MARSH & McLENNAN ADVANTAGE INSIGHTS

Microsoft

WINNING THE CYBER RISK CHALLENGE

RAPID DIGITALIZATION IN THE ENERGY/ POWER SECTOR CONTINUES TO OUTPACE CYBER READINESS

> “Should an attack successfully obstruct the generation-to-consumption process, much of our day-to-day lives would be rendered next-to-impossible... today, the variability and storage limitations of renewables have thrown more variables into the mix.”
>
> **Rep. John Carter**

STORY OVERVIEW

I The Energy/Power (E/P) sector's **speed of digitalization is outpacing its building of cyber defense capabilities and overall risk management adaptation.** According to the Marsh Microsoft 2019 Global Cyber Risk Perception Survey, a primary technology driver is cloud computing, which is widely perceived to have an extremely high level of associated cyber risks.

II Meanwhile, **geopolitical issues are increasingly making the E/P sector an attractive target** for cyberattacks. More than half of the sector's respondents expect the government to do more to protect them against nation-state cyber attackers.

III The sector's **internal threat vectors are primarily its people**, who are commonly targeted by sophisticated attackers; its processes, which have room for improvement in having cybersecurity as an end-to-end component; and its technology, which encompasses interdependent legacy-with-modern systems.

IV The **external threat vectors are mainly the ever-expanding supply chain and the evolving regulatory landscape (as part of the clean energy transition)**, that is seeking more accountability. E/P organizations are leaning towards "softer" industry standards, rather than "hard" laws, to help improve their cybersecurity posture.

V Compared to other industries, the E/P sector is more confident in understanding and mitigating cyber risks but is just as insecure in recovering from cyber incidents. The sector has taken considerably more proactive actions on cyber risk compared to other industries, although these actions remain **largely centered on basic preparation and prevention.**

VI To advance cyber resilience, the E/P sector needs to pursue a range of strategies to build up its portfolio of cyber capabilities. This includes a holistic cyber risk assessment, proactive strengthening of internal cyber culture, being part of a cyber coalition, leveraging on transformative technologies as cyber solutions, and more.

Copyright © 2020 Marsh & McLennan Companies

MAIN MENU

4 **A SHIFTING PLAYING FIELD**

Digitalization is outpacing cyber defenses, presenting paramount risks to critical assets

8 **BETTER ORGANIZED "OPPONENTS"**

Increasing exposure to more sophisticated cyber adversaries, complicated by internal and external threat vectors

21 **HOW TO WIN**

Strategies to increase cyber resilience amid digitalization

A SHIFTING PLAYING FIELD

DIGITALIZATION IS OUTPACING CYBER DEFENSES, PRESENTING PARAMOUNT RISKS TO CRITICAL ASSETS

Increasingly over the past decade, the Energy/ Power (E/P) sector is experiencing significant disruption from trends of digitalization, decarbonization and decentralization. Local power generation, with the growth of peer-to-peer energy trading, is expected to become more widespread when greater connectivity and infrastructure are in place.

In various aspects, and especially across operational components, E/P systems have been radically modernized owing to the evolution of smart technologies and networked communication protocols. Swift digitalization and the expanding ecosystem of energy market participants have heightened cyber implications.

EXHIBIT 1: ENERGY SYSTEMS AND POWER GRIDS ARE FAST BECOMING DIGITAL ECOSYSTEMS – INTRODUCING COMPLEXITIES, NEW INTERDEPENDENCIES, VULNERABILITIES TO POTENTIAL ATTACKERS, AND UNINTENTIONAL ERRORS[I]

- According to the International Energy Agency, governments and utilities around the world are investing **$750 billion annually** into electricity generation and supply, more than in any other area of the energy sector.[II]
- Smart technologies as shown below are vital to this investment, helping transform traditional electricity systems into intelligently connected networks, including smart grids.
- Enabled by smart grids, the real-time access to supply and demand platforms alone could deliver **an annual value of $632 billion to society**[III]—more than any other individual digital initiative.

Internet of Things (IoT) nodes and smart meters are common in various parts of the systems.

Existing supervisory control and data-acquisition (SCADA) systems used for monitoring and control operations, are widely dispersed in energy transport and distribution networks.

Distributed control systems (DCS) are used for single facilities or small geographical areas.

Remote terminal units (RTU) and programmable logic controllers (PLC) are being used to monitor system data and initiate programmed control activities in response to input data and alert.

Smart engineering technology and cloud services are being integrated with legacy hardware/software.

Copyright © 2020 Marsh & McLennan Companies

This results in greater cyber risks because the surface areas for attacks are larger and most E/P organizations are not fully ready to respond to an attack across their ecosystem. Cyber threats are evolving rapidly and threat actors are rushing in to exploit the sector's critical assets through these vulnerable "gaps",[IV] but the accompanying cybersecurity investments, awareness, and ability to respond have struggled to keep up.

Two overarching challenges shifting the threat landscape for E/P organizations:

1. **Internal Challenge:** Digitalization in the E/P sector is outpacing its cyber defense capabilities
2. **External Challenge:** E/P organizations are increasingly targeted by sophisticated cyber attackers

INTERNAL CHALLENGE: DIGITALIZATION IN THE ENERGY/POWER (E/P) SECTOR IS OUTPACING ITS CYBER DEFENSE CAPABILITIES

Digital transformation is bringing multiple benefits to the sector. It optimizes valuable assets, reduces operational costs, reduces quality risks, improves profitability, enables faster and more effective decision-making, and provides new opportunities for E/P suppliers. It also favors consumers by passing on cost-savings to organizations and citizens. While the transition is positively reshaping the sector, digital transformation also puts forth a new set of risks to be managed, such as weaker security baselines (with a higher degree of exposure), and the use of potentially insecure data storage systems and data communication.

Cloud computing *is perceived to be the leading technology to drive the Energy/Power (E/P) sector through the digital transformation journey. Participants in the Marsh Microsoft 2019 Global Cyber Risk Perception Survey reported that cloud computing is the most adopted technology in 65 percent of E/P respondents' organizations, or 57 percent of all cross-industry participants.[V] With cloud computing today, the sector's networks expand into the cloud and might be connected to Industrial Control Systems (ICS), which house a multitude of equipment that often span the globe. Understandably, there is a strong correlation between cloud adoption/size of an ecosystem and the associated cyber risks.[VI]*

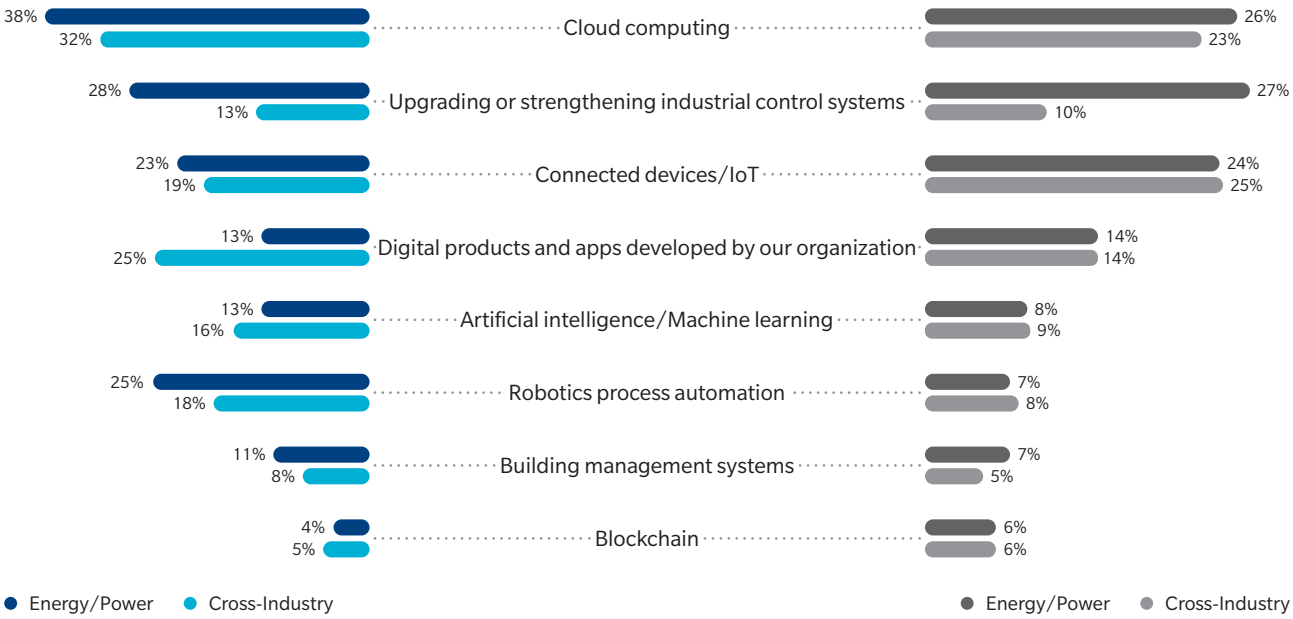
While organizations in the E/P sector recognize the potential business benefits of leveraging cloud computing, they are also aware of the associated cyber risks in moving their workloads to the cloud. As shown in Exhibit 2, according to 38 percent of E/P respondents, the perceived business opportunity presented by cloud computing is "extremely high", more than other technologies. At the same time, however, the perceived level of cyber risk associated with the technology is also higher than for most other technologies (26 percent of E/P respondents). Cloud comprises one of the biggest cyber exposures—it can be a potential point of entry for attackers as its API[1] feature has key vulnerabilities and employees of the cloud provider can potentially access the stored data.

Robotics Process Automation (RPA)*, meanwhile, is perceived to present high business opportunity (by 25 percent of respondents) with relatively low cyber risk for the E/P sector. However, given the sector's slow cyber maturity as compared to other sectors, the full extent of cyber risk implications is difficult to gauge.[VII]*

1 BRINK, 2019. The Threat from the Cloud: How Cyber Intruders Exploit Third Parties. **Application programming interfaces (API)** allows users to customize features of their cloud services to fit business needs — and also to authenticate, provide access and effect encryption, which can create vulnerabilities. The biggest vulnerability of an API lies in the communication that takes place between applications.

EXHIBIT 2A: PERCEIVED **BUSINESS OPPORTUNITY** PRESENTED BY THE TECHNOLOGY IS EXTREMELY HIGH

EXHIBIT 2B: PERCEIVED LEVEL OF **CYBER RISK** ASSOCIATED WITH THE TECHNOLOGY IS EXTREMELY HIGH



Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey; Marsh & McLennan Advantage Insights analysis

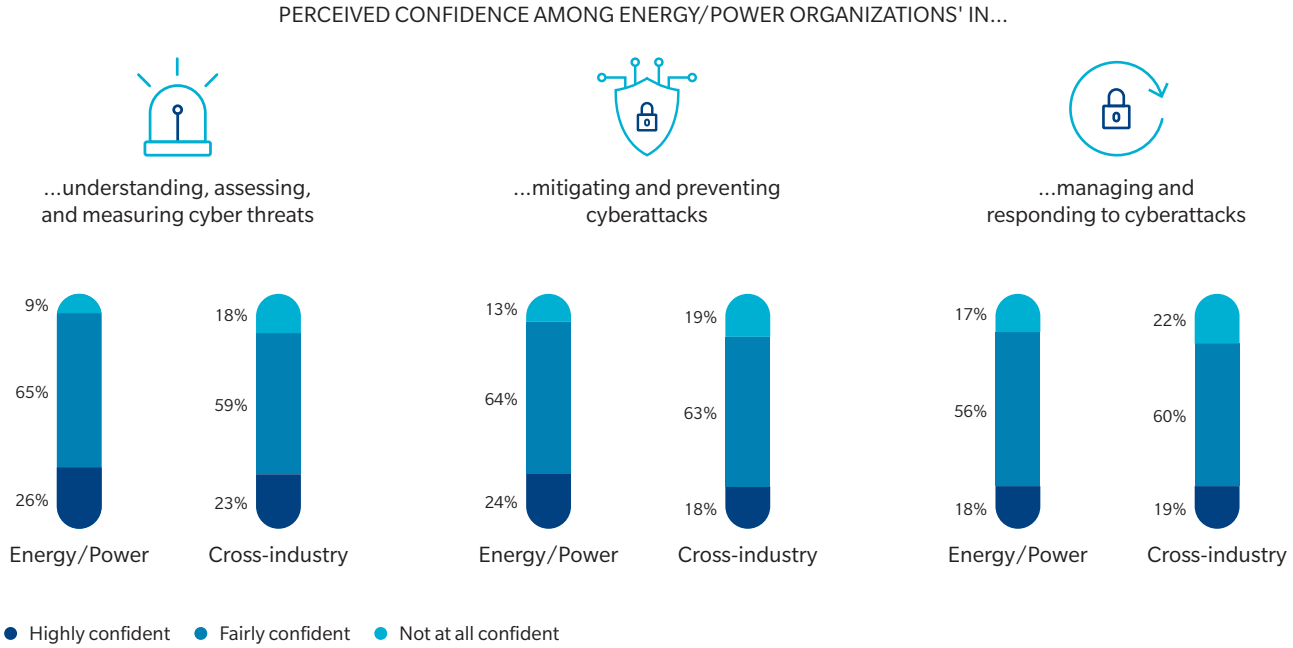
The Energy/Power (E/P) sector, like all other industries, remains optimistic about the potential value and business opportunities that transformative technologies bring. In fact, more than half the survey respondents agreed that the potential benefits and opportunities offered by new technologies and digital products are so compelling that risk is almost never a barrier to adoption.[VIII]

While the sector embraces technologies and is aware of the cyber risks, there are concerns that it is inadequately equipped to deal with cyber threats or perhaps overconfident in its ability to do so. When compared to the cross-industry average, respondents from the E/P sector are more confident in understanding and mitigating cyber risks, but are just as insecure when it comes to recovering from cyber incidents. In fact, 91 percent of survey respondents from the E/P sector are (highly or fairly) confident in understanding their cyber risk exposure, but relatively fewer are confident about their ability to manage and respond to cyberattacks. In both cases, however, the E/P sector fares better than the cross-industry averages of 82 percent and 78 percent respectively (Exhibit 3).

According to the survey, organizations in the E/P sector have flagged the following as **top barriers to enabling effective cyber risk management:** Keeping pace with new cyber threats (65 percent), finding adequate staff time to focus on cybersecurity (51 percent), and budget constraints (45 percent).

Copyright © 2020 Marsh & McLennan Companies

EXHIBIT 3: ENERGY/POWER (E/P) ORGANIZATIONS' SELF-ASSESSED ABILITY TO UNDERSTAND, PREVENT, AND MANAGE CYBERATTACKS



Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey

EXTERNAL CHALLENGE: ENERGY/POWER (E/P) ORGANIZATIONS ARE INCREASINGLY TARGETED BY SOPHISTICATED CYBER ATTACKERS

Today, both publicly and privately owned E/P systems have become prime targets for criminals and hostile governments. With an increase in geopolitical tensions, it has become clear over the past three years that a majority of the attacks have state-sponsored hallmarks, some with a particular interest in strategic infrastructure systems and/or facilities. In fact, the number of known attack groups tracked by a leading security software company has increased from 140 in 2018 to 155 in 2019.[IX] These cyber attackers are increasingly resourceful and tech-savvy; even inexperienced hackers today can access sophisticated tools on the dark web for targeting Industrial ICS.[X]

Short of outright conflict with a state adversary, geopolitical circumstances and bad actors are viewing the E/P sector as an attractive target for minimum effort-maximum impact.[XI] The attackers' goals are plausible scenarios like discrediting, distracting from a simultaneous military attack, or retaliatory operations in the E/P organizations.[XII] In many cases, the ability to disrupt enemies by bringing down the systems on which they depend has become much more strategic in conflict than conventional warfare. With so much at stake, it is unsurprising that among the E/P organizations surveyed...

60% ...are highly concerned about the potential harm that a **nation-state cyberattack** could have on their **business**

53% ...agree that governments need to do more to help protect **E/P organizations against nation-state cyberattacks**

BETTER ORGANIZED "OPPONENTS"

INCREASING EXPOSURE TO MORE SOPHISTICATED CYBER ADVERSARIES, COMPLICATED BY INTERNAL AND EXTERNAL THREAT VECTORS

An array of cyber actors throughout the value chain

A wide range of events can disrupt Energy/Power (E/P) systems, but given the increased attempts at intrusion, cyberattacks can disrupt the sector more easily than most other events (such as earthquakes, physical attacks, and operational errors).[XIII] The sector faces cyber threats across both physical and digital ecosystems – as well as within the organization, the energy market, and the extended ecosystems.

Phishing remains one of the most common means of attack, be it for monetary gain or sweeping, nontargeted attacks (elaborated in Exhibit 4). Ransomware poses an equally concerning threat – take the example of WannaCry, which disrupted 80 percent of gas stations of a major Chinese oil company in 2017. Other threat actors include credential theft and advanced persistent threat (APT).[2] In recent years, botnets that can detect and infect SCADA systems have been discovered and those targeting IoT have become pervasive. There has also been a sharp growth in crypto-mining malware in 2018,[3] targeting ICS computers, and disrupting productivity by increasing load on the industrial systems.

EXHIBIT 4: PHISHING – ENERGY/POWER (E/P) SECTOR AS COLLATERAL DAMAGE EVEN WHEN IT IS NOT A TARGET

In the fall of 2017, hackers gained entry into the network of a number of electrical-distribution companies based in the EU and US, targeting core systems in control of operations. This was possible due to IT (Information Technology) security gaps and OT (Operational Technology) networks connected to IT networks through new technologies and was successfully achieved through a malicious email campaign spoof, or what is termed as **phishing**.

The threat actors managed to establish vantage points within the OT networks from which to launch attacks at a future date.

Specifically, the Dragonfly Syndicate[4] has been blamed for the breach of the EU and US electrical companies to gather intelligence and build capabilities to compromise OT systems. Groups like Dragonfly are increasingly acquiring private-sector offensive tools, enabling them to deliver exceedingly sophisticated cyberattacks such as the hacking of Britain's energy system during their 2017 general election.[XIV]

2 **Advanced Persistent Threat** refers to a stealthy computer network threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

3 **Crypto-mining malware**, or crypto-jacking, refers to software programs and malware components developed to take over a computer's resources and use them for cryptocurrency mining without a user's explicit permission.

4 Symantec, 2017. Dragonfly: Western energy sector targeted by sophisticated attack group. **Dragonfly Syndicate**, a team of hackers that the US claims is based in Russia. The Dragonfly cyber espionage group appears to be interested in both learning how energy facilities operate and also gaining access to operational systems, to the extent that the group now potentially has the ability to sabotage or gain control of these systems should it decide to do so.

Copyright © 2020 Marsh & McLennan Companies

CYBER THREATS ATTRIBUTABLE TO INTERNAL AND EXTERNAL THREAT VECTORS

Within the Energy/Power (E/P) ecosystem there are significant threat vectors that pose cyber vulnerabilities to every organization. They can serve as reasonable assessment points for organizations' cyber prioritization:

Internal cyber threat vectors remain the most urgent yet understated sources of cyber risk for any organization and industry. It includes insiders **(people)**, the internal way of working **(processes)**, and the internal tools that are used **(technology)**.

Insiders generally refer to people—employees, former employees, contractors/vendors, and business associates. According to Oliver Wyman's The Increasing Threat from Inside, insider threats represent a growing contribution to an organization's overall cyber risk exposure and many have underinvested in this area. Insurance data also pointed to humans as a key internal threat because two-thirds of cyber insurance claim incidents are the direct result of employee behavior.

For the E/P sector, human errors contribute to a majority of cyber risks, and employees are commonly targeted by sophisticated attackers. Nation-states have conducted extensive reconnaissance of their targets, identifying specific employees for social engineering, as well as testing whether known vulnerabilities have been patched.[xv] In the past year, malware was increasingly delivered through malicious links as phishing emails to employees, as it is believed to be the easiest way to gain access to the organization's internal networks or sensitive data.

In the face of a cyberattack, a cyber incident response plan[5] can determine an organization's ability to isolate the problem, mitigate, and restore normal activities in a timely manner. For instance, when the organization's internal network is compromised and its employees are caught off-guard, people tend to panic and ask questions: What do we do? Who do we call? Who's responsible for what? What is our current capability and strategy for business continuity? How and when to activate the response plan? How are we tracking the incident?

5 **A cyber incident response plan** is a comprehensive set of agile and adaptive response mechanisms and governance focused on risk identification, regeneration, and rapid recovery from a cyber incident.

Cyber Challenges to the Energy Transition, a recent report by Marsh & McLennan Companies and World Energy Council, explores the importance of and practical steps to formulate the E/P sector's cyber incident response plans. It does so by applying a dynamic resilience framework and hypothetical gaming exercises to develop "muscle memory" and respond to system breaches.

For most employees, managing cyber risks in the Energy/Power (E/P) sector is still largely perceived to be the domain of the Information Technology (IT) department. 90 percent of E/P survey respondents indicated that the responsibility for cyber risk sits mainly with their IT teams, similar to the cross-industry average of 88 percent. The lack of cybersecurity experts for the sector, specifically the smaller subset of security experts who also understand ICS and have relevant expertise, will continue to compound the issue as it is no longer sufficient to rely only on IT experts to front the fort.

Similarly, 72 percent of the E/P respondents believed that the primary responsibility lay with the executive leadership—that is, Board of Directors and CEO/President—more than with the risk management team (48 percent). Unfortunately, at the board level, cybersecurity is often deprioritized, or is merely a minor item on the board agenda, until something goes wrong and it is too late. Leaders can do more to advocate cyber messages and enforce an organization-wide cyber awareness program before a breach should even happen.

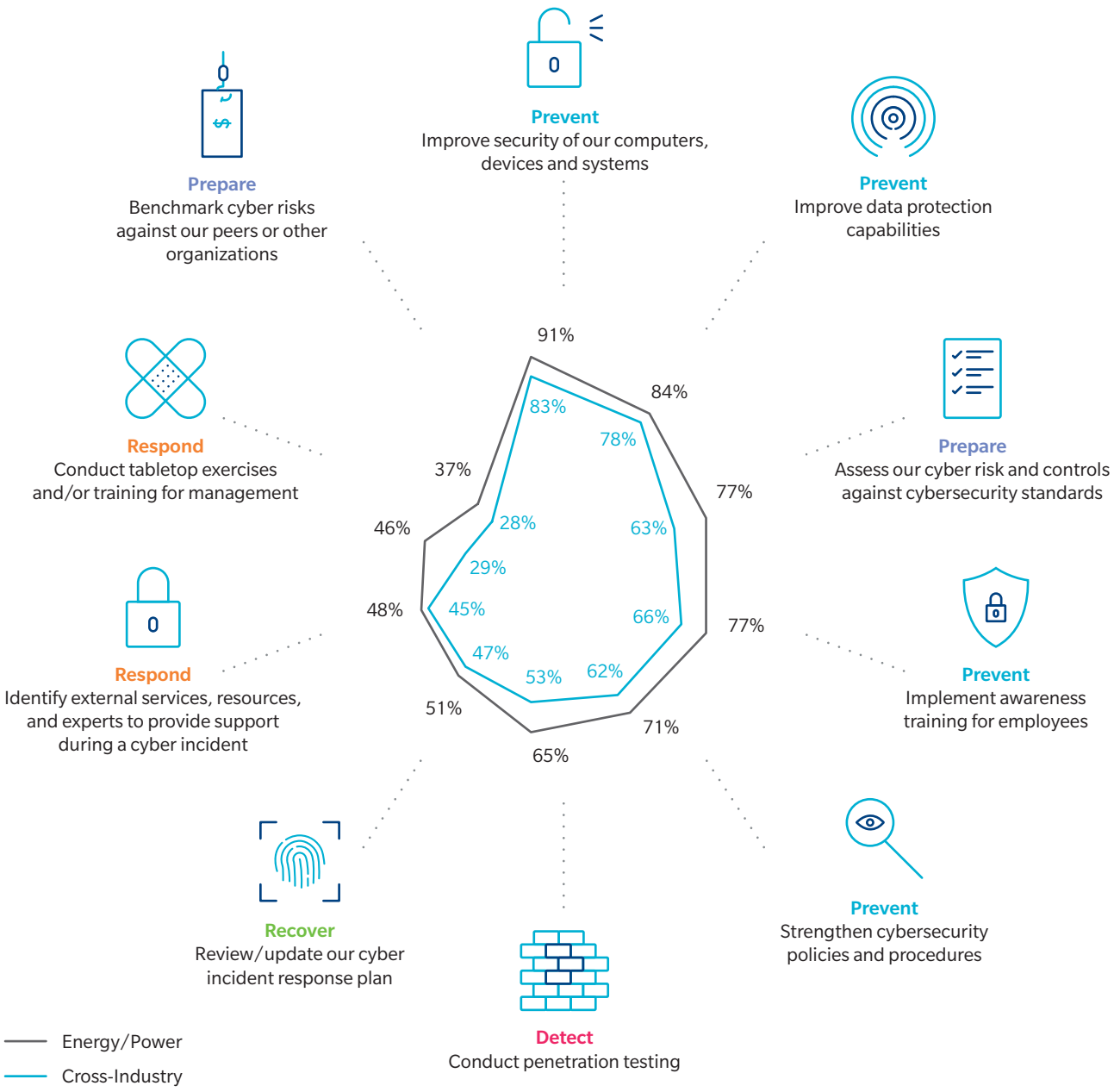
There is opportunity for improvement in ensuring that cyber risk management is truly "risk-driven", with a top-down organization-wide responsibility that distributes across departments. This is underscored by 20 percent of E/P sector respondents who have flagged a lack of clarity about the primary organizational owner of cyber risk management as a key barrier to effective cyber risk management.

Processes encompass the (formal and informal) procedures or protocols that guide actions of employees. Positively, the E/P sector has taken considerably more proactive actions on cyber risk compared to other industries in general, though these actions are still largely centered on basic preparation and prevention (Exhibit 5). For instance, 91 percent of E/P organizations have made improvements in hardware security, 84 percent in data protection capabilities, 77 percent implemented awareness training, and 71 percent strengthened their cybersecurity policies and procedures.

Over 75 percent of the E/P organizations have assessed their cyber risks and controls against cybersecurity standards in the past 12 to 24 months (Exhibit 5). In fact, E/P organizations have prioritized the number and types of internal (86 percent) and external (74 percent) IT vulnerabilities as topmost crucial considerations during their cyber risk assessment/measurement.[XVI]

Copyright © 2020 Marsh & McLennan Companies

EXHIBIT 5: TOP 10 CYBER RISK-RELATED ACTIONS TAKEN BY ENERGY/POWER (E/P) ORGANIZATIONS IN THE PAST 12–24 MONTHS



Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey; Marsh & McLennan Advantage Insights analysis; NIST cybersecurity framework

Cyber risk quantification is an essential building block of internal risk diagnostic and cyber risk assessment. It provides both the IT and non-IT groups of stakeholders with a common baseline language to understand their cyber risk exposure and prioritize the appropriate response strategies that maximize their investments. Unfortunately, risk quantification has largely been overlooked as an effective method to measure cyber risk exposures—only 36 percent of the E/P respondents said their organizations measure their cyber risk exposure quantitatively (Exhibit 6a). A significant proportion still do so qualitatively (47 percent) or have no method to measure (16 percent) – of which, one-third cited the **lack of data** to measure and model cyber risks effectively.

EXHIBIT 6A: ENERGY/POWER (E/P) SECTOR'S CURRENT STATE OF CYBER RISK MEASUREMENT

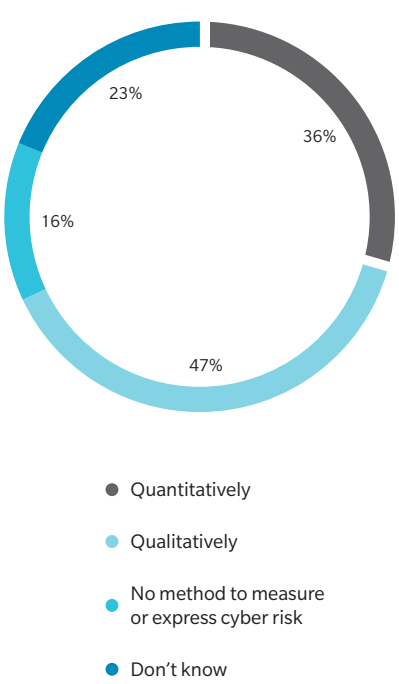
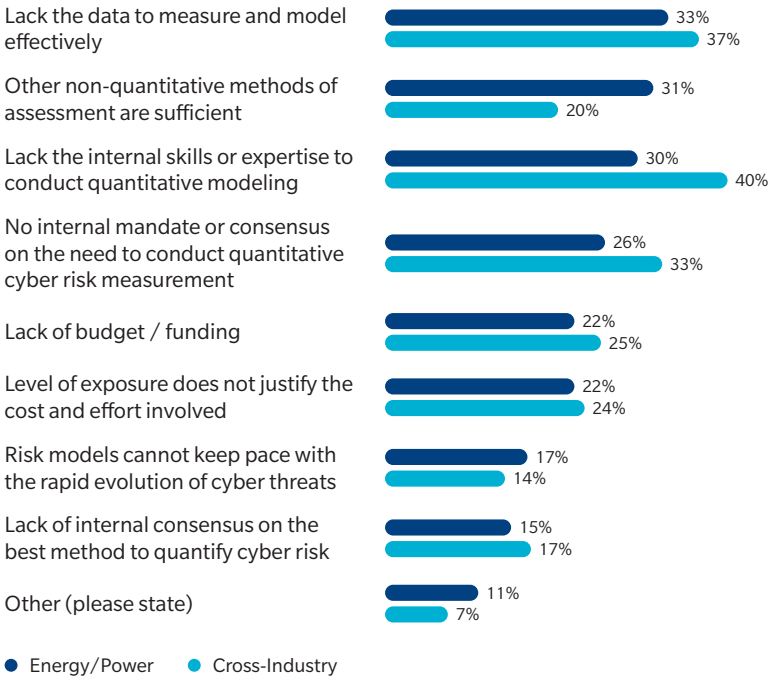


EXHIBIT 6B: **AMONG THOSE WHO DO NOT MEASURE QUANTITATIVELY,** THEIR REASONS FOR NOT DOING SO



Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey

WHY IS THERE A LACK OF DATA TO MEASURE AND MODEL CYBER RISK EXPOSURE EFFECTIVELY?

The trends of decarbonization and decentralization of Energy/Power (E/P) sector have seen significant growth in smaller scale distributed generation (such as wind, solar and combined head and power) and distributed networks which link transmission network to most homes and businesses at a lower and safer voltage. These distributed networks are not operated by national grids and have lesser visibility and monitoring capabilities than transmission networks. [XVII] *Therefore, while data exist, the national grid and other decentralized E/P organizations have lesser ability to access them within the increasingly decentralized environment.*

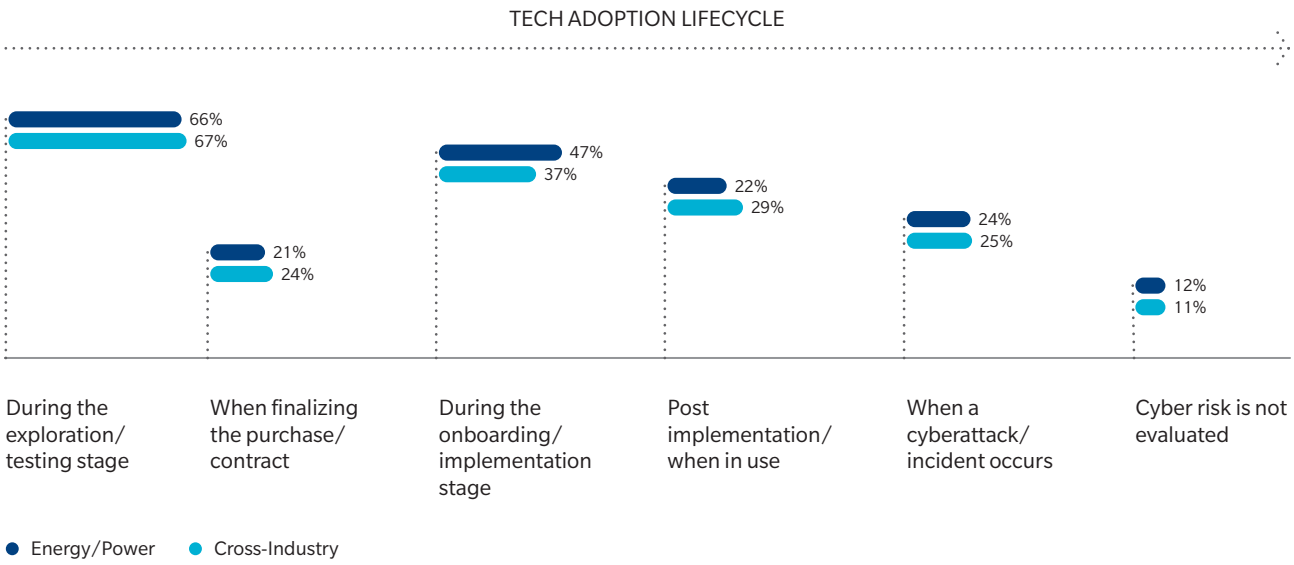
Copyright © 2020 Marsh & McLennan Companies

Cyber risk quantification is the sum of cyber risks in all parts of an ecosystem. As operational, information technology, and communications systems become more interconnected within organizations and across the energy supply chain, E/P players might be able quantify their own cyber risks but can find it increasingly challenging to arrive at the full picture of their cyber risk exposure.

Legacy technology and interdependent systems are key characteristics of the Energy/Power (E/P) sector. Two different types of technologies co-exist in today's E/P systems—legacy (older technologies with a lifespan of 30–60 years, designed before cybersecurity concerns came about)[6] and modern (state-of-the-art digitalization and smart devices) systems. The interdependence between legacy and modern systems, coupled with real-time business requirements and the risk of cascading effects, all demand E/P organizations to treat security enhancement as a major part of their business development.

For instance, the upgrading or strengthening of the sector's core assets (ICS) is perceived to pose much higher cyber risks to the E/P sector than other industries in general—27 percent for the E/P sector, versus a cross-industry average of 10 percent (Exhibit 2). In the process of digitalizing ICS, key cyber implications—such as unsupported (or prohibitively difficult and expensive patches for) software/firmware, slow response time to the availability of patching/updating older systems, and weak authentication/encryption, especially for the hardware-based systems—are often overlooked, resulting in heightened cyber risks.[XVIII]

EXHIBIT 7: STAGES OF NEW TECHNOLOGIES ADOPTION/IMPLEMENTATION WHERE ORGANIZATIONS EVALUATE THEIR CYBER RISKS



Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey; Marsh & McLennan Advantage Insights analysis

6 European Parliament, 2019. Cybersecurity of critical energy infrastructure

A cybersecurity firm specializing in ICS has found major security gaps such as plain-text passwords, direct connections to the Internet, and weak anti-virus protections in the OT/ ICS space.[XIX]

Similarly, in the course of new technology adoption, the evaluation of cyber risks should be an end-to-end one with the understanding that cyber risk is a systemic business risk. Currently, a majority of organizations assess their cyber risks during the initial phase of the project. Almost two-thirds of organizations across all industries do so during the testing phase (Exhibit 7), and almost half of the E/P respondents (47 percent) note that their organizations also do so during the onboarding/implementation stage.

While organizations are at varying levels of maturity in terms of risk assessment capabilities, and at different stages of digital transformation, it is imperative to continually assess cyber risks throughout all key stages on an ongoing basis – from the exploration phase until post implementation. Organizations that applied additional security hardening measures to new technologies, or conducted due diligence on vendors, had 2 to 3 times more confidence in cyber resilience than their peers.[XX]

This can potentially also be facilitated with a cyber or security team being included in the entire process, including key decision-making processes in new technology projects – and not only as an after-thought or pre-signoff. It is crucial to move towards a more "risk-driven" approach by embedding cyber risk management as part of an overall risk management strategy and processes from beginning to end.

In response to all the internal cyber threat vectors, a robust and pervasive cyber resilient culture is essential. This will ensure that cyber resilience is instilled in each person in the organization, for all (core IT security and technology) process execution, amid the use of all old and new technologies.

Education is key to building a strong cyber risk management culture. For an organization to be truly resilient in this evolving cyber threat landscape, all employees should be invested in the organization's cyber defense strategy. Building a cyber risk management culture is an ongoing journey where organizations educate their members and embed cyber awareness as part of the employees' DNA – for one to behave in a cyber resilient manner when no one else is looking. A recent

EXHIBIT 8: A STRONG CYBER CULTURE – CYBER RESILIENCE BUILDING DRIVEN BY SENIOR MANAGEMENT[XXII]

The board of a Spanish electric utility company recognized that being at the forefront of digital transformation required strong cybersecurity and resilience capabilities. However, it also recognized that privacy and critical infrastructure protection regulations are not enough to ensure compliance with all IT security.

In response, a company-wide cybersecurity risk policy to promote a strong cybersecurity culture was approved.

To lead this cultural change, a global cybersecurity committee was also established. The goal was to promote cybersecurity and resilience by design and default throughout the organization. Most importantly, it aimed to embed the idea that cybersecurity is everyone's responsibility, going beyond individual organizations.

This was accomplished through strong leadership involvement – the global Chief Information Security Officers had emphasized on collaboration throughout and was responsible for independent oversight and adequate cyber trainings for the board, senior management, and all employees.

Copyright © 2020 Marsh & McLennan Companies

publication by Oliver Wyman, Building a Cyber-Resilient Culture, highlights a best practice towards structurally building a cyber-resilient culture, based on industry experience.[XXI]

Education can be imparted through various channels such as awareness campaigns, trainings, certifications, mock drills, and even rewards and consequences programs. What sets leading players apart, however, is having strong executive buy-in, the involvement of senior management (see Exhibit 8) and the presence of two-way communication (between employees and the core teams behind cyber initiatives).

External cyber threat vectors are as critical as internal ones. With digitalization, key external cyber sources stem from the growing **supply chain**, including trusted partners, and the evolving **regulatory landscape**.

Supply chain risk (or third-party/vendor cyber risk) is growing exponentially. As Energy/Power (E/P) infrastructure rapidly modernizes, and pressure mounts to move operations to the cloud, players become more reliant on and integrated into third-party operations. An increasing number of systems are interconnected across the supply chain, with interdependencies across the supply chain—including other critical and dependent key sectors such as telecommunications, maritime, healthcare, and sewage facilities—and this interconnectivity will only continue to increase. The implicit risks are amplified by the internet-based relationships within the E/P sector, and between suppliers and consumers.

This interdependency heightens the challenge of maintaining cyber resilience for all organizations in the supply chain. Organizations that now operate in the complex supply chains are exposed to

This expansive supply chain or "hyperconnectivity also means that your risk is now my risk and that an attack on the 'weakest link' can have consequences affecting us all", former US Secretary of Homeland Security, Kirstjen Nielsen, recently said.[XXIII] In today's environment, businesses need to not only secure their "house" but also cooperate along the entire supply chain to ensure that the whole "neighborhood" is secured.

EXHIBIT 9A: PERCEPTION OF THE SOURCE OF CYBER RISKS IN SUPPLY CHAIN

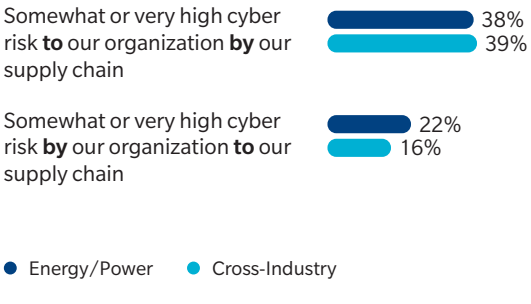


EXHIBIT 9B: ORGANIZATIONS THAT ARE CONFIDENT ABOUT PREVENTING CYBER RISKS FROM RESPECTIVE GROUPS OF 3RD PARTIES

Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey; Marsh & McLennan Advantage Insights analysis

weaknesses in other companies, who may not have the same focus on cyber risk management. Given these factors, business leaders increasingly recognize that cyber is a risk that can be understood, measured and managed – but not completely eliminated. According to the Marsh Microsoft 2019 Global Cyber Risk Perception Survey, partners in the interconnected supply chains of the E/P sector were faced with a bigger threat from cyber risks than perceived by their own organizations according to 38 percent of E/P sector respondents (see Exhibit 9a).

A closer look at the ecosystem reveals that cyber risks stemming from mergers and acquisitions (M&A) and external consultants are more challenging in the E/P sector (49 percent and 64 percent respectively) than all industries in general (44 percent and 53 percent respectively) (Exhibit 9b). While M&A activity is accelerating in the E/P sector, especially for oil and gas companies, cybersecurity forms a critical part of the due diligence in the deals and should be done throughout the M&A life cycle. This includes appropriate security or privacy counsel over general consumer privacy and data security laws, and country-specific standards, such as the Federal Energy Regulatory Commission's Critical Infrastructure Protection Reliability Standards in the US.[XXIV]

In general, E/P sector respondents are more likely to say that their organizations are "hands-on" in implementing cyber risk management measures than in expecting their suppliers to implement them (see Exhibit 10). Almost half of the E/P organizations have taken supply chain (or third-party) cyber risks into their own hands. In the process of adopting new technologies, 44 percent of the E/P sector respondents highlighted that their organizations have never accepted system security claims

EXHIBIT 10: DISPARITY BETWEEN WHAT MEASURES ENERGY/POWER (E/P) ORGANIZATIONS EXPECT OF THEMSELVES VERSUS WHAT THEY EXPECT FROM THIRD-PARTIES

Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey; Marsh & McLennan Advantage Insights analysis

Copyright © 2020 Marsh & McLennan Companies

for the new technologies or assumed security protections that have been built-in, and instead chose to perform their own due diligence.[XXV]

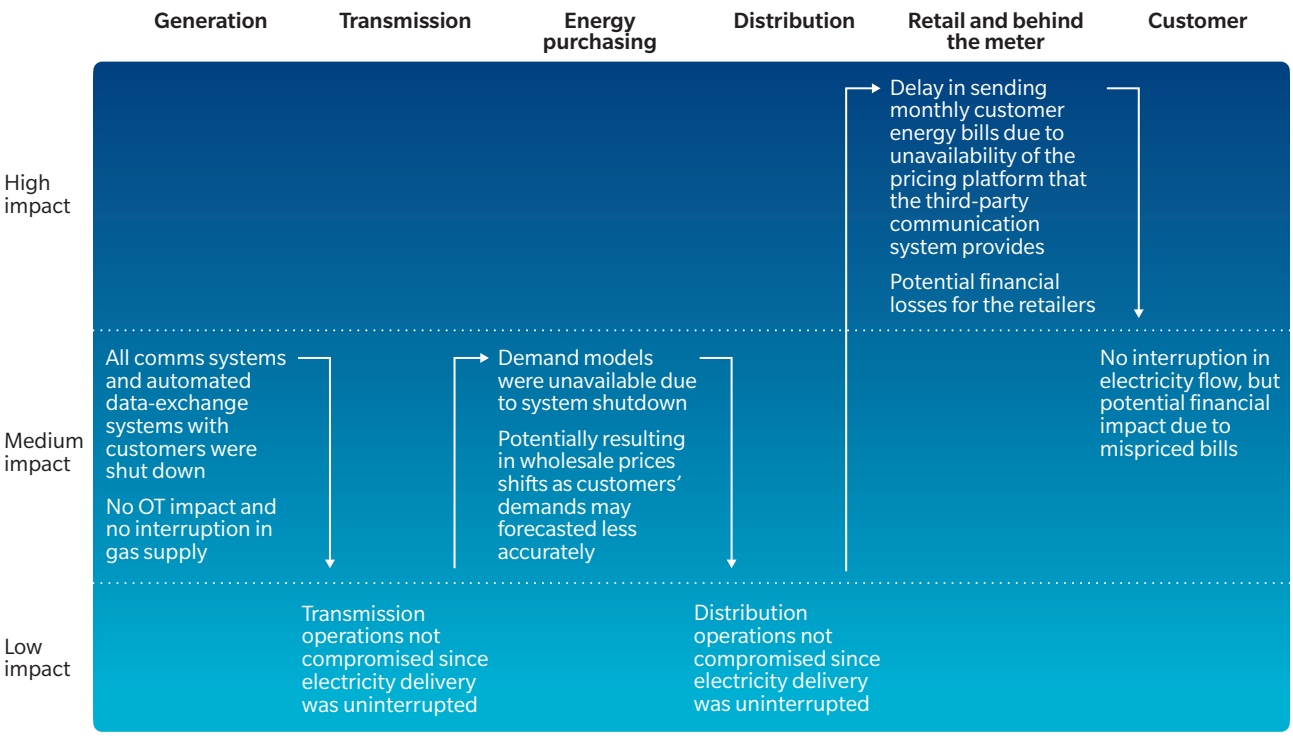
This non-reliance on external stakeholders is prudent, given the sector's criticality of operational efficiency and the increasingly complex Directors' and Officers' liability lawsuits, even years following cyberattacks.[XXVI] Organizations can ill-afford to fully outsource cyber risks and should prioritize vendor risk management as the ecosystem expands. Even those that think they are vigilant in managing their own systems are vulnerable if just one of their other partners is penetrated.

Two high-profile incidents are timely reminders – cyberattacks in Ukraine and Saudi Arabia both leveraged supply chain vulnerabilities to impact operations at two energy sector organizations. Similarly, a 2018 report by the US Department of Homeland Security also revealed that hackers have begun using third-party vendors as "staging-targets" to gain access to hundreds of utility ICS in the US.[XXVII]

In any case, when a power grid or energy infrastructure goes down, it is not just the lights that go out. The impact range from financial instability/potential markets crash, reputation loss, property damage, societal collapse such as disruption/injuries/loss of life, public safety, and environmental liabilities – all of which are not likely to affect stakeholders within the ecosystem equally (see Exhibit 11).

From a policy and legislative perspective there has been a significant increase in the regulation of data privacy and cybersecurity globally and across all industries, with a primary focus on data protection and supply chain security. In the E/P sector in particular,

EXHIBIT 11: THE CYBER ECOSYSTEM – UNEQUAL IMPACT OF A CYBERATTACK THROUGHOUT THE ECOSYSTEM OF A US ELECTRONIC COMMUNICATIONS SYSTEM PROVIDER'S PLATFORM[XXIX]



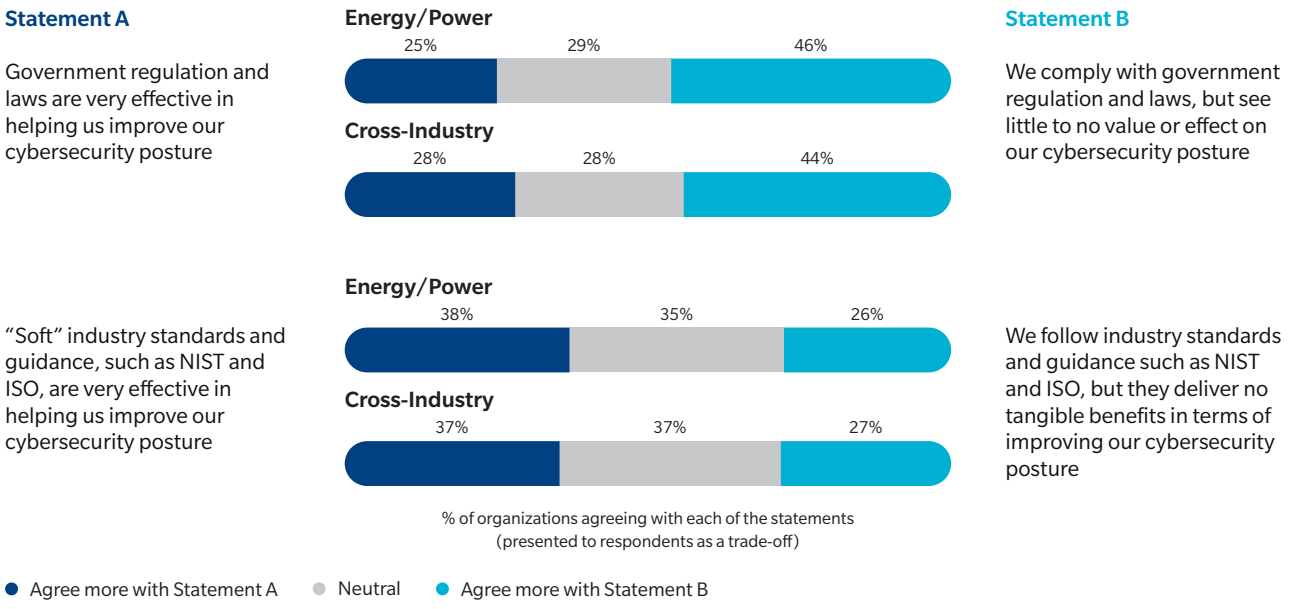
the regulations address accountability issues or establish standards or requirements as a baseline for organizations to address cybersecurity appropriately. As such, E/P players need to watchfully position their cyber posture with regulators' expectations.

For instance, Energy/Power (E/P) organizations in the EU are subject to the Network and Information System Directive which requires operators of essential services to increase security of network and information systems, including compliance through supply chain.[XVIII] In the US, mandatory enforceable energy market regulations such as the North American Electric Reliability Corporation have been continuously developed and have included Critical Infrastructure Protection standards to include supply chain protections.

When compared to other industries, the E/P sector reasonably expects the greatest threats/concerns in both regulations and cyber, often at the crossroad of the two. **Regulation and cyber threats** were highlighted as the topmost concerns in the E/P sector (19 percent and 18 percent respectively), while other industries in the survey felt that economic uncertainty (15 percent) is a bigger threat than regulation (9 percent). While regulations continue to evolve with the complexity of the sector's fast-paced growth and digitalization, E/P organizations stand to benefit from clearer regulations and standards.

In terms of what type of standards work (or not) for the E/P sector, there are mixed perceptions on the effectiveness of "hard" government regulations and laws in helping organizations improve their cybersecurity posture across all industries (see Exhibit 12). Organizations tend to see limited effectiveness in government regulation of cyber risk, with the clear exception of nation-state attacks (see External Challenge, Page 7).

EXHIBIT 12: ACROSS INDUSTRIES, ORGANIZATIONS' PERSPECTIVES ON THE VALUE OF REGULATIONS AND STANDARDS



Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey; Marsh & McLennan Advantage Insights analysis

Copyright © 2020 Marsh & McLennan Companies

Like other industries, the E/P sector complies with government regulations and laws despite not fully agreeing on the merit of their cybersecurity posture—46 percent see little to no value, similar to the cross-industry average of 44 percent (Exhibit 12). However, more than half of the survey respondents point out that national or international cybersecurity regulations are essential to encourage cybersecurity best practices and minimize harm to private enterprise.[xxx] All industries—including the E/P sector—were more welcoming of "soft" industry standards as an effective means to help improve the organization's cybersecurity posture. The softer approach often gives organizations a larger degree of autonomy to evaluate available standards, assess their position, and tailor the approach to fit their business model and constraints.

At the end of the day, while regulations are essential, organizations need to bear in mind that **they can comply with all of today's standards and still be vulnerable to cyberattacks** if they fail to strategically take cyber risk management in their own hands.

In response to the many sources of cyber risks, a comprehensive cyber risk management plan, including cyber insurance, can help organizations reduce the potential (financial and non-financial) impacts stemming from physical or operational systems damages, bodily injury, business interruption, loss of financial or personal information, and other downstream effects.

In particular, **reputational risk** is deeply connected to cyber (and organizational) risks. In the event of a cyber breach, adverse reporting in the media can result in long-term reputational and financial damage. Against the backdrop of the global energy transition (and political activism, to some extent), reputational risk is already a concern as a growing number of players seek to

EXHIBIT 13: ENERGY/POWER (E/P) ORGANIZATIONS' STATUS WITH REGARDS TO CYBER INSURANCE

Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey; Marsh & McLennan Advantage Insights analysis

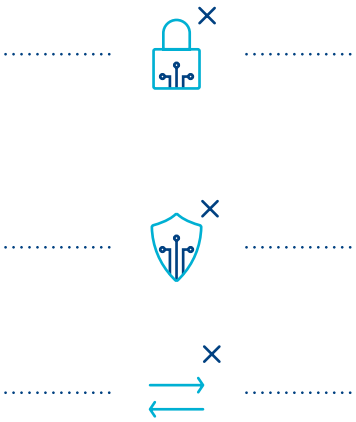
delicately find a balance between public and shareholders' expectations while they move from the less favored fossil fuels to more publicly appealing renewables.[XXXI]

A data breach insurance policy in the Energy/Power (E/P) sector averages around $15,000 for $1 million of coverage globally. This relatively hefty premium is largely due to industry analysts' predictions of the extensive cyber implications – for instance, attacks on 50 generators in the northeastern part of the US alone can affect 93 million people.[XXXII]

An insurance policy that includes coverage for physical damages will typically cost much more.

It is worrying that only 13 percent of surveyed E/P organizations indicate that existing cyber insurance solutions meet their organizations' needs.[XXXIII] Only 41 percent have a cyber insurance policy in place and 37 percent do not have any plans to purchase a cyber insurance policy in the near future (see Exhibit 13). Overall, businesses continue to allocate capital more quickly towards cybersecurity technology than risk transfer solutions, reflecting a possible lack of "faith" in such policies among the IT/information security roles at these organizations, or a possible preference for deterrence over recovery for loss.

EXHIBIT 14: "**SILENT" CYBER**[7] GETTING LOUD – ENERGY/POWER (E/P) ORGANIZATIONS TO BE HEAVILY IMPACTED FROM EXCLUDED CYBER COVERAGE



To complicate the existing coverage gap, "smart" E/P organizations are heavily reliant on IT, OT, IoT, PLC's, SCADA, and ICS, and insurers have started to exclude coverages for cyber events in traditional property and casualty policies. The move was mostly driven by the Petya/NotPetya cyberattacks in 2017, which affected global business operations across industries, and reinforced the businesses' dependencies on interconnected digital infrastructure. While the initial costs of this cyber crisis were not significant to insurers, the final amount—including tail liabilities—is in excess of $3 billion in aggregated losses.

In January 2019, Allianz imposed the use of affirmative and non-affirmative endorsements across all its lines of insurance. Imposing of endorsements is meant to specifically exclude certain (previously not specified) cyber coverage and is one of the responses to "silent cyber". In July 2019, Lloyds announced that it would follow suit, starting January 2020, in drawing a clear demarcation line on whether cyber exposures are included or excluded.[XXXIV]

From a risk transfer perspective, this is a fundamental change to any insurance program. Coverage that was arguably provided under the ambiguity of "silent cyber" is now restricted, a legacy from the outdated insurance past to be watched.

7 **Silent Cyber** refers to potential cyber-related losses stemming from traditional property and liability policies that were not specifically designed to cover cyber risk.

Copyright © 2020 Marsh & McLennan Companies

HOW TO WIN

STRATEGIES TO INCREASE CYBER RESILIENCE AMID DIGITALIZATION

With the embrace of transformative technologies and a long-term move towards cleaner energy sources, the digitalization-decentralization transition is here to stay. Most players in the Energy/Power (E/P) sector have already shifted from mechanical and centralized assets to new operational-plus-digitalized systems that will increasingly expose each player in the ecosystem to cyber risks.

In order to win this digital-cyber challenge, E/P organizations should advance their cyber resilience by pursuing a range of cyber strategies and building up a portfolio of cyber capabilities. The winning game plan should encompass a range of solutions, starting from a holistic cyber risk assessment, to the continual strengthening of internal cyber culture, building and stress-testing of recovery planning, being part of a reliable coalition in building dynamic resilience, simultaneously seeking of additional risk management and transfer strategies, and more.

The MMC Cyber Handbook 2020 brings together the latest perspectives on how to take action in the face of growing cyber complexity and uncertainty.

To take this a step further, organizations can use transformative technologies to their advantage such as embedding blockchain tracking components throughout their supply chain; deploying AI-led cyber solutions to potentially detect abnormal activities before they escalate into a crisis; and leveraging on analytics and visualization to audit real-time cyber risk profile.

Winning organizations should focus equally on both cyber risk management as well as innovating with technologies; it will be prudent for organizations to consider embedding cyber throughout their digitalization journey, or risk favoring one at the expense of the other. Like parallel tracks on a railroad, cyber transformation needs to happen alongside digital transformation throughout the E/P sector's digitalization journey.

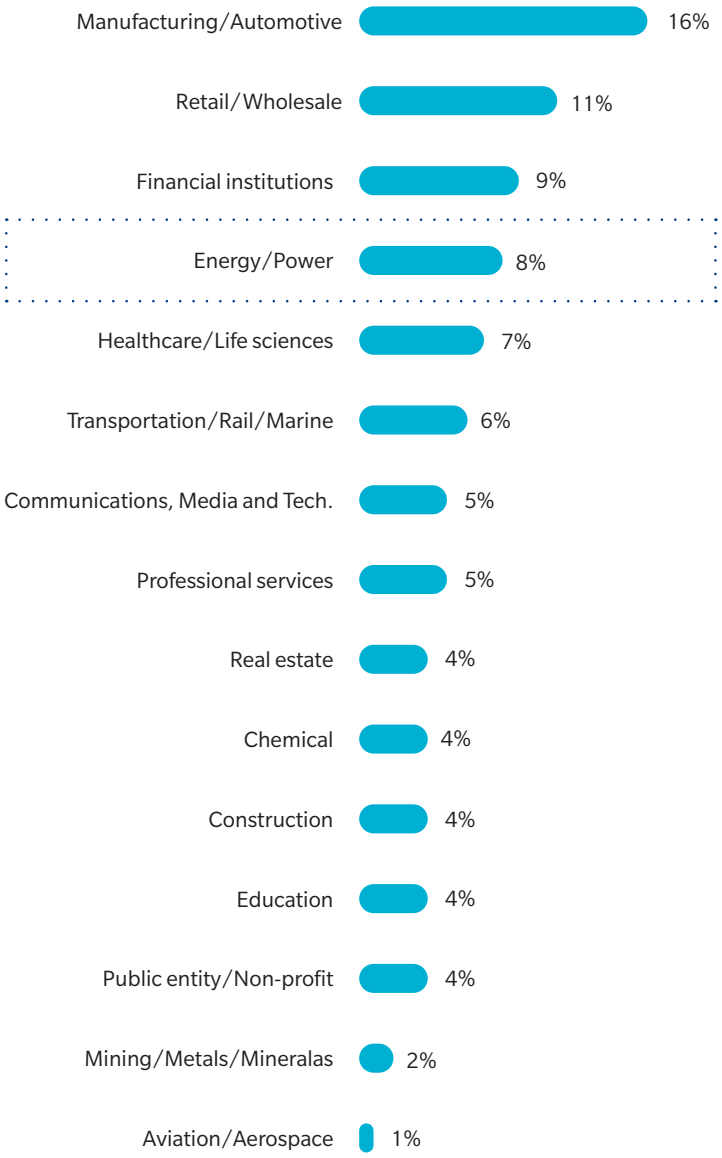
ABOUT THE MARSH MICROSOFT 2019 GLOBAL CYBER RISK PERCEPTION SURVEY

This paper is based largely on findings from the Marsh Microsoft 2019 Global Cyber Risk Perception Survey, administered between February and March 2019.

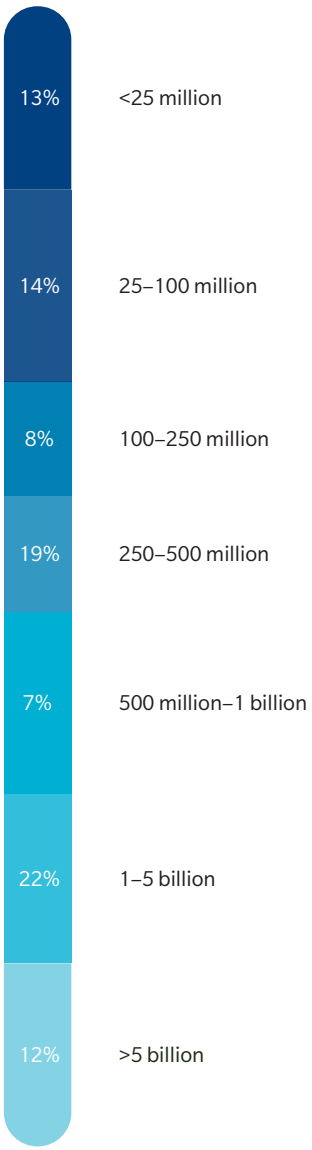
More than 1,500 business leaders participated in the survey, representing a wide range of key functions, including risk management, information technology/information security, finance, legal/compliance, C-suite officers, and boards of directors.

Of the 1,512 respondents surveyed, 121 (8 percent) were from the Energy/Power (E/P) industry, with businesses across various regions and from organizations with at least $25 million in annual revenue.

Industry breakdown of all survey respondents (N=1512)



Surveyed E/P organizations' annual revenue in $ (N=121)



Copyright © 2020 Marsh & McLennan Companies

ACKNOWLEDGEMENTS

AUTHORS

WOLFRAM HEDRICH
Partner, Finance & Risk Practice, Oliver Wyman
wolfram.hedrich@oliverwyman.com

LESLIE CHACKO
Managing Director, Marsh & McLennan Advantage Solutions
leslie.chacko@oliverwyman.com

RACHEL LAM
Research Analyst, Marsh & McLennan Advantage Insights
rachel.lam@oliverwyman.com

MARSH & MCLENNAN COMPANIES CONTRIBUTORS

MARSH & MCLENNAN ADVANTAGE INSIGHTS
Lucy Nottingham, Blair Chalmers, James Sutherland, Jaclyn Yeo, Lily Phan

MARSH
Thomas Reagan, Reid Sawyer, Kelly Butler, Soo Jono, Naureen Rasul, Linden Reko

OLIVER WYMAN
Paul Mee, Mark James, Abhimanyu Bhuchar

BIBLIOGRAPHY

I. Dagoumas A (2019). Assessing the Impact of Cybersecurity Attacks on Power Systems. Energies.

II. International Energy Agency (2018). World Energy Investment 2018. Retrieved from https://webstore.iea.org/world-energy-investment-2018

III. World Economic Forum (2019). Global Action Needed To Protect Electricity Grids From Growing Threats. Forbes. Retrieved from https://www.forbes.com/sites/worldeconomicforum/2019/04/29/global-action-needed-to-protect-electricity-grids-from-growing-threats/#94f1f3a2d28f

IV. ENISA (2013). Smart Grid Threat Landscape and Good Practice Guide. Retrieved from https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide/at_download/fullReport

V. Marsh and Microsoft (2019). Global Cyber Risk Perception Survey Report 2019. Retrieved from https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html

VI. Swiss Re (2017). Cyber: getting to grips with a complex risk. Retrieved from https://www.swissre.com/dam/jcr:995517ee-27cd-4aae-b4b1-44fb862af25e/sigma1_2017_en.pdf

VII. Protiviti (2019). Taking RPA to the Next Level. Retrieved from https://www.protiviti.com/sites/default/files/2019-global-rpa-survey-protiviti.pdf

VIII. Marsh and Microsoft (2019). Global Cyber Risk Perception Survey Report 2019. Retrieved from https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html

IX. Davis D B (2019). ISTR 2019: Targeted Attack Groups Increase Despite Growing Risk of Exposure. Symantec. Retrieved from https://www.symantec.com/blogs/feature-stories/istr-2019-targeted-attack-groups-increase-despite-growing-risk-exposure

X. Deloitte (2019). Combatting Rising Cyber Risk in the Power Sector. The Wall Street Journal. Retrieved from https://deloitte.wsj.com/riskandcompliance/2019/04/07/combatting-rising-cyber-risk-in-the-power-sector/

XI. Butler N (2018). Why cyber attack is the biggest risk for energy companies. Financial Times. Retrieved from https://www.ft.com/content/109350ea-c6f2-11e8-ba8f-ee390057b8c9

XII. Knake R K (2017). A Cyberattack on the U.S. Power Grid. Council on Foreign Relations. Retrieved from https://www.cfr.org/report/cyberattack-us-power-grid.

XIII. The National Academies Press (2017). The Many Causes of Grid Failure. Retrieved from https://www.nap.edu/read/24836/chapter/5

XIV. Unearthed (2019). Dragonfly: How Britain's energy sector was hacked. Retrieved from https://unearthed.greenpeace.org/2018/06/11/dragonfly-uk-energy-hacker-cybersecurity/

XV. F-Secure (2019). The State of the Station. Retrieved from https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/15105531/F-Secure_energy_report.pdf

XVI. Marsh and Microsoft (2019). Global Cyber Risk Perception Survey Report 2019. Retrieved from https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html

XVII. Power Technology (2018). Will data shortages cause the blackouts of the future? Retrieved from https://www.power-technology.com/digital-disruption/big-data/will-data-shortages-cause-blackouts-future/

XVIII. Hoyt M (2018). The Cyber Threat To Industrial Controls Systems. Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/04/16/the-cyber-threat-to-industrial-controls-systems/#3a6519654d68

XIX. JLT (2019). Industrial and Utility Companies Targeted by Cyber Attacks. Retrieved from https://www.jlt.com/insurance-risk/cyber-insurance/insights/industrial-and-utility-companies-targeted-by-cyberattacks

XX. Marsh and Microsoft (2019). Global Cyber Risk Perception Survey Report 2019. Retrieved from https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html

XXI. Oliver Wyman (2019). Building a Cyber-Resilient Culture. Retrieved from https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/October/building-a-cyber-resilient-culture.pdf

XXII. World Economic Forum (2018). Managing risk in the energy sector's cyber supply chain. Retrieved from https://www.weforum.org/agenda/2018/06/managing-risk-in-the-energy-sector-s-cyber-supply-chain/

XXIII. Kahla C (2019). Cyber Resilience Summit – Why it's time to boost cyber resilience. The South African. Retrieved from https://www.thesouthafrican.com/tech/cyber-resilience-summit-why-cyber-resilience-important/

XXIV. Harroch R D, Martin J, & Smith R V (2018). Data Privacy and Cybersecurity Issues In Mergers And Acquisitions. Forbes. Retrieved from https://www.forbes.com/sites/allbusiness/2018/11/11/data-privacy-cybersecurity-mergers-and-acquisitions/#3defa46272ba

XXV. Marsh and Microsoft (2019). Global Cyber Risk Perception Survey Report 2019. Retrieved from https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html

XXVI. The Insurer (2019). FedEx sued in first NotPetya-related D&O lawsuit. Retrieved from https://www.theinsurer.com/news/fedex-sued-in-first-notpetya-related-dando-lawsuit/4198.article

XXVII. Smith R (2018). Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110

XXVIII. World Economic Forum (2018). Managing risk in the energy sector's cyber supply chain. Retrieved from https://www.weforum.org/agenda/2018/06/managing-risk-in-the-energy-sector-s-cyber-supply-chain/

XXIX. Smart Energy International (2018). Cybersecurity laws you should know. Retrieved from https://www.smart-energy.com/industry-sectors/cybersecurity/cybersecurity-legislation-should-know/

XXX. Marsh and Microsoft (2019). Global Cyber Risk Perception Survey Report 2019. Retrieved from https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html

XXXI. Jones J H (2019). Industry must prepare for energy business shift: Marsh-JLT's Clarke. The Insurance Insider. Retrieved from https://www.insuranceinsider.com/articles/128877/industry-must-prepare-for-energy-business-shift-marsh-jlts-clarke

XXXII. Stanford University. 15 Days of Cyber Insurance: Energy sector. Retrieved from https://cyber.stanford.edu/15-days-cyber-insurance-energy-sector

XXXIII. Marsh and Microsoft (2019). Global Cyber Risk Perception Survey Report 2019. Retrieved from https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html

XXXIV. The Insurer (2019). Lloyd's gets tough on silent cyber. Retrieved from https://www.theinsurer.com/news/lloyds-gets-tough-on-silent-cyber/4236.article?utm_medium=email&utm_campaign=Daily%20Breaking%20news%20-%20Premium&utm_content=Daily%20Breaking%20news%20-%20Premium+CID_6737031889723dc38d9416cbcb165136&utm_source=Campaign%20Monitor&utm_term=Lloyds%20gets%20tough%20on%20silent%20cyber

Copyright © 2020 Marsh & McLennan Companies

ABOUT MARSH & MCLENNAN ADVANTAGE INSIGHTS

Marsh & McLennan Advantage Insights uses the unique expertise of our firm and its networks to identify breakthrough perspectives and solutions to society's most complex challenges. Insights plays a critical role in delivering the Marsh & McLennan Advantage—our unique approach to harnessing the collective strength of our businesses to help clients address their greatest risk, strategy and people challenges.

ABOUT MICROSOFT

Microsoft (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more. Microsoft´s Digital Diplomacy team, which partnered with Marsh on this report, combines technical expertise and public policy acumen to develop public policies that improve security and stability of cyberspace, and enable digital transformations of societies around the world.