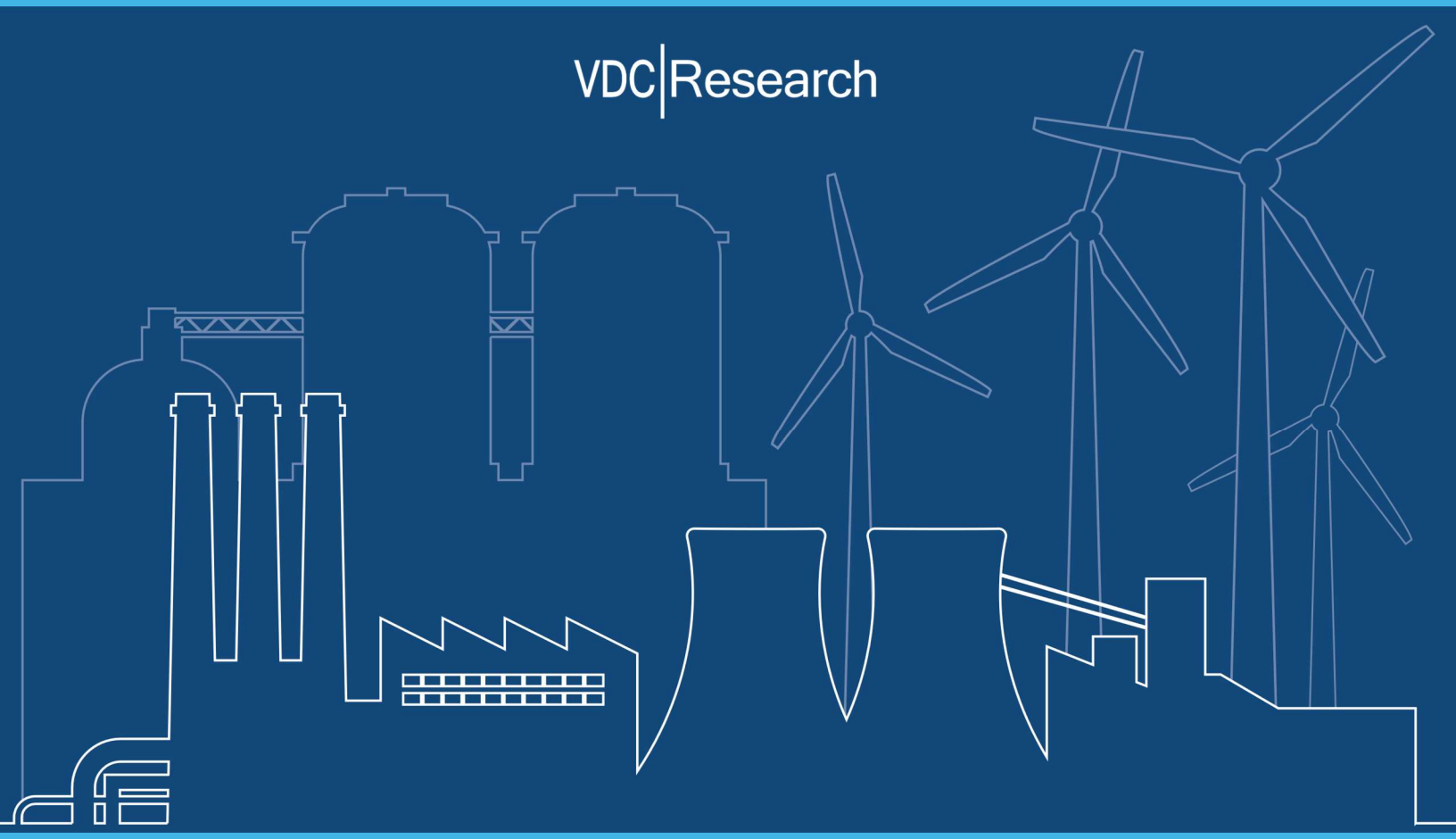
Powering Cyber Resilience in the Energy Sector



Licensed to Distribute by:

kaspersky

VDC|Research

by Jared Weiner, Director

Chris Rommel, Executive Vice President

Executive Summary

Energy and utilities organizations are accelerating digital transformation to enhance efficiency, reliability, and sustainability across generation, transmission, and distribution. As digital infrastructure expands, the industry is rapidly moving toward a "fully digital" operational model. Nearly three-quarters of surveyed organizations expect to achieve full digitalization within the next two years.

This transformation, however, increases exposure to cyber threats. Expanded connectivity across industrial control systems, substations, and distributed assets has broadened the attack surface for both cybercriminals and nation-state actors. Cybersecurity concerns now represent the most significant barrier to digital adoption, especially as organizations work to modernize legacy control environments and secure remote assets.

Key Insights at a Glance

- *75% expect to be fully digital within 2 years*
- *45% cite cybersecurity talent shortages as their top challenge*
- *50%+ experienced cyber incidents costing >$1M*
- *19 hours average downtime per breach*

Human-capital constraints further amplify these risks. More than 45% of respondents cite a shortage of specialized industrial cybersecurity talent, and fragmented governance between IT and operational teams frequently leads to inconsistent policies and delayed patching cycles.

The consequences of inadequate OT cybersecurity are substantial. Over half of surveyed organizations reported cyber incidents costing more than $1 million, and breaches caused an average of 19 hours of production interruption, highlighting the direct link between cybersecurity and grid reliability.

To strengthen resilience, energy organizations must prioritize three core capabilities:

1. **Industrial-grade protection** that provides real-time asset visibility, anomaly detection, and compliance support.
2. **Integrated platforms** (e.g., Kaspersky Industrial CyberSecurity) that secure IT, OT, and IIoT environments cohesively.
3. **Domain-expert partners** with deep domain expertise and alignment with global frameworks such as ISA/IEC standards and leading regional energy cybersecurity regulations.

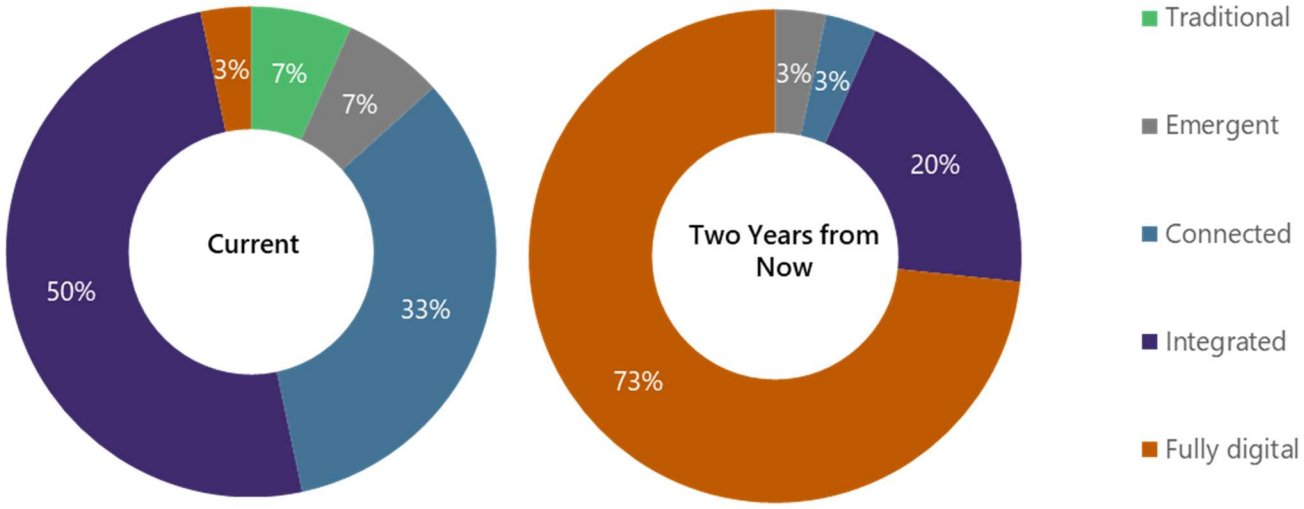
Digital Transformation in Energy & Utilities

In recent years, energy and utilities organizations have accelerated their digital transformation efforts to address mounting economic volatility, fluctuating energy prices, regulatory pressures, and the growing need to optimize grid efficiency and asset performance. In parallel, the global decarbonization goals established under the Paris Agreement have intensified the sector's drive to modernize existing infrastructure, but also to build entirely new grid capabilities to support emerging energy sources, including expanded DER systems, advanced automation, new substations, microgrids, and additional transmission lines. This shift is pushing the industry to adopt digital solutions that enable cleaner, more efficient, and more transparent energy systems.

Despite the challenges of integrating digital systems across complex grid, plant, and field operations, recent survey findings[1] suggest that the energy and utilities sector is rapidly approaching a "fully digital" future. Nearly 75% of respondents expect their organizations to be fully digital two years from now, compared with less than 5% today [See Exhibit 1]. While a complete transition will take time, rapid progress in IoT connectivity, edge computing, and grid automation including wide-area grid automation and advanced wide-area management systems for cross-substation telecontrol and relay protection is propelling energy and utilities organizations forward and expanding the digital foundation of critical infrastructure.

Exhibit 1: Energy & Utilities Organizations' Current and Expected Digital Transformation Status[2]

(Percentage of Respondents)



[1] See *Background on VDC Research* section for details.

[2] Traditional–mostly/entirely reliant on manual processes; Emergent–beginning to adopt digital technologies for specific tasks; Connected–multiple connected digital technologies; Integrated–high levels of automation and connectivity throughout the organization; Fully digital–proactive, continuous improvement of digital capabilities.

Throughout the sector, digital technologies now underpin a broad spectrum of operational objectives, from bulk power generation and ultra-high voltage (UHV) transmission to grid management, field operations and customer engagement. For UHV transmission operators in particular, digitalization supports a distinct set of objectives focused on system reliability and continuity (commonly measured through KPIs such as SAIDI and SAIFI) driven by the need for engineering modularity, system agility, and long-term ROI improvement. Survey data shows that improving production efficiency, reducing operational costs, and strengthening cyber resilience are the leading drivers behind energy and utilities organizations' digital transformation initiatives [See Exhibit 2]. These priorities are also reinforced by the growing advantages of virtualized control, embedded intelligence, and more resilient grid architectures, which together enable faster automation updates, real-time forecasting, and improved system stability. By integrating digital systems and unifying enterprise and operational data sources, energy providers can make real-time, data-driven decisions that enhance grid reliability, asset utilization, and worker safety, while next-generation substation and power plant automation systems evolve toward more software-defined, distributed control architectures that promise greater stability, resilience, and long-term economic benefits.

Exhibit 2: Primary Factor Driving Energy & Utilities Organizations' Digital Transformation Strategy

(Percentage of Respondents)

In the energy sector, digitalization now underpins every stage of the value chain. **In generation**, platforms for asset performance management, predictive maintenance, and electrical digital twins are driving greater equipment reliability and efficiency, helping operators reduce unplanned outages and optimize fuel use. In transmission and distribution, the convergence of smart grid systems, IoE (Internet of Energy) applications, and energy cloud architectures is transforming how networks are monitored, modeled, and stabilized in real time, enabling predictive analysis based on weather and grid data, dynamic power flow adjustments, and coordinated

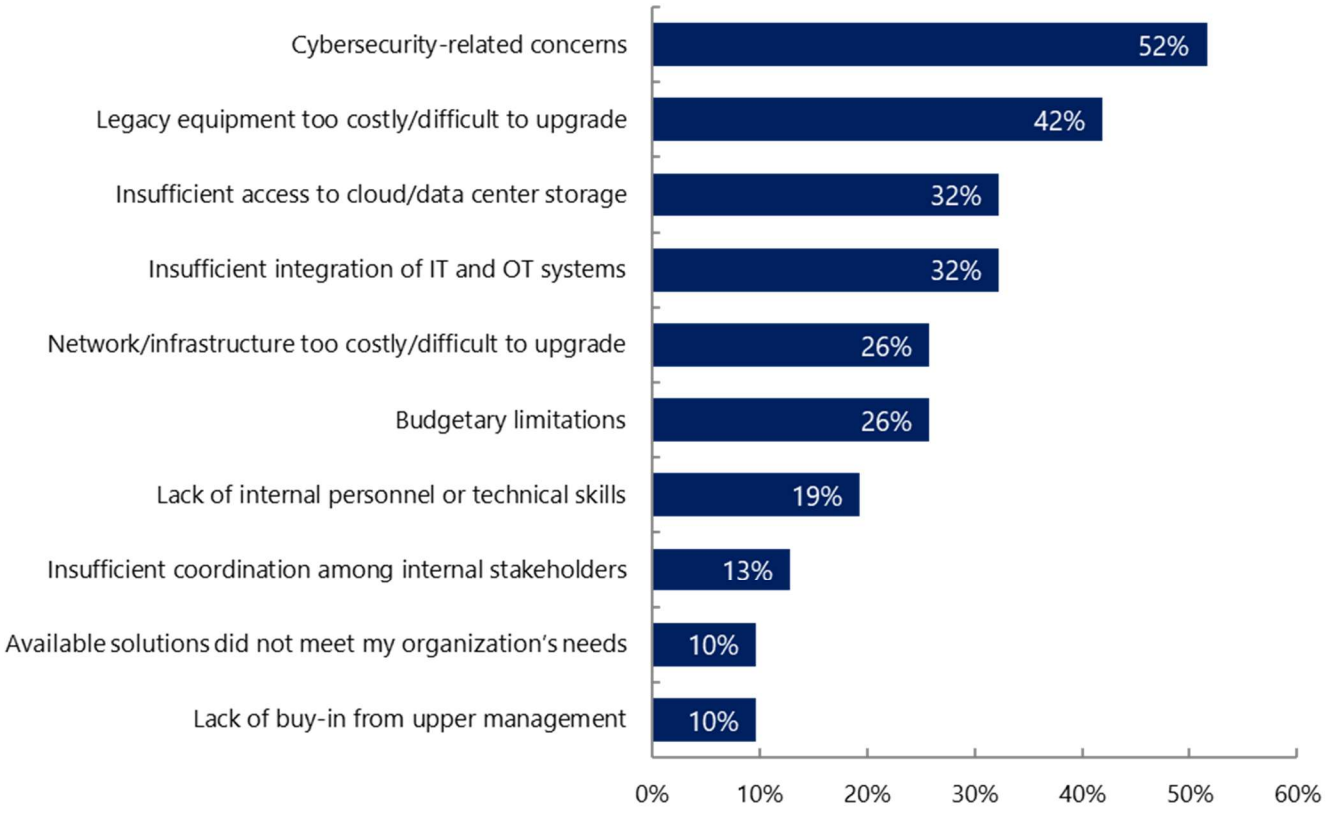
control across connected assets. Meanwhile, **utilities and service providers** are increasingly leveraging AI- and machine learning-driven analytics to optimize supply and demand, predict maintenance needs, and enhance customer forecasting and service delivery. Advancements in robotization, such as sensor-integrated drones and automated inspection systems, are further improving asset monitoring and operational safety across generation sites, substations, and transmission lines.

Yet across all use cases, the effectiveness of these technologies depends heavily on the continuous flow of data from sensors, intelligent devices, and distributed energy assets. The same connectivity that enables real-time visibility and operational efficiency also exposes critical systems to a broader and more complex array of cyber threats. Increasing reliance on digital platforms, third-party service providers, and remote access capabilities has expanded potential entry points for attackers. At the same time, adversaries ranging from cybercriminal groups to nation-state actors are intensifying their focus on energy infrastructure, recognizing its strategic importance and potential for large-scale disruption.

Reflecting this heightened threat environment, cybersecurity concerns were cited as the most significant barrier to implementing digital technologies within OT environments across the energy and utilities sector [See Exhibit 3]. The specific cybersecurity-related challenges slowing digital adoption in this sector, shown in Exhibit 4, span a wide range of issues, from regulatory compliance and inadequate security measures to persistent OT/IT integration hurdles and reliance on legacy technologies. Many facilities continue to operate aging control systems running unsupported operating systems such as Windows XP, Windows 7, Windows 8, and Windows 10, or outdated embedded firmware, which lack modern authentication and encryption capabilities. Legacy PLCs, RTUs, older IEDs and serial-connected interface or protocol converters often remain integral to plant and substation operations but were never designed for networked environments, leaving them highly susceptible to exploitation once connected. For wind farms, substations, pumping stations, and other remote or distributed assets, limited or intermittent connectivity further complicates centralized monitoring and timely patch deployment. These conditions create fragmented security postures where visibility gaps and inconsistent protections increase both cyber and operational risk.

Exhibit 3: Factors Negatively Affecting Energy & Utilities Organizations' Ability to Implement Digital Technologies in their OT Environment

(Percentage of Respondents)

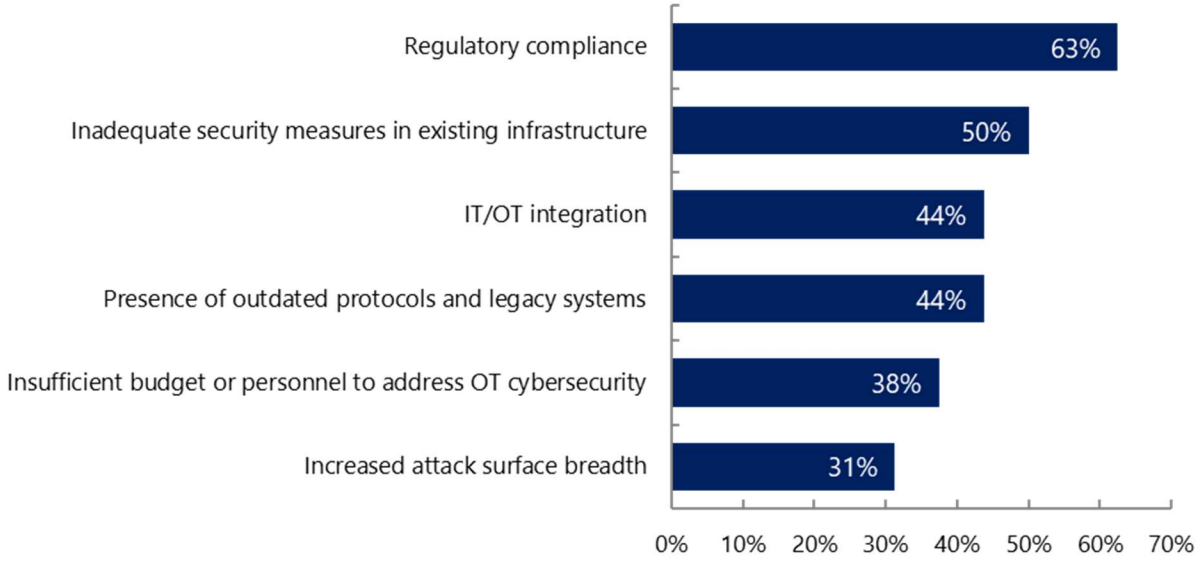


(Multiple responses permitted; not all answers shown)

Collectively, these factors underscore the scale and complexity of the cybersecurity hurdles facing energy organizations as they deploy and extend digital transformation initiatives. With connected OT systems now central to generation, transmission, and grid operations, establishing robust, efficient, and adaptive cybersecurity frameworks has become an operational imperative. The sections that follow examine emerging trends and outline practical strategies for risk mitigation, resilience, and cost efficiency in the implementation of next-generation OT solutions in the energy sector.

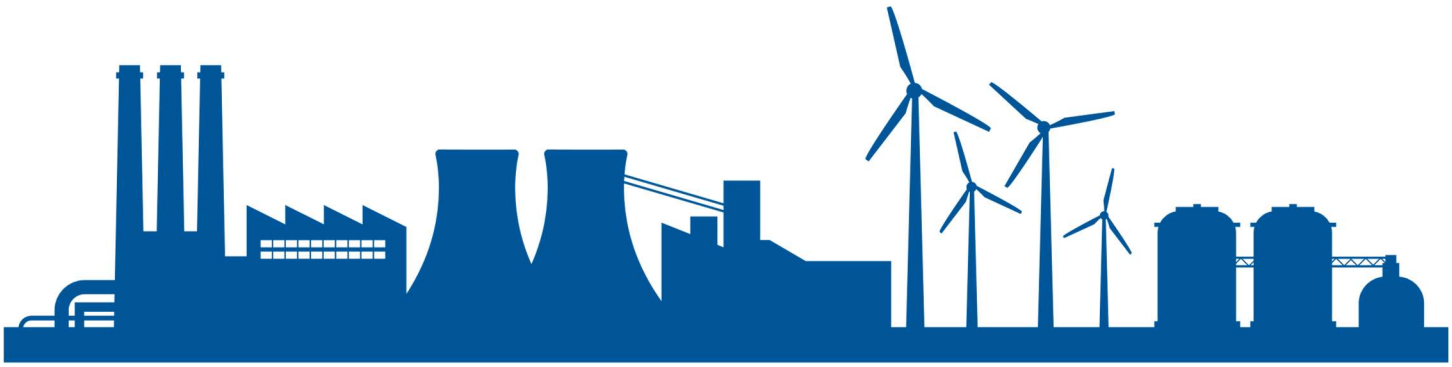
Exhibit 4: Cybersecurity-related Concerns Negatively Affecting Energy & Utilities Organizations' Ability to Implement Digital Technologies in their OT Environment

(Percentage of Respondents)



Background on VDC Research

VDC has covered industrial and other business-to-business technology markets since 1971. The analysis and supporting discussions in this paper are based on VDC's ongoing research in the OT cybersecurity market and by findings from a survey of more than 250 OT and IT decision makers familiar with the OT cybersecurity practices within their respective organizations. This survey offers insight into leading business and technical trends affecting OT organizations as well as the best practices implemented to address them. Respondents span a range of industries including energy and utilities, transportation and logistics, and manufacturing sub-sectors such as chemicals and pharmaceuticals, among others.



Human and Technical Challenges in Securing Energy Operations

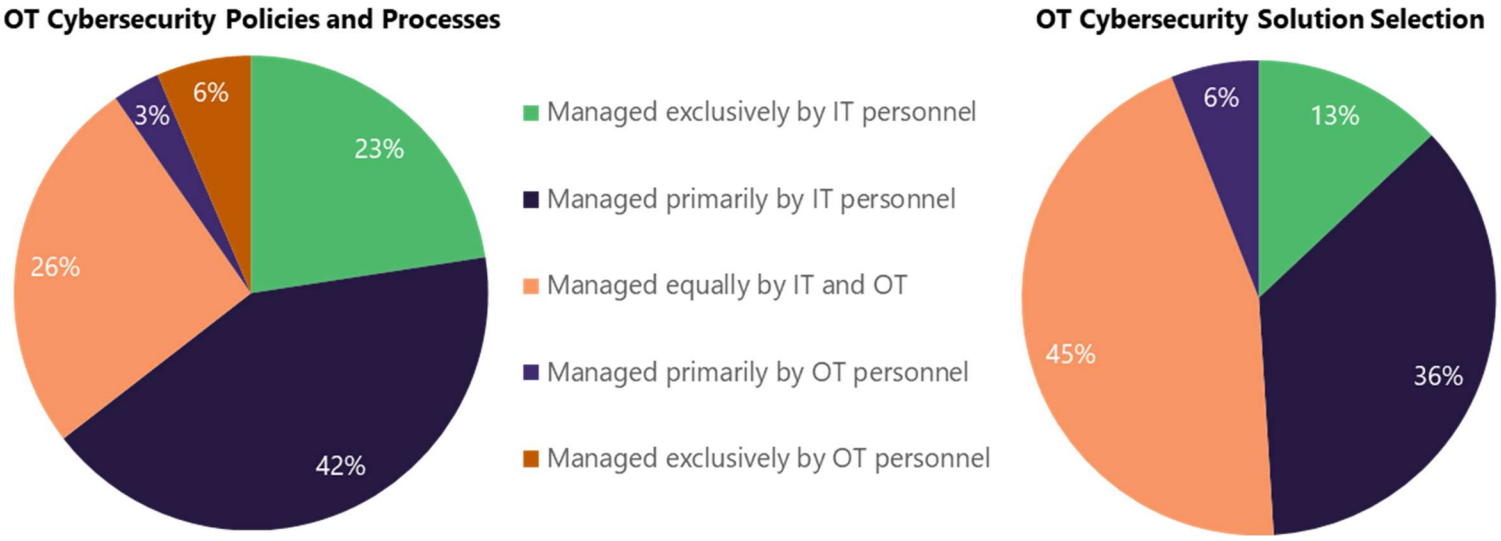
More than 45% of energy and utilities organizations cited a shortage of specialized OT cybersecurity talent as their most pressing security challenge.

The most pressing OT security challenge for energy and utilities organizations is the shortage of personnel with specialized skills across industrial control and automation cybersecurity, as cited by more than 45% of respondents. The lack of skilled OT security professionals constrains day-to-day operations and limits the capacity of control system teams to implement proactive defense strategies or coordinate effective incident response, ultimately weakening overall operational resilience. This challenge is exacerbated by the ongoing retirement of experienced engineers and plant operators, leading to a loss of critical institutional knowledge that is difficult to replace. Complicating matters further, current employment trends characterized by shorter job tenures and higher workforce mobility are eroding the long-term knowledge continuity once essential to sustaining secure and stable industrial environments. These workforce pressures are amplified by persistent technical challenges, including the complexity of integrating diverse security solutions across legacy and modern automation systems, and the growing problem of alert fatigue among overstretched protection and control personnel struggling to manage an ever-expanding array of monitoring tools and threat notifications.

Energy and utilities organizations continue to face both organizational and technical barriers that complicate cybersecurity across industrial automation and control systems (IACS). Misalignment between IT and operational teams remains a persistent issue: differences in priorities, governance models, and risk tolerances often result in fragmented security strategies. IT departments tend to emphasize data security and compliance, while engineers responsible for grid operations, SCADA environments, and substation automation prioritize safety, reliability, and uptime. Nearly three-quarters of respondents report that cybersecurity policies for control systems are managed primarily or exclusively by IT personnel, and fewer than 10% indicate management led by operations or engineering teams [See Exhibit 5]. This lack of coordination directly affects critical functions such as patch management, which in the energy sector requires meticulous planning to avoid operational disruption. Many organizations struggle to allocate the necessary downtime for patch deployment, leading to infrequent update cycles and prolonged exposure to sophisticated threats. Without unified governance, clear accountability, and automated patch management solutions aligned with ISA/IEC 62443 principles, energy providers risk leaving critical infrastructure vulnerable and undermining the resilience of their operations.

Exhibit 5: Personnel in Charge of Energy & Utilities Organizations' OT Cybersecurity Decision-Making

(Percentage of Respondents)

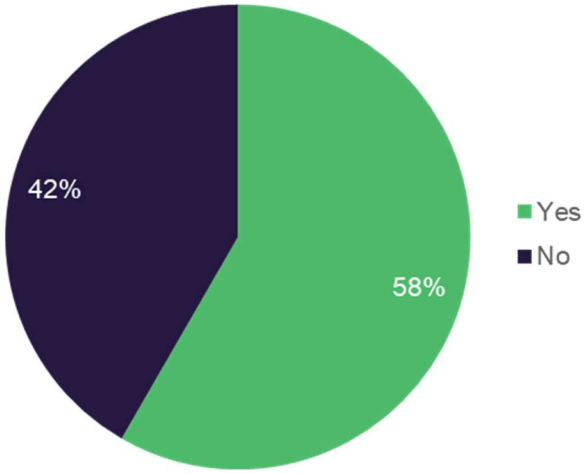


Financial & Operational Consequences of Breaches

Energy organizations that rush toward digital transformation objectives without adequately addressing OT cybersecurity risks expose themselves to severe consequences. In the energy sector, breaches are especially concerning, as disruptions to OT systems can threaten not only operational integrity but also public safety and grid reliability. The fallout from such incidents extends well beyond immediate safety hazards. Shutdowns can trigger cascading effects, from production losses and fuel supply interruptions to regulatory penalties and reputational damage. Even temporary outages can jeopardize service continuity and erode public trust. Reflecting this reality, nearly 60% of respondents reported that cybersecurity breaches in 2023 and 2024 had led to measurable financial impacts [See Exhibit 6].

Exhibit 6: Did Cybersecurity Breaches Cause Energy & Utilities Organizations to Incur Costs?

(Percentage of Respondents)



The financial repercussions of an OT cybersecurity breach in the energy sector are complex and far-reaching. Beyond the immediate costs of incident response, system recovery, or potential ransom payments, energy organizations must also account for the broader operational and economic fallout. A targeted ransomware infection that locks operators out of SCADA workstations, for example, can halt generation or transmission activities for hours or even days, leading to severe losses in energy output. Similarly, unauthorized access to PLCs or DCSs can result in equipment being taken offline or operated outside of safe parameters, which in turn can cause physical damage, extended downtime, and expensive replacement or repair cycles. Even when attackers only exfiltrate sensitive engineering data or disrupt communication networks, the resulting loss of visibility and control can trigger cascading operational disruptions and safety risks. In parallel, indirect costs such as lost revenue opportunities, contractual penalties for service interruptions, and erosion of customer or stakeholder confidence can compound quickly, amplifying the total financial impact well beyond the initial incident. Accounting for each of these cost categories, more than 50% of our survey respondents estimated cyberattack-related financial damages exceeding $1 million per incident across 2023 and 2024.

More than 50% of surveyed organizations reported cyberattack-related financial damages exceeding $1 million per incident.

Unplanned downtime has become a particularly critical performance metric for energy and utilities organizations. Downtime events disrupt power generation, delay transmission schedules, and undermine service commitments to customers, directly impacting revenue and regulatory performance targets. Although the sector has increasingly adopted condition monitoring, predictive maintenance, and other advanced reliability programs to reduce outages, cybersecurity-driven actions that can also prevent downtime are often undervalued. The connection between cybersecurity and operational continuity is clear. Survey responses indicate that the average production interruption caused by cybersecurity breaches among energy and utilities organizations was approximately 19 hours. Accordingly, energy organizations cannot afford to overlook cybersecurity as a core component of their downtime reduction strategies.

Cybersecurity breaches caused an average of 19 hours of production interruption among energy and utilities organizations.

Strategies for Strengthening OT Cybersecurity

Operators in this sector can address many of their OT cybersecurity objectives by deploying specialized cybersecurity solutions designed for converged operating environments. These solutions provide real-time visibility into network assets and traffic, detect and respond to anomalies before they escalate into incidents, and help ensure compliance with evolving industry regulations and frameworks such as the EU's NIS2 Directive, Japan's Cyber/Physical Security Framework (CPSF), Mexico's National Cybersecurity Strategy (ENCS), Saudi

Arabia NCA's Essential Cybersecurity Controls (ECC), the Kingdom of Saudi Arabia's OTCC 2022, and Malaysia's National Cybersecurity Baseline (NCSB) and MyBSS framework, among many others. By integrating threat detection, asset and network visibility, and automated response capabilities, they enable energy organizations to strengthen resilience across IT, OT, and IIoT domains. Among our survey respondents, organizations that implemented OT cybersecurity technologies exhibited greater cybersecurity maturity and fewer breaches.

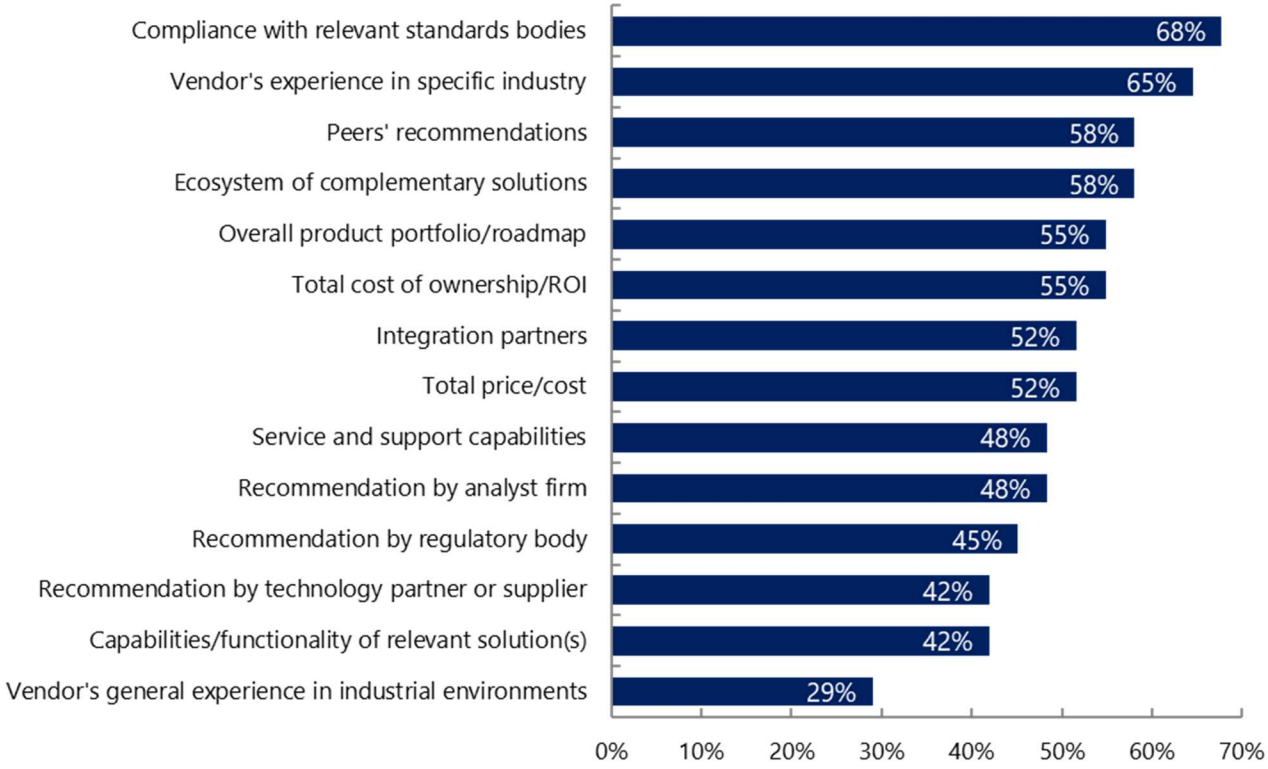
Energy organizations today may choose among a wide array of vendors offering OT cybersecurity solutions, each approaching objectives such as risk management, compliance, and operational continuity with its own unique combination of technologies, methodologies, and expertise. With such a diverse market, selecting the right partners requires careful evaluation of technical capabilities, sector experience, and the ability to integrate seamlessly into complex, converged environments. Energy and utilities organizations consider regulatory compliance and industry-specific expertise to be especially critical [See Exhibit 7].

Beyond global standards such as ISA/IEC 62443 and IEC 62351, many countries have introduced sector-specific regulations that require electricity providers and grid operators to implement rigorous cybersecurity controls, conduct regular vulnerability assessments, and adhere to standardized incident response protocols. Within the European Union, for example, the NIS2 Directive mandates that energy companies of a certain size implement baseline cybersecurity measures to protect against evolving cyber threats. Similar regulations exist in other regions, requiring strict adherence to standards and placing significant financial (and potentially even criminal) penalties on organizations that fail to comply. As a result, compliance readiness has become a key differentiator among cybersecurity vendors and an essential criterion in the selection process.

The ability to provide a broad ecosystem of complementary solutions is also an important consideration for organizations in this sector. Vendors such as Kaspersky exemplify this approach by offering unified cybersecurity solutions that address the specific needs of critical infrastructure operators and enable protection across IT, OT, and IIoT systems. Kaspersky's core OT offering, Kaspersky Industrial CyberSecurity (KICS), combines products for network visibility and endpoint protection within the native extended detection and response platform, enabling customers to deploy robust, tightly integrated cybersecurity protection from a single, trusted source.

Exhibit 7: Factors Considered Important when Organizations Select OT Cybersecurity Vendors

(Average of Responses)



VDC's View: Summary & Recommendations

Prioritize OT Cybersecurity to Protect Operations and Profitability

While IT-related breaches can be highly disruptive, the stakes are significantly higher in the energy sector, where cyber incidents targeting OT environments can lead to severe physical consequences, including equipment damage, service interruptions, environmental harm, and even risks to human safety. The financial impact can also be substantial, encompassing both direct costs such as ransom payments, regulatory penalties, and remediation, and indirect losses tied to production downtime, grid instability, and reputational damage.

Using traditional IT-grade endpoint protection in industrial environments can inadvertently increase these risks. Generic security agents may interfere with legitimate control system processes or lack OT-specific protections capable of detecting and stopping threats unique to operational technology. Both scenarios can disrupt production continuity and increase downtime.

To address these challenges, energy organizations are increasingly turning to industrial-grade cybersecurity solutions designed specifically for OT environments. Such solutions provide visibility into industrial networks, help identify vulnerabilities and configuration anomalies, and protect hardware and software components without disrupting operations. Vendors like Kaspersky, through offerings such as Kaspersky Industrial CyberSecurity

(KICS), exemplify this approach by combining OT-specific protections with complementary services such as threat intelligence, security assessment, and incident response – helping energy and utilities organizations strengthen resilience and maintain operational continuity.

Partner with Trusted Cybersecurity Providers to Strengthen System Defense

The complexity of substation and power plant protection and control solutions, grid/network management, condition monitoring, communication, measurement and other systems in the energy sector makes it difficult for most organizations to design, deploy, and manage comprehensive cybersecurity strategies independently. Persistent workforce shortages and widening expertise gaps have only intensified this challenge in recent years.

Energy organizations leveraging formal OT cybersecurity solutions experience fewer incidents and lower associated costs than those without dedicated protection. By partnering with enterprise-grade cybersecurity providers such as Kaspersky, which brings deep, sector-specific expertise across IT, OT, and IIoT domains, energy and utilities companies can strengthen their defense posture and ensure that critical infrastructure is protected by purpose-built, industry-tested technologies and further supported by expert-led professional services. Collaborating with a proven vendor offering end-to-end coverage through an integrated platform enables greater operational simplicity, improved visibility, and stronger alignment with enterprise systems.

Seek Partners with Deep, Relevant Expertise

Station buses, process buses, and telecontrol networks are common OT architectures in the power sector, and although these data models are well standardized, they connect inherently heterogeneous systems. These include intelligent electronic devices (IEDs), substation and plant control systems, equipment-condition monitoring platforms, and local automation solutions that vary across generation, transmission, and distribution operations. Energy providers must also navigate complex and often sector-specific regulatory frameworks designed to safeguard critical infrastructure.

Given the high stakes of non-compliance, power system operators, grid operators and utilities organizations should seek cybersecurity partners that understand both the technical realities of OT environments and the regulatory obligations shaping them. To meet these obligations effectively, organizations should prioritize partners with proven regulatory expertise and solutions designed for compatibility with diverse OT assets and legacy systems.

Vendors such as Kaspersky, with more than 25 years of global cybersecurity experience and proven expertise in the energy sector, offer enterprise-grade protection and deep expertise across IT, OT, and IIoT systems. Their solutions help energy organizations strengthen compliance readiness while ensuring compatibility with diverse assets and legacy systems. This approach ensures that cybersecurity programs not only enhance protection and resilience but also maintain alignment with evolving industry standards and legal requirements.