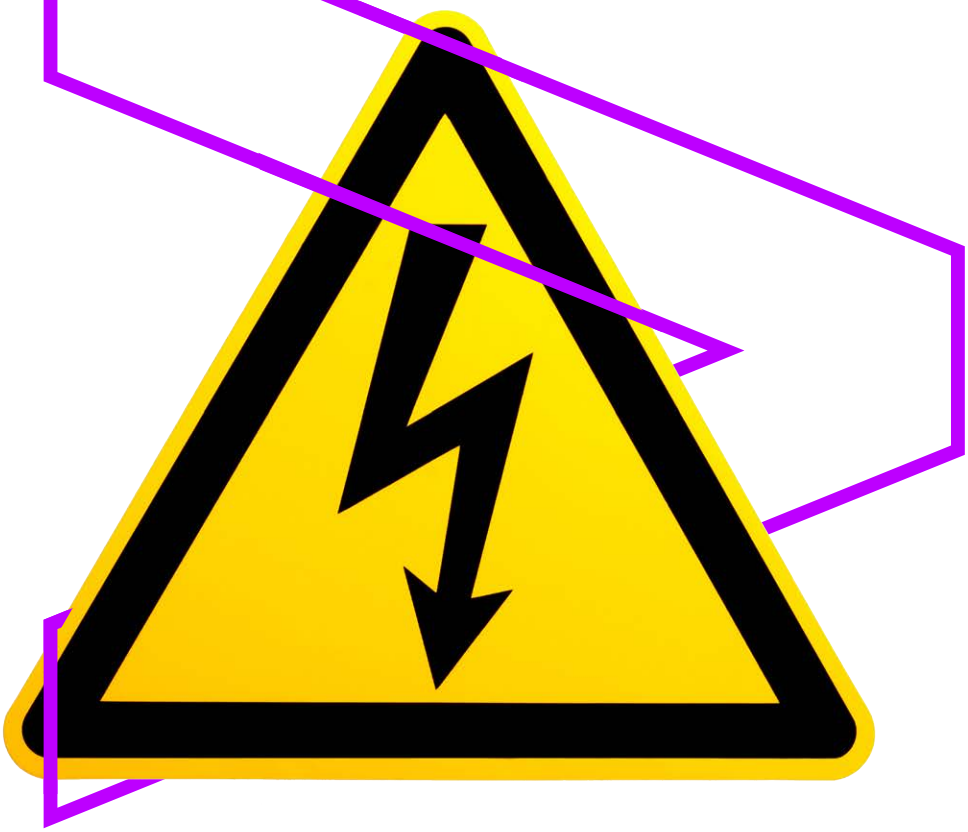
accentureconsulting

OUTSMARTING GRID SECURITY THREATS



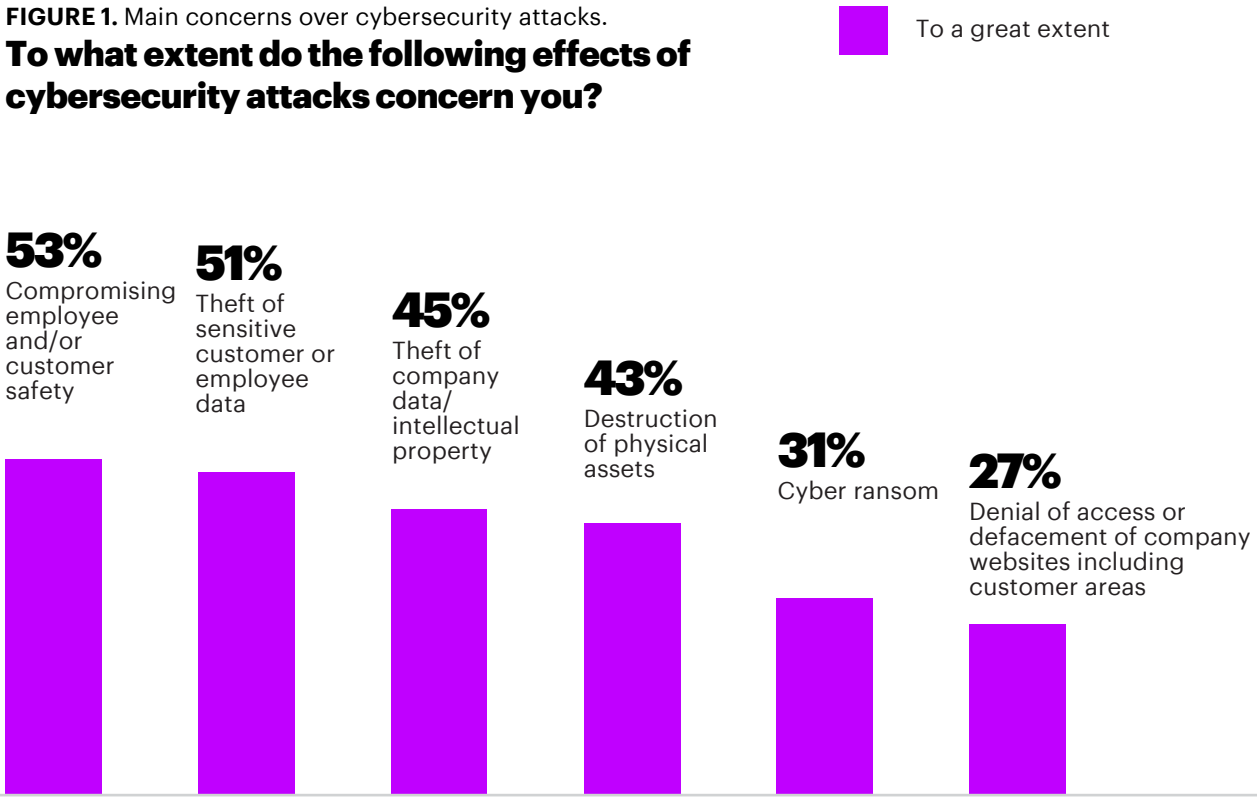
A CLEAR, SIGNIFICANT DANGER TO ELECTRICITY DISTRIBUTION GRIDS

Cyber attacks pose a clear threat to electric power systems. But as these attacks proliferate, utilities, regulators and governments continue to grapple with understanding the scale of the risks they face and determining the most effective responses.

To date, efforts to secure transmission networks have captured the most attention. But distribution grids also face major risks from cyber attack. Attacks on industrial control systems such as SCADA systems could result in blackouts, disrupting industry as well as vital services such as transportation and health. Accenture's Digitally Enabled Grid survey reveals that distribution business executives cite interruptions to supply as their greatest cyber attack-related concern, closely followed by potential impacts on customer and employee safety.

FIGURE 1. Main concerns over cybersecurity attacks.

To what extent do the following effects of cybersecurity attacks concern you?



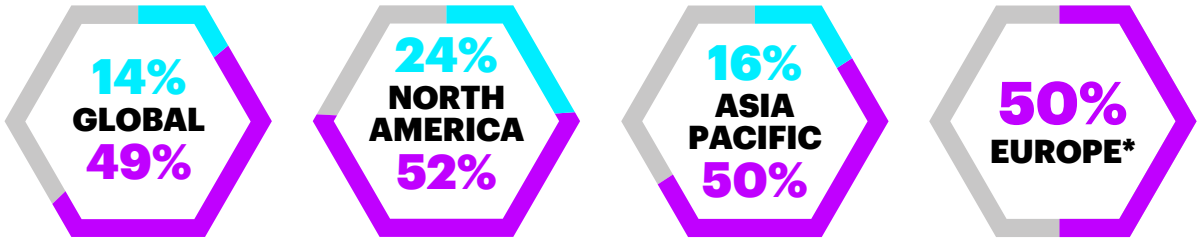
Base: All respondents.
Source: Accenture's Digitally Enabled Grid program, 2017 executive survey.

A typical distribution grid has neither the size of a transmission network nor the same risks of cascading failure. However, distribution grids have the same vulnerabilities and, as a potentially softer target, could be increasingly subject to attack. Breaches by a wide range of potential attackers could have devastating impacts along the entire electricity value chain, from generation through to consumers. A successful attack could erode public trust in the utility and raise questions about the security of all devices along the value chain. Developing effective strategies to secure smart grids against potential cyber breaches is therefore both an imperative and urgently required.

As the recent details of the CrashOverride/Industroyer attacks in the Ukraine highlighted, electricity grids are at significant risk from a potential adversary with malicious intent. However, recent attacks such as NotPetya, a highly disruptive piece of malware that masqueraded as ransomware, have also demonstrated that collateral damage to unintended targets is an increasing concern. Irrespective of motive, a successful attack could see large populations suffering major power outages, as well as causing enormous business disruption and economic damage. Accenture's executive survey indicates that more than half of respondents believe their countries' face at least a moderate likelihood of supply interruption due to cyber attack within five years.

FIGURE 2. Likelihood of supply interruption from a cyber attack.

What do you think is the likelihood that a distribution company in your country will have a cyber attack, resulting in an interruption to the electricity supply, in the next five years?



Base: All respondents; *due to limited European sample (n=25), results for this region are to be interpreted with caution and within context.

Source: Accenture's Digitally Enabled Grid program, 2017 executive survey.

ABOUT ACCENTURE'S DIGITALLY ENABLED GRID RESEARCH PROGRAM

Accenture's Digitally Enabled Grid research program provides actionable insights and recommendations about the challenges and opportunities utilities face along the path to a smarter grid. Drawing upon primary research insights from utilities executives around the world as well as Accenture analysis, The Digitally Enabled Grid examines how utilities executives expect smart grid technologies and solutions to contribute to their future networks. The 2017 executives survey included more than 100 utility executives from over 20 countries.

A RAPIDLY EVOLVING RISK LANDSCAPE

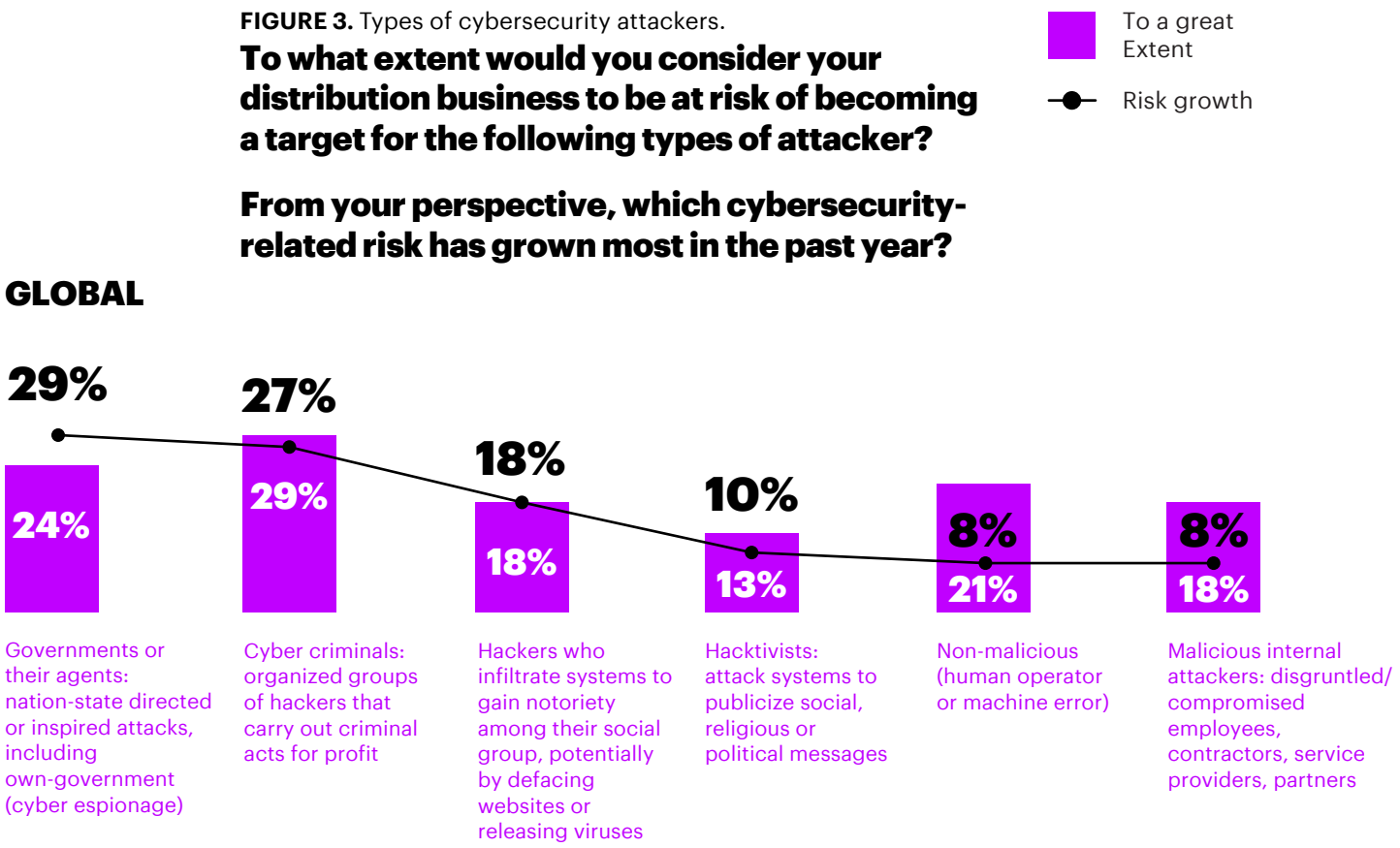
Highly sophisticated, weaponized malware requires considerable resources to develop and deploy covertly. Its use is therefore typically credited to nation-states. And while such malware remains in the possession of nation-states that generally follow international norms and use caution in the deployment of cyber weapons, not all (e.g., North Korea) live up to international norms. A potentially greater risk arises from such malware moving into the hands of cyber criminals, the development of "ransomware-as-a-service" and, eventually, to "script-kiddies" (individuals who make use of existing code/programs for malicious purposes). Exploits have already been published on the internet, enabling criminals and terrorists to download the code and potentially attack companies and governments. It's relatively easy to access many different types of malware from sites on the dark web that provide a supermarket for cyber criminals. This type of access opens a route to indiscriminate targeting of electricity companies by new types of ransomware and hackers.

Respondents to Accenture's survey recognize these risks. They see cyber criminals and governments or their agents as the two main types of attackers posing the greatest risk.

FIGURE 3. Types of cybersecurity attackers.

To what extent would you consider your distribution business to be at risk of becoming a target for the following types of attacker?

From your perspective, which cybersecurity-related risk has grown most in the past year?

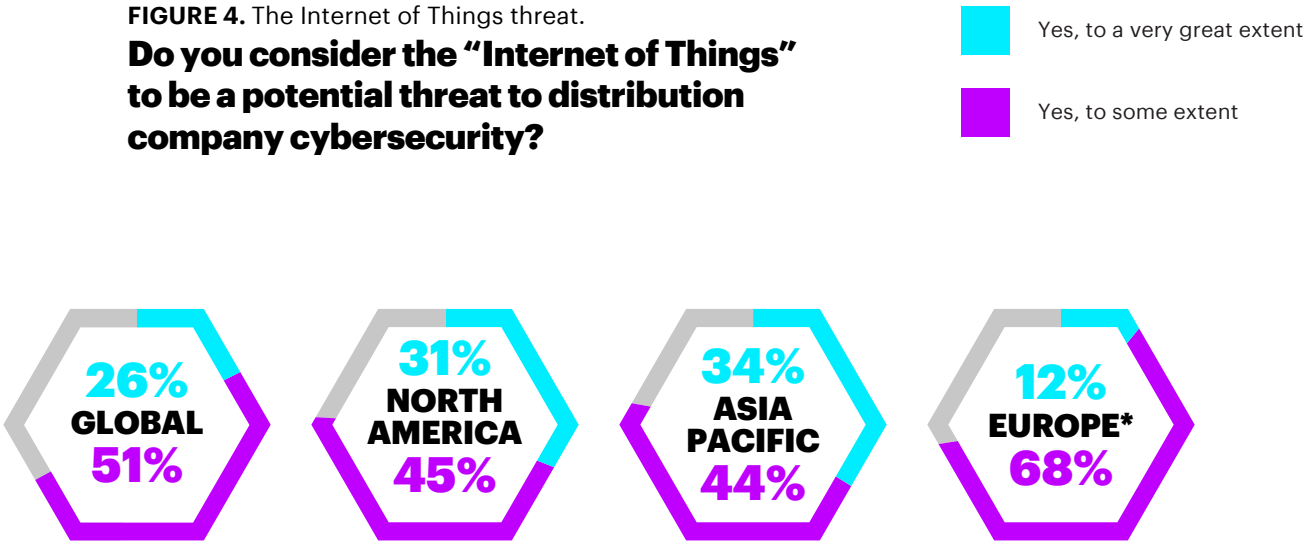


Base: All respondents.
Source: Accenture's Digitally Enabled Grid program, 2017 executive survey.

The Internet of Things (IoT) is also posing a relatively new challenge to security. Distribution utilities are particularly exposed to the localized risks from IoT hacking. At this stage, it's unclear exactly how IoT domestic devices could be controlled to impact the distribution network. But utility executives clearly see the potential danger, given the scale of IoT deployment and its sometimes-limited security. These threats could include hacking a large number of home hubs, or smart thermostats that have control over household appliances such as heating and cooling systems. That raises the potential to drive coordinated large-scale changes to energy demand that could destabilize the grid. The limited security features of many IoT components mean distribution companies should assume that what can be hacked will be hacked, and should develop appropriate defensive measures to prevent the IoT becoming an attack vector into the grid itself.

FIGURE 4. The Internet of Things threat.

Do you consider the "Internet of Things" to be a potential threat to distribution company cybersecurity?



Base: All respondents; *due to limited European sample (n=25), results for this region are to be interpreted with caution and within context.

Source: Accenture's Digitally Enabled Grid program, 2017 executive survey.

THE SMART GRID: SOLUTION ... AND RISK?

The increased connectivity of industrial control systems enabled by the smart grid will drive significant benefits in the form of safety, productivity, improved quality of service and operational efficiency. However, there is a fear that the same greater connectivity could also create opportunities for cyber criminals to launch crippling attacks. The integration of information technology (IT) with operational technology (OT) and consumer-based IoT does indeed open the potential of new attack vectors into the industrial control systems. Without effective security in place, the rich information flows carried by the digital grid could be manipulated by cyber attackers to cause malfunctions and outages, or even destruction of equipment or loss of life.

WITHOUT EFFECTIVE SECURITY IN PLACE, THE RICH INFORMATION FLOWS CARRIED BY THE DIGITAL GRID COULD BE MANIPULATED BY CYBER ATTACKERS TO CAUSE MALFUNCTIONS AND OUTAGES, OR EVEN DESTRUCTION OF EQUIPMENT OR LOSS OF LIFE.

However, electricity grids are already at risk. The current technology landscape for many utilities features control systems that work on old or vulnerable operating systems—commonly without sufficient processing power to run effective virus scans; a lack of encryption or authorization on communications channels—accompanied by limited or no security for end points such as programmable logic controllers (PLCs) and intelligent end devices (IEDs). So rather than seeing it as creating additional vulnerability, deployment of the smart grid should be thought of as a key element of the security solution for distribution businesses, offering sophisticated protection to previously vulnerable assets.

For instance, to effectively meet the security imperative, the smart grid must integrate consolidated, end-to-end IT/OT and physical security into its design. This should be achieved through certificate-based, device-level authentication (where feasible), network protocols that support encryption, application security, network segmentation, security monitoring, incident response and a hardening process to confirm vulnerabilities are managed in a timely fashion.

And while the use of mobile technology allows greater workforce efficiency and cost reductions through remote access to devices and systems, securing it is also critical. It requires effective identity and access management policies and the use of additional measures such as multi-factor authentication to prevent stolen employee credentials from being used to access systems. Access rights must be limited to the minimum required for an employee to perform their role.

Finally, the broader supply chain for the smart grid requires far greater scrutiny. Suppliers of hardware or services can have their solutions compromised by third parties, providing an easy route into the heart of a distribution business. For example, a technician might inadvertently download malware while updating software through misdirection to an alternative site. Similarly, malignant code could be hidden in the hard drives of industrial equipment.

DEVELOPING A RESILIENT DELIVERY SYSTEM

GETTING STARTED: ASSESSING THE SITUATION AND SEGMENTING RISKS

Cybersecurity for distribution grids has some significant differences from that of transmission networks. For example, significantly less real-time data or control may be possible on some distribution grids, but distribution restoration is easier in the event of interruption. While the cyber risk for a transmission system is a cascading failure, it is more likely that distribution businesses face multiple, smaller-scale attacks in the future given that transmission systems are more secure. In fact, the distribution system's substations, overhead lines and underground networks, enabled by smart grid technology, offer less protection and more vulnerability.

Distribution grids span a wide range of voltages and degrees of automation, from SCADA-controlled sub-transmission down to passively-run, low-voltage residential feeders. An effective cyber defense program begins with a comprehensive system–wide assessment of the utility's state of preparedness and current risk factors. In this phase, the utility categorizes its major assets, identifies security requirements and determines where gaps exist. The utility typically then verifies that robust processes to manage those gaps are in place, as well as to report on progress in closing them.

This entails the definition and execution of mitigation plans—with clear priorities established—and addressing the gaps in a consistent and timely fashion, with documented, audited results. As new threats emerge, so will new standards. To remain current, utilities will need to confirm they have the necessary security and compliance skills and resources in place.

Utilities are at varying stages along the cyber protection maturity curve. Some are merely working toward compliance with local security standards, while others have already achieved compliance and are working on developing security as a core business capability. In Accenture's view, the optimal approach is an effective segmentation of risks, with the implementation of the most advanced security for highest-risk, high-value assets or highest-impact customers. At this level, utilities have greater operational control, improved situational awareness, lower risk, superior control of operations and maintenance costs, and are better prepared for the impact of future disruptive technologies. Most importantly, these utilities would have stronger power grid protection and would be less likely to experience a catastrophic event.

ACCENTURE GLOBAL HIGH PERFORMANCE SECURITY RESEARCH

IN THE SPOTLIGHT: CYBER-RESPONSE READINESS

While cyber-response readiness will be key for utility distribution businesses, the latest Accenture High Performance Security research shows that fewer than 40 percent of utilities have methods, tools and skills comparable to the highest level of performance (see Figure 5). This means having a robust response plan, strong cyber-incident communications, tested plans for the protection and recovery of key assets and the grid, effective cyber-incident escalation paths and the ability to confirm solid stakeholder involvement.

FIGURE 5. Cybersecurity strategy domain: cyber resilience and response readiness (% of organizations at or near the highest level of performance for these cybersecurity capabilities).

RESILIENCE READINESS

27%
Design for protection of key assets

39%
Maintaining resilience readiness

37%
Cyber-incidence recovery

RESPONSE READINESS

24%
Ensure stakeholder Involvement

30%
Protection and recovery of key assets

38%
Cyber-response plan

Base: All utility respondents.
Source: High performance security research, Accenture 2016.

GETTING THE APPROPRIATE CAPABILITIES IN PLACE: DIFFERENTIATING BETWEEN CAPABILITY AND COMPLIANCE

The increasing convergence of physical and cyber threats requires the development of capabilities that go well beyond simple compliance. Utilities should invest in resilience as well as effective response/recovery capabilities. They should share threats and system "irregularities" seamlessly between grid control, security operations, network operations centers and beyond. This can only be effective if existing business silos between IT, OT and system operations are dissolved.

We believe distribution businesses need an agile capability that creates and leverages situational awareness, is based on changing threat actors and can quickly react and intervene. Having a security operations center (SOC) with a monitoring/analytics capability that is fully integrated into asset operations is critical to react quickly to the changing threat landscape.

Two components can potentially provide critical value here:

- Combining cyber and physical security into a single SOC.

- Co-locating or improving communication and situational awareness between the SOC and distribution operations to help build the capabilities and responses between operations and security/cyber technologists.

While the traditional approach of assessing risks and closing the gaps is still necessary, it is not sufficient on its own. Effectively, a two-speed security model is required.

Our survey has shown that many distribution utilities still have some way to go in developing a robust cyber response. More than 40 percent of respondents said that cybersecurity risks were not, or only partially, integrated into their broader risk management processes. Siloed processes could mean new threats and responses go unidentified or do not receive appropriate senior management scrutiny. The need to improve threat recognition explains why a key requirement identified by surveyed executives, particularly in North America, is the identification and sharing of threats across the industry. Utilities need to engage effectively with government and industry forums so that new threats are managed quickly and effectively.

There are additional actions utilities should take to achieve advanced security. Experience from other sectors, including financial services and retail, shows that attackers have routinely breached infrastructures that were considered 100 percent compliant with regulations. Regulation tends to be too generic and lags actual threat intelligence, making it an inadequate benchmark for effective security.

Designing and building resilient systems, in which security is embedded in the design requirements, is key. Each new substation, AMI deployment, IoT device installed or smart grid deployment initiatives should have security embedded at the earliest stage. Architecting systems for reliability and for resiliency is key.

Integrating the SOC within asset operations is critical to building a cyber-resilient grid. The asset operators need to understand the cyber situation of the grid to prevent or respond quickly to a cyber incident.

FIGURE 6. Priority actions to address cybersecurity.

What single action would make the greatest impact on your cybersecurity capability?

10%
Clear cybersecurity governance and roles definition

15%
Training and improved risk awareness

12%
The definition of a holistic security program

32%
Improved threat identification and sharing across the industry [NA: 57%]

20%
Clearer understanding of the operational technology (OT) implications for cybersecurity

11%
Updated risk management framework incorporating cybersecurity

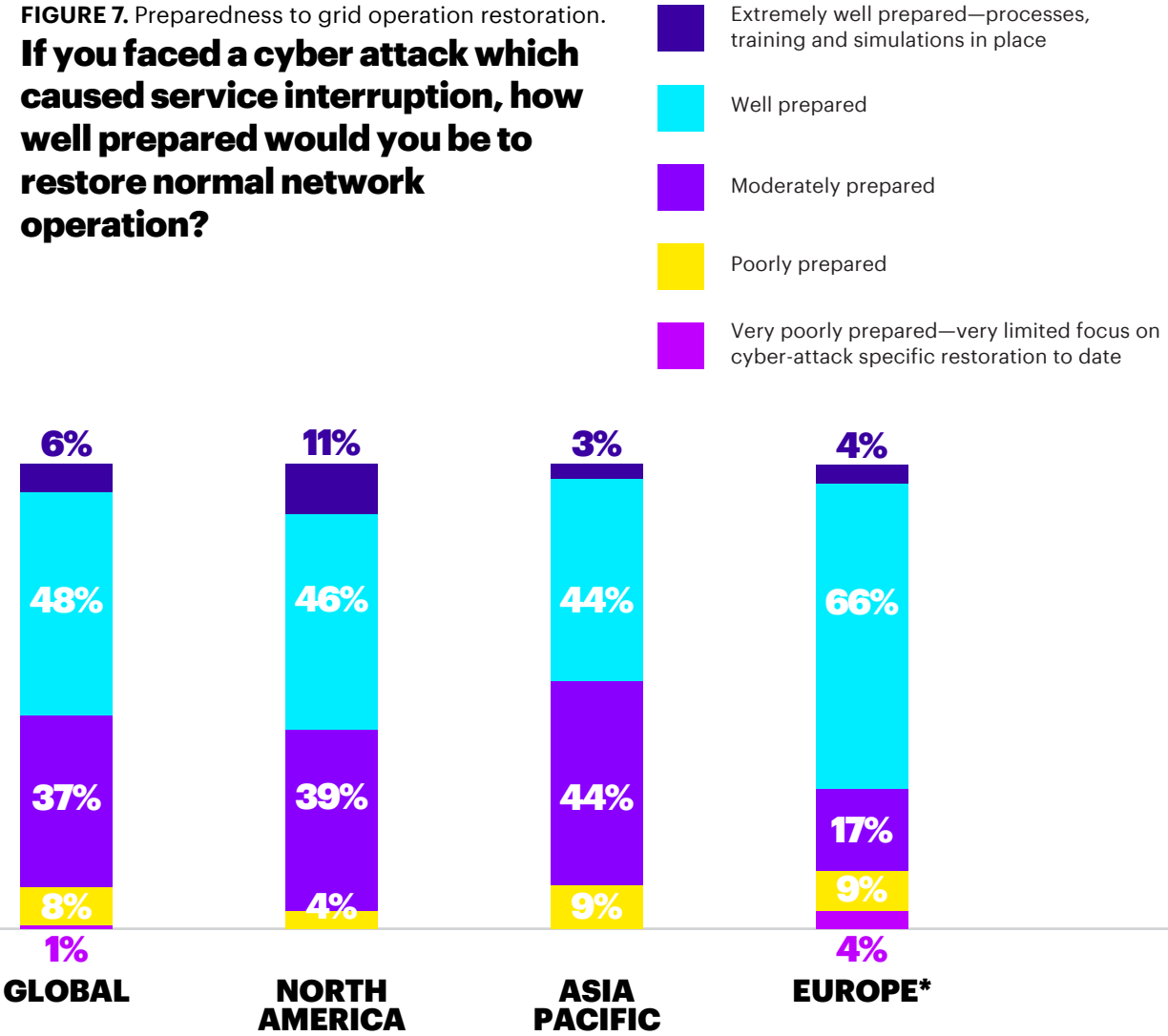
Base: All respondents.
Source: Accenture's Digitally Enabled Grid program, 2017 executive survey.

DESIGNING FOR RESPONSE AND RESTORATION

The complexity and diffuse nature of distribution electricity grids, along with sophisticated, well-funded attackers, makes perfect protection virtually impossible. Fortunately, distribution utilities are well-practiced at restoring grids after adverse weather or asset failure. The challenge is to recognize when a supply disruption is caused by a cyber attack and to respond appropriately with fewer, qualified field personnel. Demanding cost-control efforts combined with moves toward greater automation has created a potential shortage of qualified linemen and substation technicians. These factors will require improved emergency planning for utilities facing large-scale outages from cyber attacks.

FIGURE 7. Preparedness to grid operation restoration.

If you faced a cyber attack which caused service interruption, how well prepared would you be to restore normal network operation?



Base: All respondents; *due to limited European sample (n=25), results for this region are to be interpreted with caution and within context.

Source: Accenture's Digitally Enabled Grid program, 2017 executive survey.

In Accenture's survey, only half the respondents thought they were well-prepared for the specific challenges of an interruption from cyber attack. To improve preparedness, distribution businesses should simulate how to manage false-data streams, "bricked" PLCs and regain control over hijacked parts of the grid. Similarly, when a major asset fails, the distribution operators should always ask themselves if a cyber attack could have been the cause. Unlike normal outages that can be predictable and can be contained to a geographically limited domain, cyber space is not confined by clear boundaries. A cyber attack can hit multiple, dispersed geographic locations simultaneously–making it more difficult to contain and adequately respond to, as well as requiring different simulation scenarios.

Our experience has shown that the greatest challenges to effective preparedness and response are not external factors. In fact, they are:

1. The cultural and organizational silos that exist between operations and technology business units.

While the chief information security officers (CISOs) and technologists are largely responsible for protecting against OT attacks, it will be the distribution operators and technologists charge to jointly restore the electrical, OT and IT systems following an attack. Therefore, these silos must be broken down to prepare for the signs of an attack and restore the systems following the attack. If these silos remain, it will take longer to identify, isolate, remediate and recover from a successful OT attack.

2. The decreasing number of personnel available to operate the grid without technology.

Once the technology is disconnected from the grid, monitoring and operating the systems until the technology is restored is very labor-intensive. It requires substation technicians to monitor voltages, qualified linemen to manually operate switches and an increased workload on the system operators. Given the shift from large to lean workforces, this could significantly strain utilities' capabilities.

EMBRACING SECURITY AT THE CORE

FIVE MOVES TO OUTSMART GRID SECURITY THREATS

The need for cybersecurity is a reality in all sectors. While distribution grids have some specific challenges, the industry is well-versed in delivering reliable power delivery in the face of storms, asset failures and accidents. The smart grid can ultimately provide the visibility and control to improve grid robustness. However, cybersecurity must become a core industry capability, one that protects the entire value chain/extended ecosystem end to end. Developing this new capability will require ongoing innovation, a practical approach to scaling and collaboration with partners to drive the most value.

While there is no single path forward, there are some moves any distribution business should consider to strengthen resilience and response to cyber attacks. These steps could allow the building and scaling of cyber-defense capabilities:

1

INVESTIGATE A PLATFORM APPROACH TO CYBERSECURITY CAPABILITIES.
Deregulation created many small- and medium-size distribution businesses that lack the resources required to address and develop cybersecurity capabilities. For these businesses, it may be productive to find ways to pool resources or look to platform-based models and technology solutions that could help address common cybersecurity challenges without needing to build their own internal capability.

2

INTEGRATE RESILIENCE INTO ASSET AND PROCESS DESIGN.
Most utilities still operate systems and assets that were designed before the advent of computers, and certainly before the emergence of cyber attacks. Moving forward, including cybersecurity (and physical security) into asset and process design could make the distribution system more resilient. Taking it a step further, integrating not only security but natural hazard hardening into the design of distribution grids will make these more resilient at a lower overall cost.

3

SHARE THREAT INFORMATION.
There are likely to be common threats faced by distribution businesses. Sharing intelligence and information is a critical activity that could help create situational awareness of the latest threat landscape and how to prepare accordingly. However, it's not clear to what extent the imposition of data privacy and security regulations will encourage greater openness and transparency. In the absence of information sharing between utilities, external cyber experts could be employed to help create that situational awareness.

4

DEVELOP SECURITY AND EMERGENCY MANAGEMENT GOVERNANCE MODELS.
Developing a cybersecurity governance model should reflect the prevailing corporate culture. For example, a top-down, centralized business should reflect that culture in its cybersecurity governance model. Similarly, a business that is less centrally controlled and managed should adopt a similar approach to the governance of cybersecurity. In other words, there is no single approach. Each distribution business needs to consider its organizational and operational context in order to devise the most effective approach.

5

DEVELOP RELATIONSHIPS WITH REGIONAL SECURITY OFFICIALS AND WITH CYBER-RESPONSE EXPERTS.
Whether national security and intelligence officials or private sector cyber response and legal experts, expertise to help contain, investigate and manage the consequences of the response will be required. Developing those relationships now, modeling the interactions and planning the response will be critical to an effective, efficient response.

EXECUTIVE SPONSORSHIP AND CONTACT

Stephanie Jamison
Managing Director
Accenture Transmission and Distribution Services

CONTRIBUTORS

Michael Rossman
Managing Director
Accenture Security

Tom Ryan
Principal Director
Resiliency, Risk and Crisis Management, Accenture

Michael Teichmann
Managing Director
Accenture Security

ABOUT ACCENTURE'S DIGITALLY ENABLED GRID RESEARCH PROGRAM

Accenture's Digitally Enabled Grid research program provides actionable insights and recommendations around the challenges and opportunities utilities face along the path to a smarter grid. Drawing upon primary research insights from utilities executives around the world as well as Accenture analysis, The Digitally Enabled Grid examines how utilities executives expect smart grid technologies and solutions to contribute to their future networks. Learn more at www.accenture.com/digitallyenabledgrid.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.