DNV

WHEN TRUST MATTERS

THE CYBER PRIORITY

The state of cyber security in the energy sector

ABOUT THIS RESEARCH

The Cyber Priority explores the state of cyber security in today's global energy sector, investigating executives' understanding of the cyber risks their businesses face and their strategies for managing the evolving threat.

The research draws on a survey of 948 energy professionals and a series of in-depth interviews with industry leaders and security experts. It was developed and created by DNV and Longitude (a Financial Times company).

Fieldwork was conducted between February and March 2022. Respondents were based across Europe, the Americas, the Middle East and Africa, and Asia Pacific. They included publicly listed companies and privately held firms, spanning energy industry services, power transmission and supply, renewables, and oil and gas.

Organizations surveyed vary in size: 34% reported annual revenue of USD 100 million (m) or less during the last fiscal year, while 25% had annual revenue exceeding USD 500m. The survey respondents represent a range of functions within the industry, including those with in-depth knowledge of cyber security along with engineers, managers and C-suite executives.

The Cyber Priority is published by DNV, the world's leading resource of independent energy experts and technical advisors, and draws on insight from the following individuals:

- Jalal Bouhdada, Founder and Chief Executive Officer, Applied Risk
- Shaun Gregory, Executive Vice President and Chief Technology Officer, Woodside Energy
- Stian Nordby, Operations Manager – Digital Services & Innovation Center, TechnipFMC
- Margrete Raaum, Chief Executive Officer, KraftCERT
- Andre Ristaino, Managing Director of Automation Standards, International Society of Automation
- Leo Simonovich, Vice President and Global Head of Industrial Security and Digital Security, Siemens Energy
- Trond Solberg, Managing Director, Cyber Security, DNV

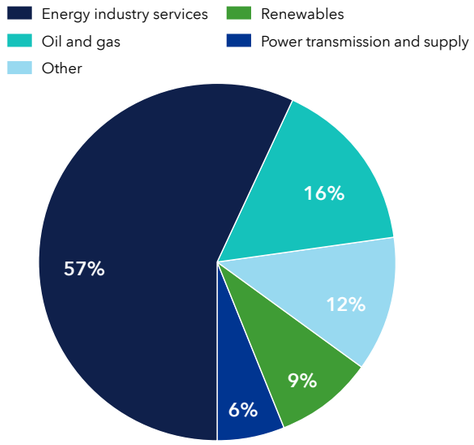
948
Energy professionals surveyed

98
Countries represented

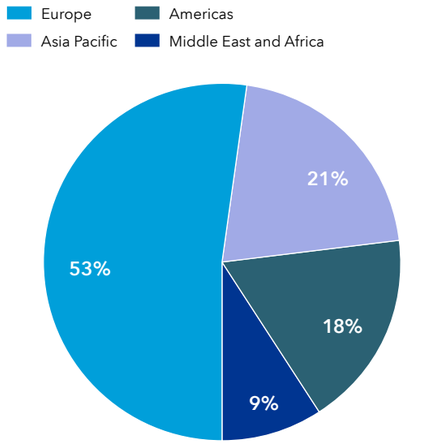
64%
Develop, operate or support operational technology (OT)

7
Interviews with industry executives

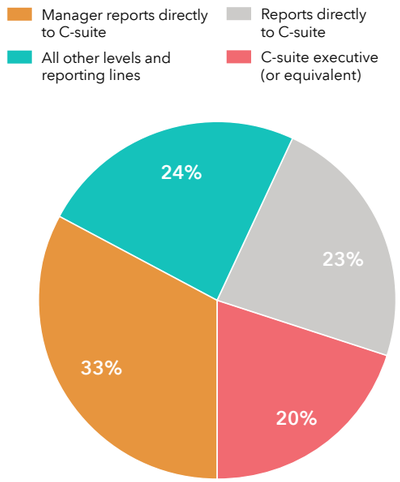
Respondents by sector



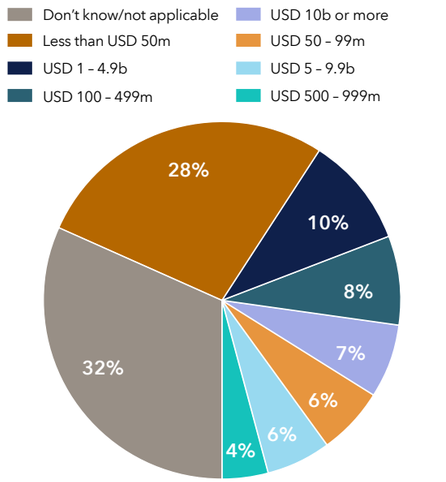
Respondents by region



Respondents by seniority



Annual revenue by fiscal year



*Respondents from the energy services sector include a broad range of providers to the industry, including EPC companies, asset management and inspection firms, consulting businesses and logistics companies.

CONTENTS

1 A SECTOR WAKING UP TO THE THREAT

1 A SECTOR WAKING UP TO THE THREAT

When hacking group DarkSide launched its 2021 ransomware attack on the Colonial Pipeline, the situation escalated rapidly.

Within hours, the owners of the facility, which provides around half of the motor fuel consumed on the East Coast of the United States, had suspended operations, leading to soaring prices, panic-buying at fuel stations and the eventual payment of a Bitcoin ransom worth millions of dollars.[1]

Coming after a series of attacks disabled Ukraine's power grid in the mid-to-late 2010s, leaving hundreds of thousands of people without power, the Colonial Pipeline incident was described as a wake-up call about the growing threat of cyber-attacks in the energy industry.[2,3]

Hackers seize a new opportunity

Energy is one of the top three industries reporting cyber-attacks,[4] and it faces specific challenges. While all industries must prevent hackers from stealing sensitive data from their IT environments, energy businesses also need to manage the threat to their operational technologies (OT) – the computing and communication systems they use to manage, monitor, and control industrial operations.

As OT becomes more networked and connected to IT, cyber-attackers – who include foreign powers, terrorists, competitors, and criminal gangs – are seeing an opportunity to seize critical infrastructure, whether to demand a ransom, steal intelligence, or create widespread disruption. An additional attraction for these hackers is that the industries that they typically targeted in the past, such as financial services, have become harder to infiltrate following widespread efforts to secure key entry points.

In turn, two-thirds (67%) of the 948 energy professionals who responded to our survey acknowledge that the shock of recent incidents has driven them to make major changes to their security strategyb and systems.

The new wave of attacks

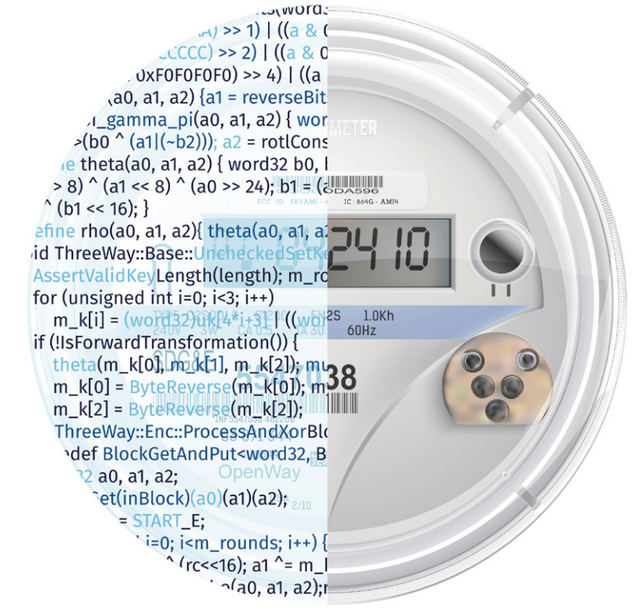
Energy executives are under no illusion about the scale of the threat faced by the industry at large. Most believe that a major incident is probable at some scale within the next two years, resulting in disrupted operations (85%), harm to the environment (74%), and loss of life (57%). Respondents in the Middle East and Africa are more likely than those in Europe and the Americas to have this expectation.

We do see some variation by sector, however, with all industry verticals showing concern about asset shut-down and energy supply disruption, while respondents from oil and gas and energy industry services are more likely to worry about environmental damage than those in the power transmission and supply and renewables sectors.

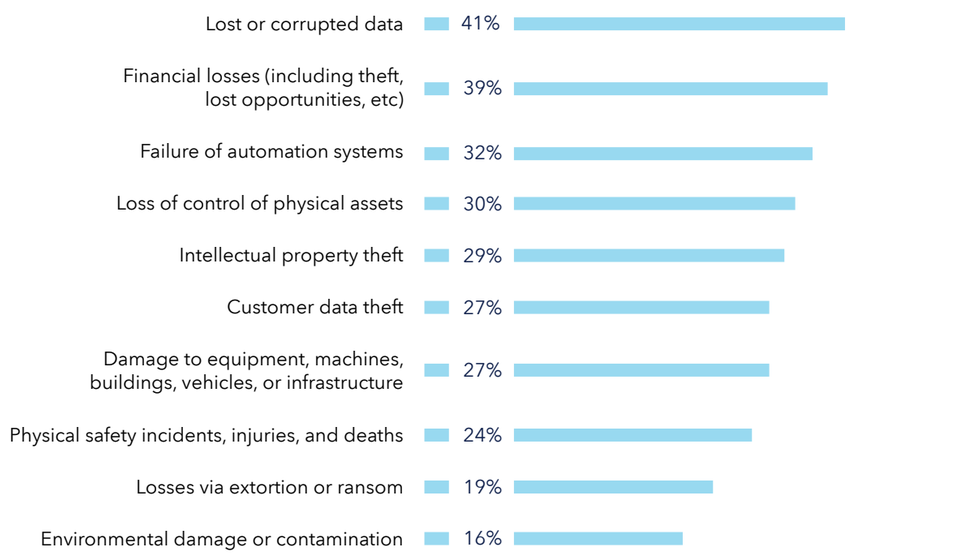
Hoping to escape the worst

Although executives anticipate a serious incident in the global industry, they are less likely to believe that their own organization will be affected by the most extreme, life-threatening consequences of a breach.

Asked to specify what concerns them most about a theoretical attack, they point first to disrupted services and operations (57%), reputational damage (42%), data breach (41%), and a corresponding hit to profits (39%). In comparison, just 24% and 16% of respondents, respectively, describe loss of life and environmental catastrophe as a top concern.



Cyber-attack consequences that respondents see as a top concern for their organization



[1] US says it recovered large portion of Colonial Pipeline ransom, Financial Times
[2] Ukraine power cut 'was cyber-attack', BBC
[3] People's Energy data breach affects all 270,000 customers, BBC
[4] Three plead guilty to terrorism charges in white supremacist plot to disrupt U.S. power grid, start race war, Washington Post

Parallels with the adoption of safety systems

The disconnect that we see in our data – with respondents anticipating a major industry event on one hand while hoping that their own organizations will escape the worst impact on the other – has parallels with the industry's gradual adoption of physical safety protocols over the past 50 years.

Andre Ristaino, Managing Director of Automation Standards at the International Society of Automation (ISA), explains that site owner/operators took an inconsistent approach to personnel health and safety in the late 20th century because the discipline was still being developed and institutionalized. "The consensus back then was, 'How do you measure safety? How can you predict an accident?'" he says. "But, once safety was studied, and elevated to an engineering discipline, the experts recognized that there was always a root cause."

Although many had been pushing for improved standards and regulation, it took events such as the Piper Alpha (1988) and Macondo (2010) disasters for tighter regulation to come into place, and for industry leaders to standardize and invest in measures to prevent future incidents.

"We are concerned when we hear that some energy firms may still be taking a 'hope for the best' position on cyber security. The lessons of the past, relating to safety protocols, make this plain. It will be a tragedy if it takes a series of catastrophic but preventable attacks on control systems – resulting in a less safe operating environment across the industry – for them to rethink their approach", says Trond Solberg, Managing Director, Cyber Security, at DNV.

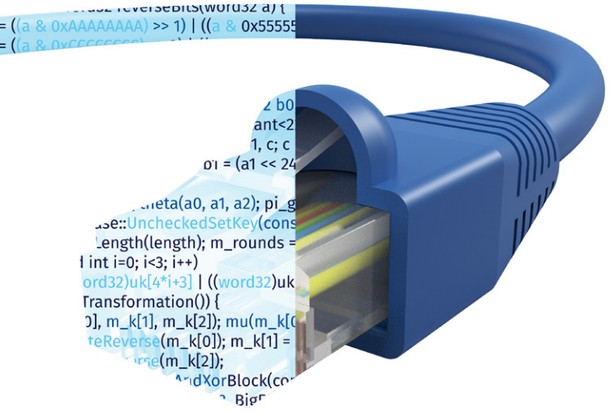
The C-suite is still coming to terms with the threat

The respondents who consider themselves to have cyber security expertise in our survey sample provide a more pessimistic perspective on the threats faced by their organizations. These 'expert' respondents[5] – who typically have first-hand knowledge of their organization's security strengths and weaknesses – are noticeably more uncomfortable about the potential for a cyber-attack on their business to cause harm to people, planet, and profits.

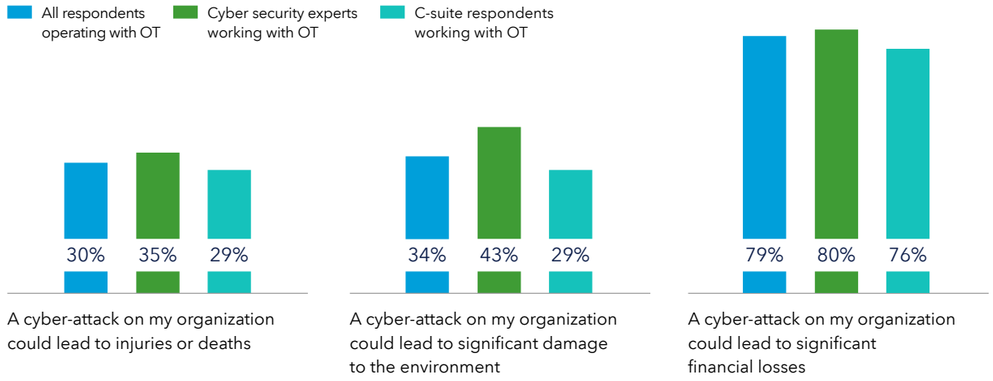
The difference between experts and non-experts is even more stark when we compare their data with that of C-suite respondents. For example, eight in 10 (80%) expert respondents agree that an attack on their organization would create significant financial losses, compared with 76% of the C-suite. Meanwhile, 43% believe an attack could lead to severe environmental damage (compared with 29% of C-suite) and 35% think an incident could cause serious injury or loss of life (29% of C-suite).

In a similar vein, C-suite respondents are less likely than the cyber security experts to consider 'malicious insiders' (64% vs. 43%), foreign powers (69% vs. 55%) or terrorists (55% vs. 43%) to be a threat to the organization, suggesting they are less familiar with the hackers behind recent attacks and more trusting of their employees' conduct and goodwill.

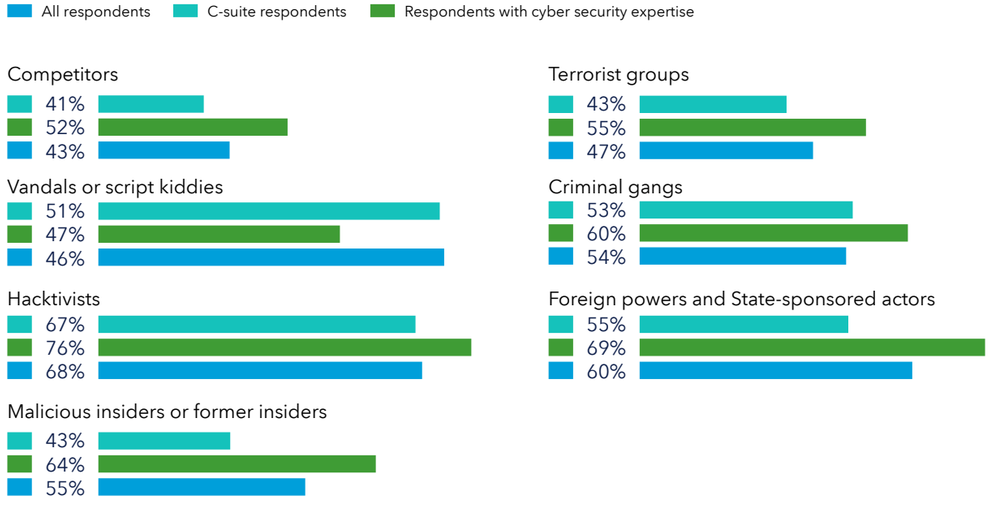
Although our research suggests that the industry is becoming more alert to the evolving cyber threat, the inconsistency between cyber experts and C-suite is concerning. Leaders are aware of the risk that their business faces, but specialist executives may not be getting their message across to all the decision-makers in the business.



Proportions that agree with these statements



The threat actors that respondents are most concerned about



[5]A group of 102 respondents who indicated that they were knowledgeable about the operation and maintenance of IT/OT systems, control systems, operational software, or similar, and keep up to date with cyber trends. These respondents were also more likely to be involved in buying and hiring decisions around cyber security.

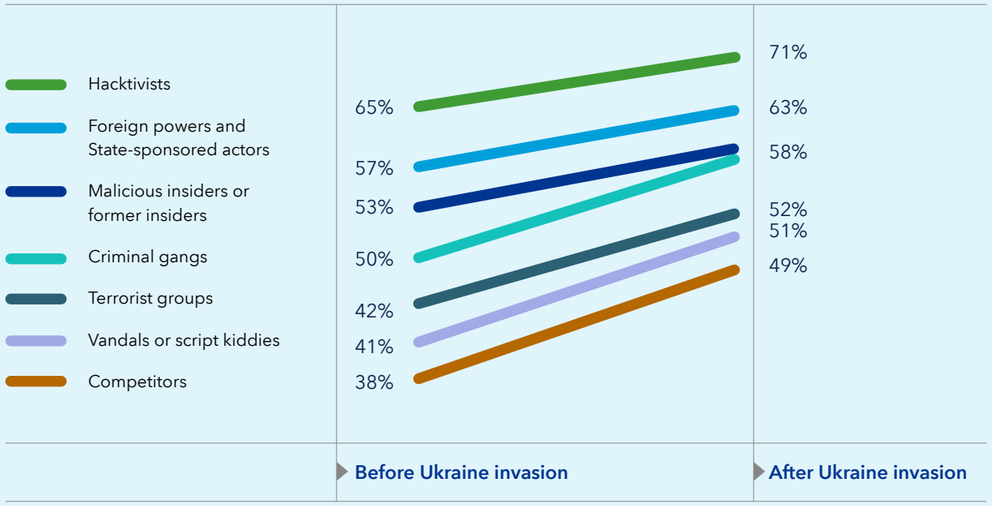
Understanding the adversary

Russia's invasion of Ukraine in early 2022 inspired fresh uncertainty in the energy industry and the rising concern of executives is reflected in their sentiments around cyber-attackers. While the fieldwork for producing this report began two weeks before the invasion, we can compare these responses with those submitted between 24 February and 9 March, when we concluded our fieldwork.

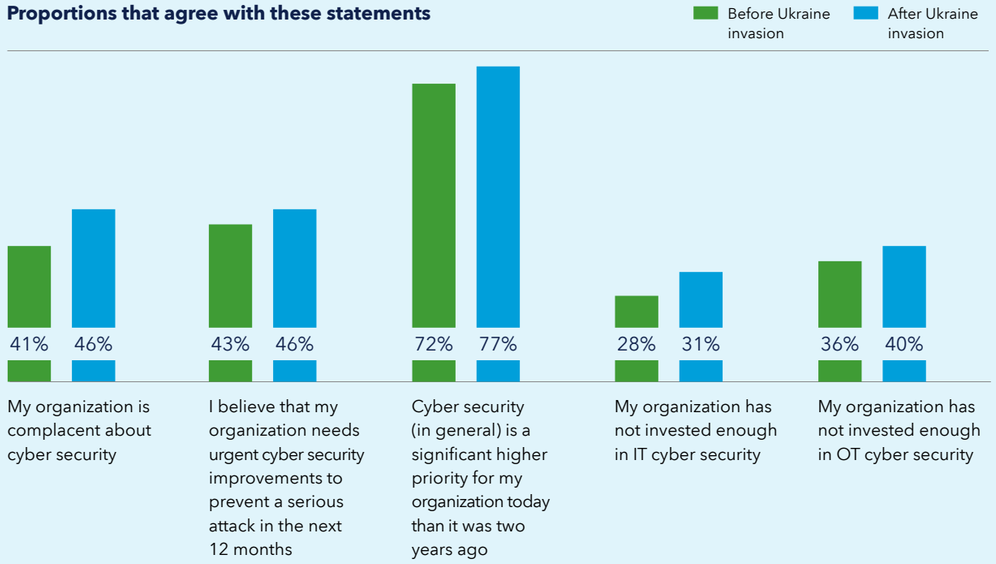
Before the conflict, respondents said the adversaries that concerned them most were hacktivists, foreign powers and malicious current or former insiders. After the invasion, we saw an understandable jump in concern around nation-states, but this was accompanied by rising apprehension across all categories. This suggests that respondents expect other opportunists – whether motivated by political causes or criminal gain – to take advantage of the confusion that follows a crisis by launching their own attacks.

In line with these findings, we also saw respondents become more aware of their vulnerability to cyber-attacks. Again, the conflict in Europe may have inspired the change in sentiment, but the outcome was a more general awareness of cyber risk. After the invasion, 77% said cyber security had become a higher priority for their organization than it was two years ago, up from 72% before the crisis. Higher proportions also flagged concerns that their organization wasn't doing enough about cyber (41% to 46%) or had underinvested in the security of its operational technology (from 36% to 40%).

The threat actors that respondents are most concerned about



Proportions that agree with these statements



Concern mirrors industry travails

How respondents perceive the risk posed by individual cyber-attackers varies across sectors within the energy industry, but can often be understood in light of the broader, longer-term challenges faced by their constituents.

In oil and gas, for example, eight in 10 (79%) firms consider themselves a target for hacktivists, which likely reflects this sub-sector's carbon footprint. Respondents from the power transmission and supply sector are more alert, relative to other sub-sectors, to the threat posed by criminal gangs and terrorists. Hackers stole 270,000 UK customer records in a breach in the early 2020s,[6] while the sub-sector has also been the target of recent terrorist plots in the US.[7]

Where apprehension could be higher

We see some broader trends, relating to individual hackers, that are worth calling out. In the renewables sector, less than half of respondents express concern about terrorist groups, criminal gangs, or foreign powers. There is, however, no reason why they wouldn't be a target for adversaries such as these, especially if they are believed to be on less high alert than businesses in other industries.

On average across all sub-sectors, there is a relatively subdued level of concern about amateur vandals and script kiddies, who frequently use pre-existing code to launch attacks. Businesses should not underestimate the risk of these amateur hackers.

[6] https://www.bbc.co.uk/news/technology-55350995
[7] https://www.washingtonpost.com/nation/2022/02/25/power-grid-terrorism-race-war/

2 FOUR KEY CHALLENGES

2 FOUR KEY CHALLENGES

Managing cyber security in an environment as complex and changeable as the energy sector is anything but straightforward. Advances in digitalization, innovation, and the energy transition are taking place against a backdrop of shifting demand and a conflict in Europe that has serious implications for global prices and flows.

As industry leaders look to strengthen their cyber defences and adjust to a landscape of emerging risks, our research identifies four key challenges that they must contend with along the way.

1. The 'wait and see' effect is holding back progress

Our research reveals some sentiments that appear, at first glance, to be at odds with one another. Most notably, respondents are aware of the growing threat to their organization but are often reactive in their approach to cyber security.

Six in 10 C-suite respondents acknowledge, for example, that their organization is more vulnerable to attack than ever before, but far fewer (44%) expect to make urgent improvements in the next few years to prevent an attack.

Indeed, one in three (35%) says their organization would need to be impacted by a major incident before it would spend any more time or money on its defences. This sentiment is more prevalent in the Middle East and Africa (44%) than it is in Europe (29%) and the Americas (39%), despite respondents in the Middle East being more likely to expect a major cyber incident in the industry in the next few years.

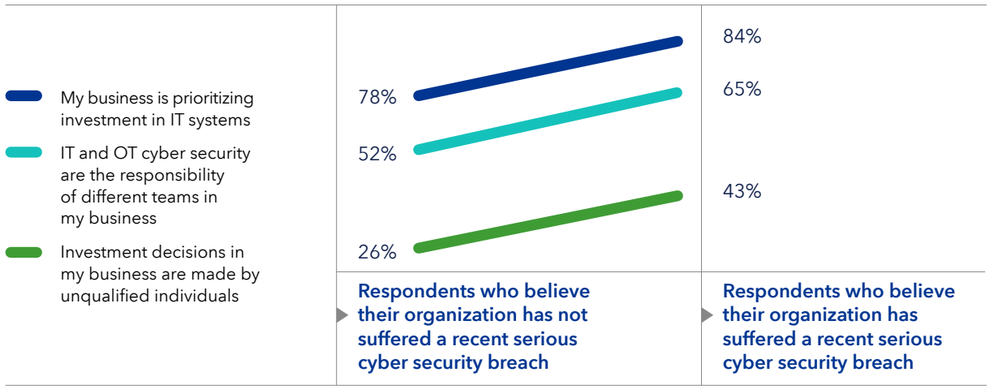
One explanation for this apparent reluctance to invest in security is that most respondents to our survey believe that their organization has so far avoided a major cyber-attack. Less than one in four (22%) says their organization has been subject to a serious breach in the last five years. Moreover, relatively low proportions say they have experienced negative impacts from attempted breaches on their IT (40%) and OT environments (28%).

It is noteworthy that respondents who believe their organization to be a leader in digitalization are less likely to think their business is underinvesting in cyber security. Fewer of these respondents say that it would take a major incident before they increased investment (26% compared with 39% of those who admit that they are not leaders), that they underinvest in IT cyber security (28% vs. 32%), and that investments are made by unqualified individuals (25% vs. 31%). This suggests that businesses that support greater spending on digital transformation are also more comfortable extending investment to protection from the associated risks.

Playing catch-up creates a muddled response

A problem with waiting for an incident before investing in cyber upgrades – aside from the fact that an incident could have a catastrophic impact on the business in the meantime – is that organizations are more likely to make hasty, suboptimal decisions.

How a breach may influence investment decisions



Among the respondents who say their organization has experienced a cyber security breach in recent years, 83% confirm that cyber security is a higher priority today than it was two years ago. Within this same group, however, more than four in 10 (43%) say cyber investment decisions are made by individuals without the expertise to do so, which compares with 26% across the total sample. This group is also more likely to say that IT and OT security are the responsibility of different teams (65% vs. 52%), and to be prioritizing system upgrades rather than broader upgrades of their capabilities and processes.

Downtime fears

When it comes to OT, the reluctance of energy organizations to invest is compounded by the knowledge that reviewing and potentially transforming cyber-security systems may interrupt business as usual.

Shaun Gregory, Executive Vice President and Cheif Technology Officer at Australia's Woodside Energy, explains that fixing OT cyber threats is complicated because it involves maintenance engineering as well as IT staff. "Say, for example, the control system running a turbine is a legacy PC that has a vulnerability and needs to be replaced, but you can't replace it until the turbine is next shut down," he says. "That shutdown may not happen for one- or two-years' time, so you are faced with a risked decision and that makes OT cyber more challenging."

War in Europe focuses the mind

For Leo Simonovich, Vice President and Global Head of Industrial Security and Digital Security at Siemens Energy, concern about the geopolitical implications of the Ukraine invasion may prove to be the catalyst that some businesses need to make real changes.

"Of the companies in the energy sector most vulnerable to cyber-attacks, there are those who know about their vulnerabilities, but haven't had the imperative to close security gaps because they fear negative impacts on operations. Then there are those who are completely unaware of their threat exposure," he says.

"But now, with critical infrastructure becoming an increasing target, there is a different risk frontier as adversaries deploy imprecise cyber weapons to cause widespread destruction. Their intent may be to target a specific sector or company within a country's broader energy infrastructure, but today's threats have far-reaching, and unintended consequences. Chief information security officers [CISOs] are asking themselves, 'Could it be me?'"

2. The air gap is closing fast

When considering the risk of a cyber-attack on their industrial control systems, energy businesses have taken some comfort from the knowledge that their OT platforms have traditionally had an 'air gap' insulating them from the IT network.

Jalal Bouhdada, Founder and CEO at Applied Risk – an industrial cyber-security firm acquired by DNV in 2021 – cautions, that the days of the air gap are numbered. "Most industries are interconnected, driven by the requirement for access to data and analytics," he says.

While their OT systems operated in siloed environments, organizations understandably prioritized cyber upgrades to their IT security instead. As a result, Bouhdada estimates that there is a gulf in maturity between the two domains that corresponds to approximately 15 years of development and investment. "On the information side, the main priorities are confidentiality, integrity, and availability of information. On the OT side, they are safety, reliability, and productivity of machines," he says. "It also doesn't help that installations were managed by engineers, whose core business was never cyber security."

Today, just four in 10 respondents think their organization is well prepared for an attack on its OT environment – whether executed directly or by infiltrating through the IT network. This is more than 10 percentage points lower than those who think they are prepared for an attack on their IT environment.

"When it comes to OT across the industry, there has been improved awareness over the past few years, but the industry is still not representing the risk very well," says Woodside's Shaun Gregory. "Most people are worried about IT cyber and the impact it can have. Not so much about the OT impacts on infrastructure."

"Most people are worried about IT cyber and the impact in can have. Not so much about the OT impacts on impacts on infrastructure."

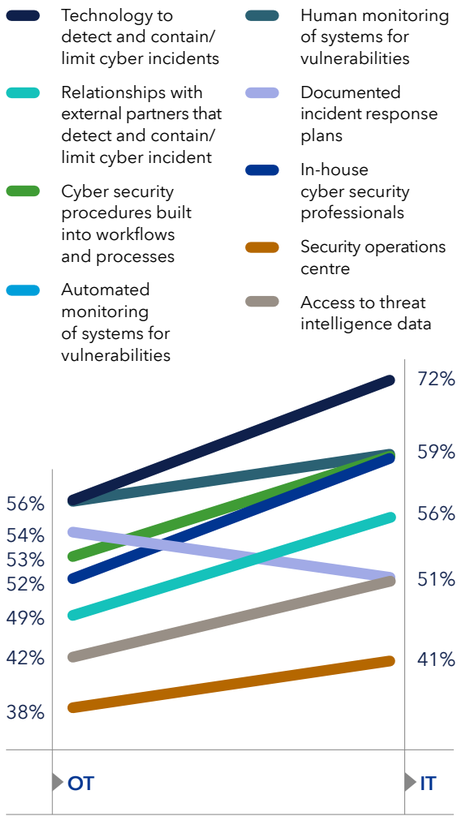
Shaun Gregory, Executive Vice President Chief Technology Officer, Woodside Energy

Mismatch in capabilities

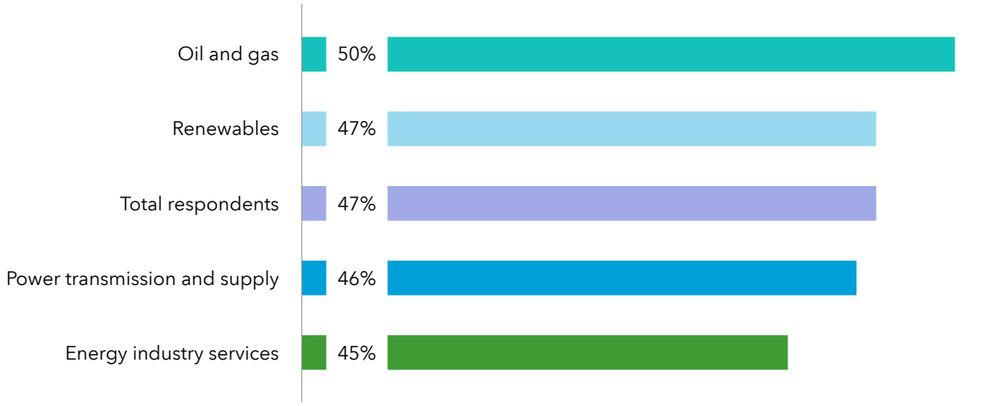
Less than half (47%) of the respondents to our survey believe their OT cyber security is as strong as their IT security. Correspondingly, four in 10 (38%) admit that they have not invested as much as they need to in OT cyber security. Across all capabilities – including technology to contain incidents, relationships with external specialists, and access to threat intelligence data – IT cyber security has manifestly been prioritized over OT.

The exception here is that the industry appears stronger at documenting the incident response plans for its OT than it is for its IT, especially within the oil and gas (63%) and power transmission and supply (74%) industries.

Organizations that have the following capabilities in place for IT and OT



Proportions that say their OT cyber security is as strong as their IT cyber security



Rising to the challenge

ISA's Andre Ristaino believes that the state of OT cyber security will improve as the cybersecurity discipline matures as a recognized profession. "ISA and the industry have a mission to elevate operational technology cyber security from an art, to a science, to an engineering discipline," he says. "OT cyber security needs to be institutionalized, much like safety was 50 years ago."

To that end, our research does at least indicate that OT security is heading up the agenda. Seven in 10 say OT security is a significantly higher priority for their organization today than it was two years ago, before the Colonial Pipeline event. Moreover, 74% of cyber experts responding to our survey say their organization understands what it needs to do to protect its OT systems.

Leo Simonovich at Siemens Energy believes that one of the priorities should be for businesses to clarify with policymakers who takes responsibility for industrial cyber. "When I talk to CEOs, there is widespread recognition that industrial cyber is critical, but there is a disconnect between the emphasis they place on cyber security, and what operators are actually doing to secure physical and digital assets," he says.

"The rose has been pinned on the CISO to close the cyber-readiness gap and meet the demands of energy sector executives, but often the CISO is not equipped with the technologies, tools, and personnel to take on securing critical infrastructure from cyber-attacks. In the past, securing physical assets was the job of engineers and plant operators, who wanted to maintain their control system logic and data. Well, that is now in the cloud and it's falling to the CISO to secure the industrial internet of things," he adds.

"Often, the CISO is not equipped with the technologies, tools, and personnel to take on securing critical infrastructure from cyber-attacks"

Leo Simonovich, Vice President and Global Head of Industrial Security and Digital Security, Siemens Energy

3. A global shortage of expertise

In an unfolding cyber incident, where hackers have infiltrated the network and need to be contained, every second counts. It's therefore concerning that just 31% of respondents assert confidently that they know exactly what to do if they became concerned about a potential cyber risk or unfolding attack.

Gaps in processes and the skills-base

For Margrete Raaum, CEO at KraftCERT, a Norwegian computer emergency response team with a cutting-edge approach to industrial control systems, some issues like these can be resolved by reviewing and strengthening processes. "If your processes allow for people to do things that they shouldn't, then your processes are flawed," she says. "We've had breaches where the system lit up like a Christmas tree, but if nobody is looking at the alarms then the Christmas tree just keeps twinkling."

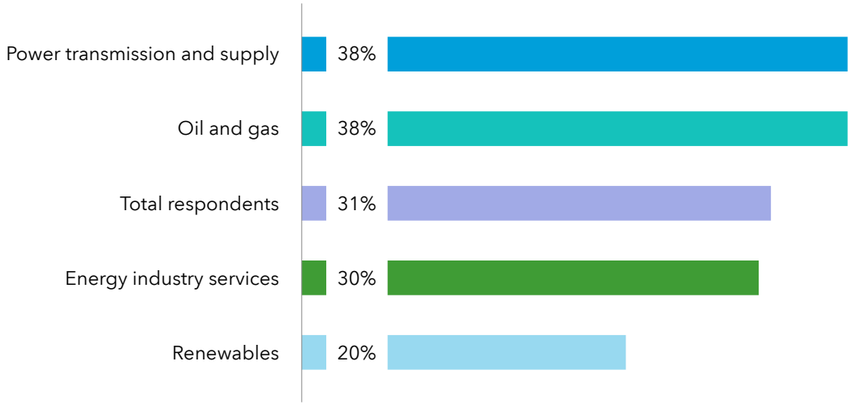
More broadly, our findings highlight the need for the industry to embed a greater number of cyber experts into the workforce. The principal challenge here is the global talent-availability crisis.

If we look more closely at the data, we see that the renewables industry is at greatest risk of employees making a misstep at the crucial moment, with just one in five respondents stressing clearly that they would know exactly how to respond.

According to the (ISC)[2] Cybersecurity Workforce Study[8], the cyber security workforce gap represents around 2.7 million professionals. Within the energy sector, the challenge is compounded by organizations' need for specialist talent that understands the OT as well as the IT domains.

"Nowadays, cyber security teams need to be trilingual to excel in the energy sector," observes DNV's Solberg. "They need to speak the language of their industry domain – be that in offshore wind, gas pipelines, or terminals – as well as the technical language of engineering and cyber security. It's no longer enough to be fluent in one of these languages. You need to be proficient at all three."

Proportions that assert confidently that they would know exactly what to do if concerned about a potential cyber attack



[8] A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)[2] Cybersecurity Workforce Study"

These requirements reinforce the need for thorough training, intuitive processes that guide individuals into making the right choices, and – on a broader level – greater collaboration, knowledge-sharing and support across the industry.

"There's a shortage of industrial cyber professionals," says Leo Simonovich. "And when you have a massive talent shortage, you need to band together to create leverage, especially if you are a small or medium-size operator. Some energy businesses barely have IT teams, let alone operational technology teams focused on security."

Training is making a difference

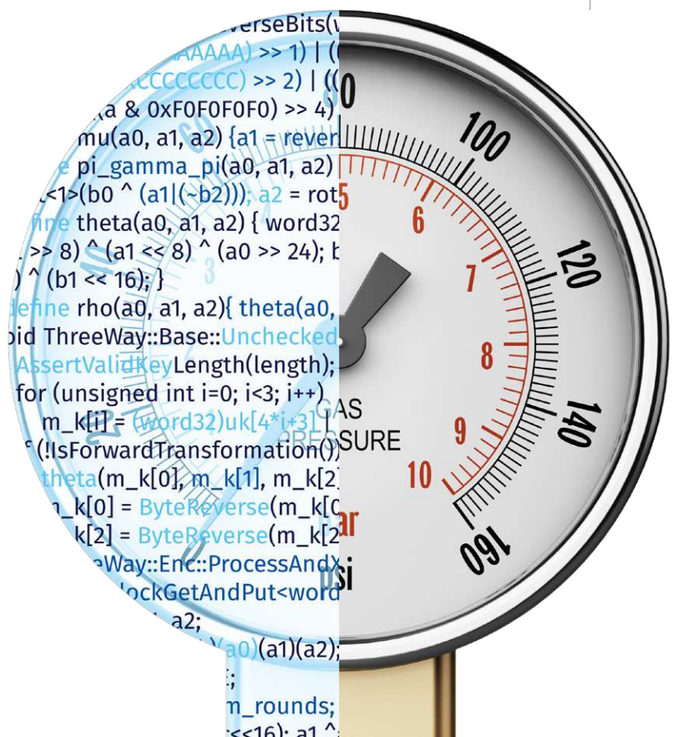
As a shortage of cyber security skills presents a challenge across all industries, talent will remain hard to come by and businesses will need to enhance their training and coaching activity.

Andre Ristaino, whose work focuses to a great extent on developing the cyber workforce of tomorrow, agrees on the importance of education. "Make sure everybody is educated before you spend any money on technology," he says. "You can't even have a conversation about what to do until then and there's no downside to getting smarter."

Stian Nordby, Operations Manager – Digital Services & Innovation Center at TechnipFMC, believes the priority should be on ensuring that cyber becomes front of mind for all employees. "It's about shifting left in the development cycle, ensuring that cyber security is something that's second nature to everyone in the business," he says. "If you're a developer, this should be something that you think about when you design your solution."

The findings of our survey provide some cause for optimism. Around eight in 10 (78%) say their organization is making education and training a spending priority in their cyber security budgets, which is currently higher than those trying to hire new specialists in IT (65%) and OT (55%) cyber security. With three in four expert respondents also indicating that their training programmes are effective, we would hope that knowledge-sharing and education around cyber security is becoming more prevalent among existing energy professionals.

Nonetheless, there is no denying that shaping the cyber workforce of the future is a major undertaking. Woodside Energy's Shaun Gregory flags a related issue that will grow as businesses focus on its people and their capabilities. "We're not producing enough gender diversity in cyber," he says. "It's like data science was 10 years ago."



4. Complex supply chains disguise critical vulnerabilities

Supply chains in the energy sector are global in scale and increasingly complex, relying on third and fourth parties whose cyber security systems and processes are harder to assess with certainty. Consequently, cyber security across the supply chain is an area in which respondents are less confident than they need to be to protect their critical systems and data.

Our research finds energy organizations notably less likely to rank themselves as strong at vendor and supplier security oversight than they are in other disciplines. Just 28% of energy professionals working within OT say their company is making the cyber security of their supply chain a high priority for investment. This contrasts with the 45% of OT-operating respondents who say expenditure in IT system upgrades is a high investment priority.

At the same time, just 12% of OT-operating companies, and 13% of all other companies, rank vendor and supplier oversight among their core areas of maturity. This falls to just 8% of respondents in the oil and gas sector.

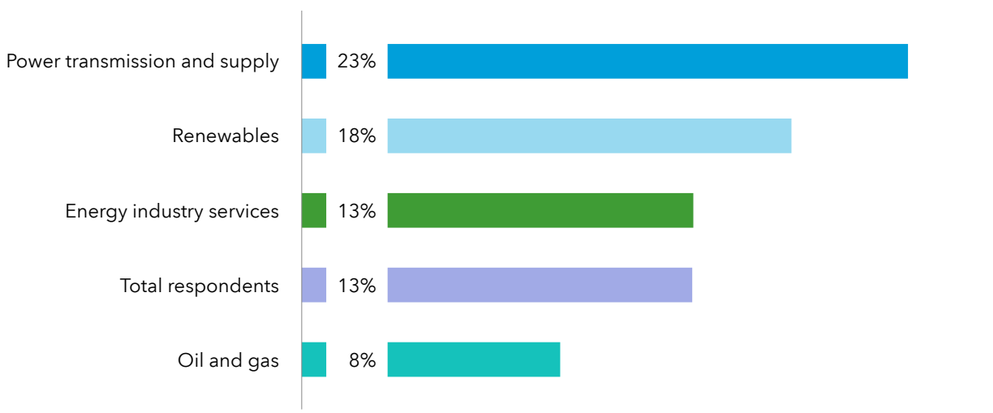
The danger is that suppliers and equipment manufacturers may not have the people, processes, or technologies in place to demonstrate the security of their products and services. As a result, energy operators could be unaware of the vulnerabilities to which they are exposed.

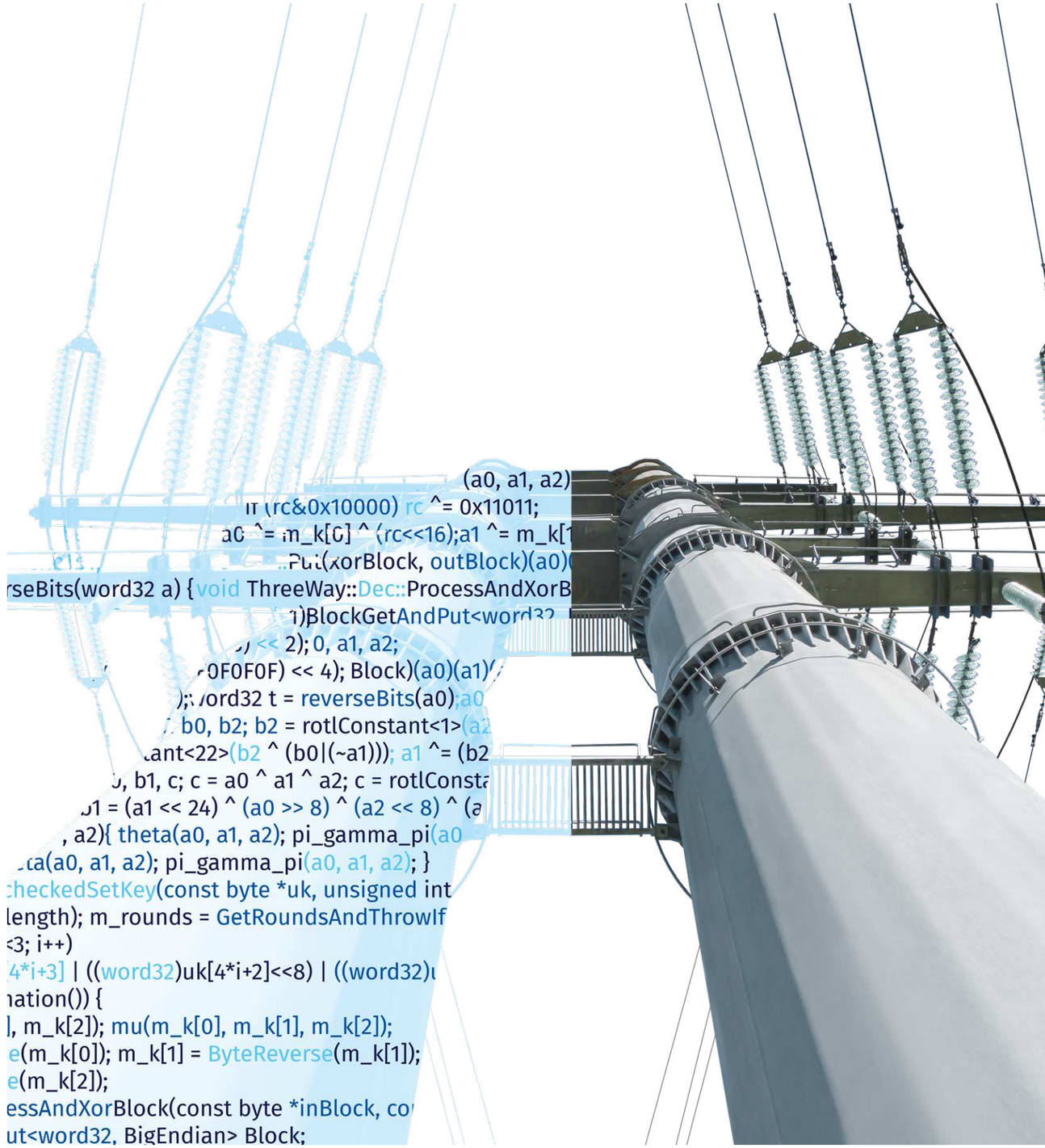
The risk often comes from lack of knowledge on the part of supply chain partners. "If system vendors don't have a full understanding of the threat picture, neither will those who buy the systems from them," says Margrete Raaum.

"There are a lot of companies in oil and gas that use standards to help them ensure security in implementation, but you still need the full cooperation of the vendor. If the vendor doesn't have enough insight, the customer's evaluation will also be flawed."

Lack of supply chain visibility is especially concerning because 'remote access to OT systems' is among the top three methods that our expert respondents expect hackers to use to exploit organizations (67%). This highlights the need for supply chain audits and vendor security requirements.

Proportions that would describe their vendor and supplier security oversight as mature





3

THREE CRITICAL TAKEAWAYS

3 THREE CRITICAL TAKEAWAYS

Our research indicates that achieving cyber security maturity in the energy sector, like the nascent safety discipline of the late 20th century, is a work in progress. It also needs to be a continuous process, and not something a business can deploy overnight and revisit at a later date.

In consideration of the specific challenges revealed by our research, along with the insight provided by experts during discussions about the findings, we recommend that energy firms adopt the following three principles, which will support them in their efforts to enhance cyber security across their IT and OT platforms:

1. Allocate budgets that can make a difference

In an industry that is investing in major digitalization and energy-transition programmes, while contending with the pressures of an uncertain trading environment, many may struggle to reserve the budgets they need to upgrade their capabilities. Around one in three respondents, on average, indicates that they are underinvesting in their IT and OT capabilities.

For some senior leaders, the default position for many years may have been to invest enough to ensure compliance with regulation and then review in due course. Today, we still see that mindset among a minority of respondents. And yet, if a severe incident takes place, even for reasons that are out of the company's hands, saying "We complied with regulation" is unlikely to placate stakeholders.

"Cyber is not something you can get through with a box-ticking compliance mindset, where you slip back into your old habits once the auditor leaves the building," says Solberg. "It's of course vital that you are compliant, but you need to go further to make sure that you are completely secure, which takes a proactive approach."

For cyber professionals, who recognize that "Without budgets, there is nothing you can do," Applied Risk's Jalal Bouhdada urges them to talk the language of the business to secure greater investment.

"Cyber executives get more attention when they can talk about the value-add," he says. "What's the return of investment from security, and how can you ensure that security can be a business enabler? You need to demonstrate how cyber security can help you in your business continuity, your permit to operate, in your reputation, in your compliance, in your dealings with regulators."

This business-oriented approach can be useful, suggests Andre Ristaino at the ISA, when technology suppliers are reluctant to invest in certification, such as the ISA/IEC 62443 standards for cyber security.

"Some suppliers end up getting much more return on investment than they anticipated because they carried out rigorous process reviews in their development organizations," he says. "Process reviews are needed for product certification. As a result of the process reviews, they found inefficiencies in their development and release processes. They fine-tuned these processes to become less costly and remove the non-value-added steps. They also elevated functional product testing processes, resulting in fewer defects getting out into the field."

2. Determine where you're vulnerable

One of the most urgent tasks facing companies in the energy sector is to identify where their projects and operations are exposed to threats before hackers can find them.

Companies need a clear and complete overview of their information and control systems – and those of their suppliers. Ensuring the security of technology platforms can be undermined if there are vulnerabilities elsewhere in the supply chain and cyber security has not been factored adequately into contracts with suppliers and subcontractors.

This far-reaching oversight allows organizations to prioritize the vulnerabilities and non-conformities they must address to stay cyber secure, and put the right people, processes, and technologies in place to build effective protection from threats. It is also not enough for companies to go through the process of discovering where they are vulnerable on a periodic basis only. It must be done iteratively to ensure resilience against new and emerging attack vectors.

A case in point is the emergence of Log4Shell in December 2021, where a previously undetected vulnerability was uncovered in a tool used in cloud servers and enterprise software across the world. Within hours of its discovery, the Log4Shell flaw showed signs of becoming the worst vulnerability discovered in years, largely because hackers could exploit it without needing authentication or special privileges. Although cyber security teams could patch the issue and safeguard their IT systems, it was less well-publicized that the nature of the vulnerability meant it was also present within industrial control system environments.

3. Balance investment between training and technology

When we asked respondents where they considered their organization to be most mature in their cyber security, they pointed more to upgrades to core IT systems and software (59%) than they did to training (41%) or the introduction of cyber security expertise (25%). As a result, it appears that less focus is dedicated to developing a workforce skilled in understanding and identifying threats, and in detecting and containing attacks.

One explanation for this focus on platforms over people is that businesses had to focus on making widespread, urgent upgrades to their existing and aging technology infrastructure, equipping it with the patches and firewalls it needed to block hackers. However, organizations today find vulnerabilities in their workforces, especially when it comes to responding to an unfolding cyber-attack.

The industry now needs to shift the balance so that its focus is more evenly distributed across these two critical areas. Businesses should certainly not reduce investment in technology upgrades, but they need to expand their training programmes while exploring carefully which specialist knowledge they do need to bring into the business.

"Cyber activity cannot take place without first-hand knowledge of industry pressures and the operational reality of energy environments," says DNV's Solberg.

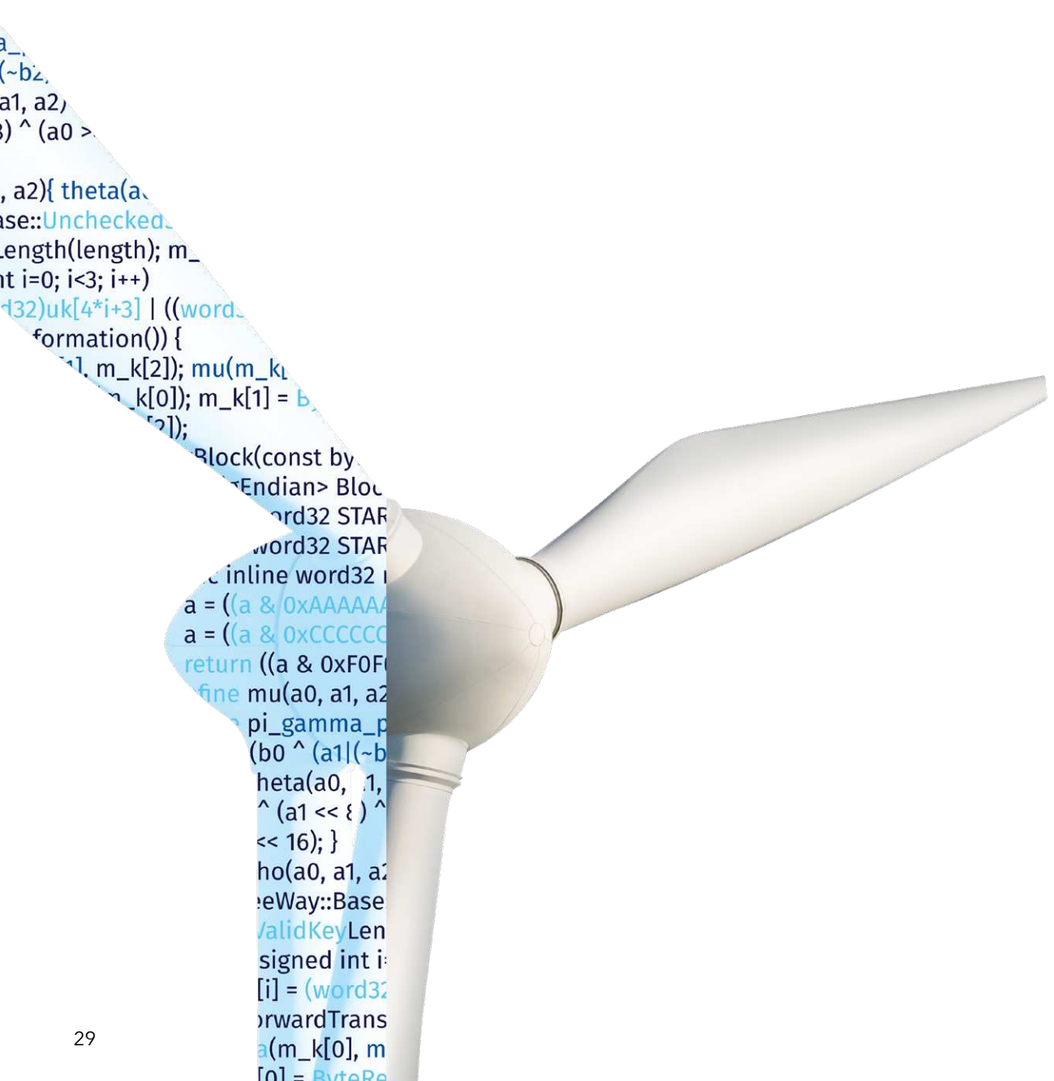
"Training in IT cyber security is vital but, for a robust cyber defence, businesses also need deep understanding of each energy domain, whether nuclear, renewables, or oil and gas, and assurance that cyber processes will not impact production or their long-term goals around the energy transition."

Cyber security professionals largely agree that there is no 'one-size-fits-all' approach to security that can be applied to all businesses. Similarly, it would be a mistake to believe that a cyber security paradigm that has been tried and tested in one industry can be replicated wholesale in a sector as complex and idiosyncratic as energy, and that two very different technical domains – IT and OT – can be treated interchangeably. It is there where external support may still take precedence over training in general cyber security standards.

CONCLUSION: A GROWING PRIORITY FOR THE SECTOR

A GROWING PRIORITY FOR THE SECTOR

The energy sector doesn't sit still. As leadership teams revolutionize their businesses to transition away from hydrocarbons, they need to respond to ongoing market uncertainty and the disruption caused by an evolving geopolitical crisis. At the same time, they must adapt to a global industry that is transforming as energy systems become more interconnected, reflecting advances in digitalization and automation.



These sector-wide challenges have a direct bearing on cyber security across the sector. Firstly, the rollcall of adversaries is changing, as environmental groups increasingly turn to direct-action methods such as hacktivism, criminal gangs 'follow the money' in a disrupted economy, and nation-states use cyberspace as a new theatre of war. Secondly, the increasingly interconnected nature of today's industry provides greater scope for attack, especially to critical OT that was previously protected by the air gap separating OT from IT systems.

In turn, our research finds some organizations making real progress toward cyber resilience, protecting their crown jewels while keeping pace with the threat. More worryingly, we also see a proportion of respondents waiting for a major incident to happen before investing in essential improvements to their defences. Organizations who increase their focus on cyber security will inevitably struggle to find the specialist talent they need and will face the broader challenge of achieving resilience across a complex and fragmented supply chain.

In this report, we drew parallels between the oil and gas industry's adoption of physical safety protocols in the 20th century and the state of cyber security in the today's energy sector. To end on a note of optimism, we would note that, when the industry focused on solving the safety challenge, it made extraordinary progress. Within a relatively short period of time – implemented global standards, improved its ways of working and use of technology, and embedded a safety-first mindset across the entire workforce.

We believe that a similar transformation is not only achievable in the field of cyber security, but will also be essential for the industry to meet its longer-term challenges around energy transition and digitalization.

As with the adoption of safety controls, these changes cannot be imported as a 'plug and play' from other industries, or without significant investment in upskilling the workforce. There needs to be careful consideration of the reality of different operational domains and an understanding of the knock-on effect of making changes within a complex network. Most importantly of all, there needs to be close collaboration and a commitment to working together across the industry.

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