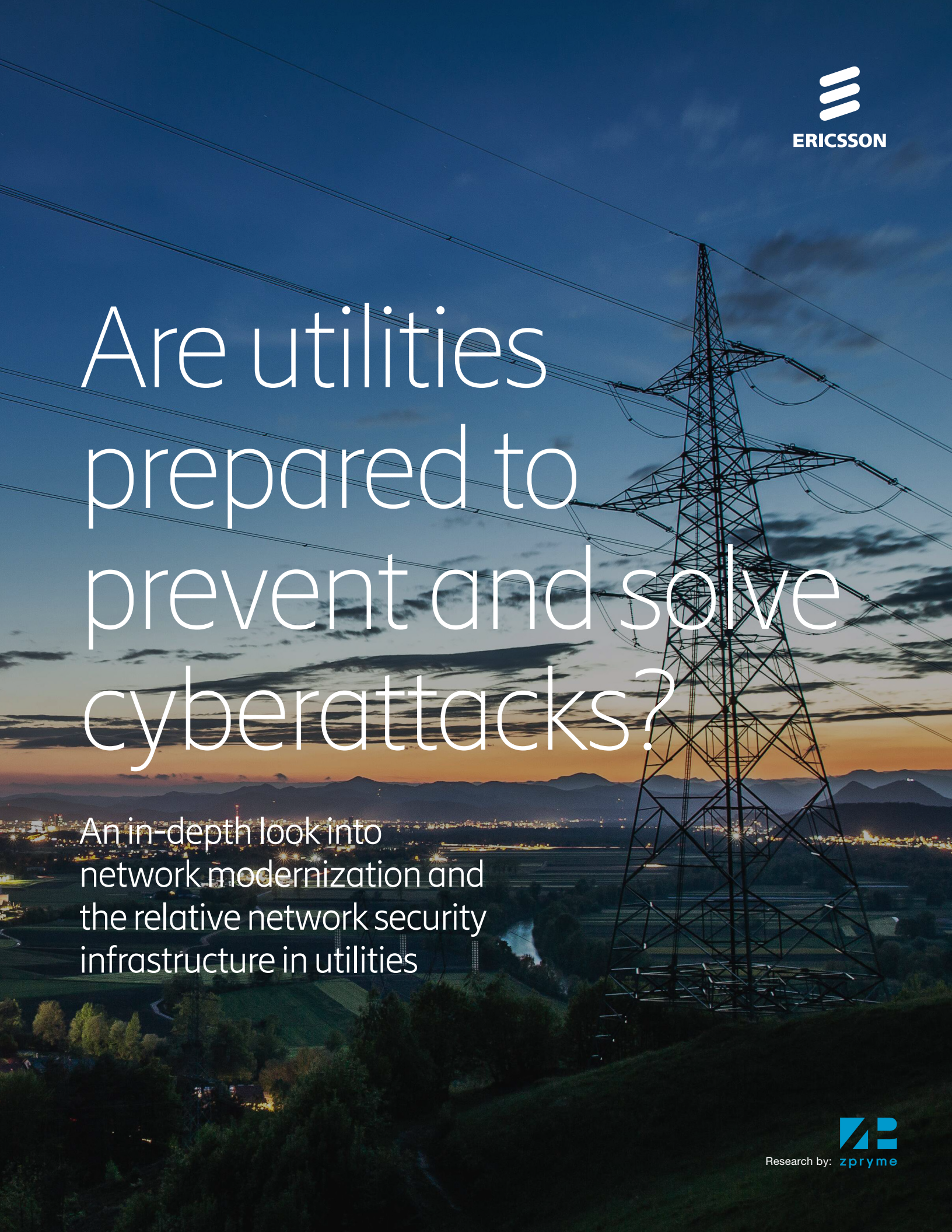


ERICSSON

Are utilities prepared to prevent and solve cyberattacks?

An in-depth look into network modernization and the relative network security infrastructure in utilities

Research by: zpryme

The utilities infrastructure as a whole is seeing radical changes. Part of those changes is the shift to digitalization and the integration of telecommunications-based systems. This shift in particular will pose its own set of challenges for utilities including changes to network architecture, network security and cellular network integration. The biggest challenge of all is maintaining network security as utilities advance their connectivity to integrate cellular networks and branch out on their use of the Internet of Things (IoT) and expand their supply chain.

The increasing adoption of wireless network systems in utilities, the increased shift to remote work, and the newfound bidirectional flow of information between utilities and consumers have expanded the threat landscape of cybersecurity attacks against utilities. Utilities, thus, must be aware of their network security vulnerabilities and prepared for any potential threats. To better understand where they stand in terms of their adoption of cellular network technologies, awareness of their systems vulnerabilities, and interests in fortifying their network security, Zpryme surveyed more than 80 utilities on the status of network security in their organizations. The results indicate a significant increase in cellular network integration in utilities. However, that increase is not matched with investments in security technologies and training.

Key findings

- 52 percent of respondents said they have Wi-Fi in their utility organizations. But 41 percent of respondents said they have both Wi-Fi and LTE.
- Only 20 percent of respondents said their utility organizations are investing in Wi-Fi 6 and/or LTE/5G.
- Employee laptops (86 percent) and IT infrastructures (66 percent) are overwhelmingly the biggest devices and network elements that consume Wi-Fi networks in utility organizations.
- 65 percent of respondents find that improved connectivity is the top value that LTE/5G can offer their businesses.
- Cybersecurity, resilience, and endpoint security were ranked the most important security solutions by the majority of respondents.
- 62 percent either don't know or don't believe that they have the skills and tools in their organizations to protect against cyber threats.

20%

of respondents said their utility organizations are investing in Wi-Fi 6 and/or LTE/5G.

65%

of respodents find that improved connectivity is the top value that LTE/5G can offer their businesses.

62%

either don't know or don't believe that they have the skills and tools in their organizations to protect against cyber threats.

Cellular networks are the way forward

Cellular networks have evolved to provide users with exceptional communications, ultra-low latency, and faster, more reliable connection. New cellular network technologies offer secure, efficient and flexible connectivity that will greatly support utilities' modernization and digital transformation efforts.

A big part of the digital transformation sweeping the utilities industry is a significant increase in cellular networks technology. So it shouldn't come as a surprise that the overwhelming majority of utilities (93 percent) have already invested in Wi-Fi or both Wi-Fi and LTE (Figure 1).

The number of utilities adopting wireless network technology is expected to increase in the coming years. There's already a strong interest in investing in newer technologies including Wi-Fi 6 network (36 percent) and LTE/5G (20 percent). Notably, 24 percent are planning to invest in both Wi-Fi 6 and LTE/5G. A relatively smaller percentage of utilities (20 percent) are already investing in either Wi-Fi 6 or LTE/5G or a combination of all networks (Figure 2).

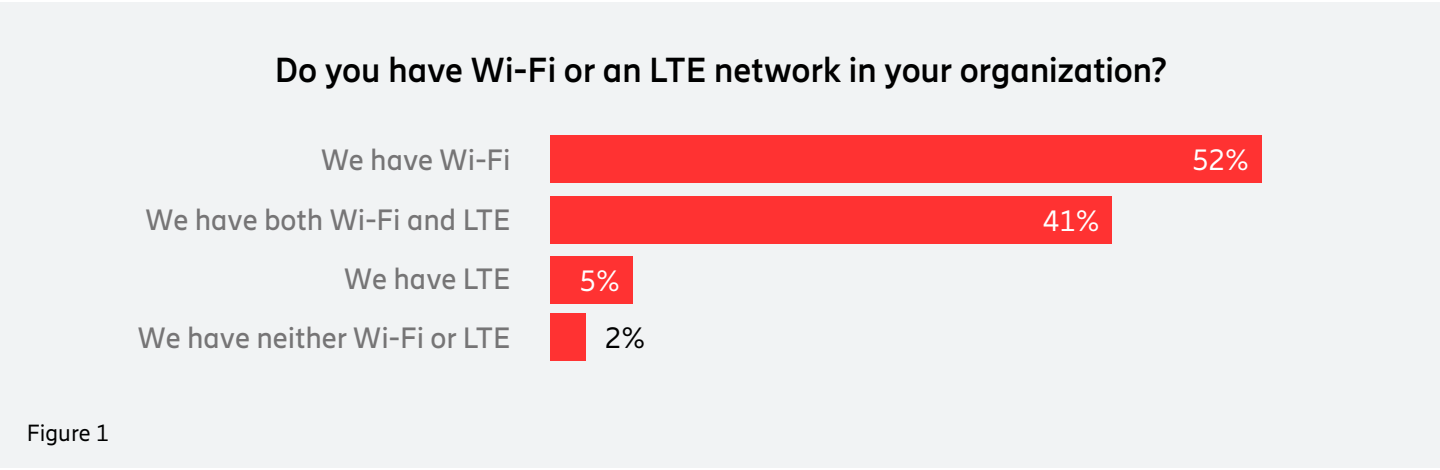


Figure 1

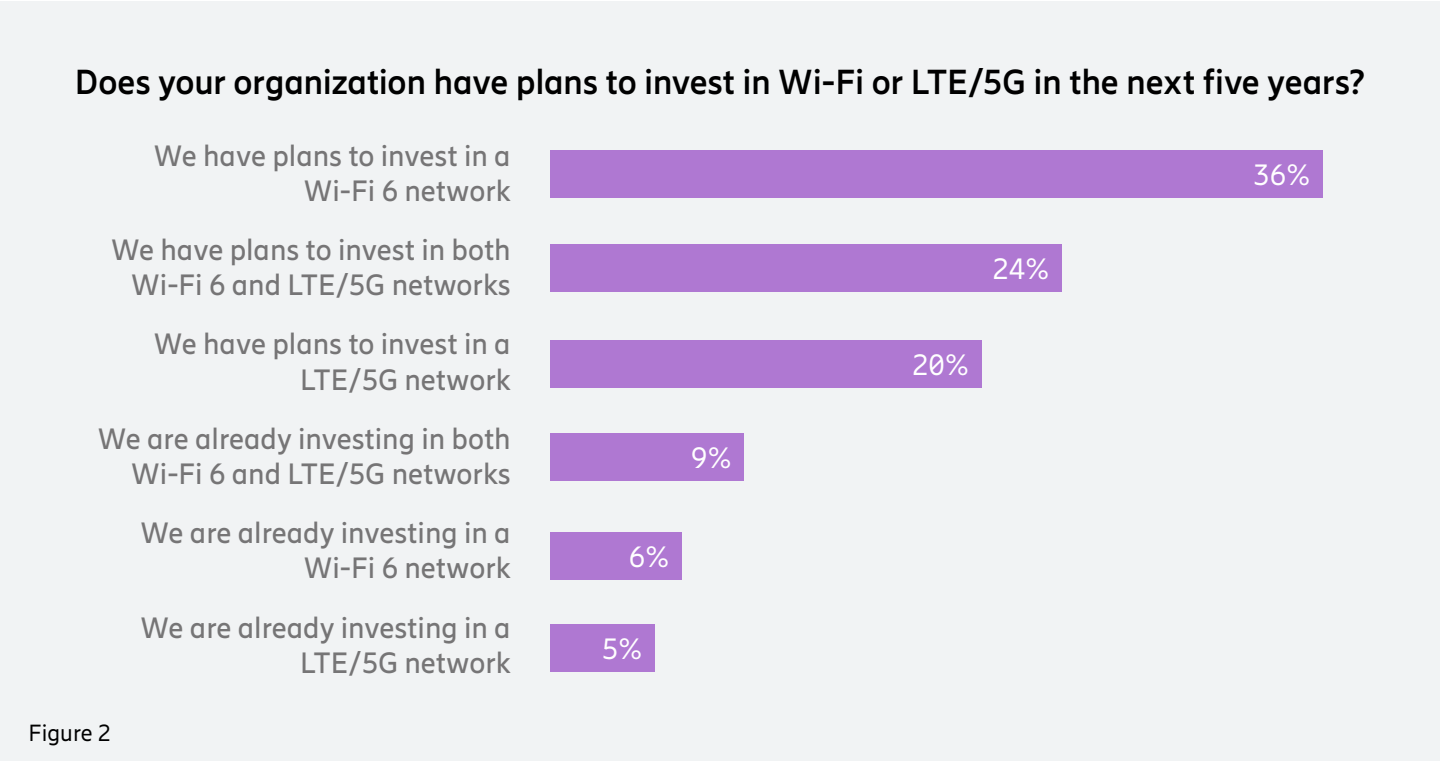


Figure 2

Unsurprisingly, especially with the rising necessity of remote or hybrid work models, employee laptops comprise 86 percent of Wi-Fi network users in utilities. IT infrastructure is also a big network element that uses Wi-Fi network at 66 percent. Smart meters are 39 percent of Wi-Fi networks. However, remote operations were found to be significantly less connected to Wi-Fi networks (32 percent), and IoT devices are 25 percent of Wi-Fi connected devices (Figure 3).

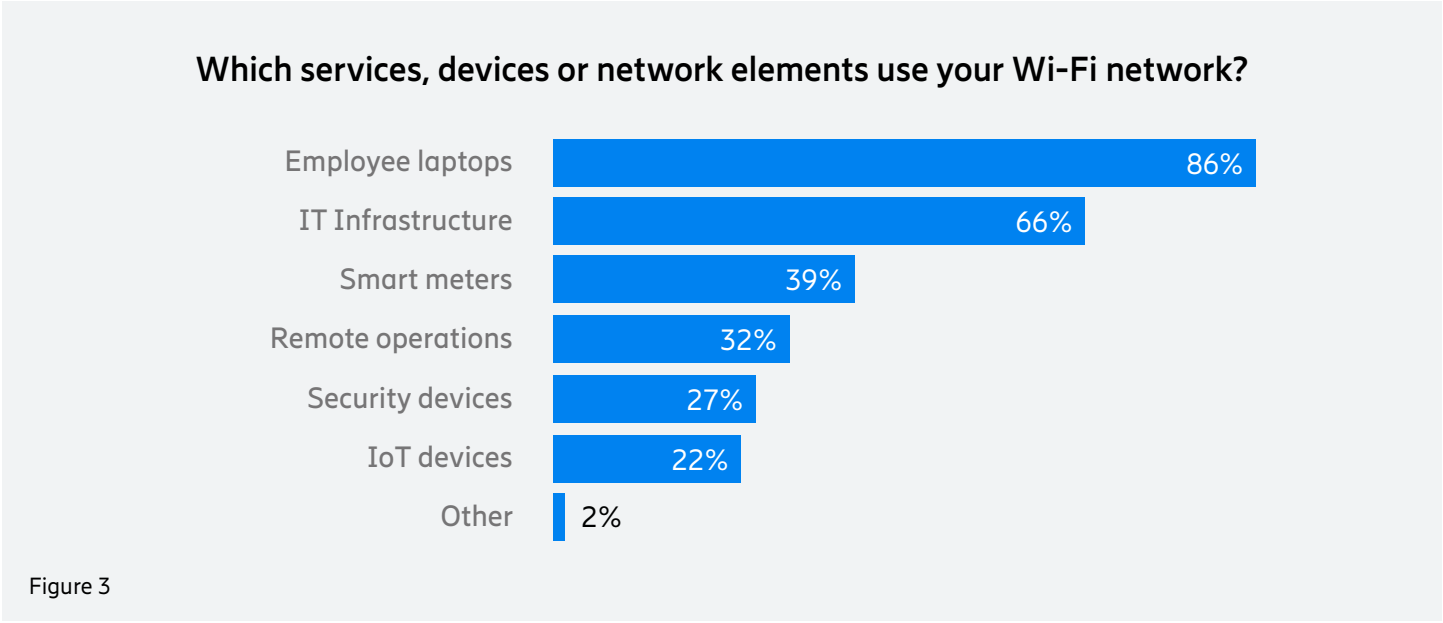


Figure 3

Consistent with the finding in Figure 2, the use of private cellular networks is projected to increase in the upcoming years as 36 percent of utilities are planning to implement LTE/5G networks within the next five years. Seventeen percent are in the process of implementing LTE/5G networks or are already using LTE/5G networks. Thirty-nine percent said they have no plans to implement LTE/5G networks in their organization (Figure 4).

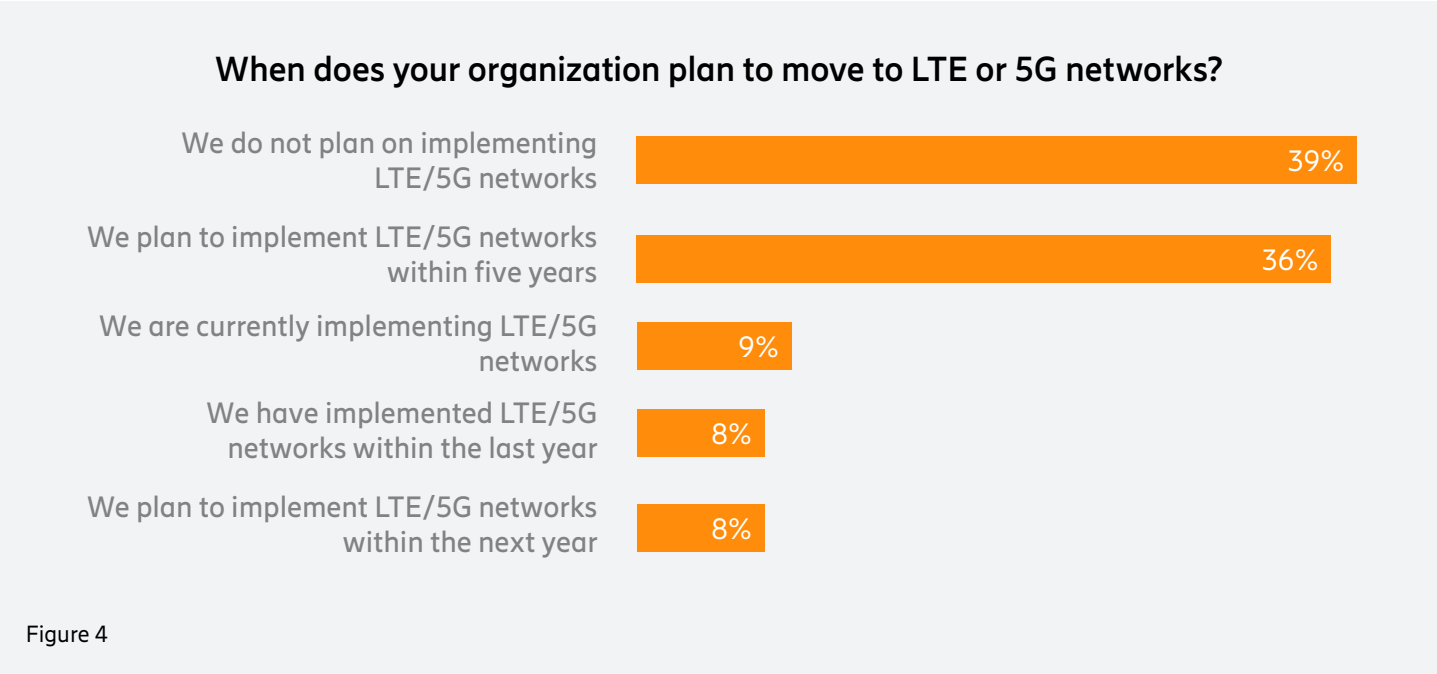


Figure 4

For utilities, private cellular networks offer value beyond the high spectral efficiency, high peak data rates, short trip time, and flexibility in frequency and bandwidth. A reliable private cellular network also means enhanced grid reliability, service/energy affordability, better safety and security and higher return of investment. However, it seems like utilities are mainly focused on issues of connectivity, as 65 percent find that an upgrade to LTE/5G networks will primarily be valuable in improving connectivity in their organization (Figure 5). Following connectivity, utilities value leading tech levels in the market (32 percent), lowering TCO of operations (20 percent) and increasing revenue (6 percent). Interestingly though, 23 percent said there is no value to private networks in their organizations (Figure 5).

What future value does your organization see in LTE/5G private networks?

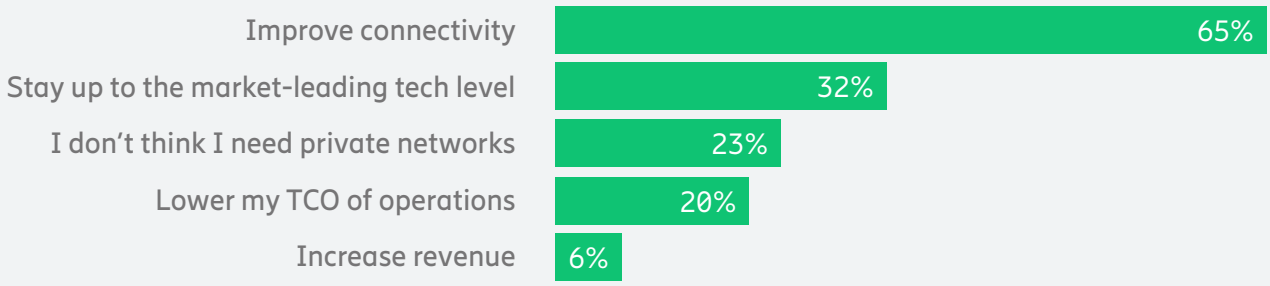


Figure 5

Network security

Is network security within utilities ready for potential threats?

Cybercriminals are persistently developing more sophisticated ways to attack the constantly evolving smart grid and network infrastructures. Therefore, utilities must take preemptive measures to curb potential threats against their infrastructure.

The four pillars of network security risk management are: 1) assessing possible avenues of attacks, 2) assessing the likelihood of an attack, 3) the ability to discover cyberattacks and 4) assessing the consequences of an attack. While 39 percent of utilities believe they have the skills and tools to discover threats and vulnerabilities that may occur in private cellular networks, it is particularly alarming that 40 percent of utility respondents don't know if they have the skills and the tools in their organizations to discover security threats and vulnerabilities, and almost a quarter of respondents say they do not have these skills within their organization. This is despite the fact that the majority of utilities are using private cellular networks or plan to deploy private cellular networks (Figure 6).

Do you have the skills and tools in your organization to discover security threats and vulnerabilities in cellular private networks?

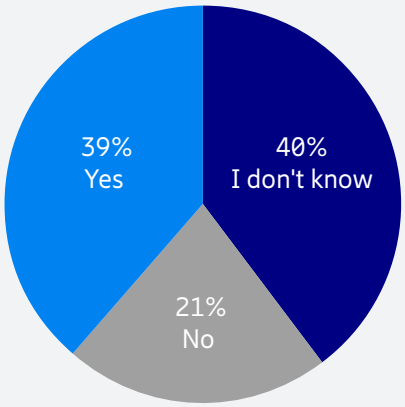
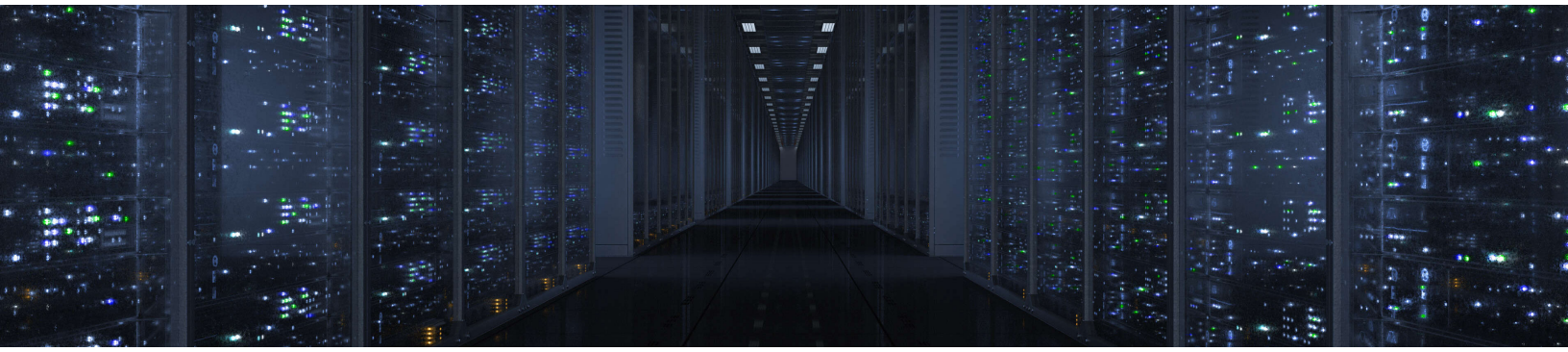


Figure 6



When asked where their security tools and personnel are housed, 60 percent of respondents said they use both in-house and outsourced security. Twenty-five percent of utilities use only in-house security personnel and tools, while only seven percent exclusively outsource their security (Figure 7). The use of in-house tools and personnel for private cellular network security is high, especially when considering the results in Figure 6 that show 62 percent of utilities either don't know or don't believe their organizations have the adequate skills and tools to discover security threats and vulnerabilities in their private cellular networks.

With increased digitalization and IoT deployments in utilities, it is not a surprise that 57 percent of respondents say that the increasing number of edge devices and distributed resources is the top challenge facing their current network security systems. The second most challenging aspect to their current network security system is not having enough internal talent to manage network security (44 percent). This is especially surprising since the majority of utilities rely on in-house personnel and tools for their private cellular security network. Thirty-eight percent of utilities say cost is also a top challenge, followed by lack of access to critical data (23 percent), not enough investment in network security (14 percent) and lack of executive buy-in (nine percent) (Figure 8).

Does your organization use in-house security personnel and tools or does it use outsourced security for private cellular network security?

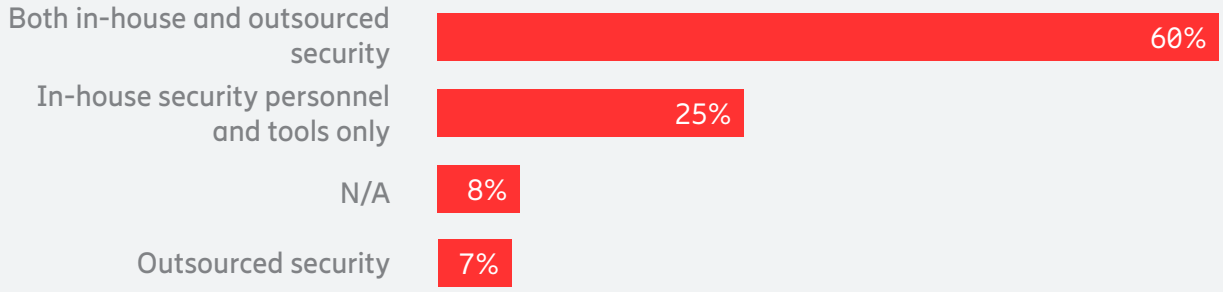


Figure 7

What challenges do you have with your organization's current network security system?

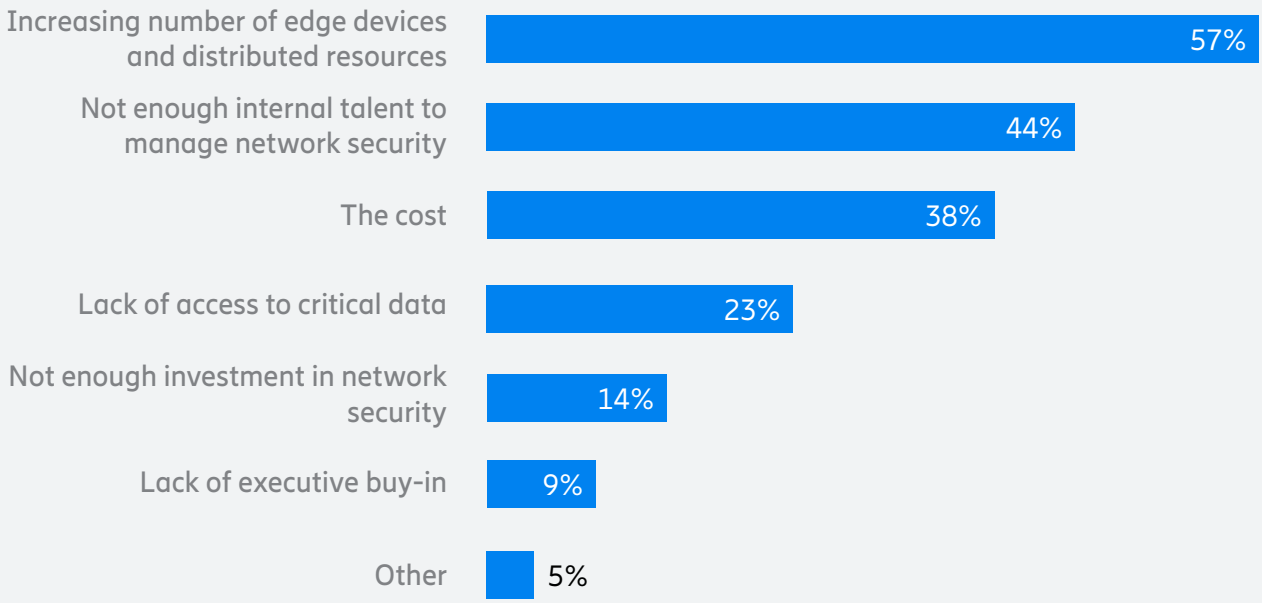


Figure 8

Utilities value cybersecurity, but not enough to invest in new security technologies

Regarding perceptions of their organizations' investment in cybersecurity, 80 percent of utilities believe that their organizations are adequately investing in network security. Only 9 percent disagree with that statement and 11 percent do not know if their organization is investing enough in network security.

The utilities' digital transformation would potentially mean an increase in Edge Computing/Multi-access Edge Computing (MEC) adoption due to a rising necessity to decentralize data storage and processing and the value that Edge Computing/MEC could bring to IT infrastructure and operations. While Edge Computing/MEC is a solution for low-latency requirements of many utility device applications, it also increases the surface area for cyberattacks by increasing the number of IoT endpoints. When asked about their plans to adopt Edge Computing/MEC, 50 percent of respondents do not plan to use Edge Computing/MEC at all. Thirty-five percent said they plan to use Edge Computing/MEC within the next five years. Nine percent said they are currently using Edge Computing/MEC. Five percent said they plan to use Edge Computing/MEC within the next year.

Do you agree with the following statement, "My organization is adequately investing in network security."?

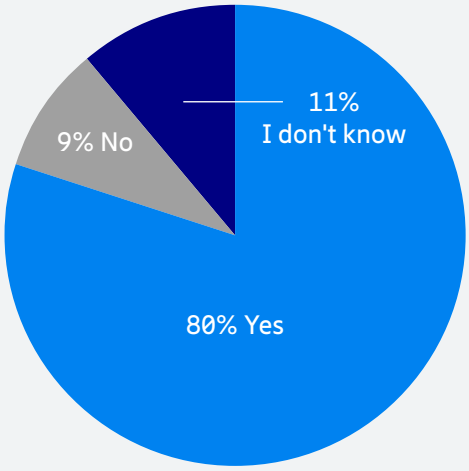


Figure 9

Does your organization have any plans to use Edge Computing/MEC?

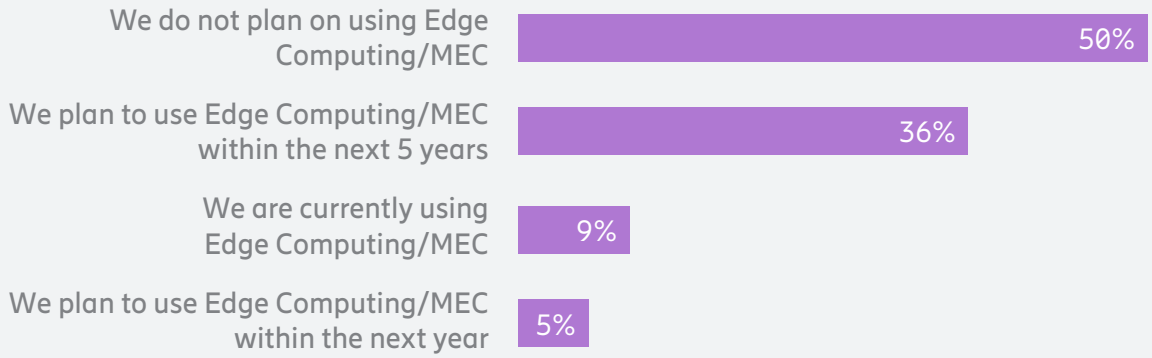


Figure 10

How important are the following network security aspects to your organization?

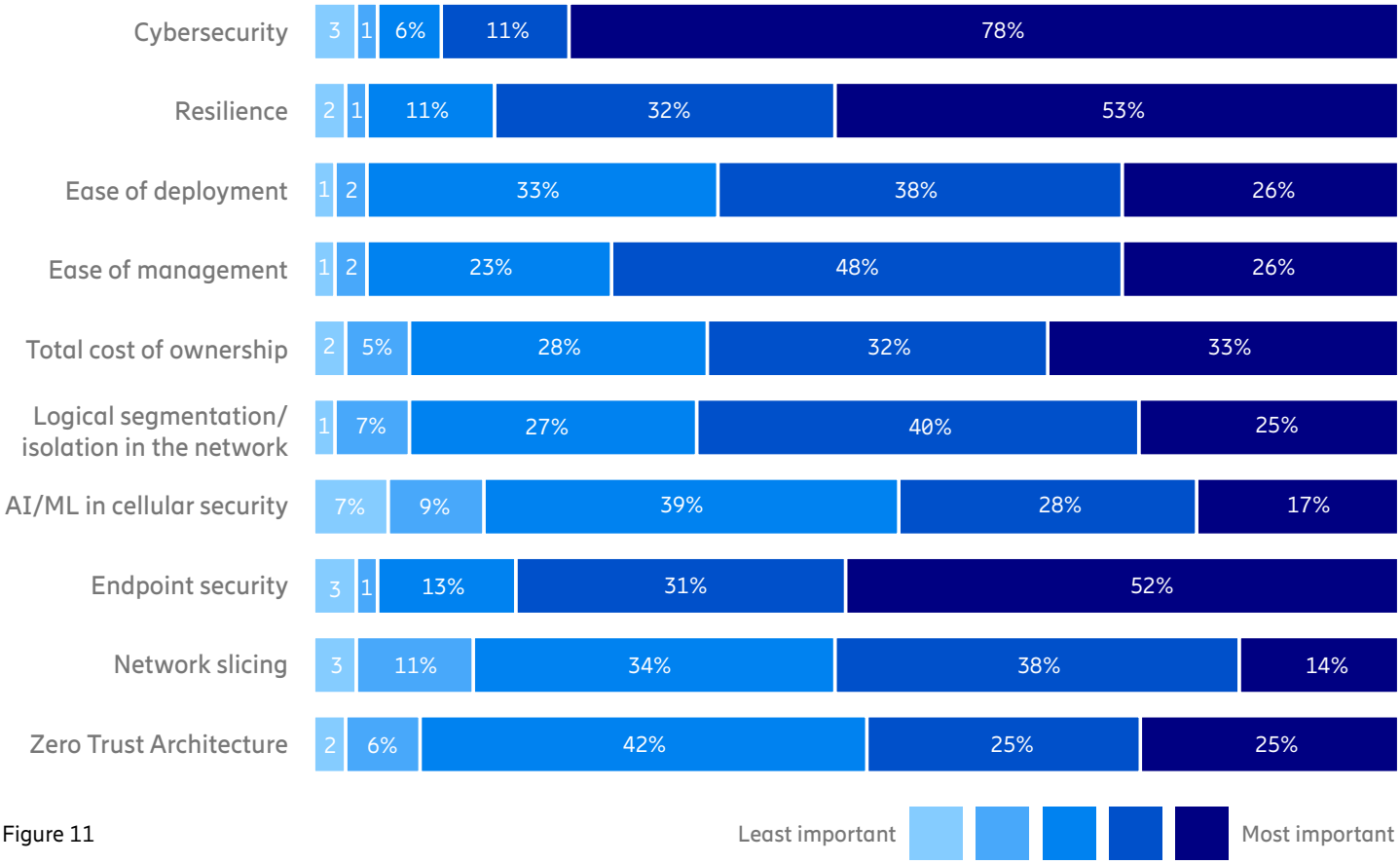


Figure 11

A well-established private cellular network must be comprehensive and multidimensional at deployment and should include device management, IT/OT connectivity, data analytics and security. However, it is also essential to prioritize capabilities and architectures being implemented. When asked about the importance of different capabilities and architectures of private cellular networks, cybersecurity was ranked most important by 78 percent of utilities followed by resilience (53 percent) and endpoint security (52 percent).

Following the top three network architectures are ease of management (48 percent), logical segmentation/ isolation in the network (40 percent), AI/ML in cellular security (39 percent), ease of deployment and network slicing (38 percent).

Zero Trust Architecture is a comprehensive IT security framework that protects organizations from malware and cyberattacks internally and externally. The new hybrid work model has accelerated the deployment of Zero Trust Architecture, as it became more necessary and urgent for organizations to secure users who are working from home. Despite it being an effective security architecture, utilities still seem reluctant to adopt it in their organizations. Our results show that 63 percent are still looking into Zero Trust Architecture for their network security. However, 13 percent and 11 percent are implementing software-defined networks and enhanced identity governance, respectively. For the eight percent that answered 'other', these do not know how their organizations are implementing Zero Trust Architecture. Five percent are implementing micro-segmentation, while only one percent are implementing intent-based networking (Figure 12).

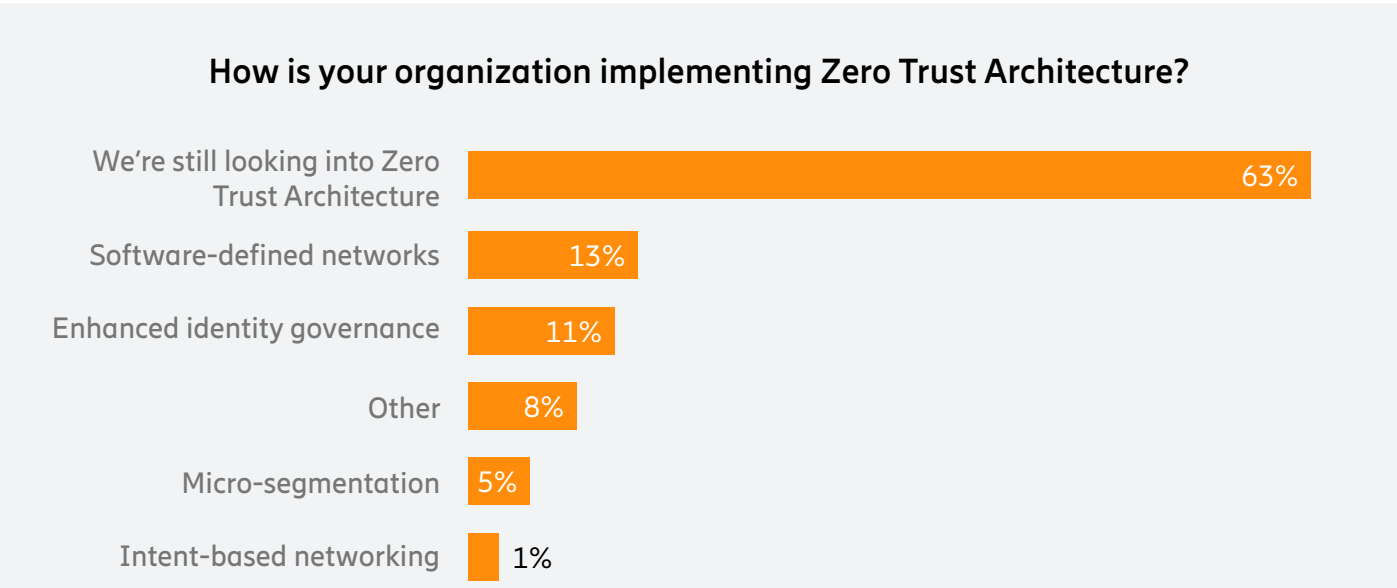


Figure 12

Network security is a tricky business, and no architectural model is one size fits all. It is up to each utility to determine the best tools and model to protect their assets and data. Whether utilities are implementing cellular networks or building their security infrastructure, there will be challenges that utilities must overcome. The biggest challenge for utilities when integrating cellular networks into existing IT/OT security systems is network security or data privacy (69 percent). Cost is also a top concern for utilities (56 percent), as is always the case with protecting major assets like cellular networks (Figure 13).

Regulatory requirements can be a boon or a hurdle for security providers in utilities. They can offer guidance and awareness of security threats to utilities, but security regulatory requirements could also raise costs and limit investments in other avenues. And with the increasing cybersecurity threats to our core energy and utilities infrastructures, regulators are implementing stricter security requirements for the industry. This is evident in the data, as 39 percent of utilities find that regulatory requirements are a potential security infrastructure challenge. For example, the U.S. federal government recently banned electric utilities that supply critical defense facilities from importing certain parts from China, adding more restrictions on utilities to protect the U.S. and its vital infrastructure from cyberattacks. This overall technology sourcing and vetting is found by 30 percent of utilities to be a top security infrastructure challenge.

The right mixture of tools and regulations for a solid security infrastructure would be incomplete without the right set of skills and expertise to implement those tools and comply with regulations. However, 38 percent of utilities say that organizational structure or lack of expertise is a top security infrastructure concern. Additionally, some would argue that those tools would significantly improve and benefit security operations if interoperability was promoted and achieved. Interoperability is still a top concern for utilities (36 percent).

What potential security infrastructure challenges do you see regarding the integration of cellular networks into your existing IT/OT security systems?

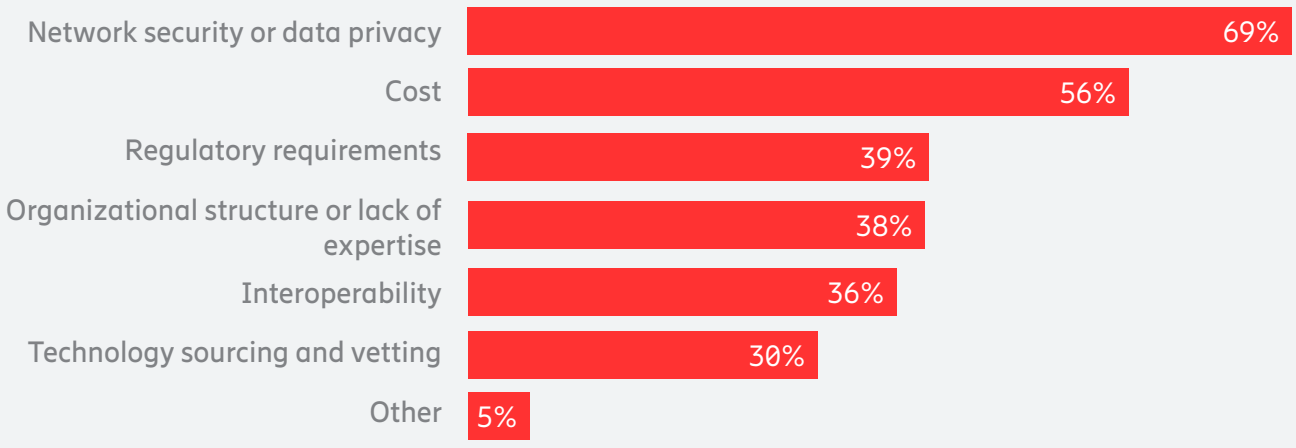


Figure 13

Supply chain security

A resilient supply chain is crucial in an industry that relies on outside vendors for day-to-day operations.

Despite the rising threat of cyberattacks in previous years and the increased attack surface and vulnerability from the newly implemented work-from-home model, 64 percent of utilities have not experienced any compromise in their supply chain in the last three years. Seventeen percent of utilities' supply chains were compromised. Interestingly, 19 percent are not aware whether or not their supply chains were compromised in the last three years, meaning that information about compromised supply chains is not shared across the organization. Though almost two-thirds of respondents reported no delays due to supply chain security breaches, 22 percent reported significant delays, between 3 and 12 months (Figure 15).

Has your supply chain security been compromised in your organization during the last three years?

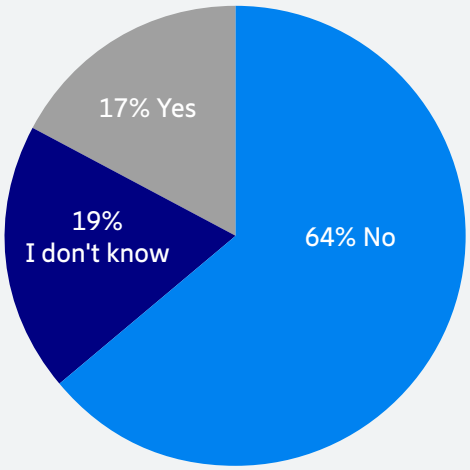


Figure 14

How long were your projects delayed due to supply chain security breach?

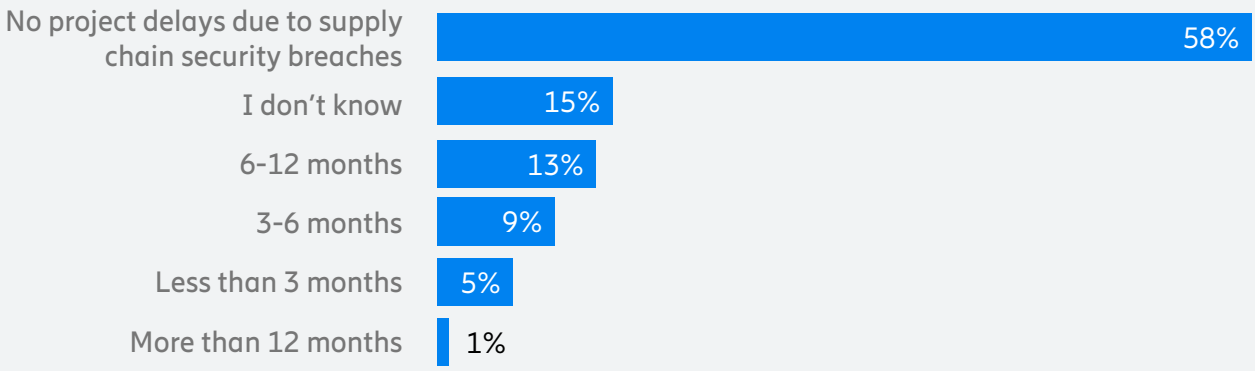


Figure 15

Conclusion

As utilities adopt IoT technologies, shift to remote or hybrid work, and switch to cellular networks, they become more vulnerable to cyberattacks. They must also navigate new technology integration, security issues and regulatory compliance while maintaining connectivity and reliability. It's crucial that the shift toward digitalization happens in tandem with an adequate and solid network security infrastructure. Experiencing a cyberattack has become a question of when, not if, and it's important that utilities understand the gravity of the issue and commit enough investment into network security solutions along with a workforce that has the manpower and skills to prevent cyberattacks and solve security challenges.

A consistent concern of utilities that has been reflected in the data is their lack of adequate internal skills, expertise, and training against cyber threats and managing network security. And if the data is indicative of one thing, it would be that security is still being addressed reactively as opposed to proactively. Utilities must actively seek measures and solutions to deter cyberattacks before they happen.

Recommendations

- Invest in training the workforce to be well versed in the advantages and potential threats that cellular network adoption poses to the organization, as well as the tools and policies they can follow to prevent cyberattacks.
- Take proactive measures to deter cyberattacks, rather than reacting once one has occurred.
- Run simulation attacks to test security tools and reliability.

Survey respondent demographics

What type of utility?	
Investor-owned	34%
Public-owned	7%
Municipal	25%
Cooperative	22%
District	7%
Other	4%

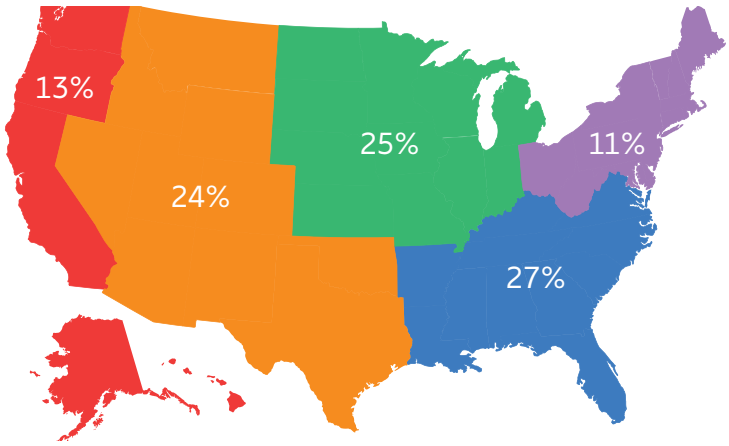
Which services does your utility provide?	
Electric	96%
Gas	23%
Water	16%
Wastewater	8%
Solid waste	5%
Street lighting	24%
Broadband	8%
Other	3%

What is the size of your utility by number of customer accounts?	
2,000,000+	25%
1,000,001—2,000,000	12%
500,001—1,000,000	15%
200,001—500,000	6%
100,001—200,000	8%
50,001—100,000	11%
25,001—50,000	13%
Fewer than 25,000	11%

What is your organization's annual revenue?	
Over 1 billion USD	41%
500 million to 1 billion USD	12%
100 million to 500 million USD	22%
Below 100 million USD	25%

What is your primary role within your organization?	
Engineering	20%
Operations	25%
Maintenance	1%
Markets/Forecasting	1%
IT/OT	21%
Customer service	4%
Executive	15%
Finance	2%
Innovation/Emerging technology	4%
Marketing	3%
Other (please specify)	6%

What region(s) does your utility serve?



Canada: 9%
International (other): 7%

What is your level of job responsibility in your organization?	
Executive/C-Level	13%
Director	14%
Management	44%
Professional staff	25%
Administrative	1%
Other (please specify)	4%

About Ericsson

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

www.ericsson.com

www.ericsson.com

SE-126 25 Stockholm, Sweden
Telephone +46 10 719 00 00

April 2022