GRID MODERNIZATION:

Key Opportunity to Strengthen Utility Cybersecurity

UTILITY DIVE | SENSUS a xylem brand

Introduction

Cybersecurity currently tops the list of electric utility executives' pressing concerns, with grid modernization following closely behind as a priority. With appropriate planning and collaboration across the enterprise – and across the industry – these two imperatives can dovetail in a way that supports long-term, robust cybersecurity plus a more resilient, reliable and flexible power system.

A new Sensus survey, conducted in partnership with Utility Dive Brand Studio, indicates that grid modernization presents a uniquely valuable opportunity to deploy strong, flexible, long-term cybersecurity. Grid modernization projects entail capital investments in advanced metering infrastructure (AMI), switchgear, sensors, communications networks, automation and other critical hardware and software that must last for many years. When utilities require that new assets include strong, built-in security features, this forms a powerful basis for grid cybersecurity. Furthermore, since many of these assets are expected to function for years or decades, this approach enhances cybersecurity for the long term – always the most cost-effective option.

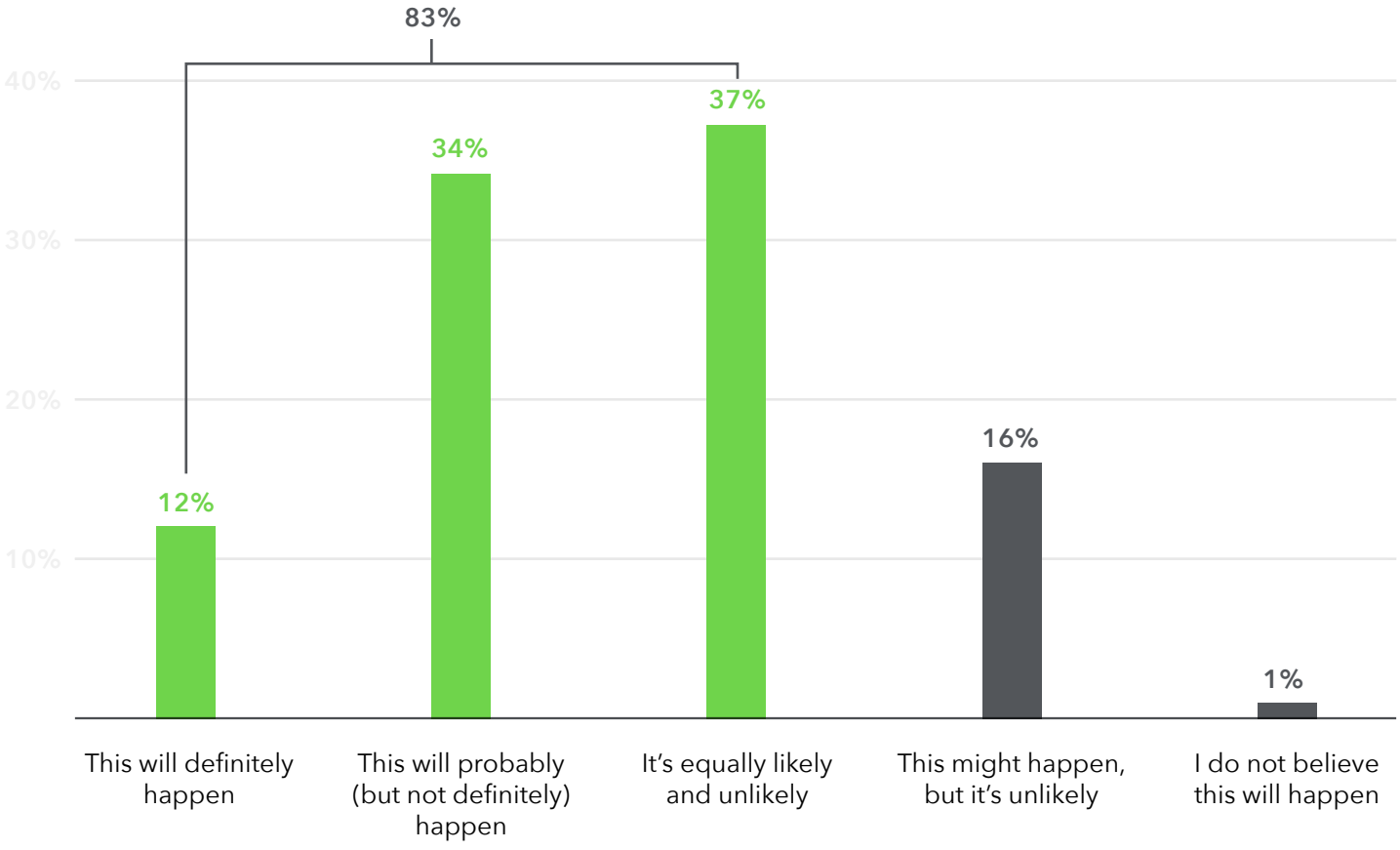
A cybersecurity guide published by the Northwest Public Power Association explains this strategic difference: "Thinking about cybersecurity from the initial stages of the procurement process assures that the business has security baked in and not bolted on. Cybersecurity protections should be implemented through all phases of the product life cycle and the broader business cycle, thus improving reliability and reducing risks."

"Baked in" cybersecurity also can attract regulatory support. Regulators are keenly focused on grid resilience and reliability, and cybersecurity has become a key consideration in support of these goals. Consequently, showing that proposed rate-based asset investments are as secure as possible (and also that they are backed up by enterprise-wide cybersecurity strategy, tools and processes) could bolster rate cases to fund grid modernization.

The urgency to make power grids more secure and resilient has never been higher. Over 80% of survey participants believe that there is at least a 50/50 chance that electricity supply in North America will be interrupted by a cyberattack sometime in the next five years. More than one in ten are certain that this will happen.

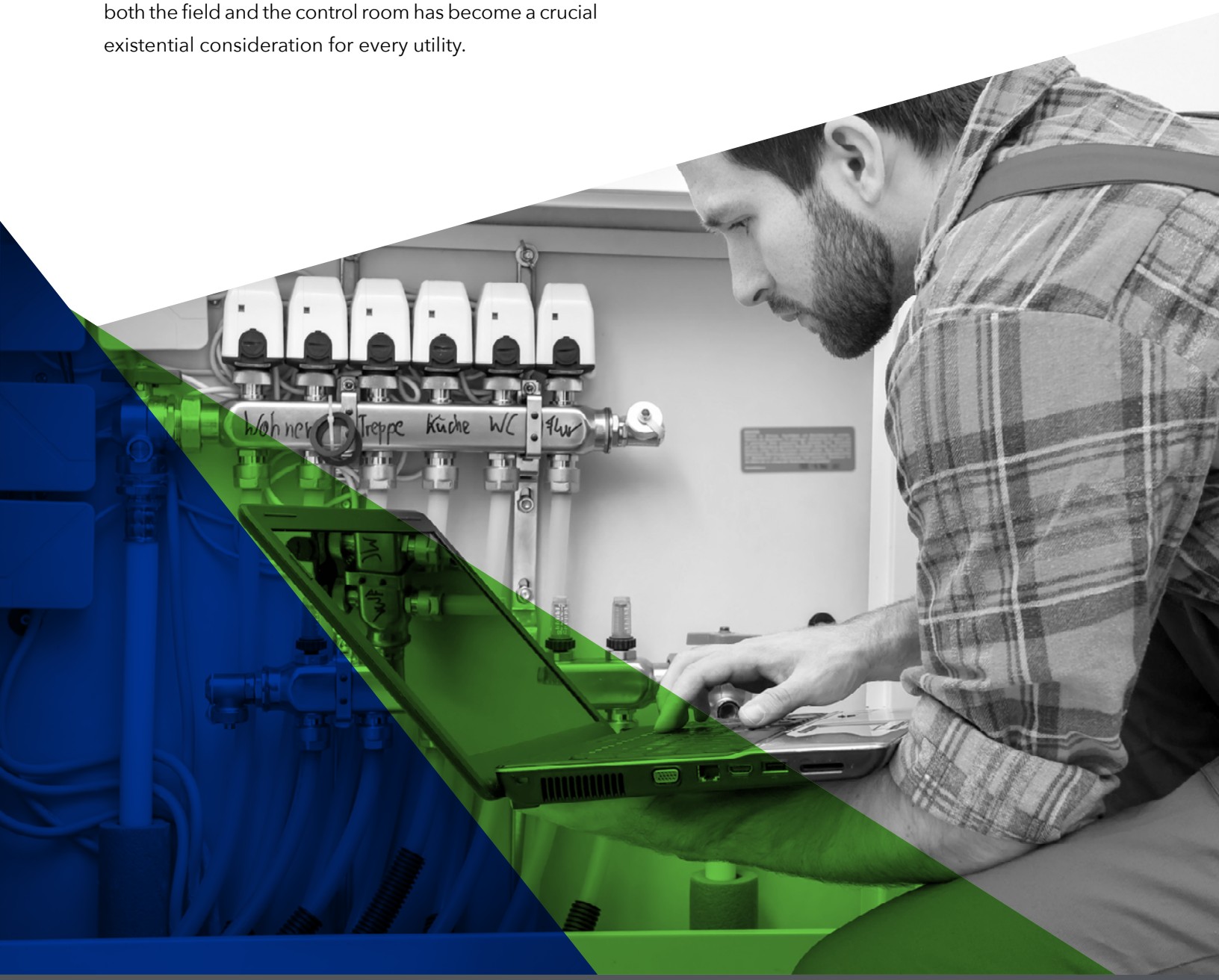
The urgency to make power grids more secure and resilient has never been higher.

WITHIN THE NEXT FIVE YEARS, DO YOU BELIEVE THAT NORTH AMERICA WILL EXPERIENCE AN INTERRUPTION OF ELECTRICITY SUPPLY TRIGGERED BY A CYBERATTACK?



Such concern echoes recent warnings from the Department of Homeland Security (DHS) about Russian cyber infiltrations of U.S. utility control rooms, which were first detected in 2016. While news coverage may have exaggerated the outage/sabotage risks posed by these specific intrusions, these incidents do show that foreign powers and criminals are attempting to lay the groundwork for future cyberattacks against North American utilities. Consequently, deploying stronger protection today in both the field and the control room has become a crucial existential consideration for every utility.

Grid modernization intrinsically poses some additional cybersecurity risks. Notably, these projects increase the digitalization of grid operations – including greater data exchange and often interoperation with third party devices and systems. This vastly expands a utility's "attack surface" (the number of points and routes by which a cyber intrusion can occur).



Key Insights

- **Grid modernization: Key to the cybersecurity long game.** Grid modernization projects are remaking utility asset portfolios, as well as practices for procurement and operations, in fundamental ways. Decisions made in the earliest stages of these projects can influence the overall level and cost of utility cybersecurity for decades.

- **Timing challenges and opportunities.** It's not easy to balance the pace of grid modernization efforts (typically more than three years for completion) with cyberthreats that evolve on a daily basis. However, the slower pace of grid modernization does allow for greater and more thorough consideration of cybersecurity up front.

- **Sharing threat information yields solutions.** The utility industry has a strong history of mutual aid in the face of emergencies, and this has extended to cyberthreats. Government, industry organizations and vendors are all playing vital roles in helping utilities keep abreast of current events, issues and opportunities. Strong cybersecurity depends not just on locking systems down, but also on keeping the lines of communication open.

- **Procurement and risk management: Overlooked opportunities.** When asked which roles/departments hold chief responsibility for utility cybersecurity, these two options were among the least frequently mentioned. Yet, they can offer surprisingly powerful support in key strategic choices to implement cybersecurity in grid modernization.

- **Cybersecurity is about people and business, not just technology.** Consistent attention and support from senior leadership, as well as awareness and training at all levels and in every department, are essential for utility cybersecurity success. Also, a cybersecurity-aware organizational culture has functional and competitive advantages.

Demographics

The Sensus/Utility Dive Brand Studio survey on cybersecurity and grid modernization was conducted in June 2018. It drew responses from 239 participants, over 40% of whom are employed by electric utilities. Also, heavily represented were utility consultants, government agencies, and nonprofits involved with utility issues.

Investor-owned utilities were most heavily represented among the utility participants, but there were also many other types of utilities – including some independent power producers and utility subsidiaries.

This survey represents a broad range of organization sizes and job levels. Over 40% of participants work for organizations with more than 1000 employees.

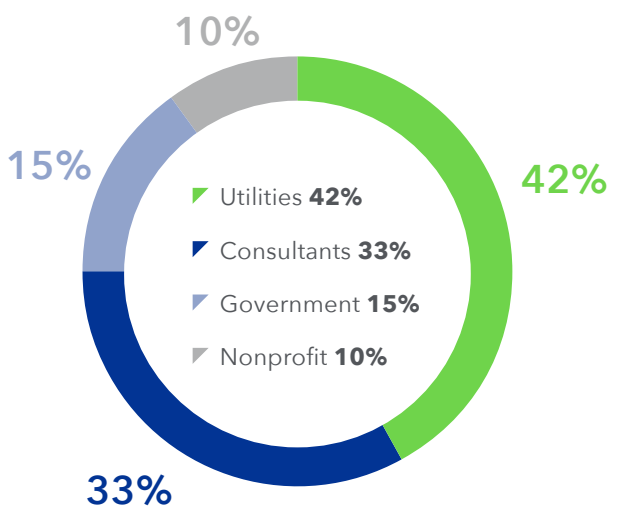
Also, of the 204 participants who work for organizations with more than 10 employees, one-third are in upper management or senior leadership.

Survey participants also listed their top three areas of responsibility. Across all participants, nearly 40% noted that business strategy and new business development is a key aspect of their job. About one in four serve in organizational leadership, policy or governance roles.

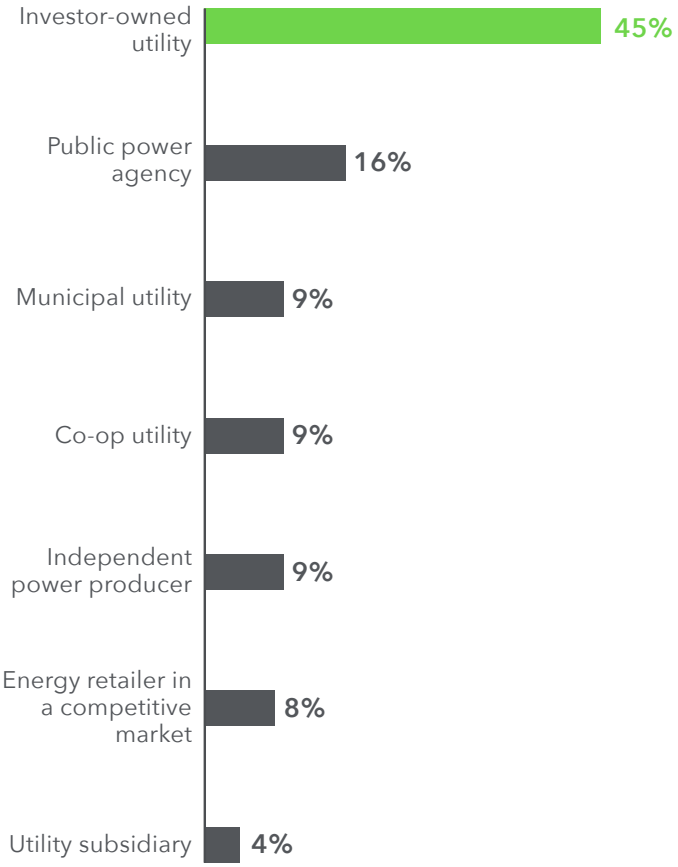
Utility participants noted the same top two areas of responsibility, along with a wide range of utility roles.

In addition to the top 10 areas of responsibility cited by utility participants, we also heard from utility professionals who work in security, information technology, customer programs, and several other capacities.

ORGANIZATION TYPE



BREAKDOWN OF UTILITY TYPE



Among our utility participants, these were the five most commonly mentioned types of grid modernization projects:

1. AMI/smart metering
2. Renewables integration
3. Advanced distribution management (ADMS), grid sensors, controls
4. Security, cyber and physical
5. Storage

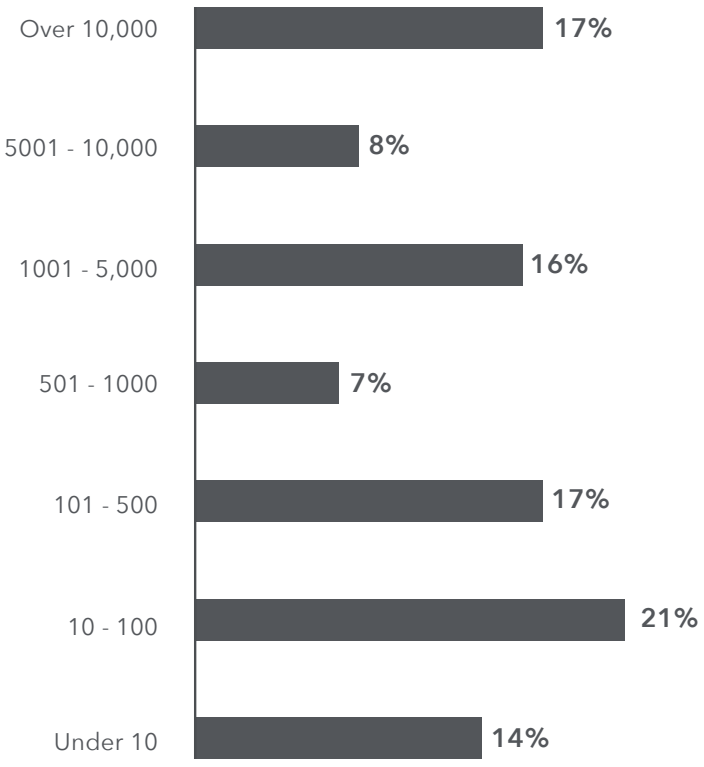
A few survey questions invited participants to share their personal insights and experiences on the intersection of cybersecurity and grid modernization. For example, one senior executive from a co-op utility shared that, "One of the first things we check now, in any project, is how secure the data is – especially for AMI."

Similarly, a senior executive from an investor-owned utility noted that cybersecurity concerns "have gotten us thinking about how/when to embrace blockchain technology."

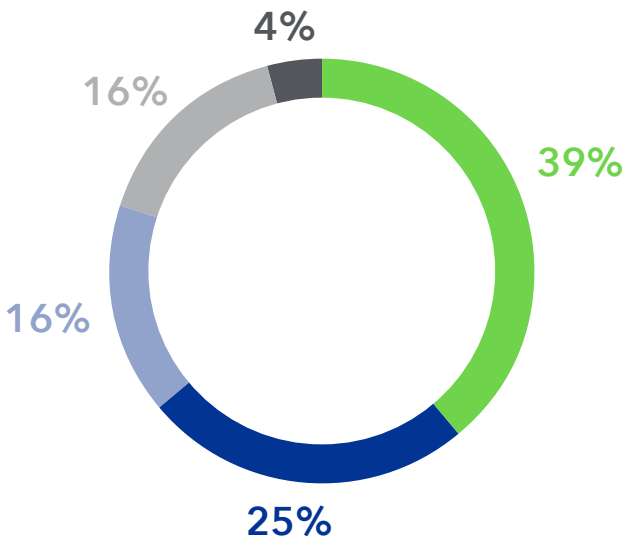
And a mid-level manager for a small municipal utility said that because of cybersecurity concerns, "We now exercise far more scrutiny in reviewing vendor proposals."

How ready are most utilities, today, to handle cyberattacks? We asked participants to rate, on a five-point scale, their utility's current level of cyber preparedness. Nearly half of utility participants believe that their organization is already mostly or fully prepared. Many believe they've made moderate progress so far. Only 12% believe their utility is currently underprepared.

ORGANIZATION SIZE BY NUMBER OF EMPLOYEES

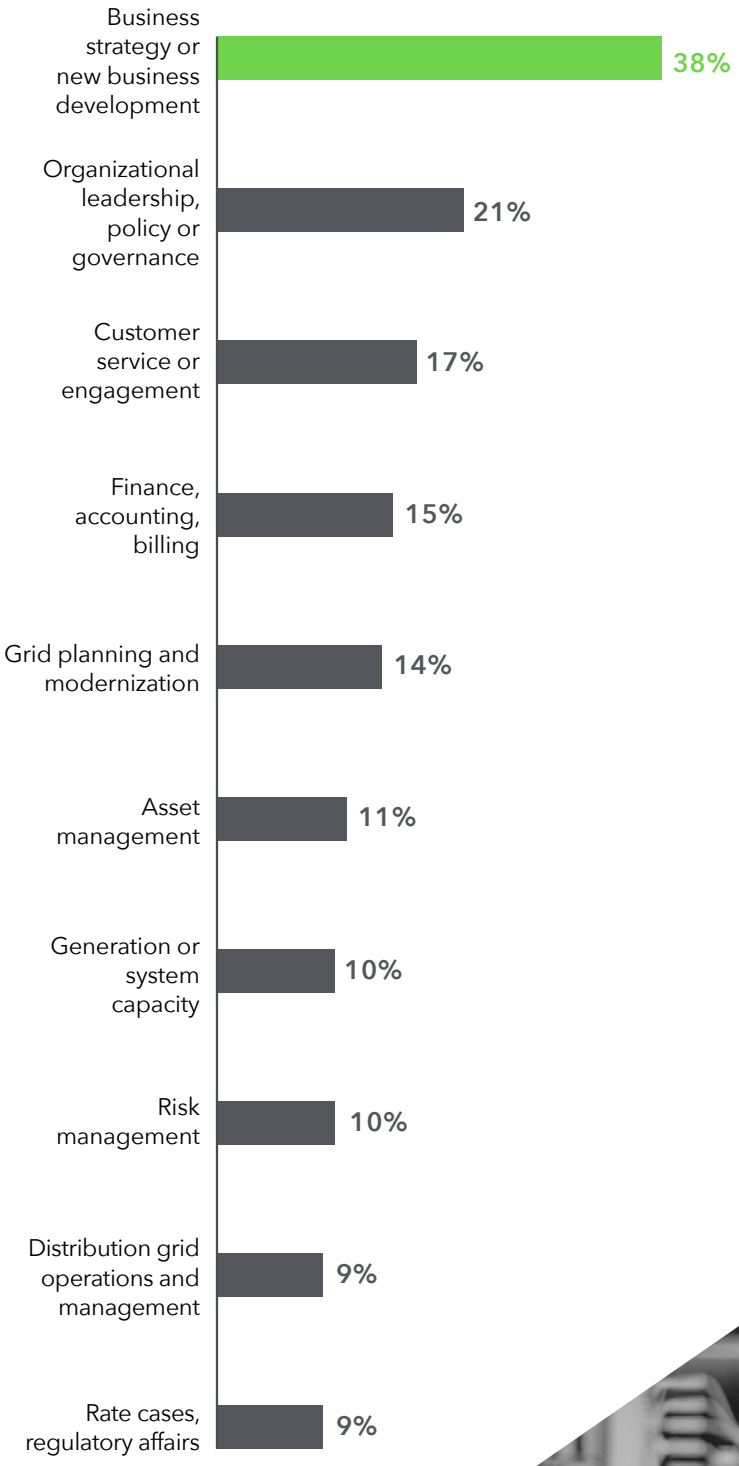


JOB LEVEL AMONG ORGANIZATIONS WITH MORE THAN 10 EMPLOYEES

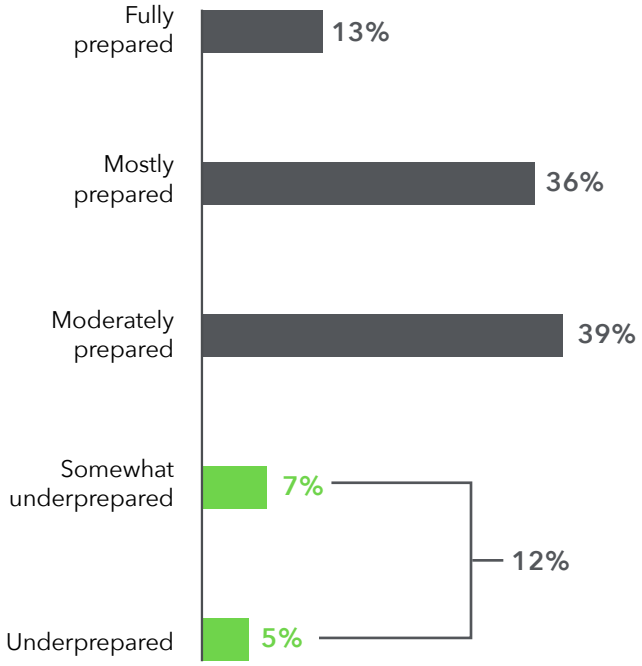


- Non-management employee **39%**
- Middle manager or team leader **25%**
- Department head or senior manager **16%**
- Senior leadership **16%**
- Independent contractor **4%**

TOP 10 AREAS OF JOB RESPONSIBILITY, UTILITIES ONLY



HOW WELL PREPARED IS YOUR UTILITY TO DETER OR RECOVER FROM CYBERATTACKS?



What Helps Utility Cybersecurity Succeed

Over the past two years, cyber and physical security has been the number one concern across the electric utility industry. Among the nearly 700 utility professionals who participated in the 2018 Utility Dive State of the Electric Utility Survey, concern about cybersecurity surpassed (by a considerable margin) concerns about distributed energy resources (DER) policy, bulk power reliability, renewables integration, aging infrastructure/grid modernization, and staffing.

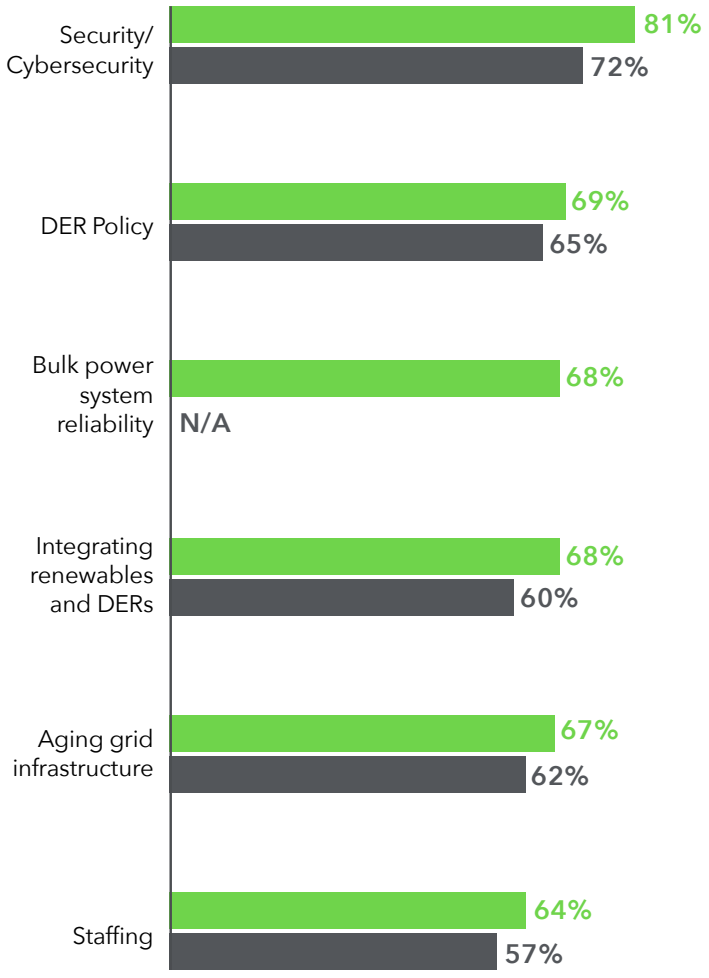
There is an ongoing, high-level conversation about cybersecurity across the industry. "CEOs are laser-focused on security of critical infrastructure," said Scott Aaronsen, vice president for Security and Preparedness at the Edison Electric Institute (EEI). "They realize the existential risk to their companies, and their responsibility as national critical infrastructure. Cybersecurity is a top priority, especially in deployment of new utility technology."

> **"Cybersecurity is a top priority, especially in deployment of new utility technology."**
>
> **Scott Aaronsen,** vice president for Security and Preparedness at the Edison Electric Institute (EEI)

WHAT ARE THE TOP POWER SECTOR CONCERNS, ACCORDING TO IMMEDIATE IMPORTANCE TO UTILITIES?

2018 2017

(Percentage of respondents who indicated each option is "important" or "very important" today)



Source: Utility Dive State of the Electric Utility Survey, 2018

People, Not Just Technology

Cybersecurity tends to be most effective when every utility employee is trained and encouraged to consider security in every aspect of their job – from how they handle email, to how they integrate DERs on the grid, to how they design demand response programs or corporate strategy.

"Social engineering" remains an effective and popular entry strategy for cyberattacks. "Phishing" emails and phone calls still often trick employees into providing access to sensitive systems or data, and "whaling" (when top executives' email or other credentials are stolen and then used to perpetrate theft) is increasingly common across all industries.

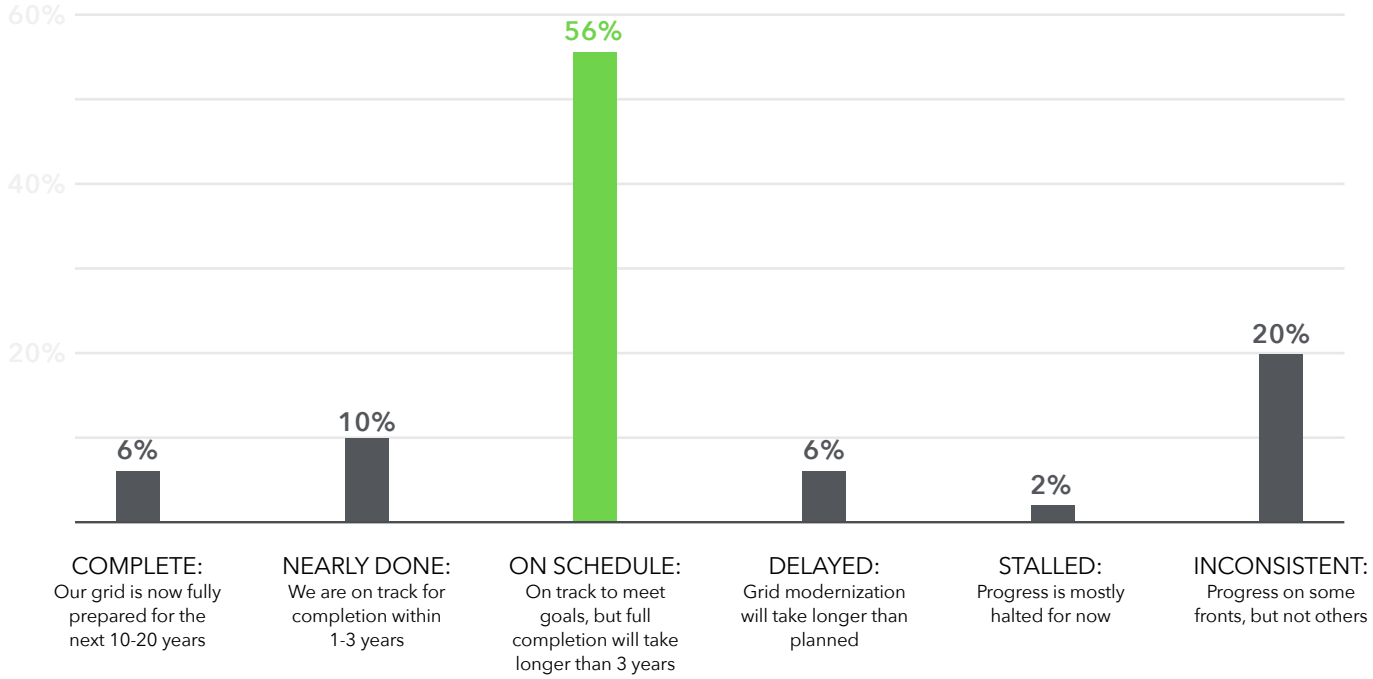
Balu Ambady, Director of Global Security Technologies for Sensus, observed, "There should be general awareness of cybersecurity across the utility. Due to the number of and diversity of attack attempts, senior executives especially need to be aware, educated and proactive."

Aligning the Goals of Grid Modernization and Cybersecurity

Over half of utility participants said that their grid modernization plans will require more than three years to complete. That might sound like an eternity in cybersecurity terms, but it's actually an opportunity to reconcile the pace of IT and security with more traditional utility operations. In particular, there's often ample time on the front end of grid modernization planning to consider cybersecurity thoroughly in product selection and system redesign.

Designing sound, ongoing cybersecurity processes for a modernized grid is as important as defining product requirements.

CURRENT PROGRESS ON GRID MODERNIZATION



"As you deploy new assets, you'll want to prepare them for quick changes," Ambady explained. "Right from the outset, establish a monthly regimen for downloading, testing and installing patches – so by the end of the month, they're all up to date. Developing this process may take a few months. But then, every month you can handle it quickly and make fast changes in response to new threats and anomalies."

The process of aligning the goals of cybersecurity and grid modernization is not always smooth, but it does generally yield important solutions. Survey participants listed several ways that cybersecurity is directly impacting operations and grid modernization at their utility, for better or worse.

For instance, an engineer with a large utility consultancy said, "On the implementation end of AMI, we had to address a lot of customer concerns surrounding security and privacy."

A senior manager for an energy retailer said, "We have hardened our systems and have full fallback positions."

> **"As you deploy new assets, you'll want to prepare them for quick changes."**
>
> **Balu Ambady,** Director of Global Security Technologies, Sensus

And one manager from a large investor-owned utility gave a very specific example of how cybersecurity has influenced key grid modernization choices: "We are investing in a field area network (FAN) that we will own, largely to bring our data in-house for security reasons."

Aaronsen emphasized that resilience, rather than complete deterrence, should be the goal of any utility cybersecurity strategy. "If you try to protect everything from everything all the time, you will fail," he said. "It's a worthwhile aspirational mission, but the practicality is: when cybersecurity fails, what do I do? How do I prepare to respond and recover? How do I work around my vulnerability?"

Opportunities and Pitfalls Where Cybersecurity Meets Grid Modernization

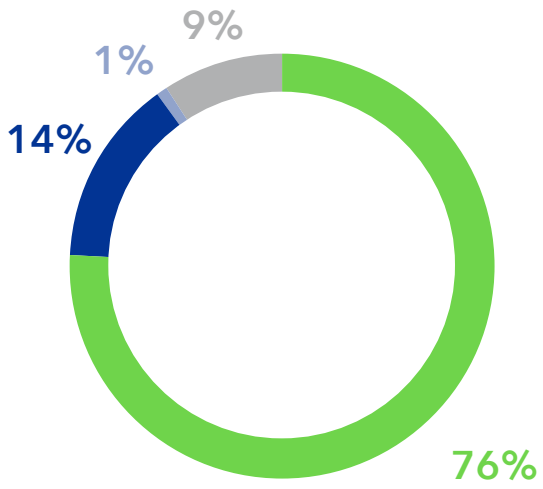
Cybersecurity is already a top priority in grid modernization efforts: 76% of utility participants rated it as very important.

However, it's one thing to say that cybersecurity is important, and another to demonstrate that importance through action. To delve deeper into this concept, we asked utility participants which issues, assets and processes are their highest cybersecurity priorities during grid modernization.

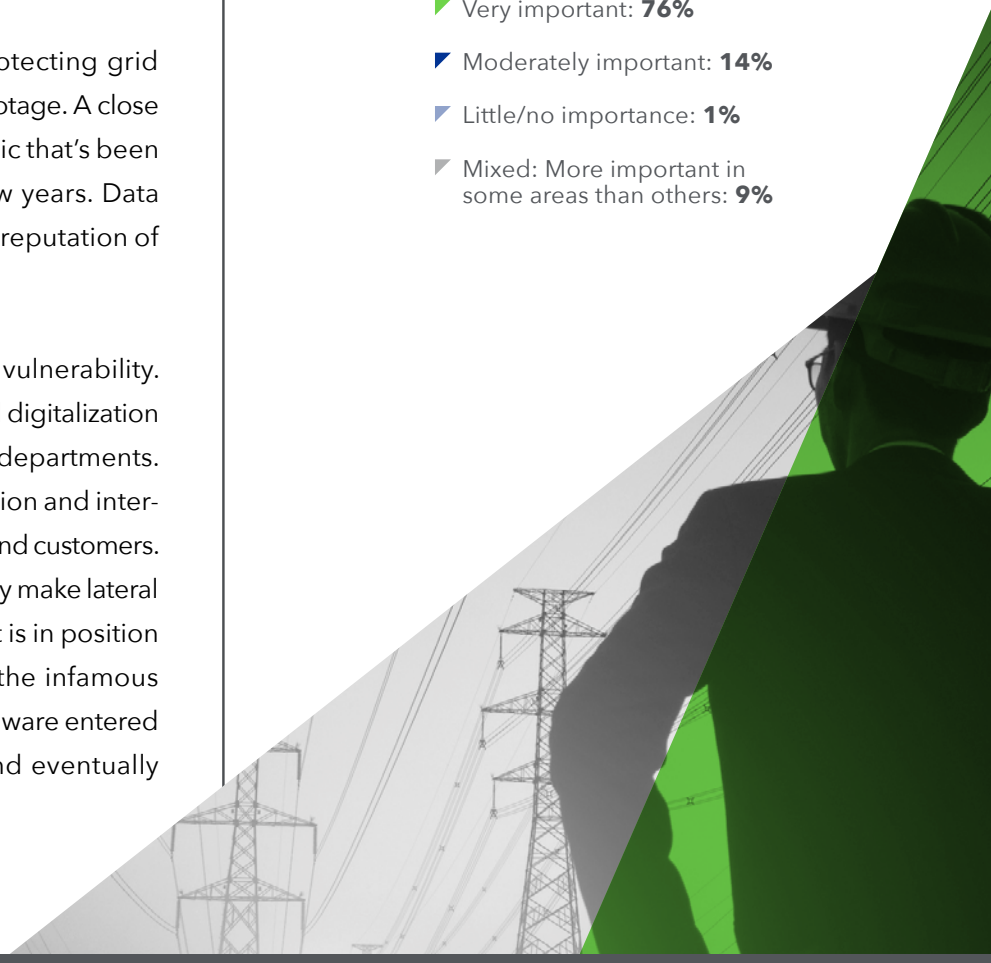
Not surprisingly, the top priority was protecting grid operations and preventing outages or sabotage. A close second was customer data privacy – a topic that's been grabbing many headlines for the last few years. Data breaches have significantly tarnished the reputation of major companies in many industries.

Attack surface is a key consideration for vulnerability. Grid modernization entails vastly increased digitalization of utility systems, and integration across departments. It also increases the amount of interoperation and interaction with third parties, including vendors and customers. This can make it easier for malware to quietly make lateral moves from one system to the next, until it is in position to steal data or do damage. That's how the infamous Target data breach of 2013 happened: malware entered via an HVAC vendor system interface and eventually migrated to point-of-sale systems.

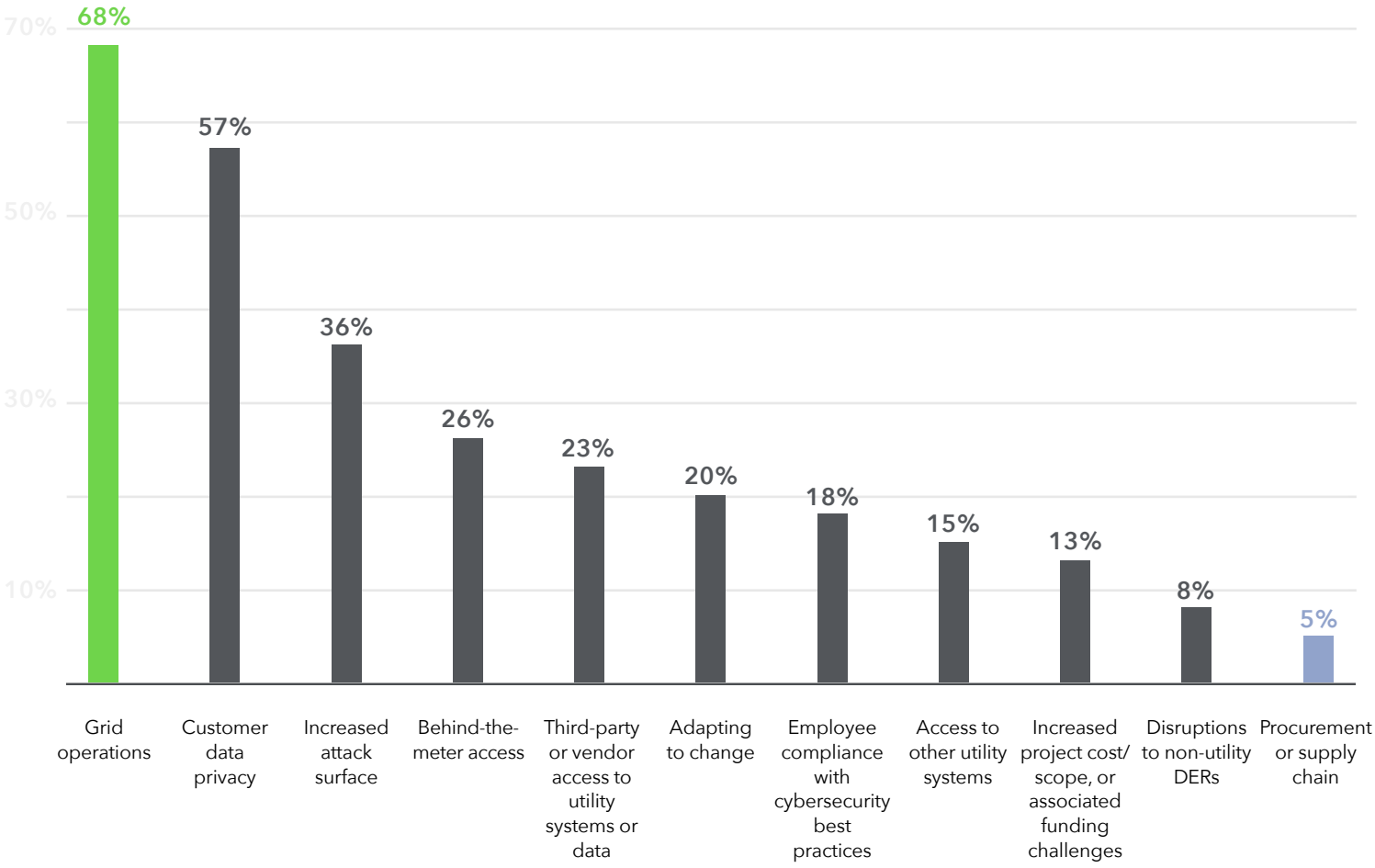
HOW IMPORTANT IS CYBERSECURITY TO YOUR UTILITY'S GRID MODERNIZATION EFFORTS?



- Very important: **76%**
- Moderately important: **14%**
- Little/no importance: **1%**
- Mixed: More important in some areas than others: **9%**



WHAT ARE YOUR UTILITY'S TOP THREE CYBERSECURITY PRIORITIES RELATED TO GRID MODERNIZATION?



The type of communication network deployed for grid intelligence can have a significant impact on resilience. "Communication network redundancy and resiliency are vital to maintaining security," said Ambady. "Moreover, a private, proprietary network is significantly more difficult to hack. You can't just buy materials at Best Buy to get into the system, like with mesh networks."

Mesh networks are often deployed for significant parts of grid communications, but this popular choice can make the grid more vulnerable. Ambady recommends that utilities consider deploying a private, point-to-multipoint network, which is more secure. That's because, in a mesh network, communication from devices at the grid edge must "hop" through multiple devices to get to signal collectors, which then communicate to the system head-end. Many field devices that communicate directly with each other provides more opportunities to hack into the network. Furthermore, if a cyberintruder accesses one meter in a mesh system, that can yield access to additional meters.

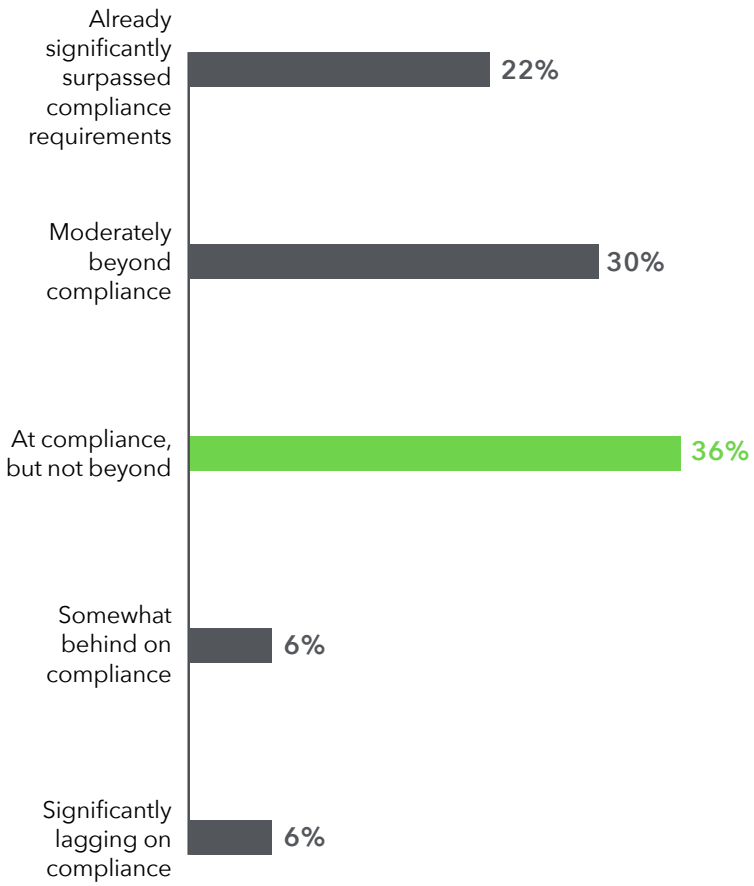
The Value (and Misuse) of Standards

Mandated standards – such as the North American Electric Reliability Council's Critical Infrastructure Protection standard (NERC CIP), as well as state or local mandates, and guidance such as the Cybersecurity Framework from the National Institute of Standards and Technology (NIST) – can play a useful role in limiting the ability of malware to migrate across a utility. Over half of utility survey participants reported that their organizations have already exceeded compliance with current standards.

Standards should only constitute a minimum baseline for cybersecurity, never a goal. Yet, more than one-third of utility participants said that their organizations are currently at, but not beyond, compliance. An additional 12% are lagging on compliance to some extent. Thus, a large number of utilities might be more vulnerable to cyberattack than they think.

Some cybersecurity standards define minimum product requirements, making them especially useful for procurement and supply chain decisions. But interestingly, very few utility participants (only 5%) listed procurement or supply chain as one of their organization's top priorities in grid modernization. This could represent a significant missed opportunity, as well as increased risk.

IS YOUR UTILITY IN COMPLIANCE WITH CURRENT CYBERSECURITY STANDARDS AND PROTOCOLS, SUCH AS NERC CIP?



Very few utility participants (only 5%) listed procurement or supply chain as one of their organization's top priorities in grid modernization. This could represent a significant missed opportunity, as well as increased risk.

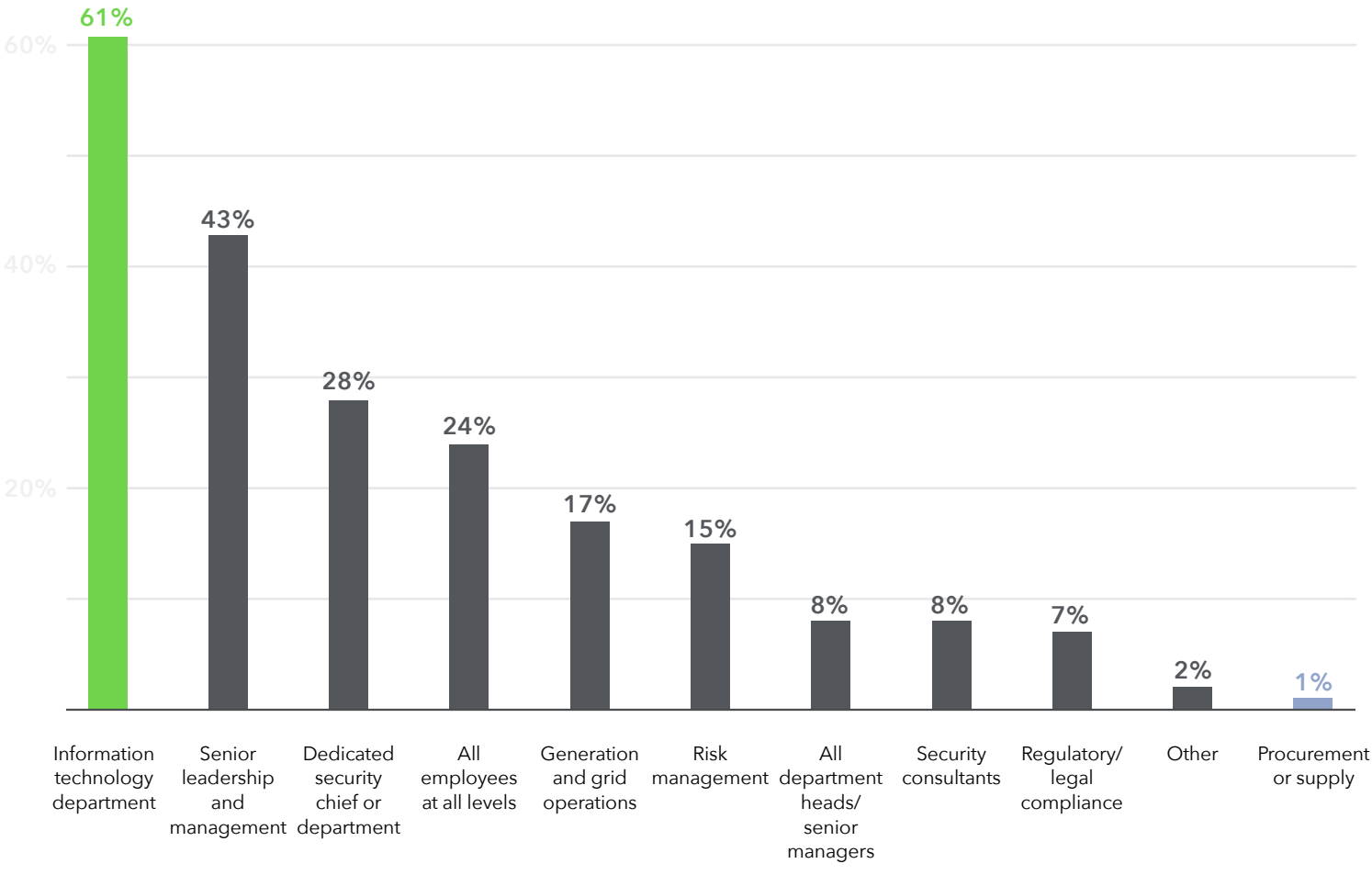
Who's Responsible for Utility Cybersecurity?

One factor that could be contributing to this commonly missed opportunity is how most utilities allocate responsibility for cybersecurity. We asked which utility departments or roles are primarily charged with responsibility for cybersecurity. Nearly two-thirds of utility participants said that their information technology (IT) department bears much of the responsibility for cybersecurity. And less than one-third reported that they have dedicated cybersecurity staff.

This could present a problem. IT departments typically have limited input in a utility's selection of assets, such as AMI systems or switchgear – or in plans for demand response programs, non-wires alternatives for building grid capacity, EV charging or DER integration. This approach can lead to cybersecurity that is "bolted on," rather than "baked in" – which tends to be less effective and more costly.

It is good news that senior leadership is the second most common nexus of cybersecurity responsibility at utilities (noted by 43% of utility participants). Direct leadership attention is essential to ensure that cybersecurity is known, and treated, as a top priority across the enterprise. At many utilities, the C Suite and board have come to view cybersecurity as a competitive advantage – as well as an existential imperative.

WHICH THREE ROLES OR DEPARTMENTS HOLD THE GREATEST DIRECT RESPONSIBILITY FOR CYBERSECURITY AT YOUR UTILITY?



That said, senior leaders are (like IT staff) typically not involved in the details of product selection, operations or programs. For these choices, it probably makes sense for procurement/supply chain, as well as all department heads, to assume a significant level of responsibility for cybersecurity. However, a mere 1% of utility participants indicated that procurement/supply chain currently holds this responsibility – and only 8% said that department heads or senior managers play this role. This probably represents a significant missed opportunity to enhance utility cybersecurity for the long term.

Risk management professionals are another potentially overlooked resource. Just 15% of utility participants noted that their risk managers hold significant responsibility for cybersecurity. Risk managers often play a key up-front role in steering all kinds of utility strategies, operations and programs. Since they are trained to quantify risk, they are in a unique position to communicate about cybersecurity in terms that are understandable, and vital, to every department and role.

At many utilities, the C Suite and board have come to view cybersecurity as a competitive advantage – as well as an existential imperative.

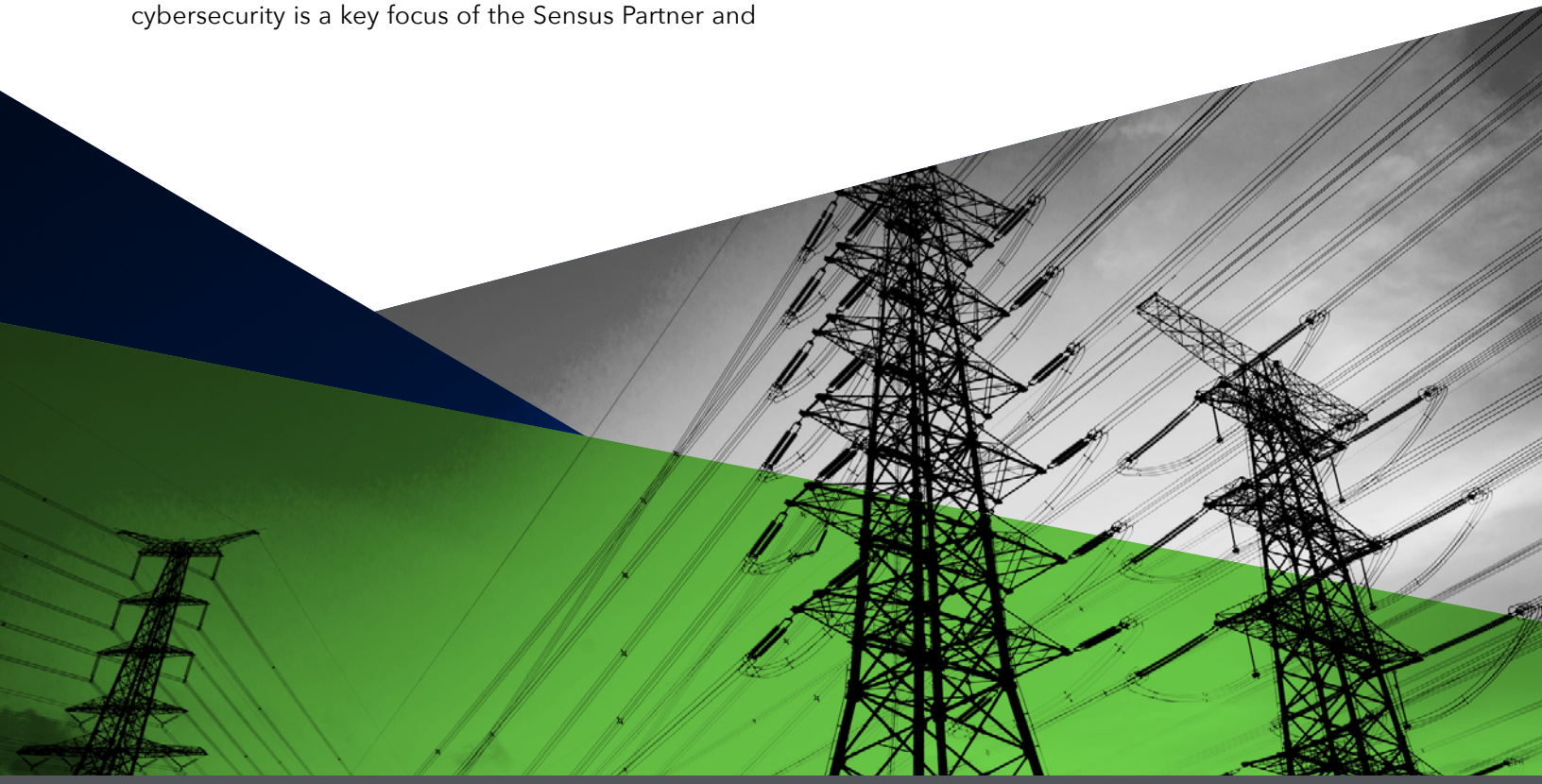
The Path Forward

There are many steps that utilities can take, and that some are already taking, to bolster cybersecurity during grid modernization efforts. Here are 10 items that should be on every utility's "to do" list.

1. Assess the vulnerability of existing grid assets and operations. The National Cybersecurity Center of Excellence (NCCoE) offers excellent guidance on three crucial areas for the energy sector: asset management, identity and access management and situational awareness.

2. Share information about threats and anomalies. The Electricity Subsector Coordinating Council (ESCC) and NCCoE communities of interest provide excellent opportunities to share cybersecurity experience, expertise and questions across the utility industry. Additionally, some vendors' user forums are engaging utilities to improve the cybersecurity of products. For instance, cybersecurity is a key focus of the Sensus Partner and Advisor Network (SPAN). Larry Cody, Senior Information Security Engineer at Southern Company (and chairs the SPAN security subcommittee) explained that this collaboration opportunity is open to all utilities that use Sensus software and equipment. "It's an excellent tool for learning what your industry peers are doing, what threats they're seeing, and how they are combatting those threats."

3. Proactively work with manufacturers to build in features that will be essential if infrastructure gets exploited. For instance, Aaronsen recently brought a group of utility CISOs to visit a major manufacturer of critical infrastructure assets. The manufacturer was touting how they would digitize everything: "We will be the industrial internet." The CISOs liked that, but they also asked whether they'd still have the ability to operate manually. According to Aaronsen, the manufacturer replied, "Oh, you want that? Sure, we can do that."



4. Educate regulators about the long-term benefit grid modernization can have on cybersecurity. In our survey, one regulator noted: "Due to our lack of technical expertise in this area, it's exceedingly difficult to know if utility investments or strategies are the most prudent selections for customers."

5. Cybersecurity teams should spend time in every department. Every utility should have a designated head of cybersecurity, and this person should coordinate with department heads and top managers in every other utility department – as well as with the C Suite. The first part of this engagement should involve a lot of listening and watching. Cybersecurity staff should go out to departments (including field operations) to learn the daily tasks, concerns, goals and priorities for each department. Taking this information into account while developing cybersecurity strategies and measures will result in more enthusiastic support and compliance across the organization.

6. Segment networks to prevent lateral malware migration, especially AMI networks. Cody observed, "If you only put firewalls around the perimeter of a network, you're assuming that everything inside that wall is safe. Not so. Assume malware might be lurking anywhere on your system, at any time. Segmentation can help you detect it and keep it from spreading."

7. Redundant security controls. "Don't depend solely on one type of security control," said Cody. He recommends multiple overlapping methods, such as zoning plus virtual private networks and firewalls.

8. Secure communication networks. Work with carriers to secure communication networks used for AMI, sensors and grid intelligence – as well as between field personnel and control room staff. Having redundant communication networks can help, in case one method is compromised. According to Cody: "Carriers often have VPNs, private clouds and other things to help you ensure that your communications and devices are talking to devices and people that you know, and that you want them to be talking to."

9. Hire data professionals to actively review and analyze logs. Utilities are collecting mountains of data with potential cybersecurity relevance, but often this is not fully (or even adequately) analyzed. Most utilities need to increase the number of data scientists and analysts on their staff, to both understand what "normal" is (and how it's changing), and to spot and investigate anomalies faster. The challenge is that data professionals are in high demand across all industries. Utility human resources departments will need to provide attractive positions for data professionals with clear career paths, as well as data science "upskilling" opportunities for existing utility staff.

10. Don't neglect the basics. Done consistently, basic cyber hygiene practices (such as keeping systems patched, and knowing how to handle email) are the most powerful and valuable part of any cybersecurity strategy. Train all utility staff, in every department, in routine cybersecurity practices – and test them (or perhaps offer recognition or rewards) for good performance. Also, cybersecurity should always be a key initial consideration when evaluating any new piece of hardware or software, or when planning a new integration between internal or external systems.

Conclusion

When grid modernization is managed with cybersecurity at its forefront, a utility's overall ability to be flexible and responsive greatly improves – in grid operations, energy resources and business models. This helps utilities address not just threats and emergencies but also industry disruption.

Cybersecurity is not a burden for utilities to manage, but an opportunity on which to capitalize.

Thus, cybersecurity is not a burden for utilities to manage, but an opportunity on which to capitalize. Many utilities already view grid modernization projects from the perspective of business diversity and competitive advantage, so applying this lens to cybersecurity could help utilities more easily achieve both goals.

sensus

a xylem brand

Sensus, a Xylem brand, helps public service providers, including utilities, cities, industrial complexes and campuses, do more with their infrastructure to improve quality of life in their communities. We enable our customers to reach farther by responding to evolving business needs with innovation in sensing and communications technologies, data analytics and services. Learn more at www.sensus.com.

LEARN MORE