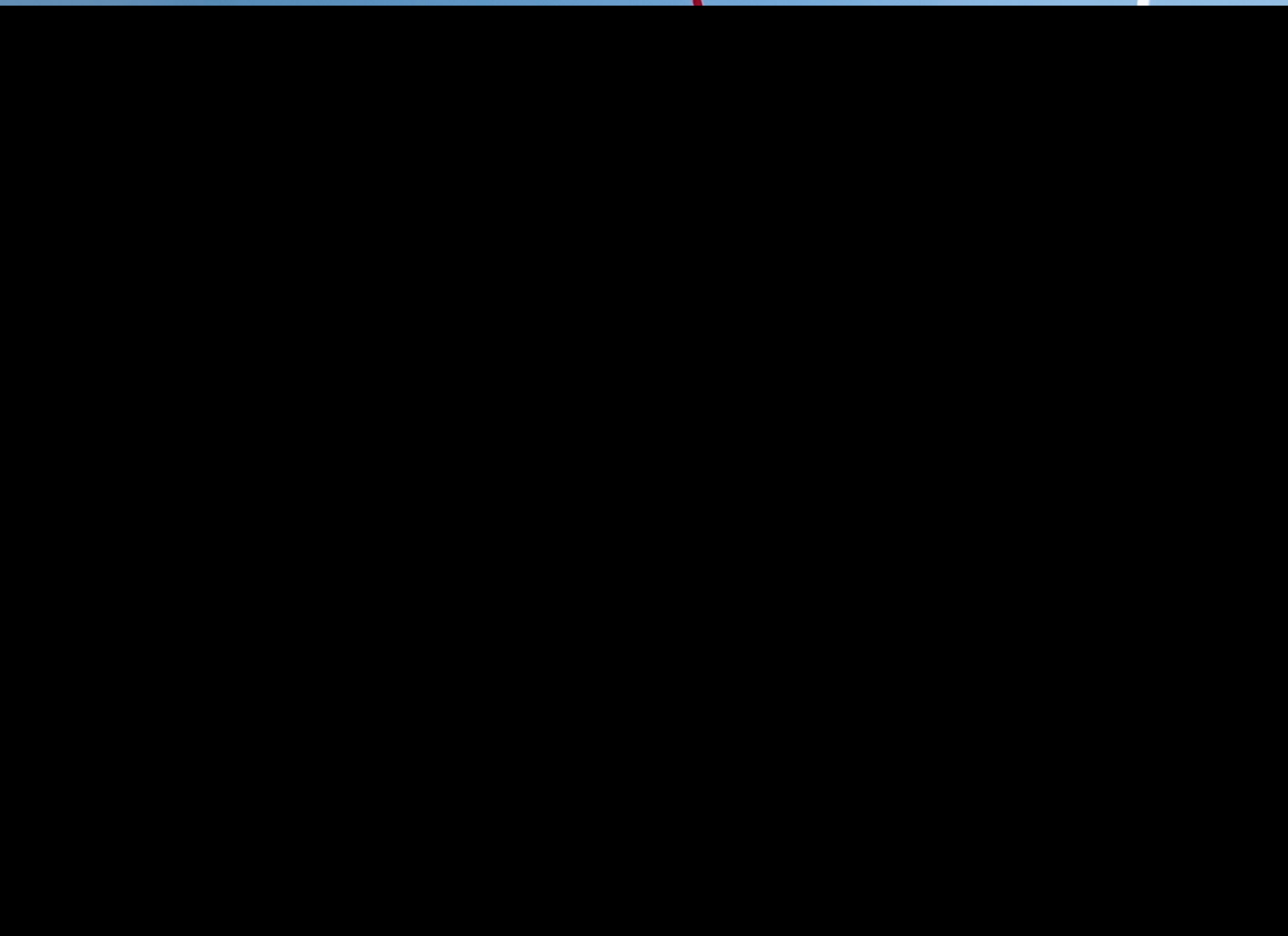


WINNING THE





4

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

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

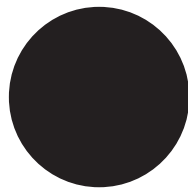
4.2 Increasing exposure to more sophisticated cyber adversaries, complicated by internal and external threat actors

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

21

21.1 Strategies to increase cyber resilience

Strategies to increase cyber resilience in digitalization



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

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

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

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 Energy/Power (E/P) sector, like all other industries, remains optimistic about the potential value and business opportunities that transformative technologies bring. 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, and digital products are so compelling that the E/P sector fares better than the cross-industry averages of 82 percent and 78 percent respectively (Exhibit

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

PERCEIVED CONFIDENCE AMONG ENERGY/POWER ORGANIZATIONS' IN...

•

...mitigating and preventing
cyberattacks

Source: Marsh Microsoft 2019 Global Cyber Risk Perception

2 ~~...~~ 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 ~~...~~, 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 ~~permission~~ ~~explicit~~ permission.

4 Symantec, 2017. Dragonfly: Western energy sector targeted by sophisticated attack group. ~~...~~, 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.

sweeping, nontargeted attacks (elaborated in Exhibit 4). Ransomware poses an equally concerning threat

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). 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

ESSENTIAL STRATEGIES FOR ENERGY AND UTILITIES


[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.

with a top-down organization-wide responsibility that contributes 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

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.



Two different types of technologies co-exist in today's E/P systems—legacy (older technologies with a lifespan of 30 years, designed before cybersecurity concerns came about) 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 1). 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.

2020

critical utility To lea
ing at the cybr
information requirede
and resilience
it also recognize
critical infrastructure
ations are not eno
ensure compliance with all secur

In respons e cybersecurity
risk poli ong
cyber s approved.

publication by Oliver Wyman, [Building a Cyber-Resilient Culture](#), highlights a best practice towards structurally building a cyber-resilient culture, based on industry experience.⁸

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 sources are as critical as internal ones. With digitalization, key external cyber sources stem from the growing digital ecosystem, including trusted partners, and the evolving digital landscape.

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

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

EXHIBIT B: ORGANIZATIONS THAT ARE CONFIDENT ABOUT PREVENTING CYBER RISKS FROM RESPECTIVE GROUPS/PARTIES

- Energy/Power
- Cross-Industry

weaknesses in other companies, who may not have the same focus on cyber risk management. Given these factors, business leaders increasingly recognize that cyber risk 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 chain 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 10). 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 PARTIES

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

for the new technologies or assumed security protections that have been built-in, and instead chose to perform their own due diligence.^{xxv}

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}

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

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.

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.

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

14% Not confident
86% Confident
...that cyber policies will respond to
cost incurred from cyber event



No plan to purchase



Do not plan to renew
current coverage



Plan to renew current
coverage




Plan to purchase in next
12 months

delicately find a balance between public and shareholder expectations while they move from the less favored fossil fuels to more publicly appealing renewables.^{xxi}

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.^{xxii}

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.^{xxiii} 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: "GETTING LOUD" ENERGY/POWER E/P ORGANIZATIONS TO BE HEAVILY IMPACTED FROM EXCLUDED CYBER COVERAGE

	<p>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.</p>
	<p>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.</p>
	<p>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 watched.</p>

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.

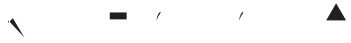


With the embrace of transformative

11/11/2019

11/11/2019

Partner, Finance & Risk Practice, W2na18yman



- I. Dagoumas A (2019). Assessing the Impact of Cybersecurity Attacks on Power System Energies.
- II. International Energy Agency (2018). World Energy Investment 2018. Retrieved from [https:// webstore.iea.org/world-energy-investment-2018](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/content/library/smart-grid-threat-landscape-and-good-practice-guide>

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.