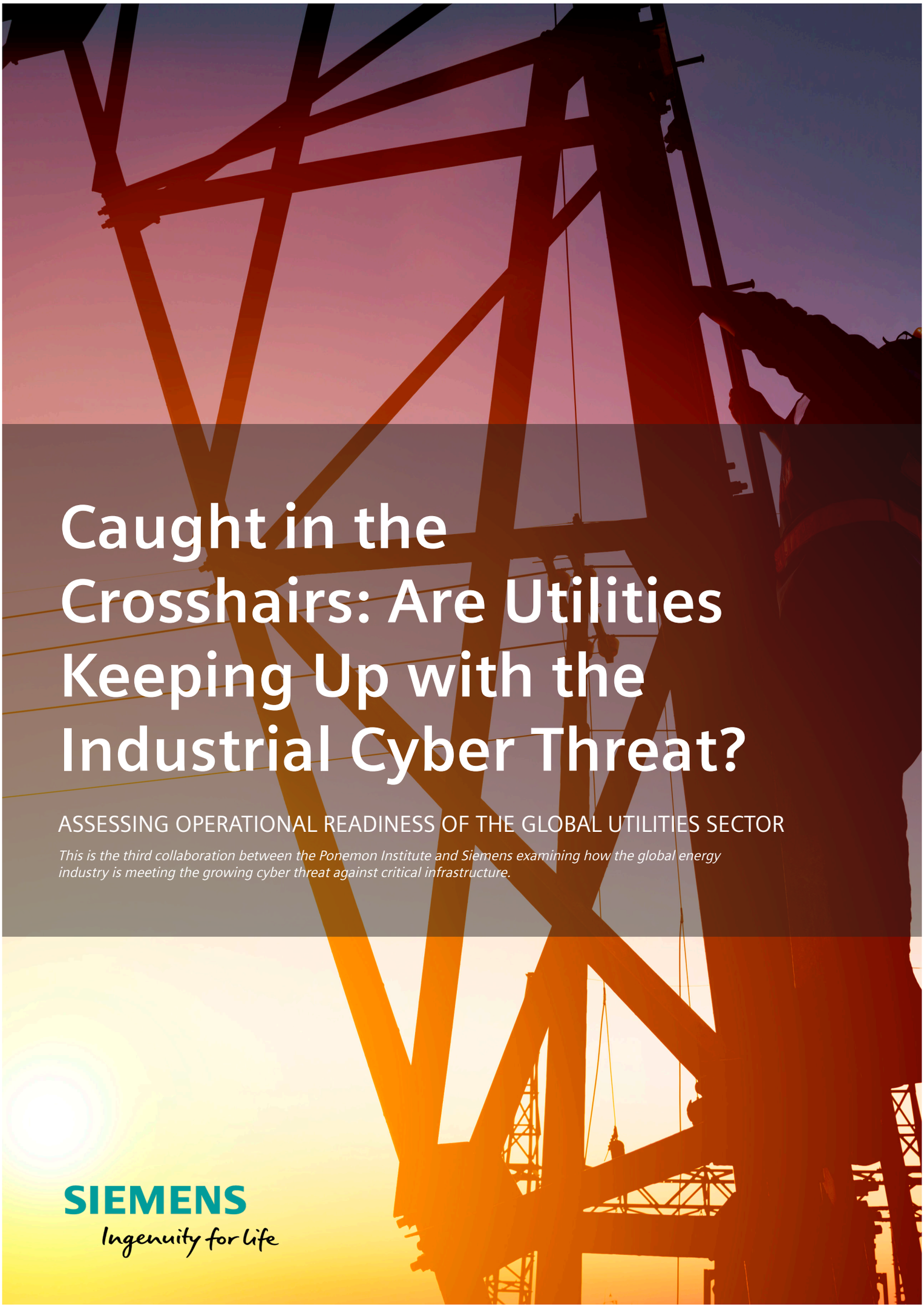


Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?

ASSESSING OPERATIONAL READINESS OF THE GLOBAL UTILITIES SECTOR

This is the third collaboration between the Ponemon Institute and Siemens examining how the global energy industry is meeting the growing cyber threat against critical infrastructure.

SIEMENS

Ingenuity for life

PONEMON INSTITUTE

The Ponemon Institute conducts independent research on privacy, data protection and information security policy. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

In addition to our research, Ponemon Institute provides strategic consulting to private and public sector organizations interested in establishing or enhancing their privacy, data protection, and security practices. To ensure that their goals are achieved, organizations engage us to assess their practices and conduct workshops and training programs.

Ponemon Institute is the parent organization of the Responsible Information Management (RIM) Council. The RIM Council draws its name from the practice of Responsible Information Management, an ethics-based framework and long-term strategy for managing personal and sensitive employee, customer and business information.

For more information go to:
https://www.ponemon.org/

SIEMENS INDUSTRIAL CYBER

Given the probability of a cyber breach is nearly 100 percent, the question for executives and security professionals becomes not whether to act, but how? Holistic cyber security emphasizes not only the need to prevent an attack but also the game plan for how to respond.

At Siemens, we take our customers on a cyber security journey that brings maturity to their industrial enterprise. This means starting with a risk-based strategy that deals in fundamentals, transforms an organization's response to the environment, and most importantly, builds their capacity to monitor and respond to threats. These threats range from connected assets in the field to control centers that run critical infrastructure, to the enterprise networks that make up the new energy value chain.

This agility is essential to dealing effectively with the growing cyber threat. The organizations that move proactively to build their capability to detect vulnerabilities, and respond to attacks, will be best positioned to meet the challenges and opportunities of a digital economy. For Siemens, a secure industrial world is an essential component of our vision for an energy industry that leverages digitalization and intelligent infrastructure.

In the past decade, Siemens has invested over $10 billion to make digitalization a core part of our own business transformation. Now we are making our industrial cyber capability and its complementary external offerings available to our customers.

For more information go to:
https://new.siemens.com/global/en/products/energy/services/digital-services/cybersecurity.html

FORWARD

The new industrial revolution is transforming the way utilities do business. Rapid replacement of traditional generation with renewables, like solar and wind, combined with digital performance management, is increasingly becoming a source of competitive advantage.

Recognizing that digitalization brings both clear benefits and the possibility of disproportionate risks, Siemens and the Ponemon Institute returned to our cybersecurity collaboration for a new report assessing the state of cybersecurity in the utility industry. We sought to assess the maturity of the industry's cybersecurity practices, as well as the type and degree of the threat observed by operators in the field. In doing so, we hope to better prepare organizations to benchmark cybersecurity efforts and bolster their defenses.

We found that the level of threat to Operational Technologies (OT) has indeed increased. Attacks now target energy infrastructure with growing severity. Successful attacks can cause shutdowns to critical product system, including safety systems. Meanwhile, many organizations report pain points in effectively aligning OT and Information Technologies (IT) cyber defenses.

Across the energy industry, many organizations share the difficult challenge of keeping ahead of attackers, while taking advantage of digitalization. We at Siemens and the Ponemon Institute believe that by building awareness, covering common blind spots and sharing best practices, we can strengthen the industry's resilience.

The stakes are high, but together, we can deliver on the promises offered by digitalization. We jointly can ensure new technologies bring efficiency, threat detection, and reliability, even in the context of increased attacks.

Leo Simonovich
Global Head
Industrial Cyber and Digital Security,
Siemens Gas and Power

EXECUTIVE SUMMARY

Siemens and the Ponemon Institute are pleased to present results of a survey "Are Utilities Keeping Up with the Industrial Cyber Threat? Assessing the Operational Readiness of the Global Utilities Sector". The study surveyed a range of utility professionals responsible for securing or overseeing Operational Technologies (OT) assets. Research was conducted to gain a clearer picture of utilities' existing capabilities, levels of preparedness, vulnerabilities, and strategic understanding of their OT cyber risk.

To help make our key findings and conclusions clear and actionable, they have been grouped into three areas: Risk, Readiness and Solutions.

The survey results show that risk is worsening, with potential for severe financial, environmental and infrastructure damage. Industry-wide, readiness is uneven and has common blind spots. In particular, this report highlights the unique cybersecurity requirements for OT, and the importance of distinguishing between security for OT and security for Information Technology (IT). This remains a major challenge for many organizations across the industry.

Industry leaders can, and should, check their organizations' readiness and implement solutions that keep up with the proliferation of both new, connected technologies and existing assets operating in brownfield environments.

This report provides three sections to assist leaders in assessing and improving their readiness against the growing cyber threat:

Risk: discusses risks reported around the world and across the industry, including the damage that would result from incoming threats.

Readiness: looks at how organizations are currently responding to the threat environment, the self-assessment of capabilities compared to anticipated attacks, and known gaps in preparedness.

Solutions: offers frameworks for thinking about how your organization can bolster their capabilities and stay ahead of the threat.

Our aim in this report is to increase awareness of the expanding risk to operating environments, provide insights to assist leaders in discovering blind spots within their organization, and raise the overall level of maturity across the industry.

WHAT RESPONDENTS SAY

HIGHLIGHTS

01

Majority of surveyed global utilities say that cyber threats present a greater risk to their OT than their IT environment. Utilities are concerned by the unique characteristics of OT, including a focus on availability, reliability and safety

02

Across the industry, 64% of respondents say sophisticated attacks are a top challenge, and 54% expect an attack on critical infrastructure in the next 12 months.

03

56% report at least one shutdown or operational data loss per year. Respondents report crippled operations by causing outages, damage, injury, and even environmental disaster.

04

25% of respondents report being impacted by mega attacks, with expertise developed by nation-state actors. Incoming attacks show greater skill in finding weakened entry points, and may be cheaply built with destructive effects as their primary goal.

05

Insider threat represents the majority of attacks in OT.

06

Only 42% rated their cyber readiness as high, and only 31% rated readiness to respond to or contain a breach as high.

07

Smaller organizations reported significantly greater concern with their own ability to complete critical cybersecurity tasks. These organizations were also less confident in their ability to understand the operational implications of an attacks and take action based on those alerts.

08

Respondents rated their organizations' ability to achieve comprehensive and continuous discovery and inventory of digital assets as being particularly low.

09

AI and big data analysis are used by 18% of organizations to monitor operations and recognize threats.

10

Respondents industrywide indicated a critical human capital gap. People with appropriate skills are scarce – in every region around the world.

INTRODUCTION

In the past five years, digitalization has transformed the utility industry. The rapid adoption of connected power generation, transmission, distribution, and end-use assets are enabling utilities to move away from centralized power generation technologies, and towards distributed energy. Coupling grid assets with software has served as a boon for utilities to reduce carbon emissions through distributed power generation, like wind and solar, but also by improving the efficiency of existing brownfield assets.

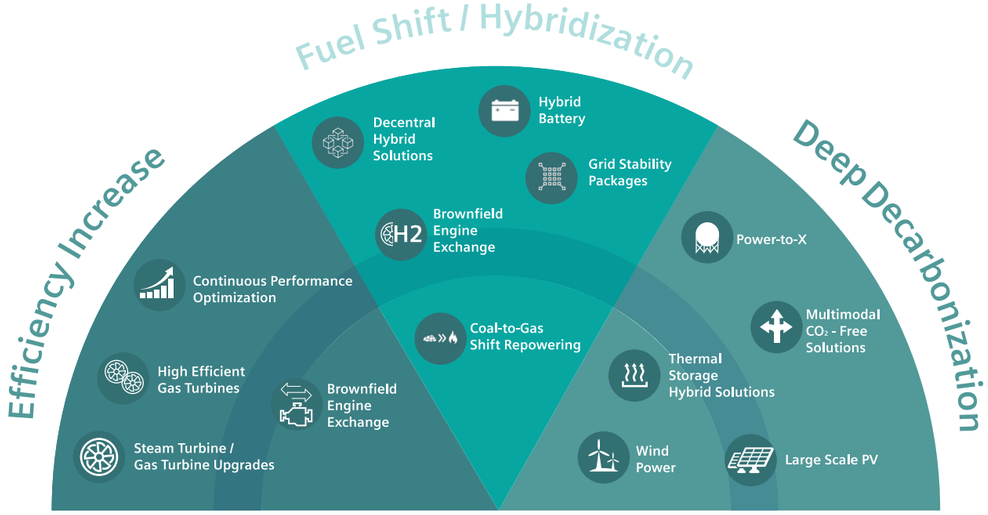


Figure 1. Energy Transition to Deep Decarbonization

As the utility industry continues its transition from analogue to digital, from centralized power generation to a distributed system of natural gas and renewable energy, existing OT technologies are increasingly equipped with IT software to help operators provide the benefits of digitalization to their customers.

IT INFORMATION TECHNOLOGY		OT OPERATIONAL TECHNOLOGY
The servers, computers, and mobile devices that enable business operations in the utility industry in offices environments	VS	The machines, systems, and networks used to generate, transmit, and distribute power
3-5 years	Component lifetime	10-20 years & legacy systems
Mature stages & advanced cyber knowledge	Cyber market maturity	Early stages & limited awareness
Loss of data	Key concerns	Impact to production, health, safety & environment
Recover by reboot	Recovery ability	Fault tolerance essential
Continuous	Connectivity	Intermittent, high delay causes serious concern
Straightforward upgrades, automated changes	Ability to update	Typically difficult to patch, changes made by vendors

Figure 2. Differences between IT and OT

At the board level, utility executives are increasingly investing in connected technologies, such as edge and cloud computing, to help gather data and make better technical and market decisions. This data helps executives extend asset life; improve reliability and efficiency; and drive uptime and ultimately better asset yields.

While the deployment of digital and networked equipment through the operating environment greatly increases the control and intelligence that organizations have over grid assets, these same technologies provide malicious attackers with new targets within a broader, more complex attack surface.

In an effort to digitize their fleet, utilities historically viewed cyber security as an afterthought. Even when new OT assets are designed with security in mind, they are often connected to broader critical infrastructure which lacks systemic security controls. As utility executives incorporate distributed and digitally connected grid technologies into their asset portfolios, their ability to withstand a cyber-attack is limited at best.

RISK

The target of attacks has shifted toward OT. The majority of respondents agree that cyber threats are a greater risk in the OT than the IT environment. Where past attacks primarily targeted data theft, current and future attacks can hijack control systems and logic controllers that operate critical infrastructure with the intent to cause physical damage and outages. This year, the majority of global utilities surveyed say, cyber threats present a greater business risk from their OT than their IT environment. Utilities are concerned by the unique characteristics of OT environments, including a focus on availability, reliability and safety.

The risk that cyber attacks pose to the OT environment is increasing in frequency and potency as malicious actors' ability to accurately target critical infrastructure assets improves, causing even greater consequences for utility sector operators, managers, and executives.

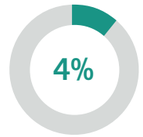
Across the industry:

of respondents say sophisticated attacks are a top challenge.

except an attack on critical infrastructure in the next 12 months.

The **frequency** of attacks has increased, with respondents reporting:

report at least one attack involving a loss of private information or an outage in the OT environment in the past 12 months.



report 10 or more such attacks within the past 12 months.

of cyberattacks on OT are not detected.

> *"Cyber threats present a greater risk to their OT than the IT environment."*

The **potency** of attacks has increased as well. When asked what made management of OT security challenging, the most frequent response was the rise of sophisticated attacks. Because many utilities manage infrastructure critical to daily life, nation-states and other malicious actors have an interest in developing cyber weapons that target utilities. Individuals and criminal organizations may now also have the backing of nation-states, or state-aligned proxy groups, interested in damaging physical assets, and may use potent cyber warfare tools originally developed by nation-states.

For example, the powerful WannaCry or NotPetya attacks, which affected 25% of all respondents in the past two years, are public examples of attacks that harness expertise developed by nation-state actors. Unlike ransomware attacks seeking financial information, these attacks systematically destroyed information and shutdown operations. Paying ransom often does not help restore operations.

As utilities transform their operations into digital enterprises, the surface for cyber attacks have expanded and will likely expand further into OT. The resulting risks to an organization's physical assets, financial liability, and reputation are high. Executives concerned about risk must pay attention to cybersecurity for OT. Utility leaders must recognize that attackers today design threats against utilities with increasing sophistication – both in terms of their destructive capabilities and their ability to identify weak points in security regimes;

The potential **consequence** and cascading effects of attacks have expanded, as illustrated by the impact of OT security events on business operations.

The Impact of OT Security Events On Business Operations

Figure 3. The impact of OT Security Events on Business Operations

The impact of these expanded risks is serious. Cyberattacks can cripple operations that depend on networked and real-time information, and respondents reported fear that outages, damage, injury, and environmental disaster could result from cascading effects on power systems. As the utility industry's technologies are increasingly connected to an IT network and a business model dependent on their continuous performance, the stakes for OT security increase. This is especially the case as operators must protect distributed power generation assets tens or hundreds of miles from a company's headquarters.

READINESS

Our survey shows that readiness across the industry is uneven due to multiple factors that range from:

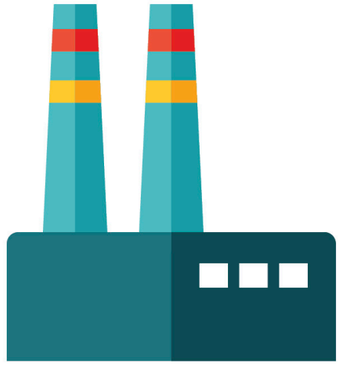
TECHNICAL CAPABILITIES TO IDENTIFY THREATS

INTERNAL ORGANIZATIONAL FAILURES

A CLEAR UNDERSTANDING OF RISK-BASED BEST PRACTICES

COMPLIANCE WITH REGULATORY REGIMES

Respondents gave mixed assessments of their own organizations' readiness to meet or respond to cyberattacks. Only 42% rated their cyber readiness as high, and only 31% were fully ready to respond to, or contain, a breach.



42% rated their cyber readiness as high

31% readiness to respond or contain a breach as high

Figure 4. Organizational Readiness to Withstand OT Attacks

This has caused many organizations to report **blind spots** related to OT:

LACK OF VISIBILITY INTO OPERATING ASSETS

LACK OF RESPONSE PLAN AND A SLOW RESPONSE TO PAST INCIDENTS

ZERO-DAY RISKS, OFTEN ASSOCIATED WITH GLOBAL MEGA ATTACKS OR INDUSTRIAL SAFETY EVENT

INCORRECT BELIEF THAT PROTECTIONS DESIGNED FOR IT ARE EFFECTIVE FOR OT

LACK OF INVESTMENT IN TRAINING AND PERSONNEL

HUMAN CAPITAL GAPS, INCLUDING DIFFICULTY PROCURING AND BUILDING INDUSTRIAL CYBER SKILLS

LACK OF ALIGNMENT BETWEEN OT AND IT SECURITY

Figure 5. Industry Blind Spots Contributing to Lack of Readiness

The complexity of addressing OT results from a convergence of factors – ranging from an inability to manage the external threat environment to immature internal compliance structures and organizational processes - internal to address the growing threat.

What Makes The Management Of OT Security Challenging

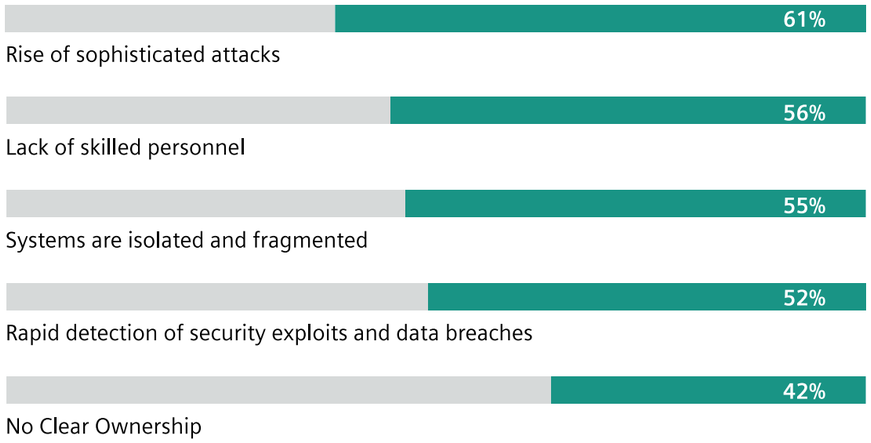


Figure 6. What Makes The Management of OT Security Challenging

As a whole, and despite improvement in developing regimes to address external and internal threats, the industry remains vulnerable to attack; companies are proving too slow to detect new threats; and are unprepared to recover from successful attacks on OT infrastructure.

Smaller organizations reported significantly greater concern in their ability to complete critical cybersecurity tasks, were less confident in their ability to understand the operational implications of an attacks, and act based on those alerts. Compared with larger organizations, utilities with less than five thousand employees reported consistently lower confidence in their ability to identify and contain threats, monitor infrastructure, and determine which resources were most important to protect.

> *"Smaller utilities reported consistently lower confidence in their ability to identify and contain threats."*

Many organizations reported using a compliance centered approach to manage cybersecurity risk. Organizations comply with regulations or develop an internal checklist to hold themselves to specified standards and practices. This approach has improved overall cyber hygiene across the industry. However, respondents acknowledge achieving compliance with regulations is not synonymous with achieving strong security posture. Organizations that rely on a compliance approach alone maybe responding to past incidents and may remain exposed to novel attacks.

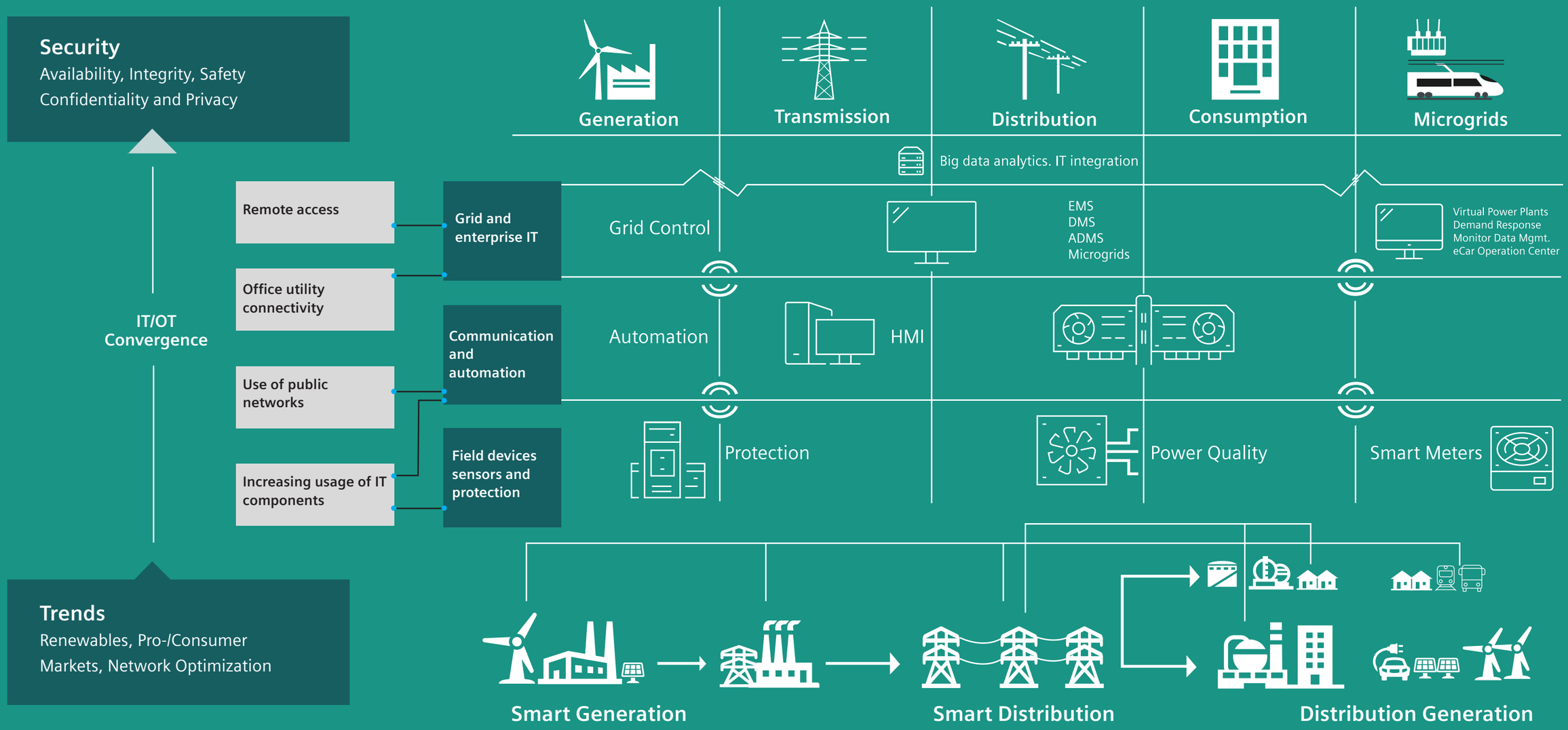
For large global operators, complying with a patch work of compliance regimes is burdensome and uneven. Practitioners from those companies report a common shift to risk-based methods that aspire to the highest security levels when measured against business priorities. Even where organizations develop their own standards, these are viewed as leveling-up security, not eliminating risk.

Looking beyond compliance,

organizations report using a risk-management approach to protect high value assets, prioritize investments, and act in a chaotic threat environment. This approach seeks to assess risks and address high-risk areas.

Yet, respondents noted that significant blind spots remain prevalent across the utility industry. Less than one third of survey respondents believed their OT and IT security approaches aligned, which suggests that utilities have a considerable capability gap that can be exploited. This disconnect is magnified by the internal organizational siloes that exist within companies, particularly between teams working with centralized power generation units, distributed and micro-grid systems, and transmission and distribution divisions. Irrespective of what governance or operating model is chosen, ownership and appropriate resourcing to address industrial cyber security is critical to ensuring a secure enterprise.

THE NEW SECURITY CHALLENGE



IN THE EVOLVING UTILITY VALUE CHAIN

The process of digitizing equipment – replacing or adding digital controls to analog equipment – helps utility managers increase their visibility into the operating status of assets in their fleet. Visibility also enhances cybersecurity capabilities by enabling operators to better understand the current status of connected assets. At its most basic level, it means knowing what is and is not connected in the OT environment, as well as how those assets behave to spot potential anomalies. Only by understanding what's happening in their production environment can operators build the confidence to take proportionate action.

However, respondents rated their organizations' ability to achieve comprehensive and continuous visibility of digital assets as low – with organizations in the United States and Europe reporting the lowest level of maturity among the other regions. This should concern leaders in all areas of the utility industry. It is difficult to provide meaningful security on a network when operators do not know what equipment exists within that network.

The Challenge of Continuous Visibility

Figure 7. The Challenge of Continuous Visibility

Exacerbating the visibility challenge for OT security is the common belief that OT systems benefit from isolation. Isolation-based solutions such as "air gaps" are common in IT, but have the additional effect of hampering visibility for OT systems. Respondents mentioned isolated and fragmented systems as the third most challenging aspect of cybersecurity, close behind the sophistication of attacks and the lack of skilled personnel. Air gaps should not be treated as a panacea for OT security, especially when considering the risk of insider threat.

> *"Insider threat represents the majority of attacks in OT."*

AI and big data analysis are used by a minority of organizations to monitor operations and recognize threats, like insider threat. Yet:

of respondents reported using big data or AI monitoring, with the practice most common in the United States (23%).

While a minority of utilities use big data and AI today, these tools can help organizations overcome sleeping malware and the detection of unknown threats. Using advanced analytics, security professionals can identify anomalies in their asset behavior. With visibility and context, an analyst can trace bi-directionally activity from the OT network to the IT network; identify gaps and unpatched systems that enabled an adversary to enter a plant; and establish control and lie dormant -- waiting to take over and force a shutdown.

> *"18% of respondents reported using big data or AI."*

Some threats by definition cannot be anticipated. Zero-day attacks exploit security vulnerabilities that are unknown until the attack occurs. Across the industry, respondents rated this risk as second only to insecure endpoints, showing widespread awareness that novel attacks can occur. When faced with a zero-day attack, utilities must respond rapidly to prevent, mitigate, or – where the attack is successful – recover from its impact.

Despite the risk that a novel attack will exploit unknown gaps in security:

of respondents say their organization has no response plan for cyber attacks. On average, responses to past malware attacks took 72 days after an outage.

The slow response times and lack of preparation indicate major opportunities to improve preparedness. Organizations should ensure that in the event of a successful breach of security, their teams will have some ability to coordinate responses and prioritize recovery efforts.

Smaller organizations took longer (88.5 days) than larger organizations (62.6 days).

Most concerning, respondents industrywide indicated a critical human capital gap. People with appropriate skills are scarce – in every region around the world, more than half of respondents indicated their organization's staffing level was not adequate to meet cybersecurity objectives in the OT environment.

In general, addressing cyber security requires expertise from control engineers, security specialists and network specialists, often working together. Where these skills are lacking, organizations may be unable to correctly evaluate solutions offered by contractors, leading to incomplete protections and missed opportunities.

Despite the human capital challenge identified in the survey, the industry overall is investing more resources into technology and compliance than into training or personnel. This investment pattern was even more pronounced for small organizations, where training was reported as less than 10% of available resources, and compliance took up more than 30% of resources.

> *"Compliance took up more than 30% of resources in smaller organizations."*

Compared to large organizations, small organizations were more likely to engage third parties to overcome the manpower shortage, particularly for monitoring and detection services.

SOLUTIONS

Recognizing that each organization has unique assets, personnel, and appetite for risk, we offer a few broad frameworks for building systems that continually improve security. Rather than prescribing one solution, the framework helps employees across a utility's enterprise evaluate and improve their cybersecurity systems.

STRONG CYBERSECURITY APPROACHES FOR OT WILL CONSIDER:

- Visibility into your systems. Know what you have. Know what it's doing.
- Skill set scarcity. Get the expertise you need. Train, hire or contract the right personnel.
- Complexity. Your systems interlock, and your solutions need to account for this.

ROBUST SYSTEMS FOR ONGOING SECURITY SHOULD BE BUILT TO:

- Keep up with developments in technology, business models, and attack modes.
- Detect when an attack or other anomaly occur.
- Respond when an incident is detected.

We believe that leaders across the industry should start by assigning ownership, checking for the blind spots identified in this report, getting visibility into their own systems, and prioritizing investment in industrial security.

Given the rising stakes and escalating threat environment, even leaders at well-prepared organizations need to consider how to maintain readiness at the threat frontier. Based on common themes among survey responses, we offer the following frameworks for thinking about how to improve cyber security for OT.

VISIBILITY

***Visibility* into systems**. To protect what you have, you need to know what you have. Visibility into the current status of your equipment and systems can help recognize attacks, mitigate damage and recover quickly. Respondents cited a lack of visibility as a major pain point in OT security work. Using analytics, AI, and connectivity can improve security for the industrial space as lower-cost solutions come onto the market.

SKILLS

***Skill* sets for OT security** are scarce, and ongoing learning must be part of any long-run security solution. Attackers will become more skilled, and defenders need to keep up. Organization needs to plan for this reality, whether that means training in-house expertise, hiring new employees, or anticipating contracting needs.

COMPLEXITY

Solutions need to account for the interconnected nature of OT systems. *Complexity* touches every aspect of cyber security. Solutions need to account for the interconnected nature of your systems. OT and IT security aren't identical, but should be aligned to work together. Executives may need to prioritize which assets or information is most important to protect.

To put another way, organizations need to have the capability to:

Keep up with changes in technology, business models, and attack modes. Utilities will face attacks that have never been seen before, and you need to be able to answer.

Detect when an attack or other anomaly occurs. Increasing use of digitization offers greater self-awareness of conditions in your systems. AI and big data monitoring are not yet widely adopted, but may help with this challenge in the near and medium-term future.

Respond when an incident is detected. At a minimum, organization should have a basic plan for responding to cyber attacks that succeed. Knowing in advance which assets to protect, and what priorities will be if an outage or other damage occurs can help teams restore service and minimize financial and reputational damage.

Building these capabilities requires support and planning within an organization. Good leadership can put technical experts in position for success and can help avoid institutional barriers that slow or block strong OT security practices. We recommend:

Clear ownership for OT security within organization. Assign a specific person responsibility for security and make their chain of command clear all the way to the C-suite. The rising stakes for security in the OT environment make good cyber hygiene a pressing issue for any organization in the utility sector.

Develop a strategy to get the visibility, skill set and security improvements around organization's needs. Back that strategy with budget and resources, so that it can be implemented. Include a plan for responding to successful, unanticipated attacks, to help reduce risk from future zero-day attacks.

Iteratively implement your cyber security strategy. Cyber security cannot be solved immediately or permanently, but leaders and experts together can prioritize risks. Securing critical resources can reduce risk rapidly. Plan with an expectation that security needs will change over time. Utilities will need to adjust defenses as new attacks develop, and as business needs change.

CONCLUSION

Cybersecurity for the OT environment sits in the crossfire of an ongoing arms race. Attackers and defenders will continue to innovate, and the systems used by utilities under normal operation will continue to advance. A sophisticated business that uses digital technologies to operate more efficiently than competitors needs to protect those technologies from attacks. Leaders within the utility industry need to allocate attention and resources to their cyber defenses commensurate with the increased risk to their businesses.

As this survey shows, readiness varies widely across organizations, and numerous blind spots affect even well-prepared organizations. It is our hope that this report helps leaders recognize these blind spots within their own organizations and provides some guidance for next steps.

While cyber security needs are complex and constantly developing, we believe that organizations that plan for ongoing learning and iterative improvements can reduce their risk significantly. This is a major but manageable challenge.

REPORT METHODOLOGY

This report is a collaboration between Siemens and the Ponemon Institute. It focuses on cyber risk in OT environments at electric utilities with gas, solar, wind assets, and water utilities, throughout North America, Europe, Middle East, the Asia-Pacific, and Latin America. The research was conducted to gain a clearer picture of utilities' existing capabilities, levels of preparedness, vulnerabilities, and strategic understanding of their OT cyber risk.

In total,

1,726

utility professionals responded to a series of questions related to cybersecurity, providing self-assessments on key areas of their company's technical and corporate readiness to address the increasing threat of cyber attacks. All respondents indicated their job involved securing or overseeing cyber risks in the OT environment. They described their roles as :