DNV

WHEN TRUST MATTERS

ENERGY CYBER PRIORITY 2023

Closing the gap between awareness and action

& 0xCCCCCCCC) >> 2) | ((a & 0x33333333)
((a & 0xF0F0F0F0) >> 4) | ((a & 0x0F0F0F0F) <<
{a1 = reverseBits(a1);word32 t = revers
word32 b0, b2; b2 = rotlConstant
^ (b0|(~a1))); a1 ^= (b2|(~b0)); }
rotlConstant<16>(c) ^ rotlConstant
a0 ^= c ^ b0; a1 ^
lude "pch.h"
lude "3way.h"
"misc.h"
CE_BEGIN
d(CRYPTO
Way_Tes
/ay::Encry
/ay::Decry
word32 STA
word32 STA
ne word32
& 0xAAAAA
& 0xCCCCC
((a & 0xF0
nu(a0, a1, a
i_gamma_
b0 ^ (a1|(~
heta(a0, a1

ABOUT THIS RESEARCH

This report is published by DNV, the world's leading resource of independent energy experts and technical advisors. It is part of DNV's Cyber Priority research exploring changing attitudes and approaches to cyber security in key industrial sectors.

This 2023 edition is the second report in the series in which we focus on the energy industry (following our 2022 Energy Cyber Priority report), and it is published alongside our first Maritime Cyber Priority report[1].

The research draws on a survey of 601 energy professionals along with a number of in-depth interviews with leaders and experts. The report also draws on additional DNV research where relevant to the findings, as indicated in the narrative and footnotes. It was developed by DNV in partnership with FT Longitude (a Financial Times company).

Fieldwork was conducted between February and March 2023. Survey respondents represent a range of functions within the industry, including those with in-depth knowledge of cyber security along with general managers and C-suite executives.

ACKNOWLEDGEMENTS

We would like to thank the following interviewees for their time and insight:

Jalal Bouhdada, Global Segment Director, Cyber Security, DNV

Muhittin Hasancioglu, independent expert, former CISO at companies including Petronas and Shell

Tor Heiberg, Executive Director IT, Skagerak Energi

Lars Idland, Chief Information Security Officer, Equinor

Adam S. Lee, Vice President and Chief Security Officer, Dominion Energy

Paul Smith, Chief Technology Officer, SCADAfence

Fredrik Torp, Chief Security Officer and Vice President Corporate Security & Resilience, Vattenfall

Swantje Westpfahl, Director, Institute for Security and Safety GmbH

601
energy professionals surveyed

92
countries represented

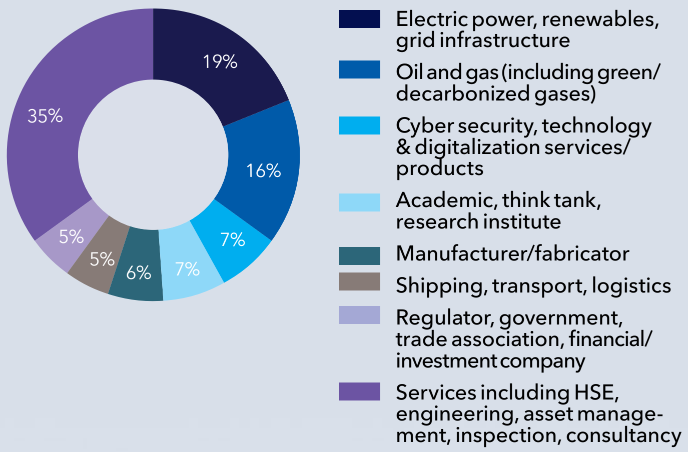
59%
support, develop or operate operational technology

8
in-depth interviews with industry leaders

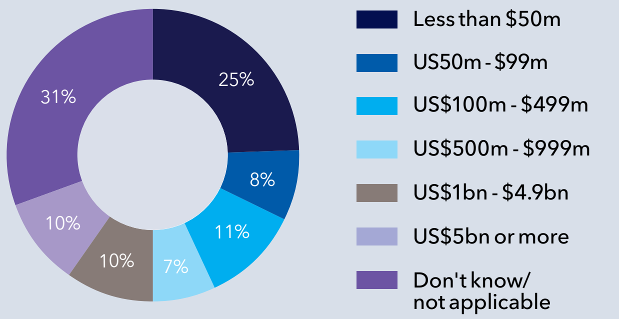
SURVEY DEMOGRAPHICS

We thank our survey respondents from across the energy industry.

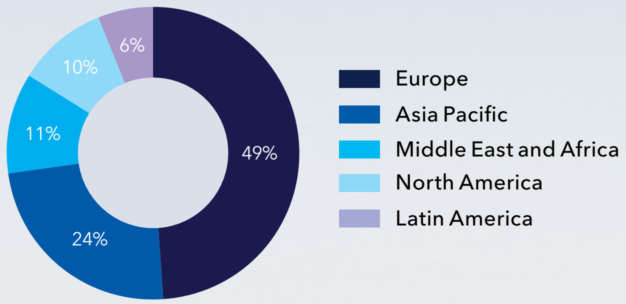
Sector



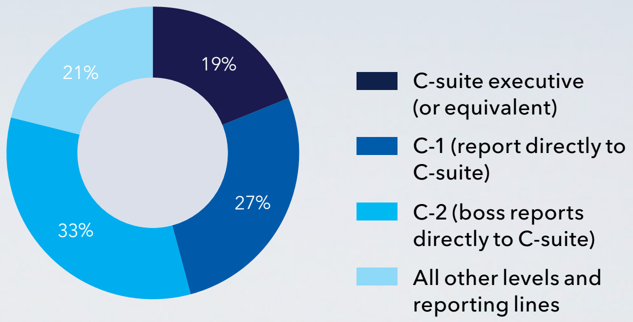
Annual revenue



Region

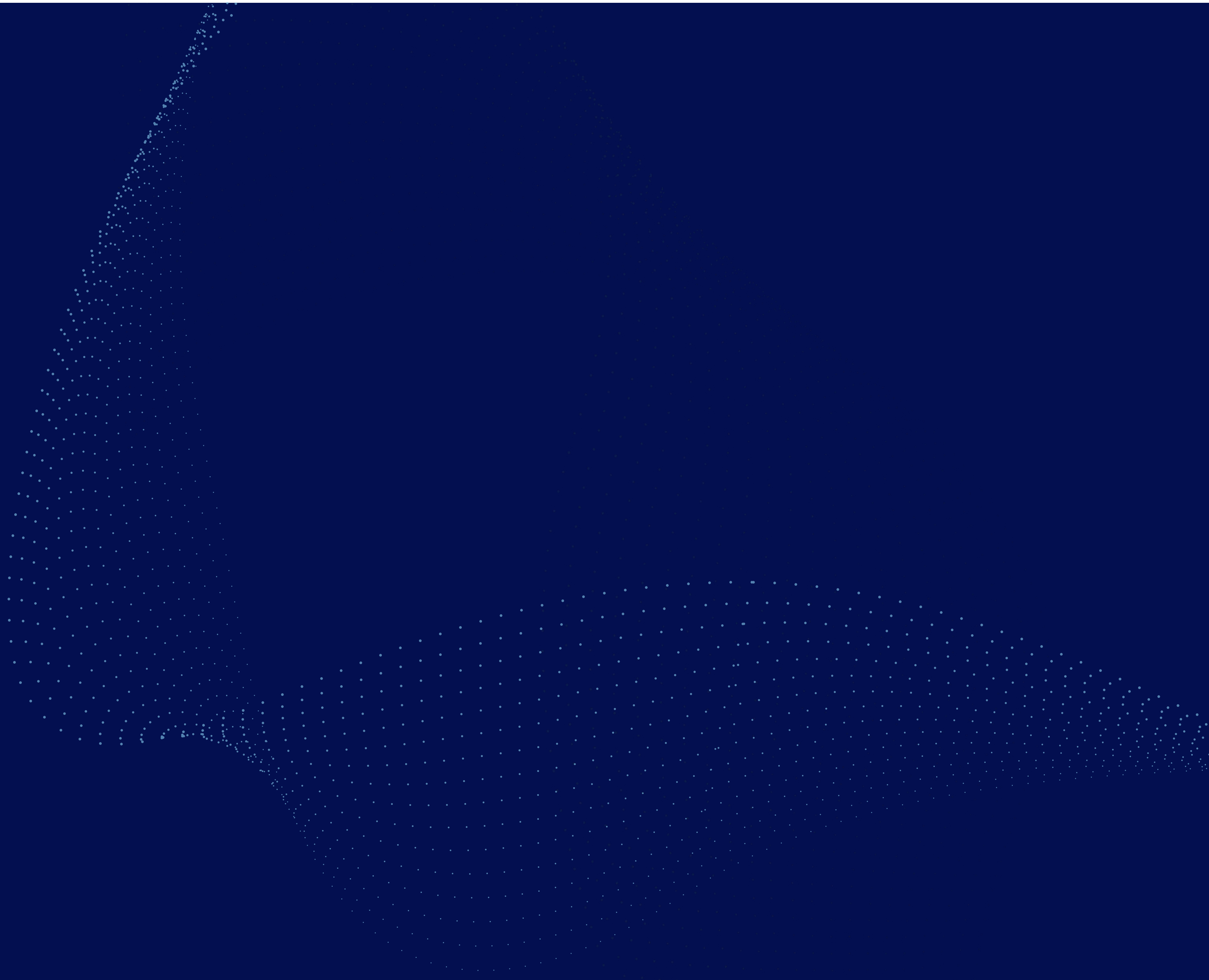


Seniority



[1] Maritime Cyber Priority 2023, DNV

CONTENTS



1 A STEP CHANGE IN CYBER THREAT AWARENESS

1 A STEP CHANGE IN CYBER THREAT AWARENESS

The energy industry is acutely aware of the growing cyber threat to IT and OT systems.

"One Thursday afternoon, we were suddenly alerted to a potential security vulnerability related to the logging software log4j. We immediately had to go through all of our software, our installations, all of our backup files – everything."

This incident, recalled by Tor Heiberg – Executive Director IT at Norwegian renewable energy company Skagerak Energi – illustrates the everyday cost and challenge of cyber security in today's energy industry.

"Even though we were not attacked, we had to drop everything and close the vulnerability. It took three full days, including Saturday and Sunday, with all hands on deck, including all of our partners and suppliers. Those hours quickly became extremely expensive."

Situations like these are increasingly common in the energy sector, impacting businesses of all sizes, across all geographies. They help explain why cyber security has now become a regular fixture on the boardroom agenda for six in 10 energy professionals in DNV's new research.

But awareness of the risk is not limited to the threat of immediate attack. Our research this year also underlines the growing strategic importance of cyber security to the energy industry. Indeed, nine in 10 (89%) energy professionals believe cyber security to be a pre-requisite for the digital transformation initiatives that are making the future of the industry possible.

SUPPORTING DIGITAL TRANSFORMATION AND THE ENERGY TRANSITION

Energy businesses are upgrading and connecting their legacy technology and infrastructure: to improve safety, increase efficiency, and decarbonize the industry through increased electrification, based on a growing share of renewable generation.

To give an example of the scale of this activity, DNV's Energy Transition Outlook 2022[2] – a forecast of the world's energy system up to 2050 – predicts that spending on the grid will double from some US$270bn a year today to around US$500bn by the 2030s. Annual investment will reach the trillion-dollar threshold by 2050.

A trillion dollars buys a lot of digitally connected infrastructure, and that's just on the grid. Nonetheless, it's an investment that's needed if the industry is to reach its net-zero ambitions.

Swantje Westpfahl, Director of the Institute for Security and Safety GmbH in Germany, believes cyber security must be an integral part of an organization's energy transition strategy.

> *"The energy transition relies on smart infrastructure grids, but smart is only good as long it doesn't get hacked."*
>
> *Swantje Westpfahl,*
> *Director, Institute for Security and Safety GmbH*

"Clean energy has created a much larger attack surface because we have new energy generation run by small computers – solar parks and wind farms – as well as smart meters expanding the grid into houses and cars," she says. "There is more risk that the whole system can get rocked if there's a successful attack."

[2] DNV Energy Transition Outlook 2022

THE GEOPOLITICAL FALL-OUT

The Russian invasion of Ukraine sent shockwaves through an energy sector whose memories of the pre-war cyber-attacks against Ukraine's energy supply remain vivid[4]. As one interviewee for this research noted, many executives in power generation and distribution became acutely aware at the time of the invasion that they were relying on the same kind of SCADA systems that the Kyiv plants were using when the cyber-related blackouts took place in the mid-2010s.

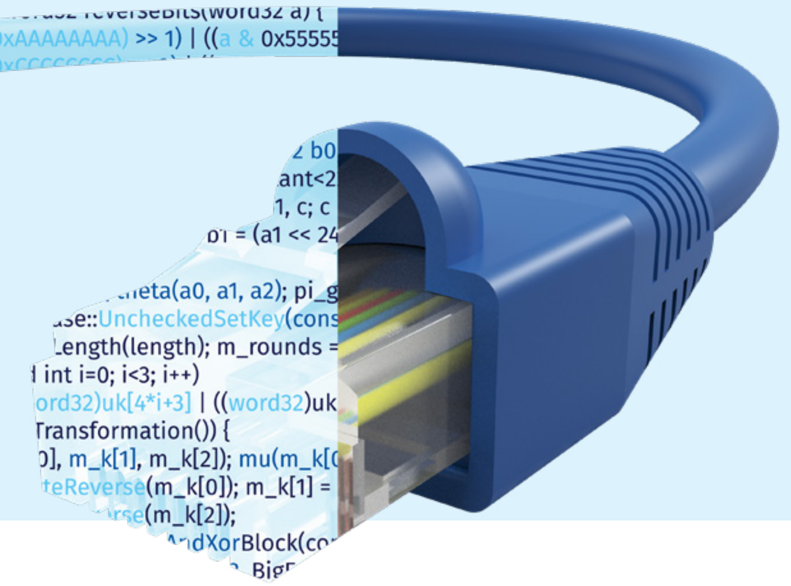
In our research, almost eight in ten energy professionals (78%) report that geopolitical uncertainty has made them more aware of the potential vulnerabilities in their operational technology (OT) – the systems that manage, monitor, automate, and control industrial operations. Moreover, two-thirds say their focus on cyber has intensified as a direct result of tensions.

The situation is made more complicated because attribution of cyber-attacks is difficult, and the connection between specific incidents and foreign powers is rarely clear-cut. "Cyber-crime groups are increasingly fragmented and many of them have fluid connections to nation states," explains Lars Idland, Chief Information Security Officer at Norwegian energy company Equinor. "There may also be collateral damage when the target was someone else, but an energy company is affected," he says.

The Russian cyber-attack on satellite internet operator ViaSat in spring 2022[5], for example, had the effect of deactivating thousands of wind turbines in Germany when their satellite-dependent monitoring systems were taken offline.

Although energy professionals in Europe are the most likely in our survey to be concerned about the impact of hostilities on their organizations, concern is also heightened in Asia Pacific, amid tensions between China and Taiwan, and in response to long-running bellicosity on the part of North Korea.

"From a conflict perspective, critical infrastructure is a clear target, because if an attacker can turn off your power grid, you lose early warning detection capabilities," says Paul Smith, the Chief Technology Officer at industrial cybersecurity company SCADAfence. "But then, you also have the largest chip manufacturer on the planet being threatened in Taiwan. If it starts producing malicious chips and pushing them globally, that is a scarier thought than most other things."



CYBER SECURITY AND THE ENERGY TRANSITION

In recent DNV research on the overall outlook for the energy industry[3], eight in ten (79%) of the most digitally advanced energy companies say that digital technologies are enabling their energy transition.

This is where cyber security comes in. Simply put, the industry cannot reap the benefits of digital transformation without robust cyber security. It's why respondents to the research who consider their organization to be digitally advanced are noticeably more likely (72%) to believe cyber-attacks are a major threat to their organization than the average (59%).

CYBER-CRIMINAL INNOVATION

Our research shows how the profile of cyber-attackers has changed since early 2022. In the immediate aftermath of the Russian invasion, we saw the industry shift into high alert with professionals expressing concern about all potential attackers. In the year since, energy executives remain highly attuned to the threat created by the Ukraine war – either by politically-driven hacktivists[6] or by hostile states – but they appear to have become less concerned about longer term adversaries such as criminal gangs and malicious insiders.

It would of course be a mistake to play down the threat of these other adversaries, not least because there may be a growing overlap between certain groups, as Skagerak Energi's Tor Heiberg explains.

"There are still criminal motives behind many cyber-attacks," he says. "My impression is that these are melting together because the cyber war between Russia and Ukraine probably has led to the development of new tools, and these tools are sold on the dark web where they can be utilized by economic criminals, and vice versa."

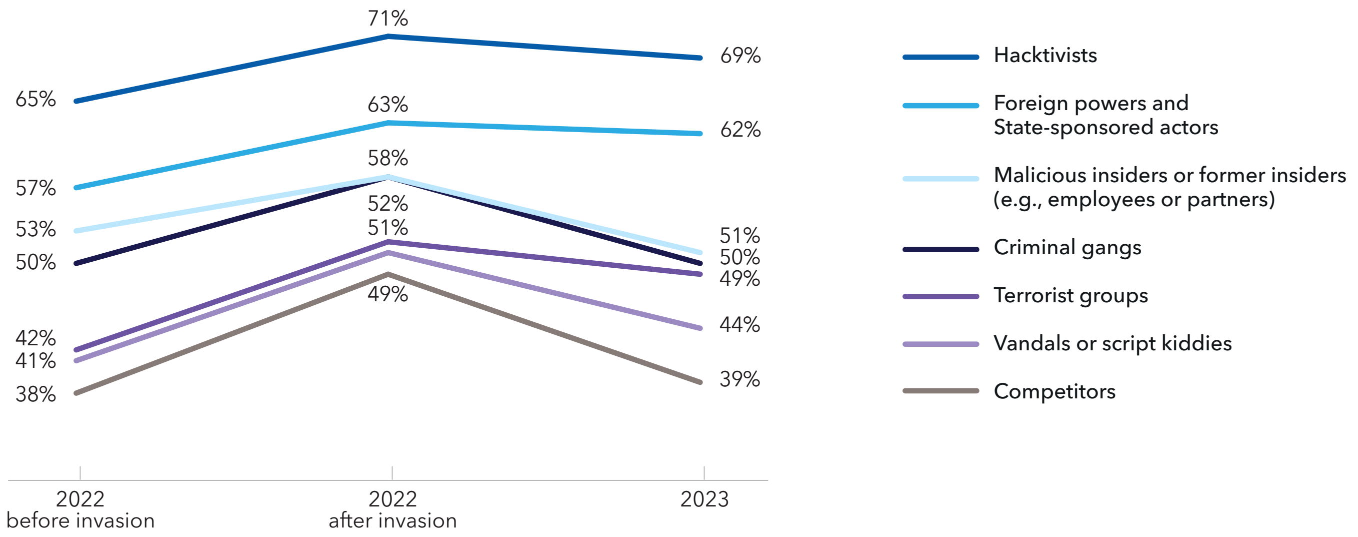
Innovation on the part of cyber criminals is indeed a persistent challenge, with new methods being shared and adopted by different adversaries. Fileless malware and 'living-off-the-land' attacks, in which cyber criminals exploit native tools within a company's system to carry out an attack, is a case in point. "We see a rise of malware-less attacks where they use a legitimate account and misuse those instead of creating malware," says Equinor's Lars Idland.

More broadly, energy businesses may benefit from broadening how they think about cyber threat actors and the specific methods they use. Fredrik Torp, Chief Security Officer and Vice President Corporate Security & Resilience at Sweden's Vattenfall, argues that it may be helpful, when assessing the threat landscape, to consider threat actors as organisations with specific objectives, who will use any means at their disposal to achieve their goals.

"Sabotage, espionage and disinformation are the main goals that the most advanced state actors have in today's geopolitical landscape," Torp says. "In addition, the advanced cybercrime groups are financially driven, and ransomware is constantly on the rise, which is another significant threat to counter."

"But cyber is only one vector that they will exploit to commit these acts," Torp adds. "As companies are strengthening their cyber defence, threat actors will increasingly focus on utilizing insiders or direct physical access to circumvent that. To be successful, it helps to have a holistic approach to security risks, where cyber is only one element."

States and hacktivists most concerning threat actors



Q: To what extent are you concerned about the potential for the following cyber threat actors to attack your organization? (Data shows moderate + high concern)

[3] Trilemma and Transition, Energy Industry Insights 2023, DNV
[4] Compromise of a power grid in eastern Ukraine, Council on Foreign Relations
[5] Russia's Viasat Hack Exposed Satellite Industry's Security Flaws, Bloomberg

2 PROGRESS HAS BEEN MADE, BUT RESILIENCE IS TOUGH

2 PROGRESS HAS BEEN MADE, BUT RESILIENCE IS TOUGH

The energy industry has woken up to the safety and business risks from cyber threats, but there are signs awareness is yet to translate into sufficient action.

RECOGNIZING THE REALITY OF CYBER

Energy professionals acknowledge that cyber-attacks in the industry are now a question of "when" not "if". With that in mind, it should perhaps be no surprise that seven in 10 energy professionals (71%) responding to our 2023 survey say they take cyber security as seriously as they do physical health and safety.

Any evidence that the industry is ramping up its security posture is to be welcomed, but our view is that more work is required before energy companies can confidently say they treat cyber as seriously as safety. This is not to play down the progress that firms have made, but to underline the complexity of the threat.

"If you walked onto a site in the energy industry without a hard hat, you would be stopped from working immediately," says Jalal Bouhdada, Global Segment Director, Cyber Security, at DNV. "On the other hand, if a business identified a vulnerable application, would it be remediated and fixed at the same speed? Despite increasing awareness, the answer is often 'no'."

One of the reasons behind this disconnect could be that leadership teams, although aware of cyber vulnerabilities, may not be fully apprised of the growing difficulty of keeping up with a fast-evolving threat both on a technical and employee-management level. It's an issue that chief information security officers (CISOs) can help address.

"When I talk to a board, I highlight that we have a risk-based strategy with strong cyber resilience to protect the company," says Muhittin Hasancioglu, independent expert, former CISO at both Petronas and Shell. "It is impossible to achieve 100% protection against cyber threats and breaches, but we do everything to enhance cyber risk management and cyber resilience to ensure any breach is to the lowest level of the digital landscape and results in a minimum impact to the company."

> *"As a CISO, my job is talk about the facts, not to give a false sense of security."*
>
> *Muhittin Hasancioglu, independent expert, former CISO at both Petronas and Shell.*

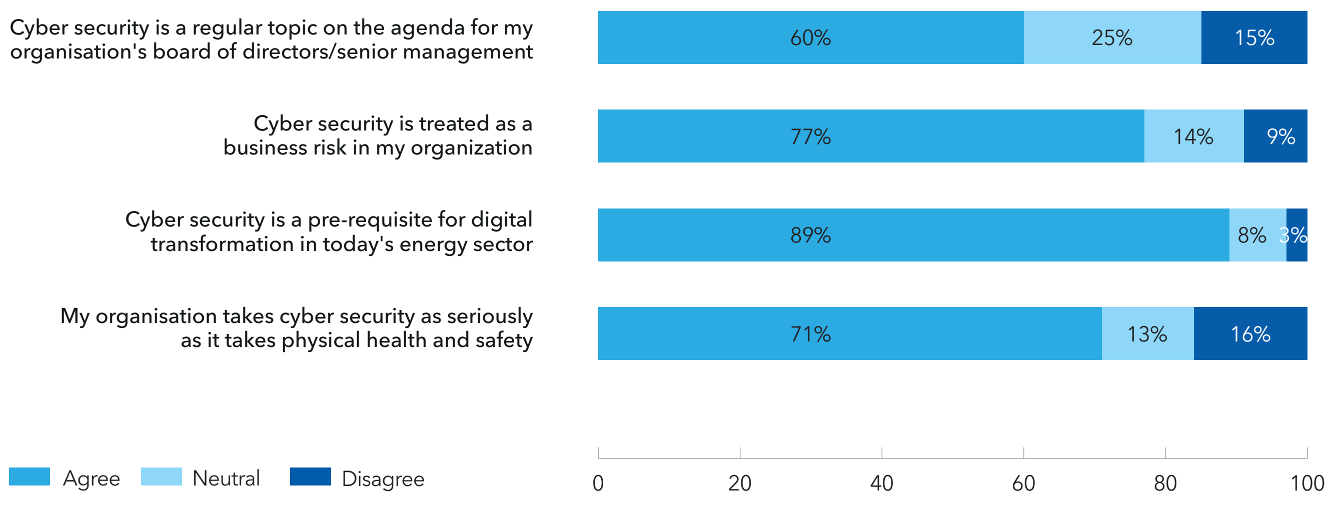
ENERGY PROFESSIONALS ARE WAKING UP TO THE SCALE OF THE THREAT

In DNV's 2022 Cyber Priority study, the majority of respondents told us that they believed a major incident in the energy industry was probable at some scale within the next two years, resulting in disrupted operations (85%), harm to the environment (74%), and loss of life (57%).[6]

In our analysis, we compared this growing awareness of cyber risk with the change in mindset around safety standards that took place in the late 20th Century. Our view was that energy operators took an inconsistent approach to health and safety until incidents such as Piper Alpha and Seacrest forced leaders to adopt standard protocols. We warned businesses against taking a similar "wait and see" approach to their cyber security, especially with respect to OT, out of concern that it would take a safety-compromising cyber-attack for energy companies to prioritize and institutionalize global security protocols and standards.

[6] Energy Cyber Priority 2022, DNV

Cyber is seen as a top business and strategic risk



Q: To what extent do you agree or disagree with the following? Percentages reflect net agreement (i.e. moderately + strongly agree).

BUSINESS RISK AND BOARD PRIORITY

The good news is that our research finds leadership teams in energy organizations paying serious attention to cyber security oversight. More than three in four energy professionals (77%) report that cyber security is treated as a business risk within their organizations.

"The level of management attention in the energy industry has changed over the last few years," says Tor Heiberg at Skagerak Energi. "Companies have known for a long time that cyber security is important, but now they also know it is expensive to underestimate the need for cyber defence. There have been incidents that were very costly and make investing in cyber defences and dedicating time to training a more rational argument."

Although leadership teams have been focusing their attention on cyber security in recent years – as operational assets become increasingly networked and connected to IT environments – the prospect of greater external scrutiny has helped sharpen this focus, especially in light of the Ukraine war.

"In standard risk assessments in the industry, war was always seen as unlikely," says Swantje Westpfahl at the Institute for Security and Safety GmbH. "But now that acts of war are targeting the energy industry, the risk assessment has been overhauled. Now classified 'very likely', measures for the prevention of cyber-attacks, and for operators of critical infrastructure to comply with related regulatory requirements, will be put into place."

ne pi_gamma_pi(a0, a1, a2) { word32 b0, b2; b2 = r
<1>(b0 ^ (a1|(~b2))); a2 = rotlConstant<22>(b2 ^ (b
ne theta(a0, a1, a2) { word32 b0, b1, c; c = a0 ^ a1 ^
> 8) ^ (a1 << 8) ^ (a0 >> 24); b1 = (a1 << 24) ^ (a0 >>
(b1 << 16); }
ne rho(a0, a1, a2){ theta(a0, a1, a2); pi_gamma_pi(
ThreeWay::Base::UncheckedSetKey(const byte *uk
sertValidKeyLength(length); m_rounds = GetRounc
(unsigned int i=0; i<3; i++)
m_k[i] = (word32)uk[4*i+3] | ((word32)uk[4*i+2]<<8)
!IsForwardTransformation()) {
theta(m_k[0], m_k[1], m_k[2]); mu(m_k[0], m_k[1],
m_k[0] = ByteReverse(m_k[0]); m_k[1] = ByteRever
m_k[2] = ByteReverse(m_k[2]);
ThreeWay::Enc::ProcessAndXorBlock(const byte *in
pedef BlockGetAndPut<word32, BigEndian> Block;
rd32 a0, a1, a2;
ock::Get(inBlock)(a0)(a1)(a2);
rd32 rc = START_E;
(unsigned i=0; i<m_rounds; i++) {
a0 ^= m_k[0] ^ (rc<<16); a1 ^= m_k[1];
a2 ^= m_k[2] ^ rc; rho(a0, a1, a2);rc <<= 1;
if (rc&0x10000) rc ^= 0x11011;

DEEPER LAYERS OF SECURITY BY DESIGN

Our research finds specific areas where energy businesses are trying to catch up with the threat.

Security by design, for example, should be the ambition for all companies – the idea that protections are built into assets and networks as they are developed, rather than retrofitted. If the industry is incorporating cyber security into the DNA of its infrastructure, it would be a big step towards it routinely treating the discipline as seriously as physical health and safety.

Some progress has clearly been made in this regard. More than half of respondents (54%) say, for example, that they consider security at every stage of the lifecycle of their assets and infrastructure. At the same time, around seven in 10 (69%) tell us that cyber is a consideration during the early phases of new infrastructure projects. If security teams are involved at these early stages, there are opportunities for them to influence asset and infrastructure planning.

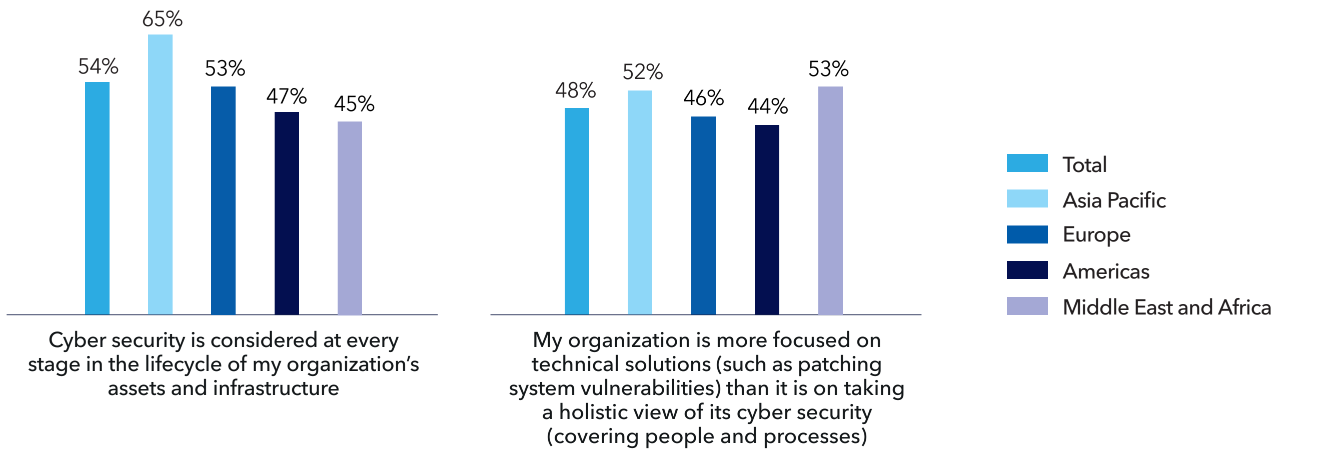
Involving cyber security professionals early in a project's development is, however, no guarantee that security by design is being delivered to a meaningful degree. Paul Smith at SCADAfence argues, for example, that security by design in the industry has not always extended to the underlying software that is baked into modern connected assets, meaning that assessments do not probe deep enough into the blueprint.

"Businesses trust the vendors they buy equipment from explicitly and assume the underlying software dependencies have been secured," he says. "But you will find a bunch of interdependent packages if you look underneath the hood. We investigated one device where the vendor had disclosed publicly to the National Vulnerability Database (NVD) two open vulnerabilities. When we ran it through a deep software bill of materials (SBOM) analysis, the firmware, it produced results in the range of something like 1,600 issues."

Lars Idland says Equinor is striving for security by design, especially as the company digitalizes operational technology. He flags, however, that achieving success relies on a serious commitment. "It is a challenge to have capability and capacity in place," he says. "You have to have people that can be in the projects, support the digitalization tasks, and try to secure it when they are developing it."

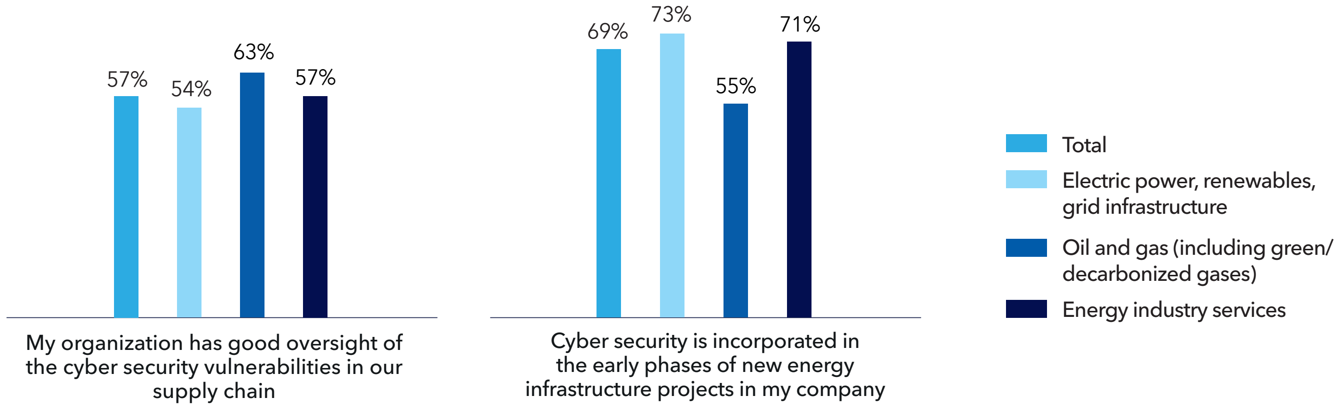
These frustrations are reflected in our research. The top challenge when companies try to enhance the cyber security of their OT, cited by 38% of respondents, is the lack of in-house cyber security skills.

Asia-Pacific companies reportedly more likely to take a holistic, lifecycle approach to cyber security



Q: To what extent do you agree or disagree with the following? Percentages reflect net agreement (i.e. moderately + strongly agree).

Oil and gas companies most confident about cyber supply-chain oversight



Q: To what extent do you agree or disagree with the following? Percentages reflect net agreement (i.e. moderately + strongly agree).

SUPPLY CHAIN VULNERABILITIES

Beyond the walls of the organization, energy professionals are increasingly aware of the cyber risks posed by their suppliers. Recent examples include serious breaches at critical energy infrastructure in the US and Europe, which resulted from the supply-chain attack on software developer 3CX earlier this year[7]. Successfully managing this risk represents another test of the maturity of cyber security relative to health and safety.

More than half energy professionals (57%) tell us that their organization has good oversight of supply chain vulnerabilities, indicating some confidence in their third-party risk management. However, they also identify the need to address supply chain vulnerabilities as one of the top-five challenges in cyber security.

The question is whether "good oversight" in this context signals that they are taking effective action, or whether they just have awareness of vulnerabilities. The picture is also less certain if we look across the energy system.

Respondents from the oil and gas sector are more likely than power companies to feel that they have good oversight of the supply chain, for example, and also to invest more in OT cyber security. This may be because oil and gas businesses are more likely to have been affected by cyber incidents. More than four in 10 (42%) oil and gas professionals said their organization had experienced negative impacts from an IT cyber security breach in our 2022 research, compared with 35% of power industry professionals.

There is a risk when vendors make assumptions about the coding in their systems and devices and are unaware of the risks these assumptions present to their clients. These gaps create significant challenges of visibility for companies when trying to achieve security by design.

With this in mind, extreme caution may be the only option. Adam S. Lee, Vice President and Chief Security Officer at Dominion Energy – which provides power to several key military and intelligence community national assets in the US – says this is the approach his organization takes. "We won't use any industrial or robotic systems that have been coded in a hostile nation state or one associated with it," he says.

"We even go as far as excluding vendors that use open-source freeware in their coding. Sometimes they will say their systems or devices are entirely coded in the US, but when you peel it back you realize they are pulling code from internet hosting services, some of which are developed in hostile countries."

A positive development here in recent times is that the industry has started to introduce new legislation to address the issue, by way of the EU Cyber Resilience Act – regulation that aims to create conditions for the development of software with fewer vulnerabilities – and new product lines coming into the market in the form of SBOM, which itemize the different components of software .

"SBOM, specifically in the OT world, has been interesting because for a long time the industry gave absolute trust to vendors," says Paul Smith of SCADAfence. "Companies would assume a new programmable logic controller or human-machine interface operating system or firmware had been quality assured, and engineers would simply run their control narratives on top of it. Some of the bigger vendors are now utilizing SBOM companies as a third-party validation check."

[7] Hackers behind 3CX breach also breached US critical infrastructure, CSO
[8] Software Bill of Materials (SBOM), US Cybersecurity & Infrastructure Security Agency

3 THREE CORE CHALLENGES

3 THREE CORE CHALLENGES

Investment, skills shortage, and poor collaboration remain major challenges.

Energy professionals are largely optimistic about the ability of their organizations to protect their business from cyber-attacks and keep up with the evolving threat. When ranking the importance of business risks to their organization, around a third (36%) said cyber security was a top three-risk. This places cyber security fourth overall among risks, behind operational and technical, safety, and financial risks. We see a similar picture when energy professionals rank these business risks in two years' time, with 34% expecting cyber security will then be a top-three business risk.

With the vectors and technologies used by cyber-attackers becoming steadily more sophisticated, in tandem with the growing connectivity of critical infrastructure, some in the industry may be in for a shock if they don't allocate sufficient resources to mitigate cyber security threats, or at least to keep threat actors at bay. Others will struggle to keep up with the demands that come from compliance with new regulation and with the need to ensure that their net-zero investments in essential technology can withstand attack.

In this section, we explore three principal challenges that energy businesses can expect to face around IT and OT cyber security as they look to the future.

INVESTMENT IS LAGGING

Despite board-level awareness of cyber risk, energy professionals are concerned that investment is not flowing at the levels required to address the issue. Less than half of energy professionals (42%) think their organization's current level of investment is sufficient to ensure the resilience of their operational assets and infrastructure. Just one in five agrees strongly that enough investment is being made.

"It's worth asking whether there is indeed a shortage of budget for cyber security being made available, or whether it is not being used effectively and teams are consequently made to look for additional funds," notes DNV's Bouhdada. "For other companies, the concern is that, while energy companies accept that cyber security risk is on the increase, they don't think an attack is something that will happen specifically to them and don't dedicate enough budget."

Today, just one in three (36%) energy professionals are confident their organization has invested enough in OT cyber security, with 59% saying that they are investing more in security this year than they did in the previous 12-month period.

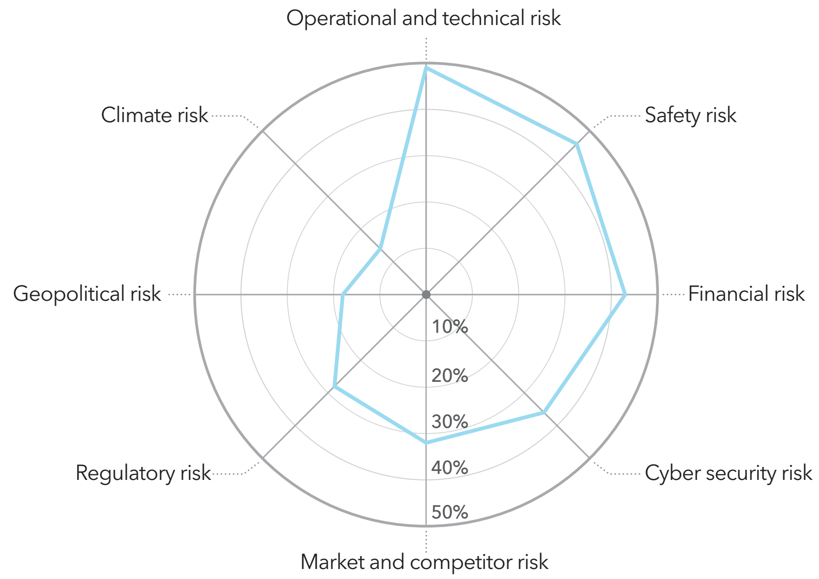
One problem is that despite commitment to cyber security on a corporate level, many energy businesses have subsidiaries that are comfortable investing less in their defences. Dominion takes a different approach to its governance, as Adam S. Lee explains.

"We're a top-down enterprise, but a lot of large energy companies have multiple subsidiaries with a great deal of autonomy," he says. "At Dominion, if I make a convincing case for an OT security standard, it becomes an enterprise-wide policy. At some organizations, subsidiaries make more of their own decisions."

Lessons may not have been learnt

Our 2022 Energy Cyber Priority research found that companies that had had a breach were significantly more likely to believe that their organization was not taking cyber as seriously as they should have been, with respect to IT (63% vs. 39%) as well as to OT (56% vs. 33%), suggesting that lessons may not have been learnt. Last year's research also identified an awareness of heightened cyber security risk, but a failure to invest accordingly.

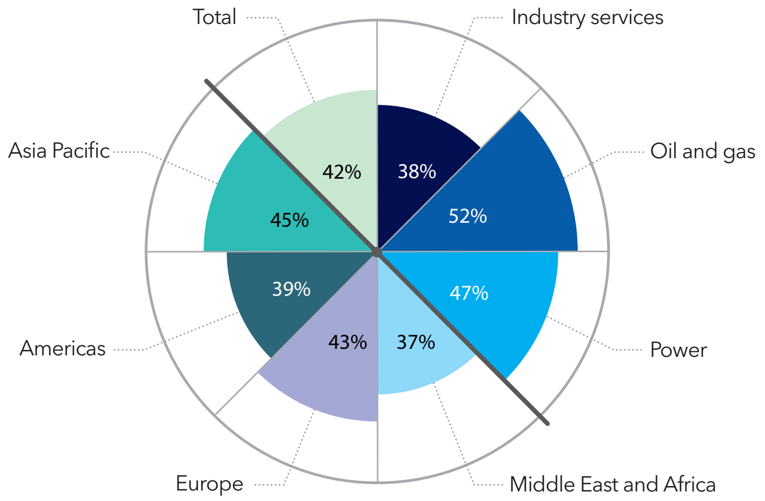
Cyber security the fourth greatest business risk



Q: Rank the following business risks, according to their level of importance to your organization today. Data shows percentage of respondents who selected these risks in the top three.

Oil and gas professionals are more likely to say their company is investing in OT cyber security

Extent to which energy professionals agree their company is investing enough in building the cyber resilience of operational assets and infrastructure



SKILLS SHORTAGES INTENSIFY

It is not just investment that is lacking from cyber security in today's energy industry. Organizations are also deeply concerned about their ability to recruit and retain the talent they need to protect themselves from cyber security threats.

The lack of in-house cyber security skills is regarded as the single most intractable barrier to maturity in the industry. More than a third of energy professionals (38%) pick out this issue. And in some parts of the world, the skills shortages are especially pronounced. In Asia Pacific, for example, 48% of energy professionals are concerned about the issue, which is in line with recent studies that found the gap between the current cyber workforce in the region and the number of workers needed to grow by 52% or 2.16 million people in a year[9].

One of the challenges that companies face is that cyber training, although vital, is very difficult to get right. Fredrik Torp at Vattenfall says that part of the problem in the industry is that standard e-learning modules can be overlong, unengaging and "painful", rendering them ineffective.

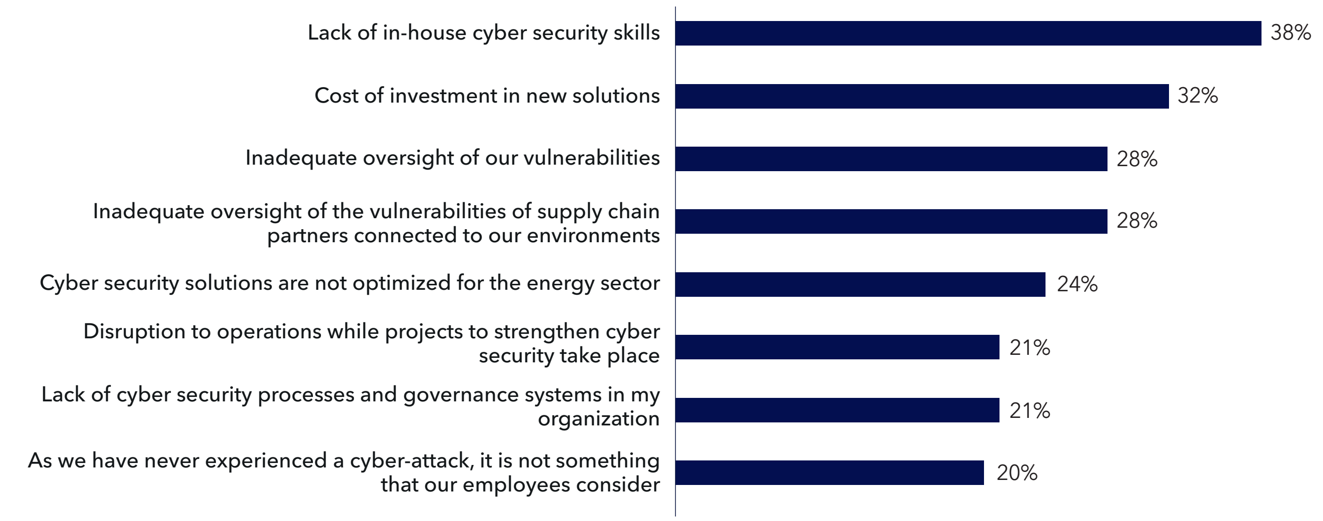
"You need to be creative about ways to train the workforce," he explains. "We've been trying out simulations as well as microburst training that you get during your normal working day. A message pops up and it takes 15, 30 seconds to finish, and then you come away with something new from that. You want people to behave differently, and you need to be able to measure that you see a change in their behaviour and provide feedback to them."

POOR COLLABORATION AND THE CYBER-PERCEPTION GAP

Our research finds that cyber security professionals struggle to communicate and collaborate with operational teams who don't share their level of understanding, as well as with executives at the most senior levels of the organization. These difficulties, combined with differences in direct experience of cyber security, is leading to a 'cyber-perception gap' among respondents.

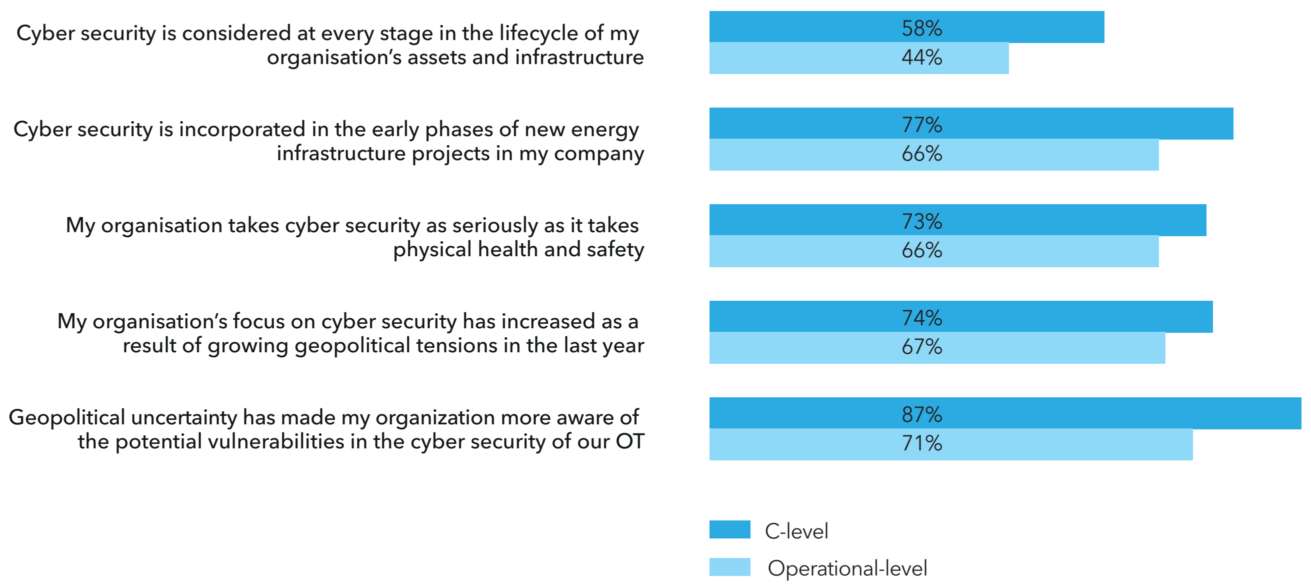
Our research suggests, for example, that some senior leaders might not have the full picture of the threat.

Talent and budget are top barriers



Q: What are the biggest challenges when it comes to enhancing your OT cyber security (select up to three)?

The C-suite has a different perspective than employees closer to operations



Q: To what extent do you agree or disagree with the following? Percentages reflect net agreement (i.e. moderately + strongly agree).

While 73% of respondents at C-suite level believe their organizations pay as much attention to cyber security as they do health and safety, the figure drops to 66% among those closer to operational practice. Meanwhile, 77% of C-suite respondents think security is emphasised early on in new projects, but just 66% of operational colleagues share this view.

Similarly, the C-suite appear more confident that geopolitical uncertainty is translating into heightened cyber vigilance. They are also more likely to think that their business is increasing its focus on cyber in light of geopolitical tensions.

Part of the problem is the inability of cyber security professionals to articulate and accurately report security challenges. Adam S. Lee at Dominion explains that shared understanding, based on clear communication, was one of his principal objectives when he started working in his current role. "One of the first things that I did was cultivate a very collaborative relationship with our CIO," he recalls. "If we have a coalition between his team and my team, we're combining the security that we have designed with how we need to build the controls, how we need to manage the risk, and how we communicate to the board, delivering the metrics that matter."

Three-quarters (76%) of respondents believe that cyber security professionals need to get better at speaking the language of energy operations. Linked to this, 76% also say their cyber security and engineering teams must learn to collaborate more effectively if the organization is to strengthen the security of its assets and infrastructure. Respondents based in the Asia Pacific region (85%) are particularly concerned.

[9] Cybersecurity Workforce Study 2022, (ISC)2

4 HIGH EXPECTATIONS FOR A NEW ERA OF REGULATION

4 HIGH EXPECTATIONS FOR A NEW ERA OF REGULATION

The energy industry is gearing up for cyber security regulation, in the hope it will unlock investment, but questions remain whether the industry is prepared for the shift.

REGULATION DRIVES INVESTMENT

Regulation is the foremost driver of investment in cyber security in today's energy industry. Almost half of respondents (49%) say changing requirements is one of the factors most likely to unlock increased budget at their organizations, making it the most commonly cited factor overall. By contrast, the next most likely catalyst for spending is a cyber incident (or near miss), cited by 38%.

As new regulation is looming, we can therefore expect cyber security functions in the energy sector to be in receipt of additional funding.

In the EU, for example, organizations providing essential services, including many in the energy sector, face tougher regulation in the form of the revised Directive on Security of Network and Information Systems (NIS2). This directive, agreed by the EU in January 2023, must be transposed into member states' national laws by late 2024. Among other measures, NIS2 widens the scope of organizations covered by regulation, increases the standards of required executive oversight and imposes new reporting changes. It also increases the penalties for non-compliance, including provisions for fines of up to €10m or 2% of an organization's total worldwide annual turnover.

Other jurisdictions are also pursuing higher standards and tougher regulation. In the US, the Department of Energy is continuing to work on the National Cyber-Informed Engineering Strategy[10], a bi-partisan plan to raise standards. The Securities and Exchange Commission, meanwhile, proposes to require public companies to disclose whether their boards have cybersecurity expertise[11]. In Australia, the Cyber and Infrastructure Security Centre recently called for an overhaul of energy sector practices given its vulnerability to attack[12].

Further initiatives are likely around the world. Organizations such as the World Economic Forum continue to push for increased regulation on cyber security in critical industries, particularly in areas such as resilience and reporting on breaches[13].

The danger of this reactive, regulation-dependent approach to budgeting is that it is inevitably geared around complying with rules rather than achieving maximum resilience.

As the Institute of Safety and Security GmbH's Swantje Westpfahl explains, new directives and standards are limited unless businesses embrace the spirit of regulation. "You can be cyber secure and you will nearly automatically be compliant, but you can be compliant without having good cyber security – this is when you should seek help," she says, adding that specialist external partners can help businesses reach the required standard.

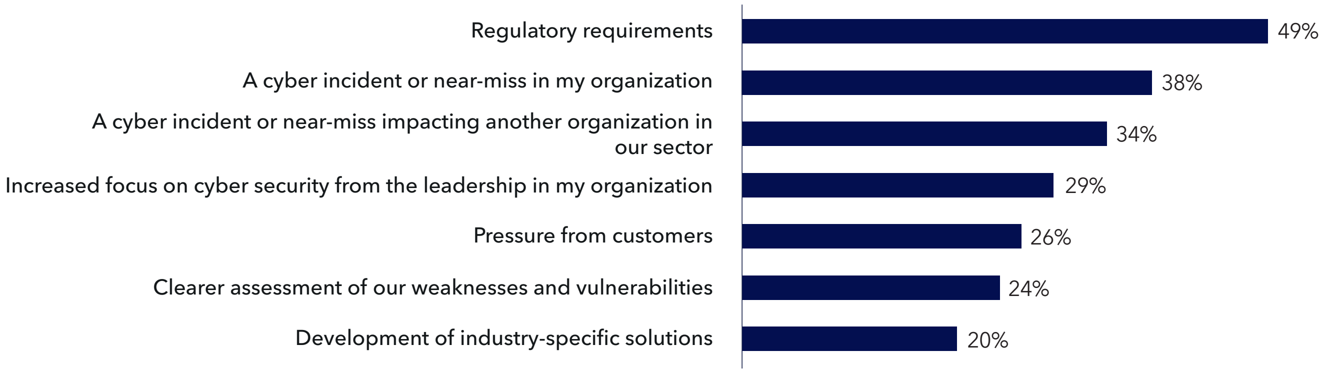
"For some things that were difficult to get into place a few years ago, like DMZ networks or backup systems, there are startups and great minds everywhere now that can do them for you. Compliance and stronger regulations can help argue for the cause and provide a baseline for best practices."

A related challenge is that lack of investment in cyber security resources in advance of regulatory change will mean that businesses struggle to turn the additional funding into an enhanced security posture when it does become available. "Translating funding into resilience is especially difficult when it comes to developing and recruiting specialist talent, considering the shortage of skilled professionals within the industry," says Jalal Bouhdada.

When it comes to the talent challenge, this is another area where some believe that government bodies, including regulators, could become more ambitious in their approach to cyber security.

"Regulation is a stick that is useful for penalizing people, but first we need to invest in educating the nation," argues Muhittin Hasancioglu. "If I were in the government, I would enhance the nation's cyber awareness and introduce cyber education at ages 11 or 12. These children can then influence other people, and they will also become the future cyber-aware digital and cyber-security skills pool. Right now, there are three-and-a-half million job vacancies in cyber security worldwide, for which we can't find people. We need to start now."

Cyber security investment follows a regulatory push



Q: What factors are most likely to lead to greater cyber funding in your organization (please select top 3)?

ENERGY COMPANIES ARE UNPREPARED FOR THE SHIFT

In this research, more than half of respondents (59%) expect regulatory authorities to take tougher action on companies that do not comply with regulation in the coming years. The penalties could be significant. As mentioned above, organizations in the EU face fines of up to €10m or 2% of their annual turnover while those in the US and Australia also face tougher penalties in the coming years.

LACK OF NIS2 AWARENESS

Despite the threat of stricter regulation, our research indicates that businesses are not moving quickly enough to ensure compliance. Looking at NIS2, as an example, a recent poll of professionals from industrial sectors carried out by DNV found that more than a third (35%) were not even familiar with NIS2, while (30%) said their company had not started to prepare for the changes.

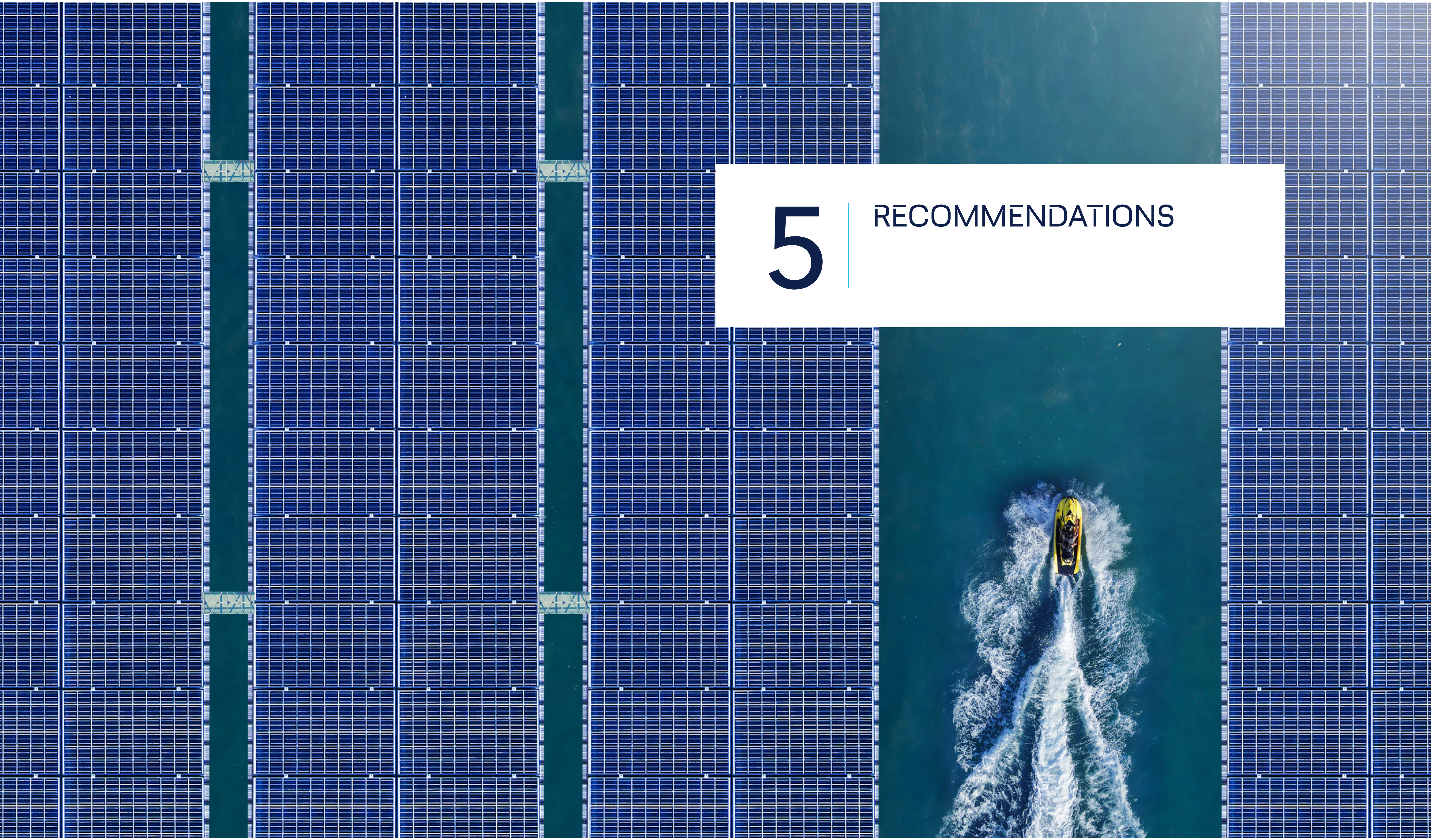
Creating suitable momentum may require regulators to hold board members more accountable, believes Dominion Energy's Adam S. Lee.

"Holding executives and boards to account if they haven't properly invested in cyber controls is going to be significant, and promulgation of these rules by regulators is already underway," he says. "I also think we will see shareholder legal suits against the CISO or the CSO (Chief Security Officer), if they haven't properly made the case to their company's board that suitable safeguards require significant investment."

We can hope that this increased regulatory attention will have the effect of improving resilience across the energy industry. Professionals expect greater regulatory scrutiny of the supply chain and of incident response, which will help focus attention on the gaps that businesses still have around their OT cyber defences.

Today, 64% of energy professionals worry that their organization is more vulnerable to cyber-attacks on their OT networks than at any other point in their history. Furthermore, 42% admit that they have not invested enough in their OT cyber security. Regulation will help unlock some of the funding they need to address the balance.

[10] National Cyber-Informed Engineering Strategy, US Department of Energy
[11] Is your board prepared for new cyber security regulations, Harvard Business Review
[12] Australia's CISC releases risk assessment advisory for critical infrastructure across energy sector, Industrial Cyber
[13] Why we need global rules to crack down on cybercrime, World Economic Forum



5 RECOMMENDATIONS

5 RECOMMENDATIONS

In the short term, we advise energy organizations to prioritize the following actions.

Step up efforts to enhance cyber security

The evidence of this research suggests many organizations have not made as much progress as is required, despite awareness of the risk and confidence among senior leaders. The clock is ticking. Tougher regulation exposes energy companies to significant compliance failures. More fundamentally, the risk of attacks in the sector is increasing at a time when dependence on operational technology (OT) is growing fast, and companies must take steps to strengthen their resilience accordingly.

Build cyber maturity

We believe that energy professionals should question whether their confidence around their cyber security posture is justifiable. In turn, they should ask how they are measuring the strength of their defences and recovery plans, how they are benchmarking performance, and whether they have identified the improvements they need to make. Once they have outlined systematically the gaps in their defences, they can put plans in place to close them.

Equinor's Lars Idland says his company approaches cyber security as a continuous process. "This is an ongoing situation," he says. "It's going from a project phase, where you find and fix things, to a situation where you continuously try to improve capabilities over time. It develops alongside the technology."

Improve communication and collaboration

Miscommunication is not just a case of cyber teams speaking the "wrong language" when collaborating with operations. Our data suggests that the C-suite is not getting the clarity it needs to assess the threat and invest appropriately. This should be concerning for all stakeholders – employees, shareholders and customers alike.

When learning to collaborate with individuals in different parts of the business, it isn't just a matter of understanding different communication styles and workplace cultures, and then exploring these through coaching and workshops – vital though this is. "It comes down to gaining respect," says Swantje Westpfahl. "You have people from different realms, with different knowledge, so there needs to be an appreciation that what they do is valuable and different from what others do."

Build capacity and unlock resources

Taking a proactive approach to cyber security can help drive competitive advantage. Organizations at the forefront of defining excellence, meeting new standards and implementing best practice will secure an edge on their less fleet-of-foot competitors.

The commercial benefits of cyber are important to highlight, considering the cost of cyber security. "We have to have acceptance from management and the board that cyber is costly and we need to spend money on it," says Skagerak Energi's Tor Heiberg. The prospect of unlocking commercial advantage is a persuasive argument in such budgetary conversations.

Prepare for new regulation

Energy firms are waiting for regulation to unlock investment, but this is the wrong way around. They should of course invest to ensure compliance – in order to avoid increasingly challenging penalties from regulators, and in recognition that stronger requirements are on the way – but should also aim to go further than what is stipulated. In practice, this means being proactive rather than 'ticking boxes,' focusing on resilience alongside compliance, and looking for new opportunities that may arise from managing cyber security effectively.

One way to ensure that the business is ready is to strengthen the case that cyber is key to enabling the future of the energy industry, which points to its broader strategic necessity. This may also be important in attracting essential but hard-to-find cyber talent into the industry.

```
(a0, a1, a2)
ıı (rc&0x10000) rc ^= 0x11011;
a0 ^= m_k[0] ^ (rc<<16);a1 ^= m_k[1
.Put(xorBlock, outBlock)(a0)(
s(word32 a) {void ThreeWay::Dec::ProcessAndXorB
1)BlockGetAndPut<word32
) << 2); 0, a1, a2;
0F0F0F) << 4); Block)(a0)(a1)(
);word32 t = reverseBits(a0);a0
b0, b2; b2 = rotlConstant<1>(a2
ant<22>(b2 ^ (b0|(~a1))); a1 ^= (b2
, b1, c; c = a0 ^ a1 ^ a2; c = rotlConsta
b1 = (a1 << 24) ^ (a0 >> 8) ^ (a2 << 8) ^ (a
a2){ theta(a0, a1, a2); pi_gamma_pi(a0
0, a1, a2); pi_gamma_pi(a0, a1, a2); }
edSetKey(const byte *uk, unsigned int
); m_rounds = GetRoundsAndThrowIf
)
| ((word32)uk[4*i+2]<<8) | ((word32)u
()) {
[2]); mu(m_k[0], m_k[1], m_k[2]);
[0]); m_k[1] = ByteReverse(m_k[1]);
[2]);
dXorBlock(const byte *inBlock, co
rd32, BigEndian> Block;
```

WHEN TRUST MATTERS

ABOUT DNV

DNV is an independent assurance and risk management provider, operating in more than 100 countries. Through its broad experience and deep expertise, DNV advances safety and sustainable performance, sets industry standards, and inspires and invents solutions.

DNV combines specialist energy industry knowledge with engineering expertise and information system best practice to keep critical infrastructure projects and operations confidently cyber secure. We provide many of the sector's most successful and forward-thinking companies with clear and practical advice to uncover their risks, build a powerful force of defence against threats, recover from attacks, and unite stakeholders against security programmes that everyone can believe in.

dnv.com/cybersecurity

Disclaimer
All information is correct to the best of our knowledge. Contributions by external authors do not necessarily reflect the views of the editors and DNV.