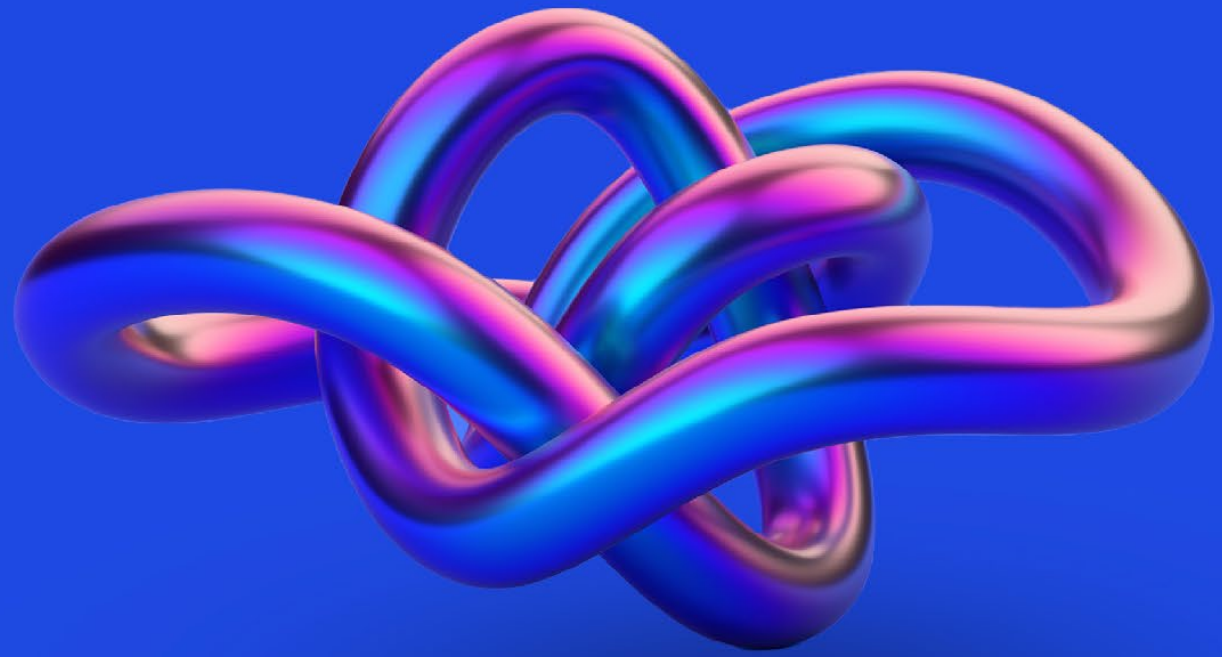
KPMG

Cybersecurity considerations 2023



Energy, Natural Resources and Chemicals

Foreword

The Energy sector is undergoing an extraordinary transformation that cuts across every subsector, including oil and gas, power & utility, chemicals, mining and natural resources, and renewables. To be clear, this is not a transition to a new way of doing business, but rather an overhaul of a series of systems that presents a tectonic shift in how energy is produced, consumed, and governed by nations, corporations, and individuals.

The pace and direction of this transformation is creating new industries, variants in existing industries, and myriad opportunities and risks. For example, utilities are morphing into renewables companies, auto makers are now also electric vehicle battery manufacturers, and oil and gas companies are in the clean technology business.

In parallel, there has never been a more challenging moment, as virtually every critical sector is seeing unprecedented cybersecurity attacks that threaten and harm every aspect of society. These threats target organizations and their infrastructure, including Information Technology (IT) and Operational Technology (OT) assets. The importance of these systems working together to support the entire enterprise is increasing rapidly, and threat actors are working to exploit this interdependence through ransomware, abuse of elevated privileges to sensitive systems, and software supply chain attacks, to name just a few modes of attack.

This dynamic is exacerbated by global events such as COVID-19, the Russian invasion of Ukraine, and various related economic disruptions. As this shift evolves, there has been a significant increase in regulations and collaboration between governments and government agencies at the federal, state, and municipal levels. This includes regulations that govern the core of the business as well as specific mandates related to cybersecurity.

The combination of large-scale changes in the industry, the unparalleled cybersecurity threats, and the ever-evolving regulatory landscape presents considerable challenges for Chief Information Security Officers (CISO).

This is not a CISO-only responsibility, but a collaborative opportunity for cybersecurity professionals, IT/OT engineering teams, executive leadership, boards of directors, third parties, consumers, regulatory bodies, and the communities in which organizations operate. For their part, CISOs will have to get comfortable with having discussions that are less about security vulnerabilities and more about the business risks posed by their organizations' potential exposures.

This report explores the set of cybersecurity considerations in the energy industry. Further, it explores actions CISOs and broader business can take in the year ahead to demonstrate to boards and executive leadership, and all other stakeholders, that effective cybersecurity is not a back-office speedbump, but a front-office enabler.

This report explores the set of cybersecurity considerations in the energy industry. Further, it explores the actions CISOs and business executives can take to demonstrate to boards and executive leadership, and all other stakeholders, that effective cybersecurity is not a back-office speedbump, but a front-office enabler.

Prasanna Govindankutty

Principal, Advisory
Energy Cyber Security Lead
KPMG

Key cybersecurity considerations for Energy in 2023

Click on each consideration to learn more.

Be resilient—when and where it matters

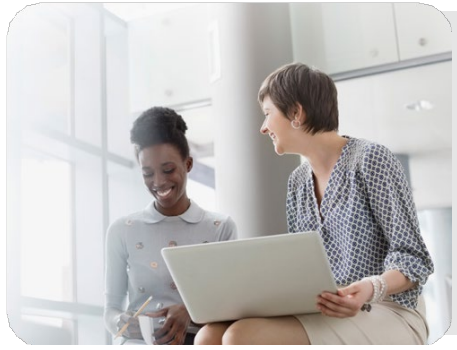
Why is it important to think beyond response and proactively plan for recovery?

New partnerships, new models

How can organizations keep security, privacy and resilience at the forefront in an environment where outsourcing and managed services are a growing priority?

Countering agile adversaries

How can security teams keep up with the pace of the changing threat landscape and the increasingly aggressive tactics of attackers?



Securing a perimeter-less and data-centric future

With the security perimeter all but gone, how can organizations pragmatically and realistically transition to a zero-trust approach that protects every aspect of their ecosystem?

Be resilient—when and where it matters

Every security system has its flaws. There is an air of inevitability that, at some point, an organization will suffer an incident, large or small, and likely more than one. Regulators are increasingly focusing on plausible scenarios and pushing companies — particularly those in strategically important industries like energy, finance, and health care—to be resilient and position themselves to recover.

Perhaps the most glaring issue is that organizations often don't see that the impact of—and recovery from—a cyber incident can be protracted. It's typically not a 72- or 96-hour event. They have to assume large-scale business disruption and a worst-case scenario. In too many cases, senior leaders haven't fully appreciated the enterprise-wide technology linkages or the business operational dependencies—paying staff, paying suppliers, communicating with customers and investors—on those connections.

The regulatory outlook

Lawmakers and regulators are paying greater attention—increasing their demands for transparency and oversight. Many organizations are concerned about navigating an increasingly complex global regulatory landscape.

36% worry about their ability to meet existing or new cybersecurity regulation when activities are outsourced to digital service providers.

31% worry about the growing demands around critical infrastructure, which is the subject of increasing regulation in the UK, the EU and the US.

28% worry about existing or new regulation related to resilience of key systems.

26% worry about more stringent incident reporting requirements.

Source: KPMG Cyber trust insights 2022

Also, many organizations have yet to truly consider what they need to do proactively to be resilient. They assume they have a backup plan and sufficient security controls. But if they don't have a plan for a particular scenario, and business operations halt, this can have severe financial and reputational ramifications, let alone regulatory. There's also a psychological component.
CISOs need to have ongoing conversations with their C-suite colleagues and the board about the nature and motivations of attackers: the harder they hit you, the more likely you are to pay, and they know it. Most organizations still struggle to understand what they're really up against.

Proactive coordination is required in and out of battle

During the chaos of an active attack, the CISO's key objective is to provide the business with the insights it needs to continue operating. They must step away from the day-to-day technical details and engage proactively and strategically with the organization about the seriousness of the situation and how, collectively, the business must respond if it wants to recover expeditiously.

A big part of the CISO's job is to be a communicator and to articulate across the enterprise the potential business impact of a breach and the value of keeping cybersecurity top of mind. Beyond that, response and recovery—the components of resilience—require coordination. This can be achieved through a small 'crisis board' comprising the CISO, CEO, CFO, and the chief legal counsel.

Unfortunately, because many companies don't think an attack will happen to them, this important group doesn't formally exist. And if it does, they believe their business continuity plan—which in many cases is several years old and aligned to an outdated set of use cases—is sufficient. It's not.

Recovering to your minimal viable business

It's about more than just building in good security because controls fail. It's about gaining clarity around what it takes to recover. Company leaders tend to look at the immediate horizon because most can't think any further when they're in the middle of an event. At that point, the CISO must be the voice of reason and talk pragmatically about getting back to minimum viable business processes: keeping the lights on, paying people, and ensuring that operations resume.

The longer it takes to get back to minimum viable business processes, the more likely the business will have an existential crisis. The bad actors don't work on your timetable. They innovate faster because they're financially motivated. That's the challenge CISOs face—they're perpetually playing catch-up.

Regulation's role in resilience

When it comes to resilience, regulations can either be seen as a foundation or a ceiling. Most organizations see it as the latter—something they must comply with; therefore, they do the bare minimum. Alternatively, it can be viewed as a foundation because there are frequently new or different actions to be taken.

Regulation plays a vital role in organizational resilience but often needs to be coordinated or aligned. This is one of the greatest challenges CISOs face as the regulatory line of sight imperatives expand to encompass a company's supply chain. It's no longer just a matter of worrying about the organization overall. CISOs have to consider the downstream implications for suppliers and other key partners and whether they're compliant with the relevant regulations, as well as the upstream implications of whether customers and investors are unclear about whether the company is compliant with the European Cyber Resilience Act.

Resilience is ultimately an organization-wide issue in which cybersecurity has a vital role, alongside other recovery capabilities and disciplines such as business continuity. CISOs can play a key part in helping organizations proactively plan for disruptive cyber events, which can vary in nature, scale, and response to classic technology or property incidents. Many CISOs may also find themselves taking on wider resilience responsibilities as organizations focus more and more on such scenarios and their consequences—yet another evolution of the CISO role.

Energy industry considerations

When a security event occurs, CISOs must help the organization appreciate the connectedness of their technology and the end-to-end business disruption that can happen across channels. Clearly, a pipeline or power station going down is major, but IT disruption can also paralyze considerable pockets of the business.

The CISO should support an organizational conversation around resilience. In any cybersecurity situation, CISOs must be prepared to enable their business partners with the insights and guidance needed to continue operating. There are many organizations where the CISO doesn't interact with the board, audit committee, risk committee, or even the rest of the C-suite on a frequent enough basis to have those effective conversations. That should change in a systemically critical industry such as energy, natural resource and chemical (ENRC).

In addition to having an inventory of cybersecurity processes on a laptop, energy CISOs should have an appreciation of how the business runs. Like their counterparts in other sectors, energy CISOs need a seat at the business strategy table in addition to the cybersecurity table. They need to know the firm's short- and long-term business objectives to ensure their security objectives are aligned.

Senior security executives should think about what recovery looks like and what steps they can take to improve the organization's ability to recover from a breach. A strong response and recovery plan is far more effective if it's pondered early and often and tested regularly. Even if no plan is perfect, having nothing and building it on the fly in the middle of a crisis is the worst time to think it through.

New partnerships, new models

Gone are the days when security teams focused solely on the security of their organization's IT systems. CISOs need to understand when to hit the brakes, and when to press go on outsourcing cybersecurity efforts and determining what skills to keep in-house today and in the future. Security has become a business priority, delivered through a shared responsibility model between the organization and service providers.

CISOs today are supporting business strategy across the organization — from operational technology and product security to complex supply chain ecosystems. Increasingly, organizations recognize that innovation is improved by collaboration between various aligned sources, from supply chain and customer service to organizational design and information security.

That combination of innovation delivered at a competitive price point to customers, wherever they might be, is how enterprises can gain competitive advantage.

However, some organizations struggle to implement robust security at scale primarily because of a lack of talent and skills, which is why they're looking at outsourcing, managed services, and transition to the cloud.

Trusted communities

External partnerships are expected to also be vital to success in hyperconnected ecosystems, but practical barriers stand in the way of collaboration.

79% say constructive collaboration with suppliers and clients is vital, but only **42%** report doing so.

60% admit their supply chains are leaving them vulnerable to attack.

78% of executives are confident that the CISO can secure their data across the supply chain.

Source: KPMG Cyber trust insights 2022

Knowing what to retain

Just as companies cannot simply outsource security, they also need the right talent and skills in-house. It takes specialized knowledge to set up a repeatable control and measurement framework under which internal staff and third-party providers can operate effectively. One of the keys is understanding what to retain in-house in terms of security responsibilities and then identifying the most effective sourcing strategy for talent in those areas.

Using the cloud as an example, strategically, CISOs have to embody multiple personas—broker, orchestrator and integrator—to align the necessary staff and third-party skills and manage risk, governance, and reporting. That can't be outsourced fully. Organizations might be able to outsource preparation and planning, but, ideally, someone in-house who understands the business and security environments—and the potentially broad impact of a cyber incident—should manage the organizational overlay and quality control.

Finding the right blend of skills

It's crucial—and easier said than done—for CISOs to understand their internal and external responsibilities, navigate the gray area between different models and disciplines, and manage those complexities by establishing the appropriate controls.

Working with outside security providers requires a unique skill set, focusing on management and governance skills rather than technical skills. Regardless of the amount of work outsourced, organizations need to retain solid in-house security knowledge and capabilities. It's also essential that dialogue between parties is clear and regular to ensure implemented controls and KPI reporting are properly managed. Furthermore, it's crucial to agree on clear incident response processes and run relevant simulations to test the system.

CISOs need to assess their skills base regularly and aim to ensure the organization is equipped to be an intelligent, collaborative customer of cloud and managed security services. Doing so requires understanding the business's future infrastructure needs and determining what the security function should look like to provide the best support. The key word is "future"—look three to five years out and work back, rather than solely looking at the company's security needs today.

Energy industry considerations

As the perimeter fades, security needs to adapt, with a focus on the zero-trust paradigm, identity, access management, data, and the right controls underpinning it all.

Like other industries, ENRC companies can't simply outsource security and turn away. The internal security team is still responsible for defining the right security controls. And one of the key considerations is ensuring the team possesses the right blend of skills. CISOs need to have the right people in the right place to stand up a fit-for-purpose control framework for third-party providers.

Strategy, governance, risk management, and reporting can't be outsourced regularly. CISOs might be able to outsource the preparation of these activities, but they need an organization to dovetail with the company's overarching business objectives.

The ability to architect cyber controls in the cloud is a different skill set relative to more security engineering. Managing cybersecurity across organizations, APIs, platforms, and technology sets at business speed is a level of complexity that most ENRC organizations need to improve upon.

One of the key imperatives is identifying the right partner organizations. Partners need to be viewed through a lens that enables the security team to assess capability, capacity, and reliability, as well as the ability to flex with the organization's business model and external threat environment. And they've got to be able to do it at a competitive value point.

Countering agile adversaries

The time from initial compromise to enterprise-wide ransomware activation is shrinking. Increasingly, rogue and state-sponsored attackers can penetrate systems with automated tooling and accelerate the exploitation of systems. Security operations should be optimized and structured to fast-track the recovery of priority services when an incident occurs, which can reduce the impact on clients, customers and partners.

Cyberattackers have two apparent motives—exploitation and disruption. The exploitation of systems is to steal or manipulate data, whether for intelligence or fraud, and disruption is for extortion or political gain. The tactics can be quite different.

Some state-sponsored attackers focus on critical infrastructure, such as oil pipelines, electric utilities, and financial systems. The mission is to cause harm or chaos and exert political or economic influence to benefit the attacker and their sponsor. They intend to monetize the misfortune of others.

The probability of success for cybersecurity incidents has increased substantially, resulting in growing ransomware attacks in recent years. And it will likely continue if security professionals don't make it harder on the attackers.

Cybersecurity teams are struggling to keep up

Cybersecurity teams are under pressure to keep up with evolving threats, with talent shortages frequently undermining security efforts.

Over 1/2 of organizations admit they are behind schedule with their position on cybersecurity

More than 50% are either very or extremely confident in combatting various cyber threats, including from organized crime groups, insiders and compromised supply chains.

59% agree that attackers are exploiting vulnerabilities in procurement and the supply chain, but they do not know whether their defenses are strong enough to stop them getting through.

#1 internal challenge to achieving cybersecurity goals is lack of key skills (40%).

Source: KPMG global tech report 2022

To make matters worse, hybrid working has expanded the attack surface, raising the number of potentially vulnerable endpoints. Adding to the challenges, shadow IT within the business often includes business applications and software-as-a-service use over which CISOs and CIOs have limited visibility or understanding of the possible exposures.

Sharpening your security operations strategy

Time matters. How quickly can an attacker be detected, how quickly can they be contained, how quickly can services be restored—and in doing so, how can you minimize information and system compromise? It's less about how they got in and more about what information they obtain. Was it mission critical? Did it leak out the back door or is it being held hostage?

The time attackers take to move from initial compromise to successful exploitation of systems is reducing. Now it might take just a few days, or even less, for an attacker to deploy ransomware across an enterprise. Attackers are also increasingly creative in automating their tactics, even to the extent of exploring the potential of artificial intelligence (AI) in helping them plan and orchestrate their attacks. The bottom line: CISOs and their teams have considerably less time to detect intrusions and take swift and decisive containment action.

There is a triangular structure in today's security operations centers (SOC), with a small but specialized threat-hunt team at the top, various Level 2 investigators in the center, and numerous Level 1 alert analysts on the bottom triaging an ever-multiplying volume of alerts. That triangle needs to be inverted. Today's SOCs require fewer Level 1s, more Level 2s, and considerably more threat hunters looking for potentially catastrophic events. One way to do that, and respond to the pace and volume of attacks, is to automate Level 1.

An effective SOC requires leveraging of more advanced technologies, bringing the relevant data together, trusting the available tools to manage the alerts, and getting the partnership between human analysts, sophisticated ML, and robotic process automation right. New data sources can be drawn in that provide greater business context to the analysis of potential attacks, exploring the fusion of cybersecurity operations with physical security, fraud prevention, and insider threat management.

Achieving that level of trust is a challenge for most security organizations. Suppose CISOs and their teams can harness AI to do that triage work, look across the firewall and the security information and event management (SIEM) system, and assess the various threat intelligence sources and vulnerability scanning tools. They can be able to start trusting. That's where the SOC is headed, but it's not there yet.

Harnessing and retaining technical cyber expertise

As for talent, attrition and retention must be front- burner priorities. Many organizations need help to create a durable career path and model for the SOC. Teams are consumed with monitoring the system and they throw more personnel at the problem rather than properly training the professionals already on the job.

As a result, people feel stuck and ultimately move on, leaving CISOs with a perpetual revolving door in the SOC. All because they haven't prioritized training. And while attackers continuously evolve their techniques, tactics and strategies and become better and faster at what they do —, CISOs don't have the resources to keep up.

Energy industry considerations

The attack surface in all energy-related sectors is expanding rapidly. Along the way, organizations have been exposed to several vulnerabilities, leaving them open to attack from evolving threats that are targeting critical infrastructure.

This is exacerbated by the rapid adoption of a hybrid work environment, increased reliance on external third parties, the influx of alternative energy businesses, infrastructure modernization, and increasing convergence of IT and OT environments.

While organizations are managing these changes in real time, adversaries are upskilling and increasingly deploying commercial-grade capabilities. This has been a particular challenge for energy companies, on whom citizens rely for critical services such as water, gas, and power.

A key consideration for the industry is to focus on recognizing the sprawl of the asset estate owned by IT and OT. Equally important is to operate under the assumption that attackers will indeed access the environment and focus on industrializing response mechanisms. This requires close coordination between vulnerability management, threat intelligence, incident response, resiliency, and cyber risk management teams across IT and OT.

Further, CISOs should de-silo operations across these teams to keep the focus on reducing "dwell time" by conducting regular gap assessments, investing in the right set of technologies, improving process engineering, and participating in enterprise resiliency exercises.

Additionally, cybersecurity teams should begin leveraging data from external sources and internal threat intelligence sources. As technologies continue to consolidate, CISOs are encouraged to enable their teams to look for opportunities to pursue alignment between programs, processes, and technologies. This will allow for a data-centric, process-oriented and technology-enabled approach to securing the attack surface and managing adversaries effectively and continuously.

Securing a perimeter-less and data-centric future

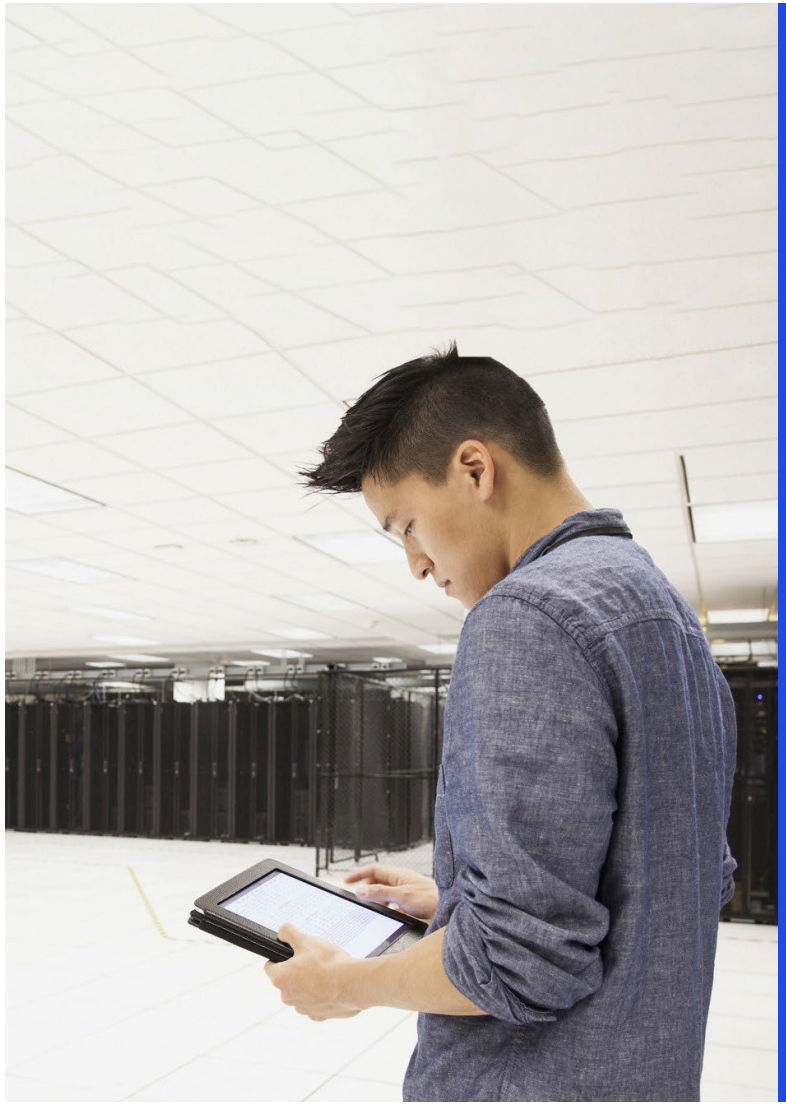
It's no surprise that business operating models have fundamentally changed over the last decade—becoming more fluid, data-centric, connected ecosystems of internal and external partners and service providers.

In this distributed computing world, to help reduce the blast radius of any potential outages or breaches, CISOs and security teams must adopt very different approaches, such as zero trust, Secure Access Service Edge (SASE) and cybersecurity mesh models.

Today, the clear business imperative is to enable employees, customers, suppliers and other third parties to connect seamlessly, remotely and securely. The accompanying security challenge is that, in a perimeter-less environment, organizations are no longer able to trust every user and device.

Zero trust for perimeter-less businesses

Zero-trust approaches can help reduce the blast radius in the event of an outage or breach and limit the impact so the incident can be better managed and contained.



Data security is a key issue for stakeholders

In a perimeter-less environment, concerns over how data is protected, used and shared are the leading factors undermining stakeholders' trust in an organization's ability to use and manage its data.

28% of executives identify 'a lack of confidence in the governance mechanisms in place' as a leading factor undermining stakeholders' trust in an organization's ability to use and manage its data.

32% also identify 'a lack of clarity over why data is required for a particular service and the benefits of sharing or providing data' as another factor.

36% are concerned over how their data is protected.

35% are concerned over how their data is used or shared

Source: KPMG Cyber trust insights 2022

SASE and cybersecurity mesh models with a foundation in zero trust have common principles in terms of how security overall is organized, distributed and aligned across the network. Perhaps most important, however, is that as more enterprises adopt a cloud-centric mindset, it has become critical to move security mechanisms closer to the data.

As an umbrella over today's perimeter-less business environment, zero trust is a framework, a way of thinking about how the design and enablement of security and identity access needs to change over time. Zero trust complements the convergence of services under a SASE model and the holistic, analytical cybersecurity mesh architecture.

New models of identity

Decentralized identity access management is a core responsibility for CISOs and a function of network traffic. The north-south traffic concept — that is, user to resource — is all about identity, while east-west traffic — lateral movement within the environment — is about segmentation and other controls.

The link between data and identity is unmistakable. In a perimeter-less environment, there's no zero trust, SASE, or cybersecurity mesh without a clear underlying focus on identity and data governance.

For CISOs, the challenge with zero trust is verifying that devices and users are who they say they are and can be trusted. This requires CISOs to think about security from an identity verification perspective, focusing on least privilege access for users within their enterprise and the many third parties with whom they interact.

Making zero trust work in practice

Zero trust should be defined in relation to every scenario, every user and every endpoint — representing a key pillar of the company's foundational security program and core principles. CISOs must play a key role not only in codifying the zero-trust model and message, but also in establishing policies, setting standards, designing software solutions, and assembling an enterprise-wide security council encompassing various technology and business leaders.

Another challenge is around funding and budgeting. CISOs must be able to explain the framework around zero trust, so the board and other corporate leaders understand that the investment is not just another new technology but a new way of thinking that is designed to support a secure, perimeter-less future.

Finding a middle ground between on-and off-prem structures is a distinct challenge, particularly with cloud- native technologies. Many companies are thinking about moving multiple processes to the cloud, but often legacy infrastructures cannot fully adapt to SASE specifications because of the advanced technology requirements.

CISOs at large, complex organizations have the challenge of managing a security posture that spans an on-prem and off-prem ecosystem that can result in higher operational costs in the short term while operating in this dual environment. Clients looking toward full cloud adoption should consider the same on-prem zero-trust principles for systems they deploy into the cloud. They should also factor in the impact of an operating model change. For example, a well-managed shared responsibility model with a cloud provider can be key to helping ensure a secure cloud architecture.

Energy industry considerations

Clearly, the entire cyberattack surface has been reimagined. As a result, the threat risk for oil and gas, power and utilities, and other ENRC companies—like all critical industries—is no longer confined within the corporation; it extends into the third-party universe.

Given the heightened threat landscape, a top priority for energy-related companies is to understand their data: where it's housed, what it's used for, how it's accessed, and how it's being secured. This reveals where the organization's critical systems reside. There are numerous data analytics tools available to help security teams predict patterns, understand the anatomy of attackers, have intelligence at scale, and make smart, timely decisions. Understanding data and ensuring that the right controls and flexible monitoring techniques are being applied can be difference between recovery and extended disruption.

As CISOs at ENRC companies increasingly incorporate a zero-trust approach, it's important to consider the risks that cloud and API misconfigurations can bring. The fact that there is a shared responsibility in connection with these third-party resources should be a focus to ensure end-to-end visibility between the internal security team and cloud providers.

Companies would do well to invest in their overall identity management capabilities and work to achieve a mature identity governance and services stack. Network segmentation is also recommended because we have seen a lot of lateral movement by attackers in data centers, OT environments, and the cloud.

Cyber strategies for 2023

What actions can CISOs and the broader business lines take in the year ahead to help ensure security is the organization's golden thread? Following is a short list of tangible steps CISOs should consider as they seek to accelerate recovery times, reduce the impact of incidents on employees, customers, and partners, and aim to ensure their security plans enable—rather than expose—the business.

People

- Prioritize a robust cybersecurity culture that is interesting, engaging and, where appropriate, fun, to inspire employees to do the right thing and function as human firewalls.
- Build a security team with the skills mix needed to manage a perimeter-less organization, including cloud and third-party dependencies.
- Communicate broadly and clearly. Ask leaders in other organizational functions about their pain points and how automated processes might help.
- Take a multidisciplinary, cross- culture approach. Establish a security ecosystem comprising internal business line specialists, security professionals, data scientists, privacy-oriented attorneys, and external policy and industry professionals.
- Embed yourself in the organization and act as a peer, a sounding board, and an advisor.

Process

- Build consistent approaches to cyber risk management with an understanding of threat scenarios and attack paths to help inform attack surface reduction and prioritize control improvements.
- Focus on fit-for-purpose security processes that feature consistent user experiences.
- Establish strict identity controls and work to achieve a mature state of identity governance and services.
- Segment legacy environments to limit the attack surface and help contain any breaches.
- Have a proactive recovery plan focusing on the organization's most critical workflows with a communication structure, and stress test it often.
- Consider subscription support models with predictable costs, any-shore delivery, and strategic results.

Data and technology

- Embrace the inevitable automation of the security function – Trust the latest tools, such as robotic processes, security orchestration, automation and response (SOAR), and extended detection and response (XDR) systems.
- Work with cloud providers to help ensure broad visibility into how products and services are configured to avoid inadvertent vulnerabilities.
- Consider cybersecurity and privacy issues up front when exploring emerging technologies, including the evolving risks associated with adopting AI systems.
- Assign responsibilities and establish accountability around how critical data is processed and managed and how it supports critical business processes.
- In the interest of speed, scalability, and trust, a transition to identity as a service in the cloud needs to happen sooner than later.

Regulatory

- Be aware of changing regulatory trends and drivers and what they could mean for the company's future technology strategy, product development, and operations.
- Consider the regulatory impacts vis- à-vis AI and automation – Establish a clear concept of what the business can and can't do in these arenas and be alive to public concerns and changing expectations.
- Explore automating compliance monitoring and reporting and task a team member to serve as a regulatory monitor to stay on top of privacy and security regulatory trends.
- Align security and privacy compliance strategy with the company's broad business strategy to help ensure stakeholders from across the organization are on the same page.
- Look beyond the letter of the regulation—and be prepared to ask yourself more fundamental questions about digital trust and how you make that central to your strategic thinking.

How KPMG professionals can help

KPMG firms have experience across the continuum—from the boardroom to the data center. In addition to assessing your cybersecurity and aligning it to your business priorities, KPMG professionals can help you develop advanced digital solutions, implement them, monitor ongoing risks, and help you respond effectively to cyber incidents. No matter where you are in your cybersecurity journey, KPMG firms can help you reach your destination.

As a leading provider and implementer of cybersecurity, KPMG professionals know how to apply leading security practices and build new ones that are fit for purpose. Their progressive approach to cybersecurity also includes how they can deliver services, so no matter how you engage, you can expect to work with people who understand your business and your technology.

Whether you're entering a new market, launching products and services, or interacting with customers in a new way, KPMG professionals can help you anticipate tomorrow, move faster, and get an edge with secure and trusted technology. That's because they can bring a strong combination of technological experience, deep business knowledge, and creative professionals passionate about helping you protect and build stakeholder trust.

KPMG. The Difference Makers

Contact us

Prasanna Govindankutty
Principal and Energy Leader – Cyber Security Services
KPMG in the US
pkgovindankutty@kpmg.com

Brad Stansberry
Advisory Industry Leader, Energy, Natural Resources and Chemicals
KPMG in the US
bstansberry@kpmg.com

Angie Gildea
National Sector Leader, Energy, Natural Resources and Chemicals
KPMG in the US
angelagildea@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia