TATA CONSULTANCY SERVICES

Building on belief

# How utilities can generate cyber confidence

TCS Risk & Cybersecurity Study: Utilities Report

# How utilities can generate cyber confidence

## Utilities perform an intricate balancing act

They generate power with heavy, expensive equipment that can last for decades, while simultaneously serving customers with contemporary information technology for billing, smart meters, and microgrids. On both sides, they must balance the demands of their customers for reliability; investors for returns; and regulators for efficiency.

Layering modern cybersecurity requirements into this mix creates incredible complexity.  Utilities' security strategies must encompass not only run-the-business IT but operating environments that are gradually becoming more connected, and thus vulnerable, via wireless technology. Tools and tactics must protect against ever more sophisticated threats and bad actors, while budget for the latest and greatest IT solution is not unlimited. Utilities also must be concerned about the security of players outside their boundaries, from contractors building new generating facilities to cloud-based services provided to consumers checking their balances for solar power credits.

# How utilities can generate cyber confidence

The tensions and challenges of the utilities industry are captured in the results of a recent TCS survey, as well as in interviews with security executives working at utilities and in other industries. Two distinct groups emerged from the research. **Pacesetters**, whose companies reported higher than industry averages for both revenue growth and profit growth between 2017 and 2021 (22% of utilities surveyed), and **Followers**, who reported lower than average revenue and profit growth during that period (32% of utilities surveyed).

## Here's what we found:

1. Pacesetter utilities firms report they are ahead of their competitors when it comes to managing external threats and internal risks. And utilities CISOs have more confidence in their security technology than we found among CISOs in the other industries we surveyed.

2. Pacesetter utilities think cloud platforms offer cybersecurity advantages over traditional infrastructures; Followers are less confident in cloud.

3. Utilities are bracing for virtual attacks on their physical plants more than on the sales and ecommerce platforms that concern other industries.

4. Compared to other industries, utilities chief risk officers (CROs) prioritize concentration risk — a concern likely driven by the sector's financial exposure due to heavy capital investment in new generating facilities.

5. Utilities CROs still worry about the adverse business consequences of economic, technology, environmental and regulatory issues, but cybercriminal activity has become their first concern.

6. The more successful the utility, the more likely its C-suite is taking a proactive approach to cyber risk and security issues.

The TCS Risk & Cybersecurity Study of more than 306 chief information security officers (CISOs) and 301 chief risk officers (CROs) was conducted in 2022 via survey and in-depth interviews amid an unprecedented upsurge in increasingly sophisticated cyberattacks from criminals, sovereign states, and other bad actors exploiting global socio-political and economic tensions. The survey respondents were drawn from North American, European, and UK-headquartered companies in four industries — utilities, banking and financial services, manufacturing, and media and information services — facing an unprecedented range of cyber threats and increased risks, whether to business data, customer data, operations, trade secrets, or supply chains.

In this report, we examine the greatest security risks utilities face, explore how effectively these 76 CISOs and 76 CROs are creating security strategies, and offer suggestions for improvement based on our work with utilities worldwide.

# Business advantage or misplaced confidence?

The most successful utilities are more likely to report they are ahead of their competitors when it comes to managing external threats and internal risks (see Figure 1). Some consider their ability to protect their systems a definite plus for their brand. “Our reputation is one of our CEO’s biggest concerns,” said the director of information and cybersecurity for a US-based utility. “He wants us to be the trusted advisor, the authority, when it comes to giving our customers advice about the best way to consume our services. A major incident would put a dent in that trust and be very damaging. Why would customers take our advice if we can’t even manage our own infrastructure?”

While Pacesetters may rightly express confidence in their ability to manage internal and external threats, much of the industry’s cybersecurity strategies are still often carried  out in IT and operating technology silos. IT cybersecurity typically supports back-office customer-facing operations, including billing and the smart meter infrastructure. And, yes, security investments here are generally strong to safeguard customer payment data and ensure timely billing and revenue cycles.

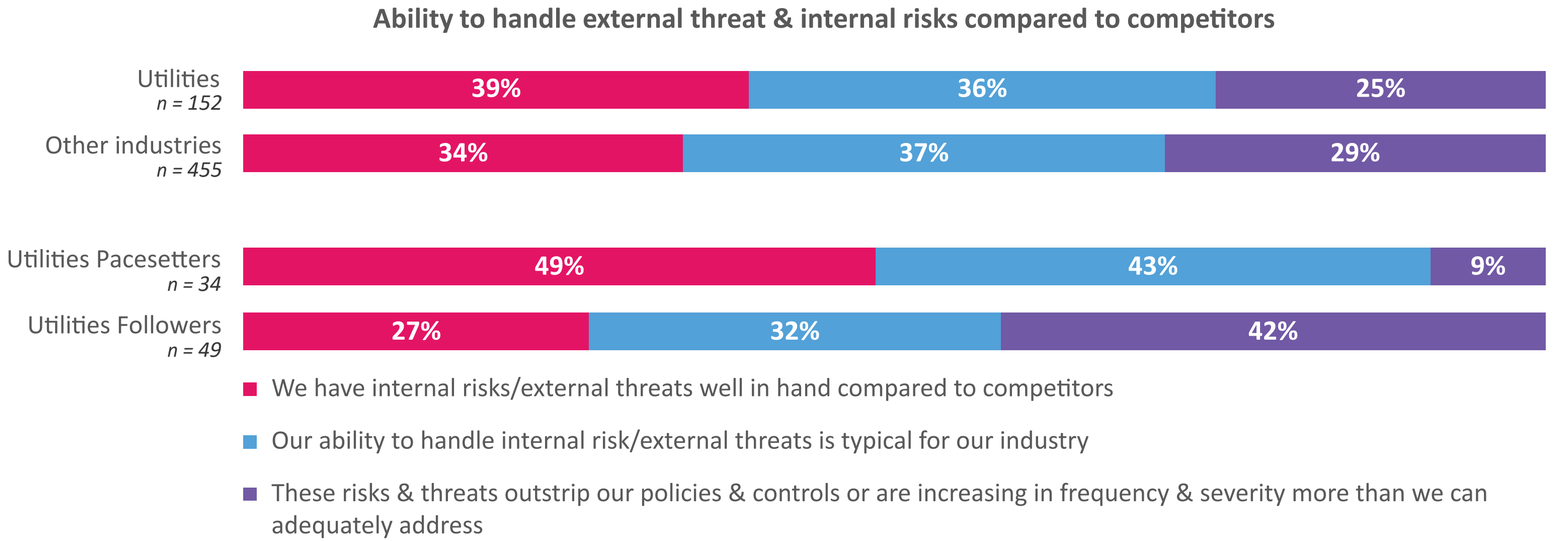


**Figure 1**

# Business advantage or misplaced confidence?

However, in our experience, the generating plants are less secure than the survey results seem to reflect. Power generation operating technology is based on a much older infrastructure and is not covered by the IT cybersecurity budget. In part, this is because much of the operating equipment is “dumb” in the sense it isn’t — or didn’t used to be — connected to any communications network. That is, a technician must drive to the equipment’s location to maintain or adjust it.

The increasing challenge is that as 20- and 30-year-old equipment nears the end of its life, the modern equipment replacing it is often Internet-capable and wireless-ready. We have seen situations where the business buys this equipment because it wants the capabilities those features enable. Meanwhile, the company cybersecurity officials are not consulted on the purchase. That’s how a security gap opens — and why utilities must ensure they take a comprehensive security approach that spans IT and operating technology capabilities and vulnerabilities.

Nevertheless, most utilities CISOs — in contrast to CISOs in other industries — say that they are successfully deploying advanced technology to combat sophisticated threats (see Figure 2).

**Utilities CISOs are more likely to feel confident about their current advanced cyber capabilities than CISOs in other industries**

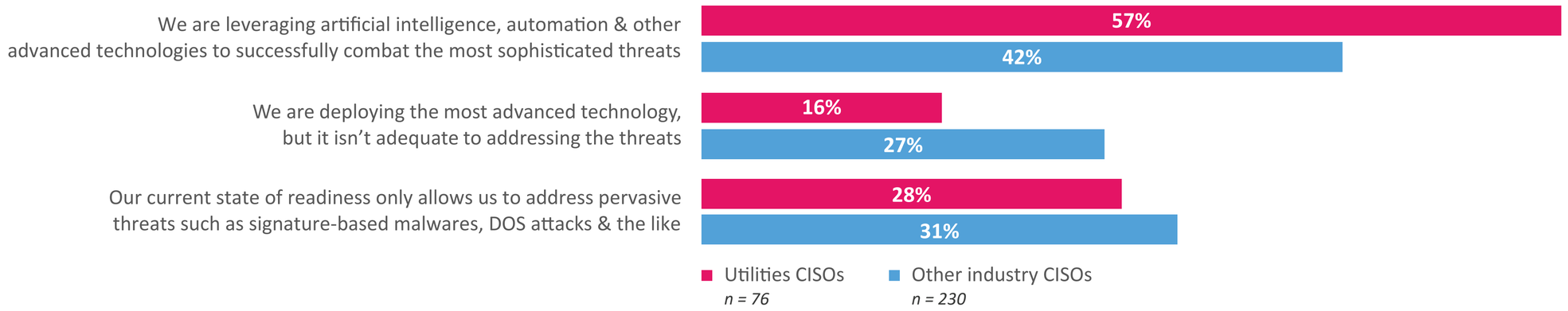


**Figure 2**

# Business advantage or misplaced confidence?

A majority of utilities security executives also seem at least somewhat confident they can avoid serious repercussions from any cyberattacks that do occur, with Pacesetters expressing the most confidence (see Figure 3).

The concern here is how a utility defines a “major cyber incident” and the measures it’s using to guard against it. Security can become a conversation about a very specific measure depending on whether consumer, investor, or regulator demands  are on the table. Reliability, shareholder returns and efficiency sometimes compete, despite the fact they are interrelated. And they do influence security investments, or the lack of them. Sometimes a utility thinks certain requirements can be met by investments made in a discrete project, such as the Payment Card Industry Data Security Standard (PCI DSS) for consumer privacy and payments. Then it may not realize a section of its infrastructure that leverages customer information is not compliant with this standard and leaves it unprotected.

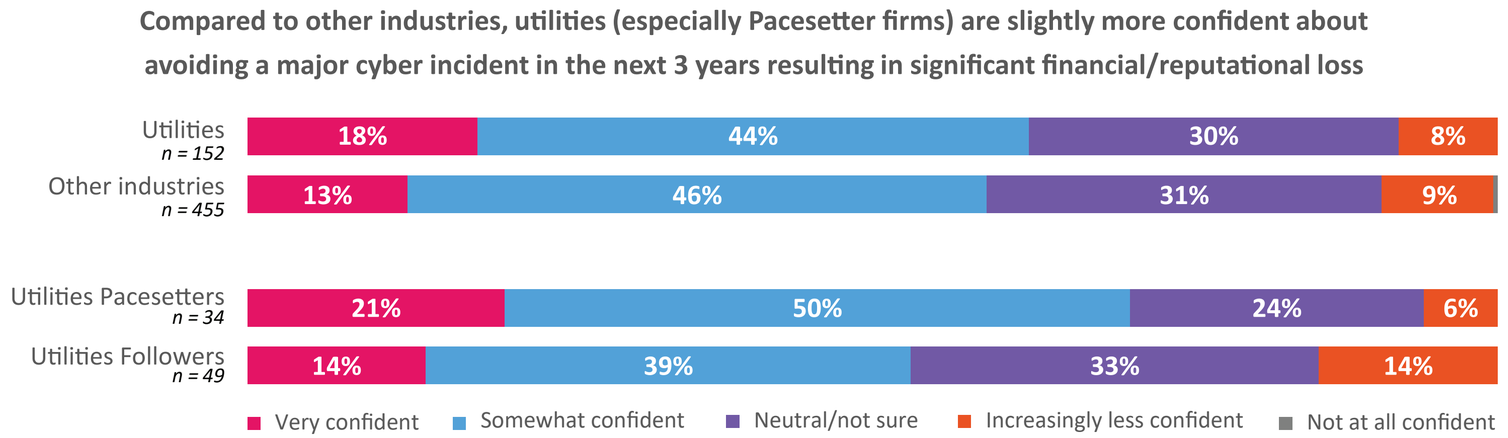


Figure 3

# Cloud and security

The more financially successful a utility company, the more likely it is to say cloud platforms offer cybersecurity advantages over traditional infrastructures (see Figure 4). Openness to cloud platforms also correlates with greater confidence in dealing with internal risks and external threats. (Executives at utilities that aren't yet convinced about the security of cloud platforms are most likely to say they worry about having sufficient tools and policies to protect and manage business data hosted in the cloud.) Pacesetters may be more comfortable with cloud computing because they are more technologically sophisticated and recognize that major cloud services providers offer security levels above and beyond those of the average enterprise.

"We've had all our eggs in one basket, which is the on-premise basket," said a utilities cyber executive. "We are concerned that if we get hit, the whole basket is gone. So one of our strategies is diversifying our risk into cloud providers. We have to trust they are doing their job. But if one of these 10 different cloud providers gets hit, we're okay with a one-tenth impact versus if everything got hit."

**Utility firms are more likely to be open to doing business on cloud platforms & in cloud environments than are companies in other industries**

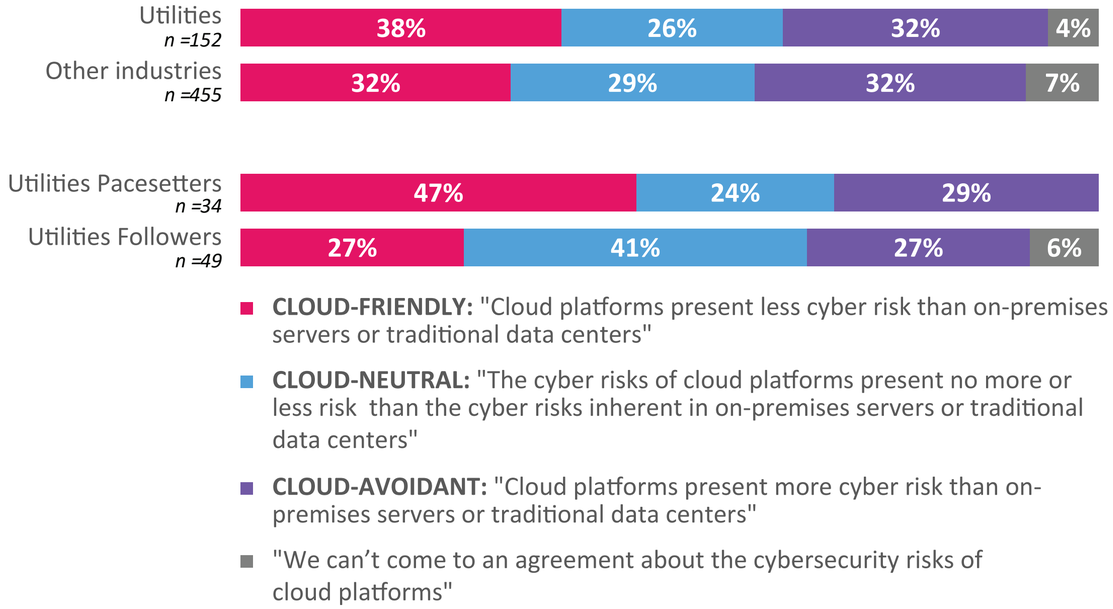


**Figure 4**

# Cloud and security

Utilities cyber executives who say their companies are more “cloud-friendly” (i.e., see cybersecurity advantages in using cloud platforms) or “cloud-neutral” (see neither cyber advantages nor disadvantages to cloud platforms) are more likely to feel confident about their posture toward internal risks and external threats than are the CISOs and CROs at companies where strong doubts about the security capabilities of cloud platforms still hold sway (see Figure 5).

These attitudes will continue to shift, however, as cloud platforms and cloud-based service providers take the lead in deploying cutting-edge cybersecurity approaches to combat the utility industry’s most intractable cyber threats, and as cloud-based operating processes become the rule rather than the exception.

“Our finance and our other business sectors, they want to move faster,” said an IT security executive at a US-headquartered utility. “They want to be more effective in their work. So, we're adopting cloud faster for those areas to learn more from it. But then we will be slower in certain areas just because we are in this constant learning mode and we're still not yet comfortable with the cloud. So, we want to test it out with areas that we're willing to be [cloud-based] to load that risk appetite there and go with it.”

**Cloud-friendly & cloud-neutral utilities are more likely to have greater confidence in their position toward internal risks & external threats than cloud-avoidant utility companies**

*n = 146; not included: can't come to an agreement about cyber risks of cloud platforms*

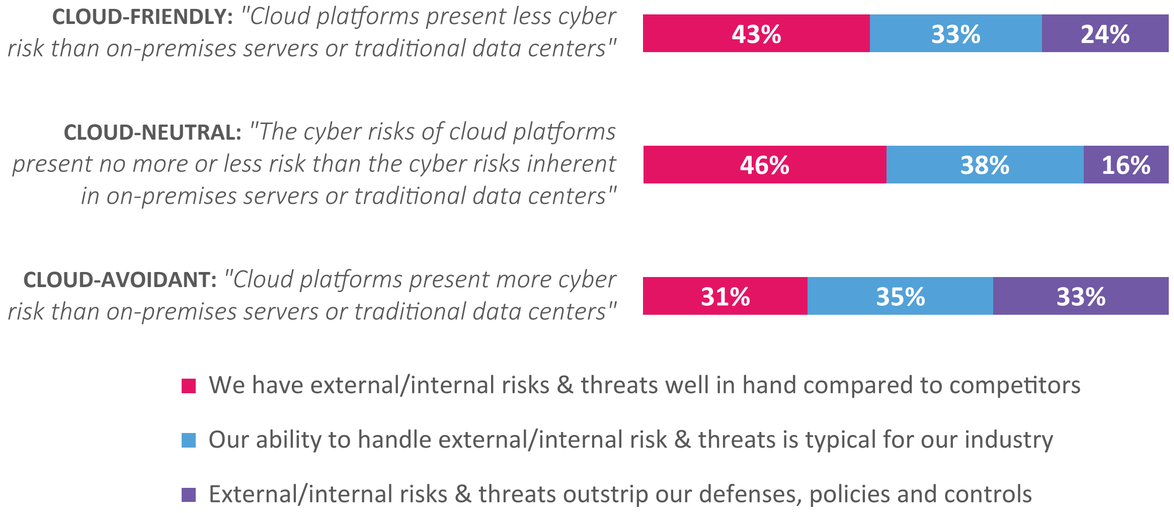


**Figure 5**

# Digital threats & physical assets

Where other industries expect their sales and e-commerce platforms to be frequent targets, utilities are bracing for virtual attacks on their physical plants (see Figure 6), a sensible posture given the potential vulnerabilities of operating technology and power generation facilities. Still, utilities expect their finance processes, customer databases and R&D departments to take the brunt of cyberattacks over the next few years.

| Corporate functions where CISOs & CROs expect to see the greatest number of cyberattacks between now & 2025 | Utilities *n = 152* | Other industries *n = 455* | Utilities Pacesetters *n = 34* | Utilities Followers *n = 49* |
|---|---|---|---|---|
| Finance | 1 | 1 | 1 | 1 |
| Customer databases | 2 | 2 | 3 | 2 |
| R&D | 3 | 4 | 2 | 3 |
| Plants/production/procurement | 4 | 8 | 4 | 4 |
| Sales/ecommerce | 5 | 3 | 7 | 4 |
| Human resources | 6 | 6 | 5 | 8 |
| Marketing | 7 | 5 | 6 | 9 |
| Ecosystem partners | 8 | 10 | 9 | 6 |
| Distribution/supply chain | 9 | 9 | 8 | 7 |
| Legal | 10 | 7 | 10 | 10 |

**Figure 6**

# Digital threats & physical assets

CROs ranked the “expansive attack surface” of their utilities’ operations as the greatest obstacle to assessing risk and implementing security solutions (see Figure 7). “Legacy technology” took second place and “decentralized leadership” third among six possible answers. These risk executives also said the independence of their companies’ operating and digital technologies are a larger problem than any interdependencies between them.

(Similarly, utilities CISOs cited “breaches caused by connected smart devices” as their second-highest security concern when asked about the challenges of managing converged information and operating systems; see Figure 8.)

Identifying a utility’s “crown jewels,” or key assets, across its infrastructure is critical to assessing risk and setting security priorities. A critical aspect of this work is identifying the 20- to 30-year-old devices that have been fully depreciated and so may no longer be in financial records. Just because the device is off the books does not mean it is risk free, particularly if it is still in use.

Utilities must understand and catalog what each of these devices do and whether they have USB ports, RJ-45 adapters, Wi-Fi, or RFID and whether and how they are connected to the company’s infrastructure. At the very least, these assets should be behind firewalls or air-gapped, isolated from the network so it’s impossible to establish external connections to them.

Utilities must also develop strategies for how to monitor device status. It’s critical to know when one of the older devices is replaced and what security vulnerabilities its replacement has and how it will be secured. Ideally, a utility will evaluate whether the connectivity capabilities of the new device are worth the security risk they represent. Is it truly critical that a trigger switch automatically signal its failure to the rest of the environment or is there a safer way to achieve the same end? The answer may very likely be “yes,” but answering that question should involve the company’s security professionals as well as its operations experts.

| **The greatest obstacles to cyber risk assessment & security implementation, according to utilities CROs** | **Utilities** *n = 76* |
|---|---|
| The expansive attack surface of our operations | 1 |
| Our legacy technology | 2 |
| Decentralized leadership | 3 |
| Independence of our OT & IT | 4 |
| Regulatory restrictions/lack of regulation | 5 |
| Interdependencies between OT & IT | 5 |

**Figure 7**

***Note:*** *question was only asked of CROs in the utilities industry*

| **The top security concerns of managing converged IT & OT systems, according to utilities CISOs** | **Utilities** *n = 76* |
|---|---|
| Leak of sensitive or confidential data | 1 |
| Breaches caused by connected smart devices | 2 |
| Increased regulatory pressures | 3 |
| Lack of expertise in one or the other system | 4 |
| Lack of visibility into both systems | 5 |
| Little to no control of security policies | 6 |
| Not able to accomplish isolation or containment when a breach occurs | 6 |

**Figure 8**

***Note:*** *question was only asked of CISOs in the utilities industry*

# Challenges to security & risk mitigation

While utilities security executives recognize the breadth of their IT and operating infrastructures makes them vulnerable (see Figure 9), their challenge in quantifying risk and its mitigation costs may relate to the difficulty in achieving an overarching view of that expanse. The need to inventory physical assets and their digital connectivity is clearly a cybersecurity activity but it might not be recognized as such. Similarly, identity and access management, usually an IT-led effort, is critical to physical security since they have actual hands-on access to facilities and equipment. The issue is an important one to resolve: without clear evaluation of risks, utilities will not know what cybersecurity talent they need to recruit or which legacy systems to address first.

| **The greatest challenges to cybersecurity & risk mitigation initiatives, according to CROs & CISOs** | **Utilities** *n = 152* | **Other industries** *n = 455* | **Utilities Pacesetters** *n = 34* | **Utilities Followers** *n = 49* |
|---|---|---|---|---|
| Assessing cyber risks & quantifying relevant costs | 1 | 5 | 5 | 1 |
| Skill sets to manage, engineer & support cybersecurity technology | 2 | 2 | 1 | 4 |
| Reliance on legacy IT systems | 3 | 3 | 10 | 2 |
| Accumulated complexity of our own business processes & operations | 4 | 4 | 7 | 8 |
| Lack of collaboration across enterprise units (business, IT & security) | 5 | 8 | 4 | 10 |
| Workforce changes/requirements (e.g., work from home, bring-your-own-device, etc.) | 6 | 1 | 5 | 4 |
| Difficulty in demonstrating return on cybersecurity investments | 7 | 6 | 3 | 12 |
| Competing interests for the board or senior leadership | 8 | 11 | 2 | 10 |
| Outdated, siloed & non-integrated security tools | 9 | 12 | 11 | 9 |
| Lack of diversity in staff assessing cyber risks & threats | 10 | 7 | 8 | 2 |
| Difficulty in mandating that our current vendors adopt advanced technologies & policies | 10 | 9 | 8 | 4 |
| Budget constraints | 12 | 10 | 12 | 7 |

Figure 9

# Challenges to security & risk mitigation

While citing cybercriminal activity as the number-one cause of adverse consequences for their companies' businesses and operations in recent years, utilities CROs also point to economic and technology issues as top challenges, demonstrating that the latter has affected the utilities industry far more than has been found in many other industries (see Figure 10). In addition, these executives rate environmental risks as having a much greater impact on their companies' operations than do their peers in other industries.

But utilities CROs say that, after cyber risks, they will shift their priorities in the next three years (see Figure 11) to mitigating regulatory risks (ranked as the second priority for the years ahead, up from fifth among past concerns) and global political impacts (ranked third between now and 2025, up from seventh as among their concerns in previous years).

Utilities have always been among the more highly regulated industries: initially as natural monopolies in the communities they operated and later as the environmental risks of carbon-based power sources became known and the potential impacts of alternative power sources, such as nuclear energy and off-shore wind farms, have received attention. More recently, with utilities foundational to national infrastructures in an era of state-sponsored cyberattacks, government agencies (such as the US departments of Commerce, Energy, and Homeland Security) have issued cybersecurity directives to utilities, returning regulatory compliance to the spotlight, now with geopolitical implications.

| Causes of the most negative impact on companies' businesses & operations in the past 2 years, according to CROs | Utilities *n = 76* | Other industries *n = 225* |
|---|---|---|
| Cybercriminal: hacking, phishing, ransomware, DDoS, etc. | 1 | 1 |
| Economic: interest rates, inflation, exchange rates, etc. | 2 | 2 |
| Technological: automation, infrastructure breakdowns, obsolescence, etc. | 3 | 6 |
| Environmental: extreme weather, natural disasters, climate change, etc. | 4 | 11 |
| Regulatory/legal: compliance, intellectual property disputes, etc. | 5 | 7 |
| Generational: aging, Gen Z/Gen Alpha adults, digital natives vs adopters, etc. | 6 | 8 |
| Global political: treaty negotiations, wars, global economics, etc. | 7 | 4 |
| Operational: mismanagement, waste, fraud, etc. | 8 | 5 |
| Reputational: public confidence, investor confidence, etc. | 9 | 3 |
| Domestic political: government spending, political movements, etc. | 10 | 10 |
| Societal: voluntary & involuntary migration, social instability, diseases, etc. | 11 | 9 |

**Figure 10**

| Top risks CROs say they'll be focusing on between now and 2025 | Utilities *n = 76* | Other industries *n = 225* |
|---|---|---|
| Cybercriminal: hacking, phishing, ransomware, DDoS, etc. | 1 | 1 |
| Regulatory/legal: compliance, intellectual property disputes, etc. | 2 | 9 |
| Global political: treaty negotiations, wars, global economics, etc. | 3 | 4 |
| Economic: interest rates, inflation, exchange rates, etc. | 4 | 2 |
| Generational: aging, Gen Z/Gen Alpha adults, digital natives vs adopters, etc. | 5 | 6 |
| Technological: automation, infrastructure breakdowns, obsolescence, etc. | 6 | 3 |
| Environmental: extreme weather, natural disasters, climate change, etc. | 7 | 8 |
| Reputational: public confidence, investor confidence, etc. | 7 | 10 |
| Societal: voluntary & involuntary migration, social instability, diseases, etc. | 9 | 5 |
| Operational: mismanagement, waste, fraud, etc. | 10 | 6 |
| Domestic political: government spending, political movements, etc. | 11 | 11 |

**Figure 11**

# Proactively setting priorities

## Leadership priorities

Utility company boards of directors are more focused on holistically managing cyber risks than boards in other industries (see Figure 12). This may be because attacks on utilities that have crippled operations get executives' attention. "When Colonial Pipeline got hit, one of our board members asked what we do to protect against that particular threat. That's still reactive, but in the past, we wouldn't even have had a regular briefing in the front of the board," said one IT security leader. "They recognize cybersecurity is an important risk they need to understand better because they have pressures from a consumer perspective and from federal and state regulators as well."

| Cyber risk & security priorities arising out of board-level discussions | Utilities *n = 152* | Other industries *n = 455* | Utilities Pacesetters *n = 34* | Utilities Followers *n = 49* |
|---|---|---|---|---|
| Ensuring cyber risks are holistically managed & mitigated across our company & its larger ecosystem | 1 | 3 | 3 | 2 |
| Improving visibility of cyber risks & ensuring compliance to regulatory & industry requirements | 2 | 1 | 2 | 4 |
| Creating & adopting a comprehensive cybersecurity governance model | 3 | 4 | 1 | 6 |
| Increasing cybersecurity maturity of our company relative to industry peers & adopting emerging models like zero trust | 4 | 2 | 5 | 1 |
| Focusing on ecosystem risks & collaboration for oversight, monitoring & mitigation of those risks | 4 | 5 | 6 | 3 |
| Creating a 'resilience-by-design' culture & adopting such standards & controls | 6 | 6 | 3 | 5 |

Figure 12

(Additionally, 91% of utilities cyber executives indicated their boards now discuss cyber risk and security on a regular cycle or at every meeting. But only 80% of CISOs and CROs in other industries reported their boards doing the same, with another 15% saying such issues were discussed at best "occasionally, or as necessary.")

# Proactively setting priorities

In our experience, successfully mitigating cyber risks requires leadership and coordination from the board down to the function, business unit, and even department level. According to our research, more than two-thirds of the more financially successful utility firms' C-suites take a proactive approach to cyber risk and security issues (see Figure 13); in contrast, the C-suites of less financially successful utilities take a lackluster approach to engagement on cyber issues.

Similarly, at these more successful Pacesetter utility companies, the CISO and CRO are more likely to collaborate and coordinate their work with each other's departments at least several times a week, if not daily (see Figure 14); whereas only about one-fifth of the Follower utilities' cyber executives work that collaboratively.

**Attention given to cyber risk & security issues by other C-suite & business unit leaders**

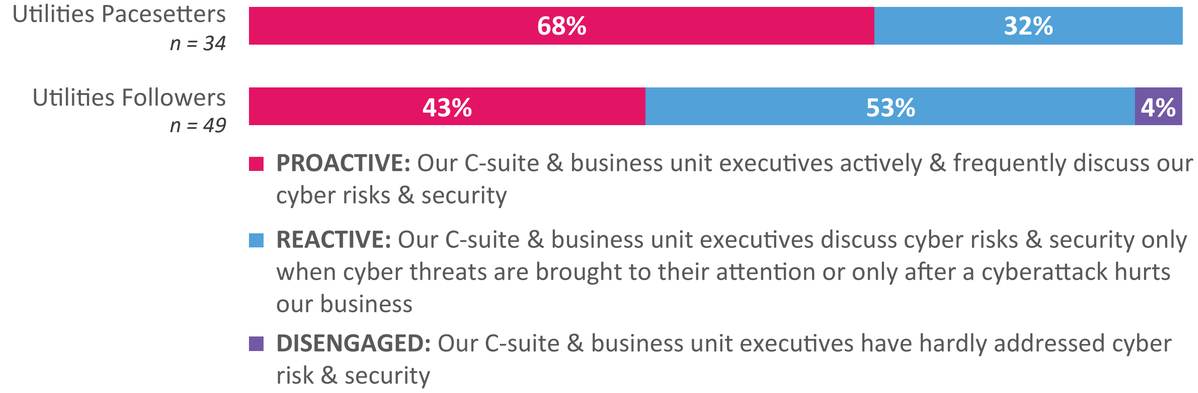


Figure 13

**Frequency of collaboration & coordination between CISOs and CROs**

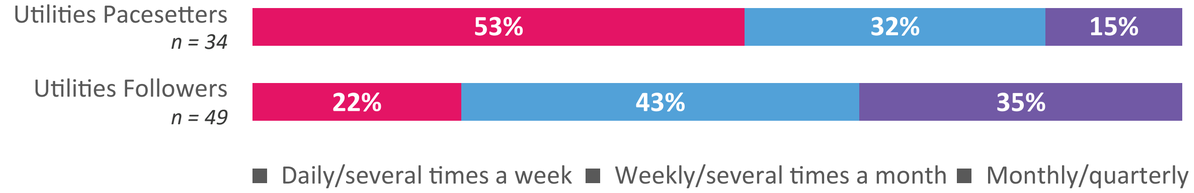


Figure 14

# Proactively setting priorities

In outlining what they intend to focus on between now and 2025, utilities CISOs differ from CISOs in other industries in the importance they intend to place on implementing zero trust security models, in which older security models like IDs, passwords, firewalls, and VPNs are enhanced or even replaced with role and data management practices that authenticate access dynamically and grant only the least-privileged access to data resources for limited times or tasks (see Figure 15).

Utilities CROs place a high premium on understanding their concentration risk (see Figure 16). Utilities deal with a significant amount of concentration risk due to their ongoing capital investments in new generation plants, transmission plants, delivery of new lines, wind farms, and solar arrays. These new capital assets and infrastructure typically are built by third-party companies specializing in such construction, which is a relatively small group. That approach can result in much of a utility's sensitive construction and operating data being held by just a few companies. Yet if one of those companies suffers a data breach, the utility may find itself a subsequent target.

"In the last two and a half years, we were notified by three different engineering firms that they got breached. They manage and store a lot of our engineers' data: construction drawings, network blueprints, etc. We require third parties to work on building key infrastructure, treatment plants, pump stations and so on. What's difficult is to quantify that risk. How can threat actors weaponize and leverage those blueprints, diagrams and so on to cause harm to us?" said an information security director.

| CISOs' work priorities | Utilities *n = 76* | Other industries *n = 230* |
|---|---|---|
| Enhancing security governance & risk management (e.g., assessing the security posture of the company, defining controls & standards, etc.) | 1 | 1 |
| Establishing a more robust cybersecurity strategy | 2 | 2 |
| Implementing models like "zero trust"/perimeterless security | 3 | 9 |
| Security talent acquisition & development | 4 | 3 |
| Strengthening enterprise-wide cyber hygiene (patching, hardening, etc.) | 5 | 6 |
| Enterprise-wide employee awareness & training | 6 | 4 |
| Executive/board mandates on cybersecurity risks | 7 | 5 |
| Managing ecosystem & supply chain risks | 7 | 8 |
| Outsourcing our security operations | 9 | 10 |
| Regulatory or industry compliance mandates | 10 | 6 |

Figure 15

| Most important to cyber resiliency between now & 2025, according to CROs | Utilities *n = 76* | Other industries *n = 225* |
|---|---|---|
| Understanding concentration risk (i.e. information assets, suppliers, geographies, etc.) | 1 | 3 |
| Integration of cyber & business strategies | 2 | 2 |
| Identification & clear ownership of digital assets | 3 | 5 |
| Identification of critical operations of core business lines | 4 | 1 |
| Fostering an organizational culture of resiliency | 5 | 8 |
| Measurements of resilience | 6 | 7 |
| Partnerships with industry groups, government agencies | 7 | 6 |
| Plans for business continuity/disaster recovery | 8 | 4 |

Figure 16

# Proactively setting priorities

## Budget priorities

While 70% of utilities CISOs reported budget increases this past year, a majority of utilities CROs saw budgets stay flat or even decrease (see Figure 17). Although this may demonstrate less priority is placed on this role at utilities firms than in other industries — even though utilities CROs are more likely than their peers in other industries to report directly to the CEO or COO, rather than to a CFO or general counsel — the reason may be due less to a lack of concern for cybersecurity risks than a perception that the economics of the utilities industry are generally firmly established, competition is well-understood (and defined differently than in other industries), and when such forces shift, they tend to do so across the industry, rather than utility by utility.

Indeed, utilities CROs say customers rank third among eight possible drivers of demand for risk management at their companies, compared with other industries where customers rank first (see Figure 18).

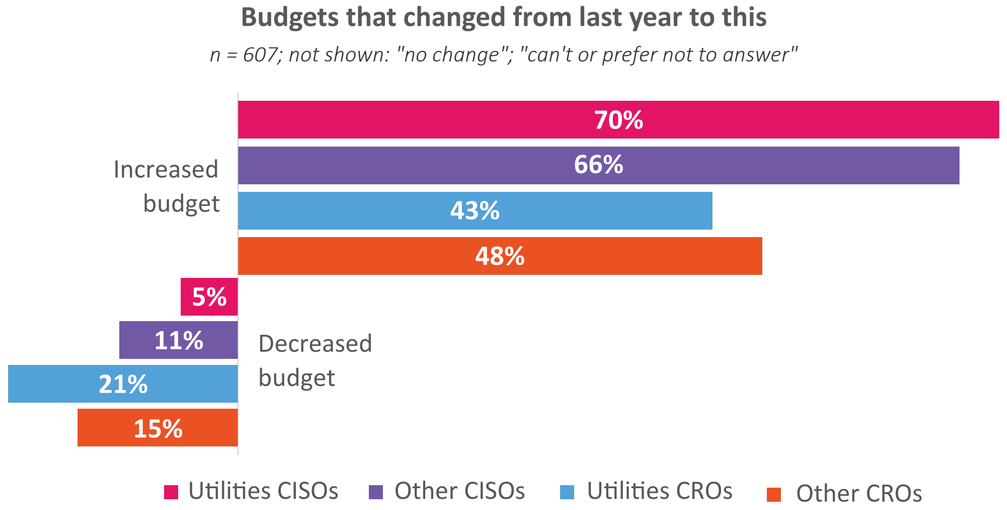


Figure 17

| The top drivers of demand for risk management, according to CROs | Utilities *n = 76* | Other industries *n = 225* |
|---|---|---|
| Investors | 1 | 2 |
| Employees | 2 | 3 |
| Customers | 3 | 1 |
| Board | 4 | 8 |
| Our industry | 4 | 5 |
| C-suite | 6 | 4 |
| Regulators | 7 | 6 |
| Ecosystem partners | 8 | 7 |

Figure 18

# Proactively setting priorities

Most of the primary budget drivers for CISOs are common across industries: the increasing digital nature of business, new and targeted capabilities offered by cybersecurity vendors, and the changing security landscape that affects every company in every industry (see Figure 19). But for utilities, enterprise-wide, cloud-powered transformations have a stronger influence on cybersecurity investment than they do in other industries, our research shows. And in contrast with the demand drivers for utilities CROs, their CISO counterparts say evolving customer expectations have more impact on their budget funding than do their peers in other industries.

| CISOs' budget priorities | Utilities *n = 76* | Other industries *n = 230* |
|---|---|---|
| Data protection & privacy | 1 | 1 |
| Emerging security technologies (such as decentralized identity, 5G security, etc.) | 2 | 3 |
| Cloud security management | 3 | 2 |
| Threat management (including ransomware protection) | 4 | 5 |
| Managed detection & response | 5 | 7 |
| Operating technology (OT) security | 6 | 10 |
| Identity management | 7 | 4 |
| Vulnerability remediation automation | 8 | 8 |
| Governance, risk & compliance | 9 | 6 |
| Advisory consulting | 10 | 9 |

Figure 20

| Top influences driving cybersecurity investment, according to CISOs | Utilities *n = 76* | Other industries *n = 230* |
|---|---|---|
| Increasing digitization of our products or operating technology specifically (e.g., embedding digital sensors in them) | 1 | 1 |
| New cybersecurity capabilities & services that meet our needs | 2 | 2 |
| Emerging technology risks generally for our industry or processes | 3 | 3 |
| Enterprise-wide transformations like cloud migrations or M&A activity | 3 | 7 |
| Changing customer expectations | 5 | 8 |
| Regulatory compliance & new regulations | 6 | 4 |
| Audits & reviews | 6 | 9 |
| Concurrent, ongoing technology updates & expenditures | 6 | 5 |
| Recent/current cyber threats & attacks at our firm, for an ecosystem partner, or involving competitors or other enterprises | 9 | 6 |
| Board/executive focus | 10 | 11 |
| Media focus on cybersecurity threats | 11 | 10 |
| A change in leadership (CISO, other C-suite) | 12 | 12 |

Figure 19

As far as how they intend to spend that budget, utilities CISO budget priorities largely track those in other industries (see Figure 20), with a higher priority on operating technology security. Utilities CISOs also express less interest in spending budget on new identity management solutions and services…which may make moving to a perimeterless, zero trust model for governing system and data access — their third highest work priority (shown earlier in Figure 15) — difficult to accomplish.

# Utilities are rich with sensitive data for hackers to target

## Because no other industry is so central to our lives and livelihoods

The role utilities play in modern life and business can hardly be overstated. And the data they hold — financial business and consumer data for recurring payments, specifications for key interconnections with public infrastructure, and even internal designs for programmable logic controllers and relays, and more — represents one of the most appealing targets for criminals, whether they engage in financial extortion or state-sponsored terrorism.

And while digital ecosystems are reshaping every global industry today, it is the utilities industry that powers those ecosystems. As a result, cyber executives at electricity, gas, and water companies face the pressure of vastly increased cyber risk while trying to ramp up their own management's awareness and sense of urgency in addressing the vulnerabilities across their own companies as well as those of their partners and suppliers.

Cybersecurity for a utility must therefore be comprehensive, but its executives still want to know where to start. On the next page, we outline five of the best practices we've seen in working worldwide with utilities who have gotten serious about securing their enterprises and their vast infrastructures.

# Recommendations for utilities

1. Rather than rely on bolting privacy and security onto points where the OT and IT environments converge, enable trust-by-design in the digital lifecycle, bringing intelligence and trust services together to deliver a secure, cross-platform environment. Ensure all communications between networked assets are encrypted, IT security updates are made automatically by default, OT security gets updated as soon as possible, and operations are protected from both internal and external risks by using zero trust (“never trust, always verify”) models for every instance in which data is stored, accessed, used, moved, or deleted.

2. Harden defenses to reduce the company’s cyberattack surface as well as to minimize business disruption. Build defensive and reactive capabilities with the goals of maximizing your cyber posture and building resiliency so that your utility company and its operations can quickly recover from and even fend off attacks when (not if) they occur.

3. Analyze enterprise risk through the lens of cloud and ERP solutions using a vendor-agnostic approach. Develop a process for ensuring cloud and third-party services are secure, for evaluating vendors’ measures to protect your organization, and for monitoring risk.

4. Align cyber risks with effective oversight and implement cyber control objectives with effective orchestration and tools. Maintain compliance and demonstrate to leadership and external regulatory agencies that you are taking effective measures to prevent loss of data, avoid infection, and mitigate other cyber risks.

5. Minimize risks associated with forming new operations before, during, and after they go live. Ensure M&A change management plans address the above four categories.

# The modern world can no longer take utility services for granted

Recent compromises to utilities themselves and to their supply and distribution networks — whether caused by nature, humans, or technology failures — have reminded all of us of just how dependent we are on the industry. Utilities CISOs and CROs are very much in a race against hackers who wish to take advantage of a growing attack surface to gain valuable data, hold operations hostage, and even disrupt a region or country.

By applying sophisticated techniques to mitigate vulnerabilities and defend against next-generation attacks, utilities cyber executives can stay one step ahead of the risks. But it requires an organization's leaders to make such vigilance a priority across the enterprise and thereby reduce the chances that, on their watch at least, cyber threats to commerce, society, and even lives shall not prevail.

TATA CONSULTANCY SERVICES

Building on belief

# Executive champions

**Santha Subramoni**
Head, Cyber Security Practice, TCS

**Margareta Petrovic**
Managing Partner, Risk & Cyber Strategy, TCS

# Contributors

**James Lemaster**
Program Director, Risk & Cyber Strategy, TCS

**Ganesh Subramanya**
Head, OT & IoT Security, Cyber Security Practice, TCS

**Rajesh Sampath**
Delivery Partner, Cyber Security Practice, TCS

For the most up-to-date content and news, download the 'TCS Perspectives' app for your iOS and Android device.

Download on the App Store

ANDROID APP ON Google play

## Get more insights

If you would like to have more information on the TCS Risk & Cybersecurity Study, please visit on.tcs.com/risk-cybersecurity

For more information or any feedback, email the TCS Thought Leadership Institute at TL.Institute@tcs.com

## About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over 50 years. TCS offers a consulting-led, cognitive powered, integrated portfolio of business, technology and engineering services and solutions. This is delivered through its unique Location Independent Agile™ delivery model, recognized as a benchmark of excellence in soft are development.

A part of the Tata group, India's largest multinational business group, TCS has over 600,000 of the world's best-trained consultants in 46 countries. The company generated consolidated revenues of US $25.7 billion in the fiscal year ended March 31, 2022, and is listed on the BSE (formerly Bombay Stock Exchange) and the NSE (National Stock Exchange) in India. TCS' proactive stance on climate change and award-winning work with communities across the world have earned it a place in leading sustainability indices such as the MSCI Global Sustainability Index and the FTSE4Good Emerging Index.

For more information, visit **www.tcs.com** and follow TCS news **@TCS**.

This Global study is brought to you by:

**TCS Thought Leadership Institute** - generating unique data-driven insights to help organizations shape the future. of business