Infosys®
Navigate your next

ASSURING DIGITAL-TRUST

TELECOMMUNICATION INDUSTRY VIEW

Infosys® | Knowledge Institute

Table of Contents

INTRODUCTION

The telecom industry is undergoing a metamorphosis as it makes the transition from traditional business models to ones enabled by advanced technologies such as 5G. This shift is necessary if telecom firms want to contend effectively with the threats of commoditization, intense competition, and fast-changing customer expectations. Digital transformation bolstered by the internet of things (IoT), cloud computing, big data and analytics, robotics, and artificial intelligence (AI) is the most effective way for telecom firms to compete in an increasingly complex marketplace. These technological advances can help companies innovate and differentiate, provide better customer experiences, build brand loyalty, and discover new revenue streams.

While transformation leads to exciting opportunities for enterprises, it also underscores the need for reliable cyber defense programs. Creating an effective cybersecurity strategy and ensuring its proper implementation are imperative.

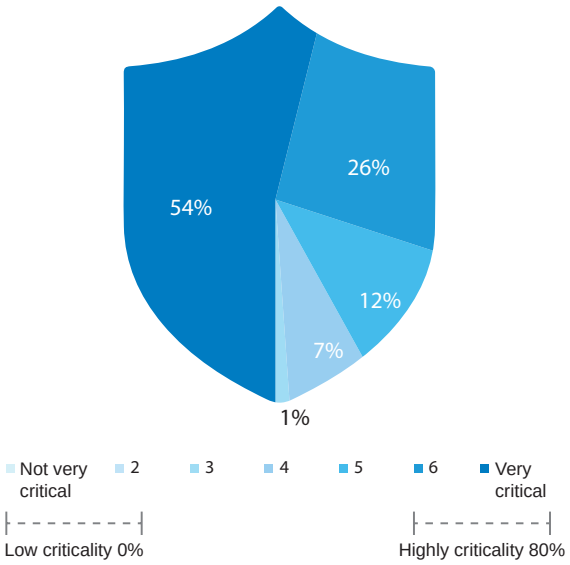
To investigate further, Infosys commissioned a study of 90 senior-level executives from telecom organizations with revenues over $500 million and located across the U.S., Europe, and Australia and New Zealand (ANZ). The study's objectives were to understand the industry's challenges, solutions, and plans for the future, and to present a holistic view of the cybersecurity landscape.

Diving into cybersecurity

In an increasingly digitized environment, where collaboration and connectivity are norms, the attack surfaces at telecom firms have increased exponentially thus exposing the industry to cyberattacks and threats like never before. Without a proper defense, these firms risk financial losses, business disruption, damage to reputation, and decline in customer trust. Given the clear need for a robust cyber defense program, how critically are enterprises viewing cybersecurity?

The survey showed that 80% viewed cybersecurity as "highly critical" to the organization.

Figure 1. How do organizations view cybersecurity?



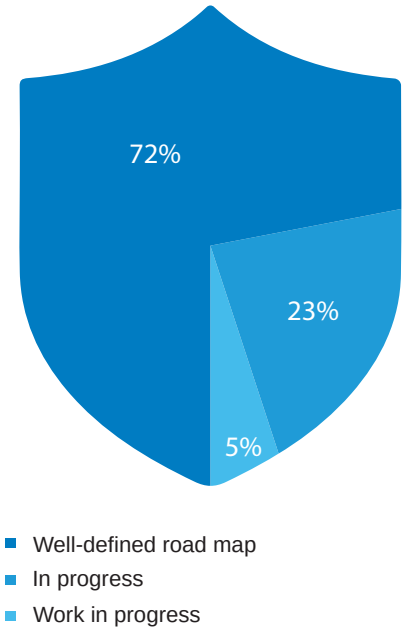
Criticality	Overall	Telecom	U.S.	Europe	ANZ
Base	***867***	***90***	***40***	***38***	***12***
High criticality (%)	83	80	80	82	75
Low criticality (%)	1	1	1	1	1

Telecom: Telecommunications

Three-quarters of firms from Australia and New Zealand consider cybersecurity "highly critical," which trails the other regions.

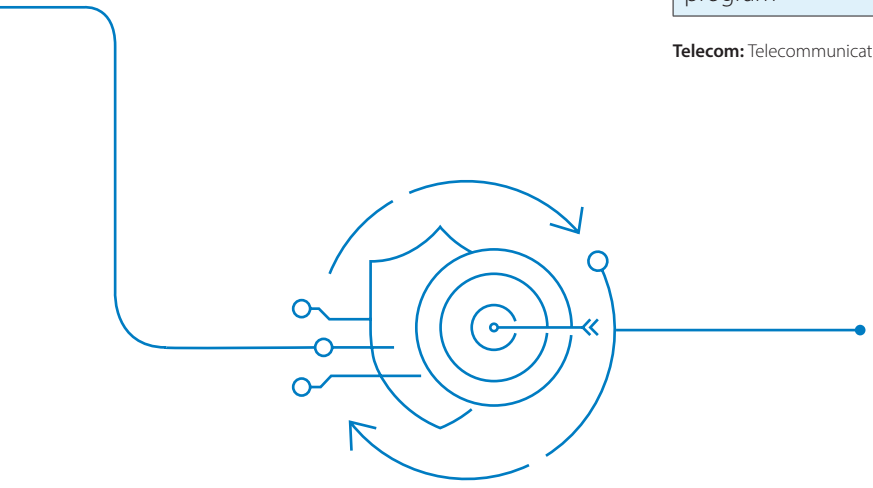
72% of telecom firms have a well-defined enterprisewide strategy, and have implemented it. Australia and New Zealand have a particularly high number of firms (83%) that have done so.

Figure 2. Maturity of your cybersecurity program



What is the current maturity of your Cybersecurity program (%)	Overall	Telecom	U.S.	Europe	ANZ
Base	***867***	***90***	***40***	***38***	***12***
Well defined enterprisewide strategy/ roadmap exists, implemented	66	72	70	71	83
Enterprisewide strategy/ roadmap exists as a guideline but implementation is in progress	30	23	25	24	17
Enterprisewide strategy/ roadmap is work in progress and therefore implementation and operations are ad hoc	4	5	5	5	-
No defined framework or program	0	-	-	-	-

Telecom: Telecommunications



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. Such support not only conveys a strong message across the company but also ensures business-wide responsibility.

Besides, these initiatives can benefit from the varied experiences of the board members and senior leaders.

Figure 3. Organizational levels that are discussing cybersecurity

Telecom	(in %)
Business CXO (CEO , COO , CFO , CMO , CHRO)	62
CIO/CTO	56
Board	42
EVP/ SVP/VP	14

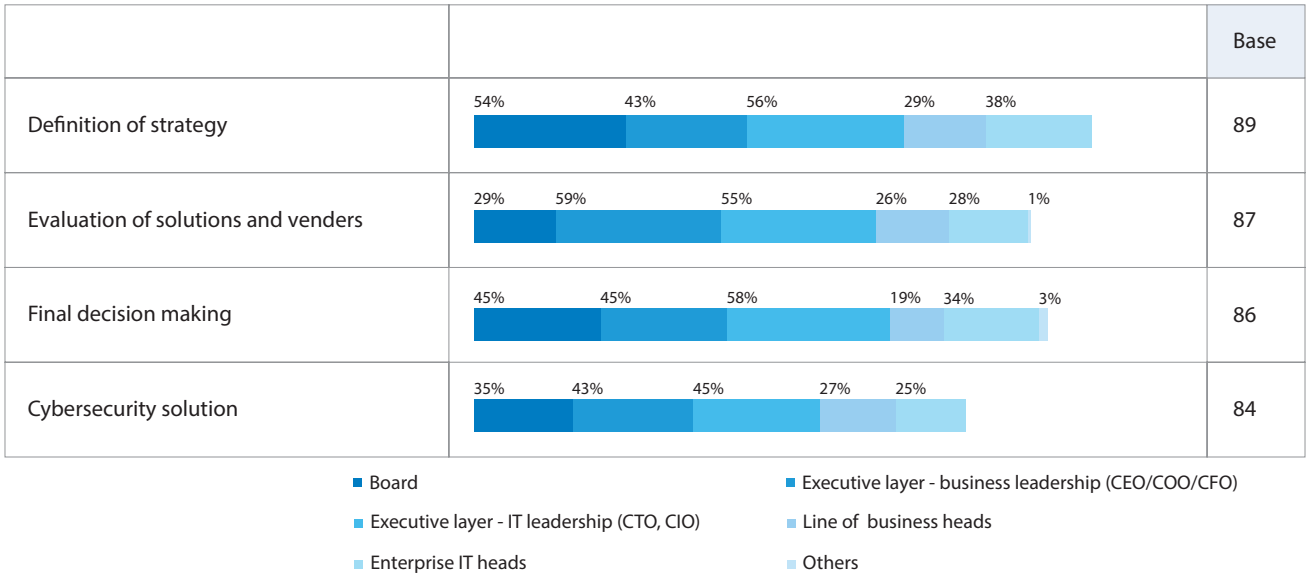
U.S.	Europe	ANZ
40	***38***	***12***
68	58	58
63	50	50
30	55	42
13	16	17

Base: 90

According to the survey, business leaders are most active in cybersecurity discussions (62%), while boards are less involved (42%). The boards of European firms are much more engaged (55%); U.S. boards are the least involved (30%). However, U.S.-based business leaders are much more active (68%) compared with those of other regions.

While the board contributes the most at the strategy definition stage (54%), IT leaders participate through out the journey.

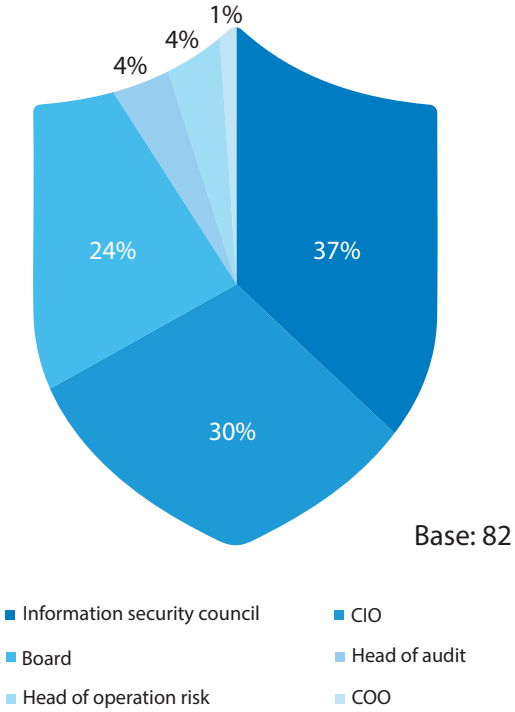
Figure 4. Key participants in the cybersecurity journey



When discussing the role of leaders, it's essential to understand the contribution of the chief information security officer (CISO). This executive is a key decision-maker in determining the success of the cybersecurity program.

Among the respondents, 37% said the CISO reports to the company's information security council, while just 24% said that the executive reports to the board. In that way, the telecom sector is not in line with the global trends in CISO reporting practices.

Figure 5. CISO reporting hierarchy



Where does the CISO organization (Chief Information Security Officer) report in to	Overall	Telecom	U.S.	Europe	ANZ
Base	***792***	***82***	***38***	***35***	***9***
Information security council	23	37	45	26	44
CIO	34	30	37	29	11
Board	32	24	11	34	44
Head of audit	5	4	-	9	-
Head of operation risk	3	4	5	3	-
COO	3	1	3	-	-
Others	1	-	-	-	-

Telecom: Telecommunications

Telecom companies must consider increasing the influence of the CISO as cybersecurity is woven into an organization's digital journey.

The most pressing cyberthreats

With cyberthreats and attacks on the rise, respondents viewed hackers and hacktivists (88%), corporate espionage (80%) and low employee awareness (73%) as the top concerns.

Figure 6. Top cybersecurity concerns

What is your number one concern regarding threats(%)	Overall	Telecom	U.S.	Europe	ANZ
Base	***867***	***90***	***40***	***38***	***12***
Hackers/hactivists	84	88	93	82	92
Corporate espionage	75	80	83	81	67
Low awareness on potential risks of security incidents among employees	76	73	75	71	75
Insider threats	75	72	78	66	75
Organized crime	67	69	63	74	75
Nation-states	60	59	53	66	58
Uneven deployment of cybersecurity solution	60	57	60	55	50

Telecom: Telecommunications

The telecom industry collects and maintains vast amounts of valuable and confidential information, such as customer and financial data. Many of the companies also manage critical infrastructure. These factors make the industry an enticing target for hackers looking to carry out identity theft, steal financial information or profit from sensitive data.

Also, fierce competition in the industry sometimes leads to corporate espionage by rivals. And high employee turnover makes the industry vulnerable to internal attacks.

Respondents from the U.S. (93%) and Australia and New Zealand (92%) expressed the most concern over hackers. The study also revealed that firms in Australia and New Zealand were least worried about corporate espionage (67%).

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. Besides, cyber defense must have enterprise-wide access to ensure maximum protection.

Top security solutions today

The telecom industry's top solutions are risk and compliance (72%), cloud access security brokers (68%), and encryption (66%).

Figure 7. Cybersecurity solutions

Top solutions implemented (%)	Overall	Telecom	U.S.	Europe	ANZ
Risk and compliance	66	72	80	71	50
Cloud access security broker	64	68	68	74	50
Encryption	64	66	70	63	58
Security awareness training	66	64	72	66	33
Identity and access management	63	62	75	58	33
Security incident management	66	60	65	63	33
Application control on server workloads	58	60	68	61	33
Tackling IoT security	60	59	70	61	17
Unified threat management	58	57	63	58	33
Intrusion prevention systems	63	54	60	55	33

Telecom: Telecommunications

Regulatory factors, such as Europe's General Data Protection Regulation and customer concerns about privacy and data usage, compel telecom firms to implement risk and compliance solutions. Failure to comply can lead to massive penalties as well as loss of reputation and customer trust.

Cloud services are well established across the telecom industry, giving 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.

In data-rich enterprises, encryption is imperative since it provides a high level of protection and mitigates risk.

The U.S. is well ahead of the other two regions in implementing a host of solutions to contain damage, while Australia and New Zealand trail.

Challenges galore

The top three problems that telecom companies face are embedding security in the enterprise IT architecture (74 percent), inadequate management support (64%), and keeping pace with fast-changing cyber technologies (61 percent).

Figure 8. Top cybersecurity challenges

Top cybersecurity challenges (%)	Overall	Telecom	U.S.	Europe	ANZ
Base	***867***	***90***	***40***	***38***	***12***
To ensure enterprise IT architecture with embedded security	67	74	70	79	75
Inadequate management support	52	64	73	63	42
Cybersecurity technology changing too fast	63	61	58	63	67
Lack of skilled personnel	49	58	45	68	67
Lack of user awareness	54	57	55	55	67
Lack of appropriate tools to automate controls and audit effectiveness	55	56	60	45	75
Too much time spent in building technology stack and less on deriving value	57	54	63	45	58
Building a cybersecurity aware culture	65	54	48	63	50
Poor integration between tools and different solutions	54	52	48	58	50
Lack of reporting on incidents	39	31	30	34	25

Telecom: Telecommunications

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

Firms most affected by this challenge were the ones in Europe (79%), while the least affected were U.S. companies (70%).

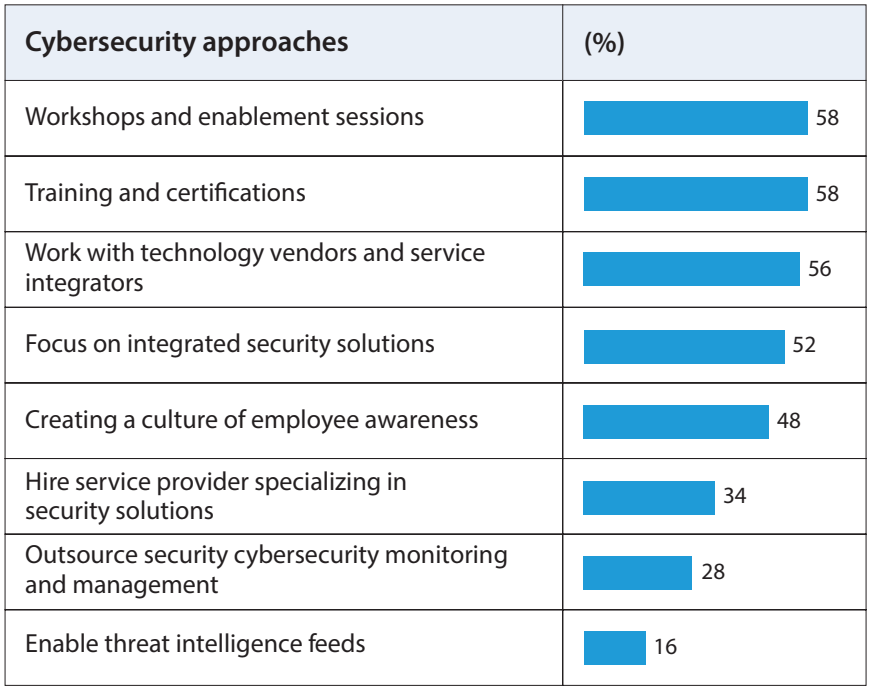
Critical to the success of major initiatives are buy-in and active support from management. In their absence, cybersecurity initiatives are bound to falter from a lack of ownership, limited cooperation and commitment from various departments, and lengthy implementation times. For U.S. firms, this was a significant challenge (73%). It was less of an issue in Australia and New Zealand (42%).

Rapid evolution in digital and cybersecurity technologies must be met with corresponding modifications in an organization's approach. Nevertheless, this is a demanding task, especially due to the pace and frequency of change and the advanced skill sets required. This skills gap is viewed as particularly daunting in Europe (68%) as well as in Australia and New Zealand (67%).

Overcoming the challenges using multiple methods

It appears that the telecom industry has more work to do in overcoming these challenges. Respondents said they employ methods such as workshops and enablement sessions (58%), training and certification (58%), working with technology vendors and service providers (56%) and focusing on integrated solutions instead of point solutions (52%). But the%ages are still relatively low.

Figure 9. Cybersecurity approaches



	U.S.	Europe	ANZ
	40	*38*	*12*
Workshops and enablement sessions	55	68	67
Training and certifications	50	66	58
Work with technology vendors and service integrators	43	74	42
Focus on integrated security solutions	45	66	33
Creating a culture of employee awareness	53	50	67
Hire service provider specializing in security solutions	25	42	42
Outsource security cybersecurity monitoring and management	25	32	25
Enable threat intelligence feeds	13	24	-

Base: 90

Examining the responses, we see that enterprises 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.

Respondents from Australia and New Zealand were the most likely to use workshops and enablement sessions (67%). European firms focused more on working with technology solution providers (74%) and training and certifications (66%). And the U.S. was behind in the adoption of most of these methods.

Focus areas – next moves

Telecom companies need to evolve to the next stage of cyber defense as they focus on more advanced technologies to safeguard their enterprises. The top three areas are network segregation, advanced threat protection, and user and entity behavior analytics, or UEBA.

Figure 10. Next stages of cybersecurity

Next stage of cybersecurity(%)	Implemented				
	Overall	Telecom	U.S.	Europe	ANZ
Network segregation	65	78	78	79	75
Advanced threat protection	55	64	75	53	67
User and entity behavior analytics	48	61	60	58	75
Cloud access security broker	44	61	74	53	42
DevSecOps	46	60	63	58	58
Threat intelligence platform	57	57	50	68	50
Security orchestration and automation response	46	56	55	58	50
Deception technologies	49	50	40	63	42

Next stage of cybersecurity(%)	Implementing				
	Overall	Telecom	U.S.	Europe	ANZ
Network segregation	25	17	18	13	25
Advanced threat protection	31	29	20	39	25
User and entity behavior analytics	29	23	25	24	17
Cloud access security broker	30	20	15	21	33
DevSecOps	34	27	25	34	8
Threat intelligence platform	27	26	35	16	25
Security orchestration and automation response	34	29	30	32	17
Deception technologies	36	41	50	29	50

Telecom: Telecommunications

Network segregation can provide better security to sensitive data by restricting access between network segments and limiting the impact of incidents and slowing down attacks. Advanced threat protection solutions help guard sensitive data by providing real-time visibility and contextual alerts. They allow early threat detection and lead to swift responses. UEBA helps counter attacks by predicting and identifying threats in advance and, as a result, prevents damage.

Three-quarters of U.S. firms have implemented advanced threat protection, while the same%age of firms in Australia and New Zealand have focused on UEBA.

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 building future capabilities.

Figure 11. Cybersecurity trends

H&LS	(%)	U.S.	Europe	ANZ
		40	*38*	*12*
Artificial intelligence used for real time predictive/ preventive	47%	58	37	42
Usage of blockchain technologies in developing security solutions	39%	33	39	58
Privacy and personal data protection gains significance	36%	40	34	25
Deception technologies introduced in IoT and OT (operation technology)	32%	28	34	42
Behavioural analytics becomes very important in identity man	30%	23	34	42
Continued demand for cybersecurity skills	30%	28	39	8
Introduction of automation in implementing cybersecurity solutions	23%	23	26	17
Regulatory bodies show zero tolerance on non-compliance	22%	25	18	25
New business models including cyber insurance emerge	18%	20	16	17
Cybersecurity startups to gain recognition	18%	20	13	25
Move to customization of security solutions from standard	16%	10	24	8

Telecom: Telecommunications

The survey reveals that telecom firms consider AI (47 percent) and blockchain technologies (39%) to be the top cybersecurity trends.

With AI, enterprises can accurately identify threats and trigger action to prevent damage. Moreover, it can help manage and prioritize the massive volumes of data faster and better.

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

The way forward to instill digital trust and navigate to a secure future

Telecom firms are experiencing groundbreaking changes as they switch to new technology-enabled business models to create new revenue streams, differentiate themselves, and compete more effectively. As they accumulate critical infrastructure and valuable customer data, they become an attractive target for cyberattacks. In this scenario, cybersecurity plays a vital role in protecting crucial 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 telecom firms to pursue new business opportunities more confidently. 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

For more information, contact askus@infosys.com

Infosys®
Navigate your next