Infosys®
Navigate your next

ASSURING DIGITAL-TRUST

ENERGY AND UTILITIES INDUSTRY VIEW

Infosys® | Knowledge Institute

Table of Contents

INTRODUCTION

The energy and utilities (E&U) industry is combating fierce competition from nontraditional providers while fulfilling the demands of savvy and environmentally conscious customers. At the same time, they have to satisfy stringent regulations and enhance operational performance. To handle these challenges, the E&U industry has opted for digitization to capitalize on technologies such as big data analytics, internet of things (IoT), mobile solutions, and the cloud. Digital technologies have disrupted the entire energy value chain from customer interactions to power generation. The new digital core has enabled smart operations, automation of manual processes, intelligent customer interactions, and modernization of electric grids. Further, the convergence of operational technology (OT) and IT has made it possible for much higher levels of operational efficiencies than before.

However, these gains increase vulnerability to cybersecurity threats and attacks. The E&U industry manages mission-critical infrastructure in many countries, making those firms targets of hostile nations. Companies in the energy sector are frequently attacked, and this is expected to worsen as cyber criminals increase their technological sophistication.

Guarding and defending against these threats has assumed paramount importance.

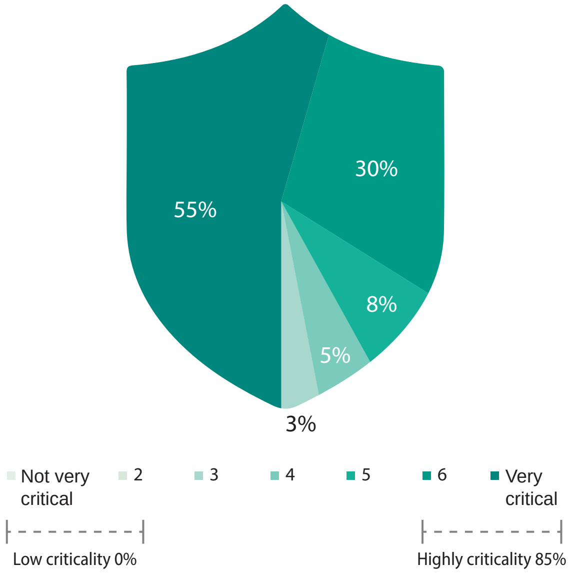
To investigate further, Infosys commissioned a study of 40 senior-level executives from E&U organizations with revenues over $500 million and located across the U.S., Europe, and Australia and New Zealand (ANZ). The study's objectives were to understand the industry's challenges, solutions, and plans for the future and present a holistic view of the cybersecurity landscape.

Diving into cybersecurity

Phishing and malware attacks through emails and inadvertent employee action have compromised customer and company data and led to financial losses and business disruption. Given the clear need for a robust cyber defense program, how critically are enterprises viewing cybersecurity?

Infosys research revealed that 85% of respondents across all countries surveyed viewed cybersecurity as critical to their organization.

Figure 1. How do organizations view cybersecurity?

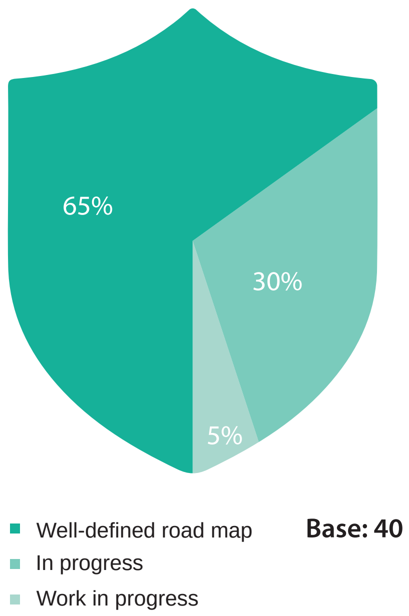


Criticality	Overall	E&U	U.S.	Europe	ANZ
Base	***867***	***40***	***18***	***15***	***7***
High criticality (%)	83	85	89	80	86
Low criticality (%))	1	8	0	0	0

E&U: Energy and Utilities

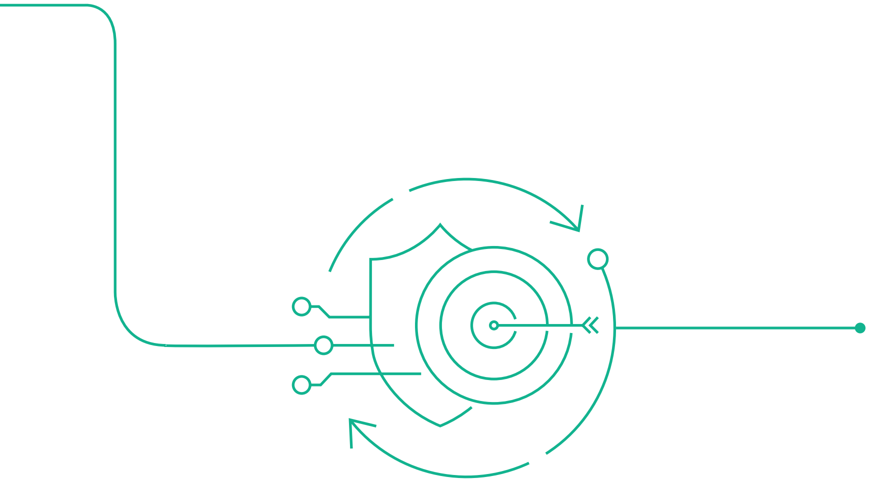
A significant 95% of respondents said they have a well-defined enterprisewide strategy that is either implemented or is being implemented. Australia and New Zealand were ahead in having completed implementation (86%) while Europe lagged (53%).

Figure 2. Maturity of your cybersecurity program



What is the current maturity of your cybersecurity program (%)	Overall	E&U	U.S.	Europe	ANZ
Base	***867***	***40***	***18***	***15***	***7***
Well defined enterprisewide strategy/roadmap exists, implemented	66	65	67	53	86
Enterprisewide strategy/ roadmap exists as a guideline but implementation in progress	30	30	33	33	14
Enterprisewide strategy/ roadmap is work in progress and therefore implementation and operations are ad hoc	4	5	-	13	-
No defined framework or program	0	-	-	-	-

E&U: Energy and Utilities



Higher the board's involvement, the better the chances of cybersecurity success

All critical initiatives must have the backing and involvement of the board and senior management. Not only does their support convey a strong message across the company, but it also ensures business-wide responsibility. Besides, these initiatives can benefit from the varied experiences of board members and senior leaders.

Figure 3. Organizational levels that are discussing cybersecurity

E&U	(%)	U.S.	Europe	ANZ
		18	***15***	***7***
CIO/CTO	63	61	60	71
Business CXO (CEO , COO , CFO , CMO , CHRO)	53	56	47	57
Board level	33	44	20	29
EVP/ SVP/VP	23	28	27	-

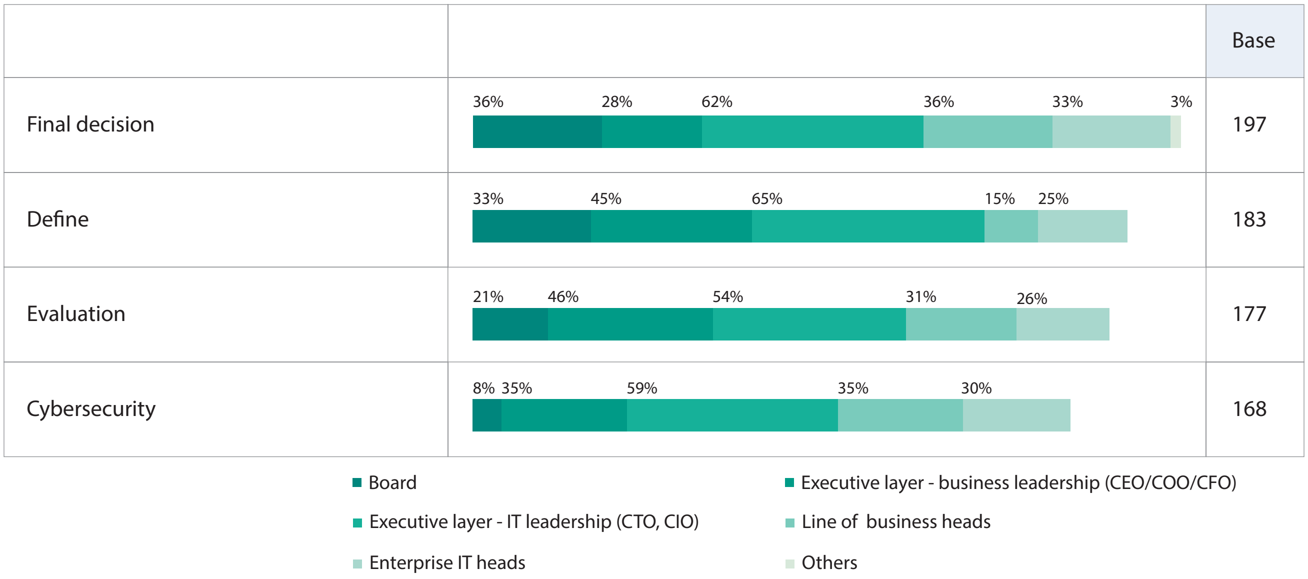
Base: 40

The survey shows that the responsibility for cybersecurity programs mostly lies with business leaders (63%) and IT leaders (53%). Only 33% of respondents said their board is involved.

In the U.S., boards play a more active role (44%). Both the business leaders (71%) and IT leaders (57%) from Australia and New Zealand are actively engaged in cybersecurity programs.

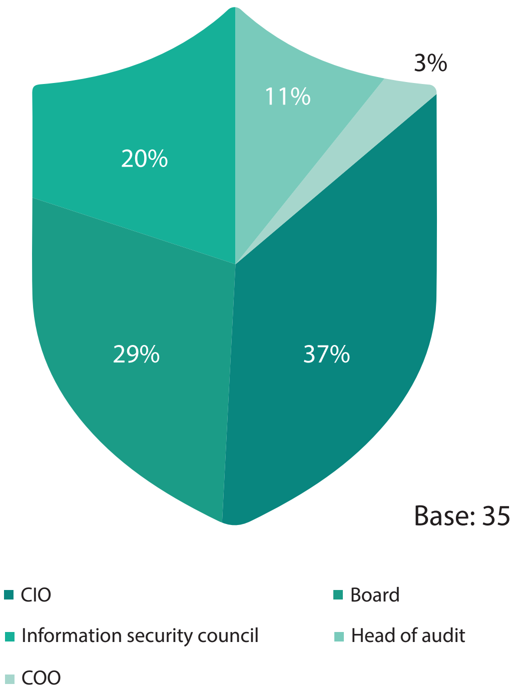
While boards contribute most during the final decision-making stage (36%), business leaders participate actively in evaluating solutions and vendors (46%) and defining the cybersecurity strategy (45%). More than half of respondents said that IT leaders stayed engaged during the entire lifecycle. There is a clear need for boards and senior management to increase their participation and contribute to a successful cybersecurity journey.

Figure 4. Key participants in the cybersecurity journey



When discussing the role of leaders, it's essential to understand the contribution of the chief information security officer (CISO). That executive is a key decision-maker in determining the success of the cybersecurity program and ensuring it remains aligned with the business strategy.

Figure 5. CISO reporting hierarchy



Where does the CISO organization (chief information security officer) report in to	Overall	E&U	U.S.	Europe	ANZ
Base	***792***	***35***	***16***	***12***	***7***
CIO	34	37	44	8	71
Board	32	29	25	42	14
Information security council	23	20	13	33	14
Head of audit	5	11	19	8	-
COO	3	3	-	8	-
Head of operation risk	3	-	-	-	-
Others	1	-	-	-	-

E&U: Energy and Utilities

According to respondents, CISOs mostly reported to the chief information officer (37%) and the board (29%). E&U firms must take steps to elevate the role since the CISO is the linchpin of the cybersecurity program.

The most pressing cyberthreats

The respondents' top three concerns are hackers and hacktivists (80%), insider threats (75%), and low awareness of potential risks among employees (75%).

Figure 6. Top cybersecurity concerns

What is your number one concern regarding threats(%)	Overall	E&U	U.S.	Europe	ANZ
Base	***867***	***40***	***18***	***15***	***7***
Hackers/hacktivists	84	80	78	80	86
Insider threats	75	75	78	73	71
Low awareness of potential security risks among employees	76	75	78	67	86
Nation-states	60	70	78	53	86
Corporate espionage	75	70	56	73	100
Organized crime	67	70	67	80	57
Uneven deployment of cybersecurity solution	60	58	67	67	14

E&U: Energy and Utilities

E&U industry firms collect and maintain a considerable amount of sensitive data, from both the company and the consumer. That makes them a frequent target for cyberattacks. Hackers stand to benefit greatly if they can access that data to facilitate identity theft, steal financial information, or exploit confidential data.

Hostile groups can attempt to disrupt companies or even countries through targeting critical infrastructure. E&U firms consider nation-states, organized crime and corporate espionage (each 70%) as serious concerns. Often, the actions of employees, knowing or unknowing, can cause significant damage, since they have greater access to sensitive internal information.

Respondents from Australia and New Zealand expressed strong concerns about corporate espionage (100%), hackers (86%), low security awareness among employees (86%), and nation-states (86%). Nation-state threats were also prominent concerns (78%) for U.S. companies. European respondents were most concerned about hackers (80%) and organized crime (80%).

THE ENTERPRISE IMPERATIVES

Enterprises must always be hyperalert to effectively counter cyberthreats. The appropriate defense should have touchpoints across technology, processes, and people to address all concerns and imminent threats. Cyber defense must also have enterprisewide access to ensure maximum protection.

Top security solutions implemented today

To counter threats and attacks, E&U firms most frequently use intrusion prevention systems (61%), identity and access management (60%), and cloud access security brokers (59%).

Figure 7. Cybersecurity solutions

Top solutions implemented (%)	Overall	E&U	U.S.	Europe	ANZ
Intrusion prevention systems	63	61	61	50	83
Identity and access management	63	60	67	53	57
Cloud access security broker	64	59	56	57	71
Security awareness training	66	55	56	46	71
Risk and compliance	66	55	72	47	29
Security incident management	66	55	56	47	71
Tackling IoT security	60	54	59	53	43
Unified threat management	58	53	67	33	57
Application control on server workloads	58	48	33	47	86
Encryption	64	38	50	27	29

E&U: Energy and Utilities

As E&U firms digitize their operations for business purposes, the cloud gains increasing significance. At the same time, it gives rise to new security requirements. Enterprises often choose to let cloud access security brokers do the heavy lifting by applying security, governance, and compliance policies across multiple cloud services.

Another way in which enterprises are dealing with these concerns is through security awareness training. By educating employees on various cyber scenarios, an enterprise can benefit immensely by averting potential damage.

Implementation of intrusion prevention systems (83%) and use of cloud access security brokers (71%) are the highest in Australia and New Zealand, while identity access management solutions are deployed most frequently in the U.S. (67%). Europe has been slower to implement security solutions overall.

Challenges galore

E&U industry executives said they are most challenged by the rapid changes in cyber technologies (68%), inadequate management support (65%), lack of user awareness (63%) and the difficulty of embedding cybersecurity in the enterprise IT architecture (63%).

Figure 8. Top cybersecurity challenges

(%)	Overall	E&U	U.S.	Europe	ANZ
Base	***867***	***40***	***18***	***15***	***7***
Cybersecurity technology changing too fast	63	68	61	67	86
Inadequate management support	52	65	61	60	86
Lack of user awareness	54	63	72	40	86
To ensure enterprise	67	63	56	60	86
Lack of appropriate tools to automate controls and audit effectiveness	55	60	67	53	57
Building a cybersecurity aware culture	65	58	61	53	57
Lack of skilled personnel	49	53	44	67	43
Too much time spent in building technology stack and less on deriving value	57	48	39	47	71
Poor integration between tools and different solutions	54	48	61	33	43
Lack of reporting on incidents	39	45	61	33	29

E&U: Energy and Utilities

Rapid evolution in digital technologies must be met with corresponding modifications to the cybersecurity approach. However, this is a demanding task, especially given the pace of change as well as the advanced skill sets required.

The E&U industry must safeguard against damage caused inadvertently by unaware employees as well as those with malicious intent. Insider threats can pose a higher risk since employees have easier access to confidential information. However, building a cybersecurity aware culture is not easy as it involves changing mindsets and processes.

It's no longer enough to protect the perimeter. Efforts must start at the design stage, especially as the enterprise becomes more connected. However, entrenched legacy systems can hamper efforts to embed security into enterprise IT architecture since doing so requires both cultural and large-scale systemic changes and can lead to business disruption.

Respondents from Australia and New Zealand said they were significantly affected by the top four challenges, while those same challenges seemed to have a lesser impact on European firms.

Overcoming the challenges using multiple methods

E&U enterprises rely on methods such as training and certifications (70%), working with technology vendors and service providers (68%), and creating a culture of employee awareness (43%) to overcome the existing challenges.

Figure 9. Cybersecurity approaches

Cybersecurity approaches	(%)	U.S.	Europe	ANZ
		18	*15*	*7*
Training and certifications	70	72	73	57
Work with technology vendors and service integrators	68	67	60	86
Creating a culture of employee awareness	43	44	33	57
Workshops and enablement sessions	40	67	20	14
Hire service provider specializing in security solutions	38	39	33	43
Outsource security cybersecurity monitoring and management	33	39	27	29
Focus on integrated security solutions rather than point sol	30	22	40	29
Enable threat intelligence feeds	15	17	20	-

Base: 40

Australia and New Zealand work extensively with technology vendors and service integrators (86%) and attempt to create a culture of employee awareness (57%). Europe was far behind in both these areas. And those two regions trailed the U.S. in providing training and certifications.

Examining the responses, we see that enterprises overall are adopting approaches that include:

- Implanting security at early stages by propagating a security-first culture through training and workshops.
- Ensuring scalability by replacing siloed solutions with integrated systems.
- Partnering with external experts to keep pace with changes in digital and cyber technologies.

Focus areas – next moves

Recognizing the importance of a solid cybersecurity strategy, E&U enterprises are exploring network segregation, deception technologies, and advanced threat protection to enhance their defenses.

Figure 10. Next stages of cybersecurity

Next stages of cybersecurity	Implemented				
	Overall	E&U	U.S.	Europe	ANZ
Network segregation	65	50	50	40	71
Deception technologies	49	47	53	43	43
Advanced threat protection	55	45	50	33	57
Threat intelligence platform	57	44	59	33	29
DevSecOps	46	44	47	40	43
User and entity behavior analytics	48	35	44	27	29
Security orchestration and automation response	46	33	39	33	14
Cloud access security broker	44	27	41	21	-

Next stages of cybersecurity	Implementing				
	Overall	E&U	U.S.	Europe	ANZ
Network segregation	25	30	39	27	14
Deception technologies	36	29	29	29	29
Advanced threat protection	31	30	28	40	14
Threat intelligence platform	27	31	24	40	29
DevSecOps	34	31	41	20	29
User and entity behavior analytics	29	38	28	40	57
Security orchestration and automation response	34	35	39	27	43
Cloud access security broker	30	24	18	29	33

E&U: Energy and Utilities

Network segregation can provide better security to sensitive data and drastically reduce damage inflicted by attacks by restricting a breach. In Australia and New Zealand(71%) of firms have implemented these types of solutions.

Another important set of tools is deception technologies, which detect intrusions and redirect them to an expert security team for disarming. These technologies help detect attacks in advance and prevent significant damage. U.S. enterprises (53%) are ahead of other regions in implementing deception technology solutions.

Advanced threat protection solutions help guard sensitive data by providing real-time visibility and contextual alerts, which also detect threats early and enable swift responses.

European firms lag in implementing solutions in most of these areas.

THE INFOSYS PERSPECTIVE – SCALE WITH ASSURANCE

Infosys ensures enterprises become SECURE BY DESIGN by helping them imbibe the concept of security at the very early stage of their business lifecycle. Our focus is to drive an enterprise mindset to build systems, platforms & solutions which are based on "secure by design" principles thereby ensuring that security is embedded deeply and not as an afterthought. We adopt defense-in-depth mechanism to ensure that it becomes extremely unlikely for threats to enter our client's network. We strive to provide visibility of the threats, vulnerabilities and incidents on our clients network using comprehensive dashboards while ensuring compliance with industry standards, policies and processes. We help our clients in embedding 'secure by design' at an early stage to reduce the attack surface and minimizes risks. We help organizations to build a mindset that incorporates security in everything that they do.

Infosys is committed to building a resilient cybersecurity program and drive our customers to operate at scale, while increasing operational efficiency and reducing costs. Our scalable, AI-ML based managed detection and automated incident response platform enables integrated incident monitoring and orchestration helps prevent, detect and respond to advanced cyber-attacks. With our strong team of security experts, best practices, automation, deep industry insights and actionable intelligence, commercial flexibility and frictionless delivery of operations through global cyber defense centers, we are ready to scale our customers' digital journey and amplify security, hence the promise of SECURE BY SCALE. Boosting our ability to deliver at scale and providing our customers access to the best talent, is our collaboration with Ivy League universities like Purdue, to reskill and upskill employees globally.

Infosys helps enterprises SECURE THE FUTURE by continuously adopting newer technologies and keeping pace with changing times. Our clients also have access to advanced threat-hunting capabilities, forensics, malware analysis and the latest in technology innovations incubated in the Infosys Security R&D Labs. Nurturing the culture of innovation and research to co-create solutions, deepens the value we deliver for enhanced protection against known and unknown threats. With the advent of newer technologies like Blockchain and IoT, security has become the need of the hour with enterprises seeking new age cybersecurity solutions that can help overcome enterprise security challenges. Infosys prepares enterprises for the future by catering to this need and helping them stay ahead of these threats.

Shaping cybersecurity of the future – trends to watch

The sustainable cybersecurity approach is the one that takes care of today's needs and anticipates tomorrow's requirements. Given the pace at which the business environment is changing, it would be myopic to ignore the building of future capabilities.

Figure 11. Cybersecurity trends

Cybersecurity trends	(%)	U.S.	Europe	ANZ
		18	*15*	*7*
Continued demand for cybersecurity skills	45%	39	60	29
Usage of blockchain technologies in developing security solutions	38%	28	47	43
Privacy and personal data protection gains significance	33%	39	40	29
Artificial intelligence used for real time predictive/ preventive maintenance	28%	28	27	29
Introduction of automation in implementing cybersecurity controls and compliance	28%	28	13	57
Behavioural analytics becomes very important in identity management	25%	22	27	29
New business models including cyber insurance emerge	25%	11	40	29
Deception technologies introduced in IoT and OT (operation technologies)	23%	22	20	29
Regulatory bodies show zero tolerance on non-compliance	20%	33	7	14
Move to customization of security solutions from standard solutions	20%	17	27	14
Cybersecurity startups to gain recognition	13%	22	7	-

E&U: Energy and Utilities

Respondents cited continued demand for cyber skills as another trend to consider. There is a significant shortage of high-quality cybersecurity skills in the market today, making it challenging to run a cybersecurity program optimally. cybersecurity professionals will need to bring in business skills along with their technical expertise to satisfy today's evolving demands.

Blockchain's inherently secure nature and distributed ledger technology make it another top option for boosting cybersecurity programs.

As the digital revolution creates exponentially more data, government concerns about privacy and protection also increase dramatically. Companies must be careful to navigate Europe's General Data Protection Regulation and others that are likely to follow.

THE WAY FORWARD TO INSTILL DIGITAL-TRUST AND NAVIGATE TO A SECURE FUTURE

E&U firms globally are becoming more digitized so that they can respond more intelligently and efficiently to demanding market conditions. In this scenario, cyber threats grow exponentially and can impact not only business systems but also industrial controls. cybersecurity thus plays a vital role in protecting critical business assets and earning the trust of customers.

To give cybersecurity the place it deserves, the board and senior management must engage meaningfully both during the strategy and execution phase. At the same time, the CISO must be empowered to play a more influencing role across the organization.

Further, cybersecurity must be an integral part of every stage of the business lifecycle. Infosys recommends enterprises adopt security at each phase, including design and scale, to build a holistic defense.

However, this path is challenging and demands significant changes, both systemic and cultural. It requires senior leadership support, educating employees, and instituting a security-first mindset. The alternative to this path is to bear financial losses, damage to reputation, loss of customer trust and may even lead to a threat to the business' survival.

On the other hand, an effective cybersecurity program can enable E&U firms to handle risks and support business operations better. Indeed, it is a game changer.

Notes

Notes

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

Infosys®
Navigate your next

For more information, contact askus@infosys.com