Infosys®
Navigate your next

ASSURING DIGITAL-TRUST

HIGH-TECH INDUSTRY VIEW

Infosys® | Knowledge Institute

Table of
Contents

INTRODUCTION

High-tech firms are undergoing a disruptive phase as they strive to adopt new business models to stay agile and accelerate innovation. Doing so is the only way to differentiate themselves from the competition, satisfy the demands of tech-savvy customers, and generate better business results. In this race for survival, high-tech firms must quickly adapt to new ecosystems, gain deeper insights into customers, introduce new design thinking, and explore new market segments. Embracing digital technologies can help these enterprises deliver on these business outcomes.

The proliferation of digital technologies drives increased automation and connectedness and provides an opportunity to enhance customer understanding and engagement. It also significantly impacts high-tech supply chains by extending their reach.

However, there is a downside to this digital wave. As early adopters of new technologies, high-tech firms can be exposed to as-yet-undiscovered vulnerabilities. That puts mountains of sensitive data at risk, making cybersecurity a crucial aspect of the industry's transformation.

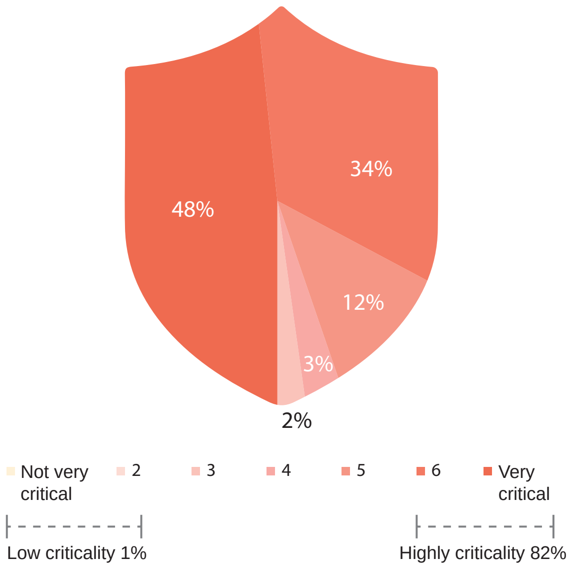
To investigate further, Infosys commissioned a study of 106 senior-level executives from high-tech organizations with revenues of over $500 million and that are located across the United States, Europe, Australia and New Zealand (ANZ). The study's objectives were to understand the industry's cybersecurity challenges, solutions, and plans for the future, and also to present a holistic view of the cybersecurity landscape.

Diving into cybersecurity

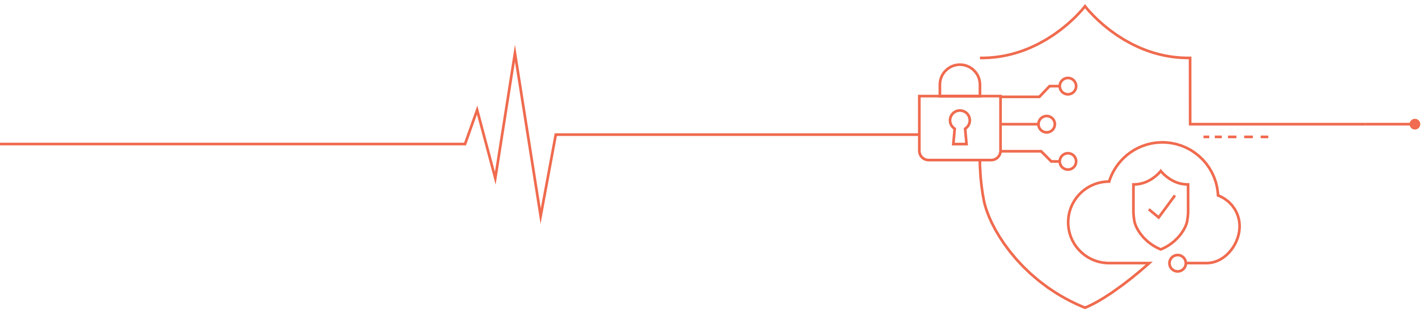
High-tech firms encounter frequent malware attacks, partly as a result of their employees' use of the latest gadgets and apps, which may not be entirely secure. Also, the significant amounts of intellectual property (IP) and customer data that they carry make them targets for cybercriminals. That creates a larger "attack surface" that must be protected.

Infosys research found that 82% of overall respondents consider cybersecurity as most critical to their organization. In the U.S., 87% rated it a high priority.

Figure 1. How do organizations view cybersecurity?

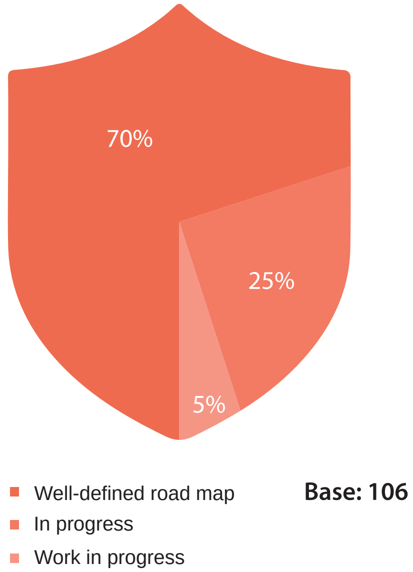


Criticality	Overall	High-Tech	U.S.	Europe	ANZ
Base	***867***	***106***	***55***	***38***	***13***
High criticality (%)	83	82	87	76	77
Low criticality (%)	1	1	-	3	-

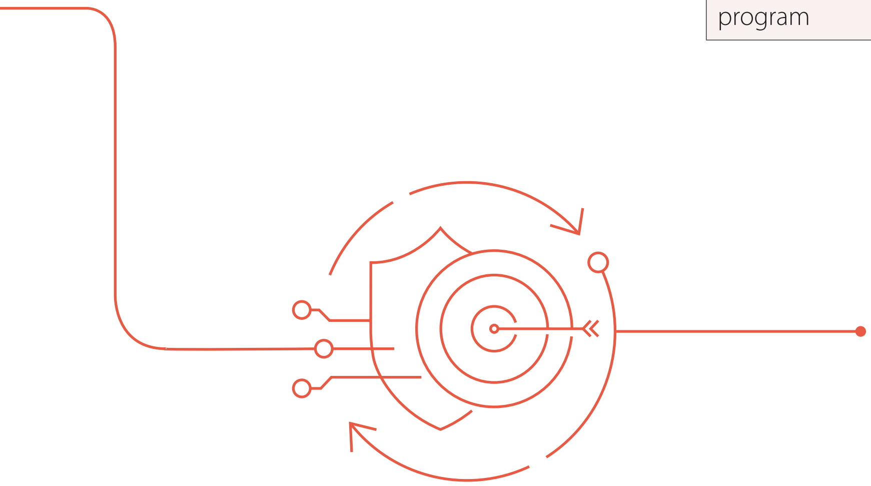


Of those surveyed, 95% said they have a well-defined enterprise-wide strategy that has been implemented or is being implemented. Results from the three regions are within a few%age points of each other. In Australia and New Zealand, the remaining respondents (31%) are in the process of implementing an enterprise-wide strategy.

Figure 2. Maturity of your cybersecurity program



What is the current maturity of your cybersecurity program (%)	Overall	High-Tech	U.S.	Europe	ANZ
Base	***867***	***106***	***55***	***38***	***13***
Well defined enterprisewide strategy/ roadmap exists, implemented	66	70	71	68	69
Enterprisewide strategy/roadmap exists as a guideline but implementation in progress	30	25	25	24	31
Enterprisewide strategy/ roadmap is work in progress and therefore implementation and operations are ad hoc	4	5	4	8	-
No defined framework or program	0	-	-	-	-



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 it convey a strong message across the company, but it also ensures business-wide responsibility. In addition, these initiatives can benefit from the varied experiences of the board members and senior leaders.

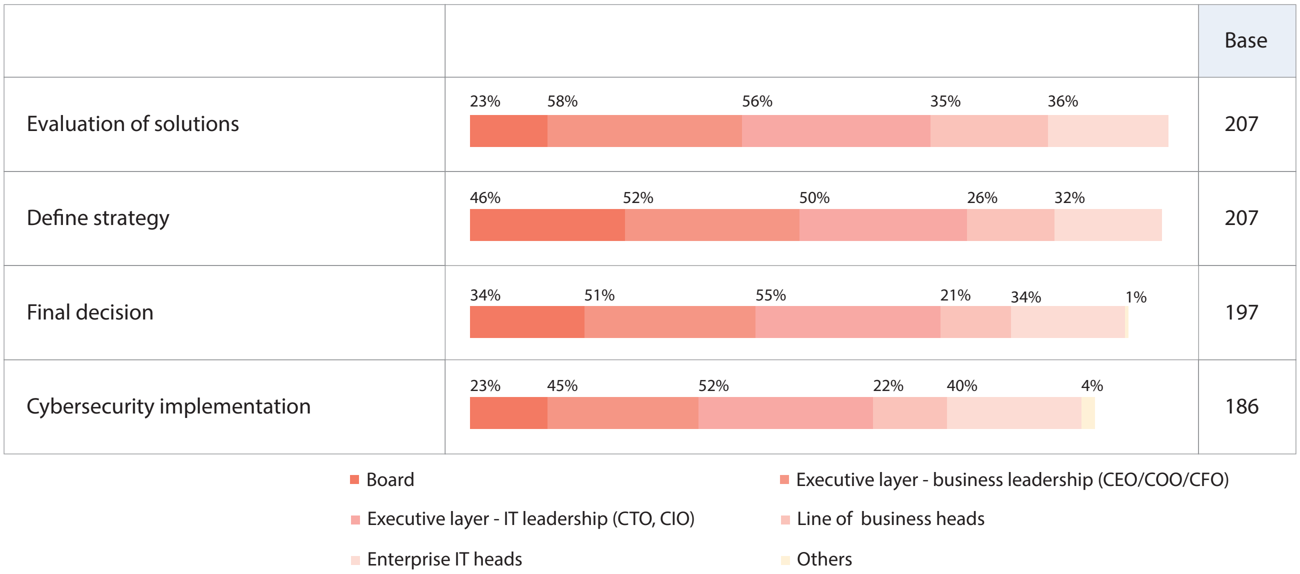
Figure 3. Organizational levels that are discussing cybersecurity

High -Tech	(%)	U.S.	Europe	ANZ
		55	***38***	***13***
Business CXO (CEO , COO , CFO , CMO , CHRO)	61	67	58	46
CIO/CTO	58	62	47	69
Board	43	42	47	38
EVP/ SVP/ VP	13	16	11	8

Base: 106

Only 43% of the respondents said that their board is involved in strategy discussions, while 61% of business leaders are active in that process. Europe has the highest number of respondents (47%) who reported board involvement, while Australia and New Zealand have the lowest (38%). Business leaders from the U.S. (67%) are more engaged than those from other regions.

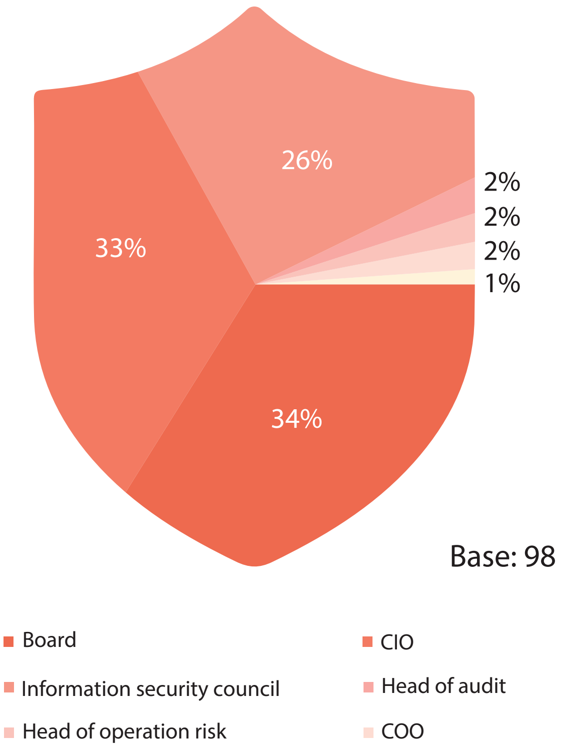
Figure 4. Key participants in the cybersecurity journey



As expected, the board contributes the most in defining the cybersecurity strategy (46%), while business leaders engage most during the evaluation of solutions (58%). IT leaders are active throughout the process.

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 that it remains aligned with the business strategy.

Figure 5. CISO reporting hierarchy



Where does the CISO organization report in to (%)	Overall	High-Tech	U.S.	Europe	ANZ
Base	***792***	***98***	***49***	***36***	***13***
Board	32	35	33	28	62
CIO	34	33	29	42	23
Information security council	23	26	29	25	15
Head of audit	5	2	2	3	-
Head of operation risk	3	2	2	3	-
COO	3	2	4	-	-
Others	1	1	2	-	-

Survey findings show that the numbers of CISOs reporting to the board (35%) and the chief information officer (33%) are almost equal. A large number of respondents from Australia and New

Zealand (62%) said that their CISOs report to the board. In contrast, only 28% of European respondents use that reporting structure.

High-tech firms must consider increasing the influence of the CISO so that cybersecurity is woven into an organization's digital journey.

"The CIO is not the best person to manage cybersecurity because it now encompasses enterprise risk management and corporate governance. The public nature of security breaches necessitates interactions with both legal and privacy officers who are not technology savvy." - leader, risk analytics platform provider in the U.S.

The most pressing cyberthreats

Rising threats and cyberattacks have made the high-tech industry anxious about hackers and hacktivists (86%), low security awareness among employees (78%) and insider threats (75%).

Sensitive information in the form of IP and customer and financial data attract criminal hackers looking to profit. Also, intense competition can lead employees to steal valuable data and sell it to rivals.

Figure 6. Top cybersecurity concerns

What is your number one concern regarding threats(%)	Overall	High-Tech	U.S.	Europe	ANZ
Base	***867***	***106***	***55***	***38***	***13***
Hackers/hacktivists	84	86	89	82	85
Low awareness on potential risks of security incidents among	76	78	82	71	85
Insider threats	75	75	76	75	69
Corporate espionage	75	74	76	63	69
Organized crime	67	67	58	79	69
Nation-states	60	58	53	61	69
Uneven deployment of cybersecurity solution	60	58	58	61	46

U.S. respondents express more concern about these top three issues than respondents in other regions. Respondents from Australia and New Zealand are the most apprehensive about low security awareness among employees (85%) and are least concerned about insider threats (69%).

It's clear that companies must invest heavily to address the multiple cyberthreats facing their business interests.

"Organizations are finding it extremely challenging to identify real cyber threats. While technology seems to be all-pervasive when dealing with cybersecurity, it is important not to forget that cybersecurity begins in the real world with processes and people" - *CEO, information technology and satellite communication organization in the U.K.*

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

To counter threats and attacks, high-tech enterprises most frequently turn to risk and compliance (66%), encryption (65%), and identity and access management solutions (62%).

Regulatory frameworks, such as Europe's General Data Protection Regulation (GDPR), and customer concerns about privacy and data usage, compel high-tech firms to implement risk and compliance solutions. Failure to comply with regulations can lead to massive penalties and loss of reputation and customer trust.

In data-rich enterprises, encryption is an imperative since it provides a high level of protection and mitigates risks effectively. Identity and access management solutions are also key parts of a cybersecurity portfolio that can allay fears about corporate espionage and insider threats.

Figure 7. cybersecurity solutions

Top solutions implemented (%)	Overall	High-Tech	U.S.	Europe	ANZ
Risk and compliance	66	66	65	70	54
Encryption	64	65	69	57	69
Identity and access management	63	62	71	54	46
Security incident management	66	61	67	51	62
Intrusion prevention systems	63	60	62	59	54
Security awareness training	66	58	69	49	38
Unified threat management	58	56	57	51	62
Cloud access security broker	64	55	59	46	23
Tackling IoT security	60	55	56	50	62
Application control on server workloads	58	51	58	39	54

Challenges galore

The top three problems that enterprises face are building a security-first culture (65%), embedding security in the enterprise IT architecture (63%) and lack of user awareness (62%).

Figure 8. Top cybersecurity challenges

Challenges that you face while implementing cybersecurity (%)	Overall	High-Tech	U.S.	Europe	ANZ
Base	***867***	***106***	***55***	***38***	***13***
Building a cybersecurity aware culture	65	65	62	68	69
To ensure enterprise IT architecture has security embedded in it	67	63	65	55	77
Lack of user awareness	54	62	56	71	62
Too much time spent in building technology stack and less on deriving value	57	58	62	63	31
Cybersecurity technology changing too fast	63	58	60	53	69
Inadequate management support	52	56	55	61	46
Lack of skilled personnel	49	51	49	53	54
Lack of appropriate tools to automate controls and audit effectiveness	55	51	44	55	69
Poor integration between tools and different solutions	54	45	38	53	54
Lack of reporting on incidents	39	42	40	47	38

Safeguarding against damage caused by unmindful employees, as well as those with malicious intent, should be a top priority. Insider threats can pose a high risk since employees have easier access to confidential information. However, building a cybersecurity aware culture is not easy because it involves changing mindsets and processes. In many cases, employees may not be sufficiently informed of the security threats their devices and practices can pose.

It's no longer enough to protect the perimeter. cybersecurity 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.

Australia and New Zealand grapple most with challenges related to building a cybersecurity aware culture (69%) and embedding security in the IT architecture (77%). European firms struggle most with lack of user awareness (71%).

Overcoming the challenges using multiple methods

The high-tech industry must deal with the fact that simple perimeter defenses are no longer adequate to secure the enterprise. They must instead take an enterprise-wide approach that begins at the design stage, progresses through growth, and focuses on future conditions as well.

High-tech firms focus on training and certifications (65%), workshops and enablement sessions (55%), integrated solutions over point solutions (46%), and working with technology solution providers (46%) to overcome the challenges.

Figure 9. Cybersecurity approaches

Cybersecurity approaches	(%)	U.S.	Europe	ANZ
		55	***38***	***13***
Training and certifications	65	75	53	62
Workshops and enablement sessions	55	65	50	23
Focus on integrated security solutions rather than point sol	46	45	45	54
Work with technology vendors and service integrators	46	55	34	46
Creating a culture of employee awareness	43	47	42	31
Hire service provider specializing in security solutions	40	47	34	23
Outsource security Cyber Security monitoring and management	27	33	24	15
Enable threat intelligence feeds	15	22	11	-

Base: 106

Examining the survey responses, we see that enterprises are adopting cybersecurity 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.

Compared to the other regions surveyed, more U.S. respondents confirmed that they have employed these methods to address their security challenges. Europe is behind in all areas, while Australia and New Zealand have lesser use of workshops and enablement sessions (23%).

Focus areas – next moves

High-tech firms are set to evolve to the next stage of cyber defense as they focus on more progressive technologies to safeguard the enterprise. The top three areas are network segregation, advanced threat protection, and threat intelligence platform.

Network segregation can provide better security to sensitive data by restricting access between network segments and limiting impact of incidents and slowing down attacks. Advanced threat protection solutions help guard sensitive data by providing real-time visibility and contextual alerts, thereby detecting trouble early and enabling swift responses. Threat intelligence platforms signal the intent to counter advanced attacks since they can predict and identify danger in advance and prevent damage even before it occurs

Figure 10. Next stages of cybersecurity

Next stages of cybersecurity (%)	Implemented				
	Overall	High-Tech	U.S.	Europe	ANZ
Network segregation	65	66	75	55	62
Advanced threat protection	55	64	67	55	77
Threat intelligence platform	57	61	65	51	69
Deception technologies	49	54	51	53	69
DevSecOps	46	48	46	46	62
User and entity behavior analytics	48	47	47	37	77
Security orchestration and automation response	46	47	49	39	62
Cloud access security broker	44	40	40	37	46

Next stages of cybersecurity (%)	Implementing				
	Overall	High-Tech	U.S.	Europe	ANZ
Network segregation	25	24	20	26	31
Advanced threat protection	31	20	20	21	15
Threat intelligence platform	27	23	22	27	15
Deception technologies	36	31	33	34	15
DevSecOps	34	28	28	32	15
User and entity behavior analytics	29	28	27	34	15
Security orchestration and automation response	34	27	22	37	23
Cloud access security broker	30	27	29	24	31

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

Cybersecurity trends	(%)	U.S.	Europe	ANZ
		55	*38*	*13*
Privacy and personal data protection gains significance	44%	38	47	62
Artificial intelligence used for real time predictive/ preventive instances	43%	47	45	23
Usage of blockchain technologies in developing security solutions	38%	33	47	31
Deception technologies introduced in IoT and OT (operation technology)	35%	38	29	38
Continued demand for cybersecurity skills	35%	38	32	31
Importance of behavioral analytics in identity management	25%	25	24	31
Introduction of automation in implementing cybersecurity	25%	25	32	-
Regulatory bodies show zero tolerance towards non-compliance	22%	22	16	38
Emergence of new business models including cyber insurance	22%	20	24	23
Cybersecurity startups to gain recognition	14%	16	11	15
Move from standard to customized security solutions	13%	15	16	-

Respondents said that privacy and personal data protection (44%), artificial intelligence (43%) and blockchain technologies (38%) will influence the future direction of cybersecurity in their enterprises.

The digital revolution has unleashed vast amounts of data, giving rise to concerns about privacy and protection. Consequently, regulations such as GDPR have come into play, and more are likely to follow.

AI can help enterprises proactively and accurately identify threats and trigger action to prevent damage. Besides, it can enable the handling of massive volumes of data faster and better.

Blockchain's inherently secure nature and distributed ledger technology make it one of the most viable options to boost cybersecurity programs.

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

The high-tech industry is undergoing a tectonic shift as it relies on digital transformation to deliver integrated and fulfilling experiences to demanding customers. In the process, there are massive changes to business and operating models and the value chain.

In this scenario, cybersecurity 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 that 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 support from the senior leadership, education of employees and inculcating a security-first mindset. Without a strong cybersecurity, enterprises are exposed to risks such as financial losses, damage to reputation, loss of customer trust and in extreme cases, failure to survive in the market.

On the other hand, an effective cybersecurity program can enable high-tech firms to pursue their digital plans and benefit from the transformational gains it promises. 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