Infosys®
Navigate your next

ASSURING DIGITAL-TRUST

Infosys® | Knowledge Institute

TABLE OF CONTENTS

From the CISO's desk 4

Introduction 5

Cybersecurity survey methodology 6

Executive summary 7

Diving into cybersecurity 9

- Enterprises acknowledge the role of cybersecurity in digital transformation 10
- Developing an enterprisewide cybersecurity strategy 12
- Higher board visibility increases the cybersecurity program's success rate 13
- The cyberthreats enterprises are most concerned about 15

The enterprise imperatives 17

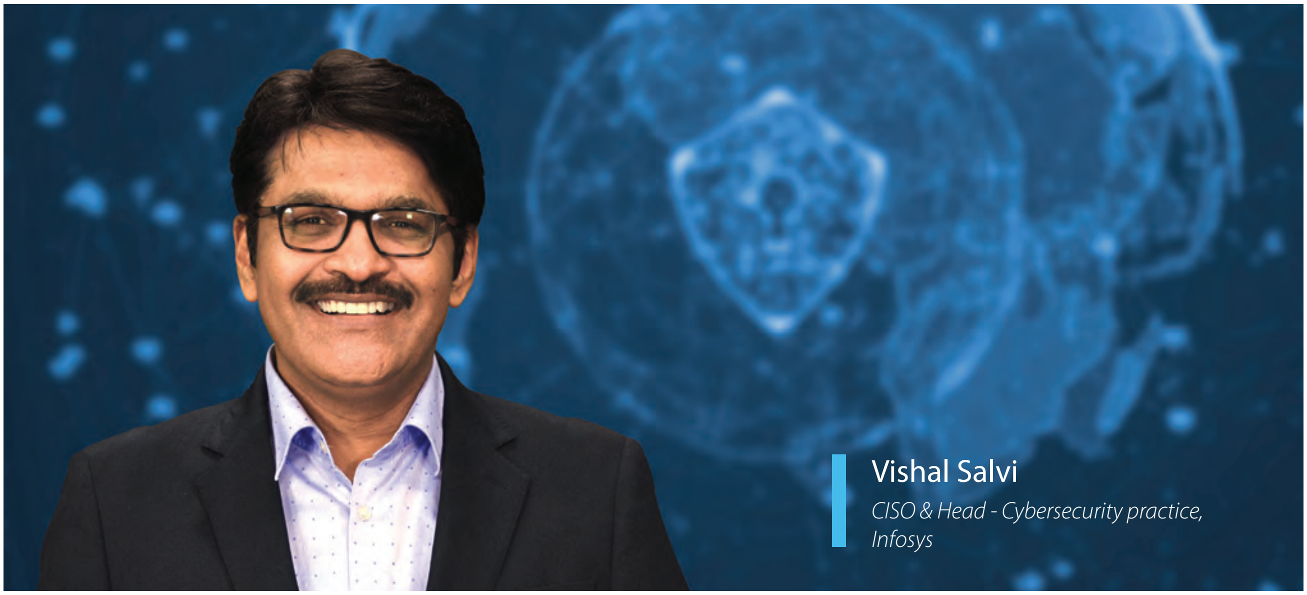
- Top security solutions implemented today 19
- Challenges galore 22
- Overcoming the challenges using multiple methods 24
- Focus areas – next moves 27

Shaping cybersecurity of the future with new technologies 29

External service providers play a valuable role 31

The Infosys perspective – scale with assurance 33

The way forward to instill digital trust – navigating to a secure future 34



Vishal Salvi

CISO & Head - Cybersecurity practice, Infosys

FROM THE CISO'S DESK

When I started my journey into the world of IT security (yes, that's what it was called) right after Y2K, it was hardly considered a career option, and you can say it was pure coincidence. So much has changed ever since — IT security became information security and is now known as cybersecurity .

With organizations adopting digital in a fundamental way, cybersecurity has become a foundational requirement, which is also evident from the findings of the Digital Radar survey. Every leader has rated cybersecurity as the number one priority. For widespread adoption of digital, cybersecurity becomes imperative. In its absence, organizations will be exposed and struggle to instill confidence and gain the trust of stakeholders.

However, embedding cybersecurity has remained a difficult problem to solve for a long time. Billions of dollars are being spent on building controls, but rate of attacks and breaches have only increased over time. As organizations adopt advanced technologies, modernize technology assets and become more connected, vulnerabilities in the systems are increasing. So are the incentives for bad actors to exploit these vulnerabilities.

At Infosys, our mission is to enable our customers to securely navigate their next and help them by assuring digital trust — build security by design, manage scale and protect them from future threats. Therefore, we are constantly investing in modern, cutting-edge security offerings and solutions, and building competent teams to deliver that promise.

When we undertook this survey, we aimed to provide insights which will help shape your thinking on the cybersecurity journey. I hope you find this report interesting and insightful as much as we enjoyed creating it for you.

INTRODUCTION

In today's hyperconnected and digitized world, cybersecurity has become an important strategic imperative owing to the sophistication of cybercrime. Digital businesses require complex and distributed interactions among people, applications and data — on-premise, off-premise, on mobile devices and in the cloud. The result is an increase in the attack surfaces that are hard to protect and defend. As the perimeter continues to diminish, visibility into the environment gets tougher. Operational Technology (OT) and the Internet of Things (IoT) massively expand the scope of security strategy and operations. When a massively distributed fleet of autonomous devices that can make decisions is combined, directly affecting the physical state of people and things, there is a considerable risk to manage. This issue is not limited to the chief information security officer (CISO) but needs the involvement and sponsorship of the leadership and the board.

The absence of a well-defined cybersecurity program can cause substantial damage to an enterprise's operations, reputation and financial condition, and threaten its very existence. Despite an organization having the best tools for detection and prevention, eventually, a motivated attacker will find a way into the enterprise network, either via social engineering techniques and/or a zero-day exploit, for which there is no signature available for detection. Therefore, the spotlight on cybersecurity today is clearly justified.

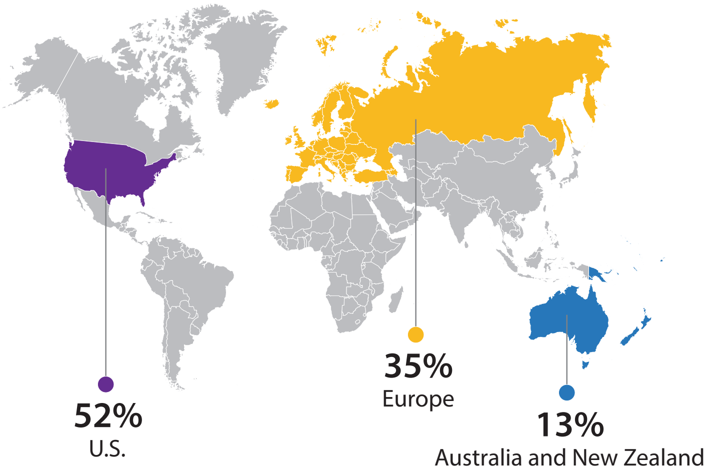
CYBERSECURITY SURVEY METHODOLOGY

The importance of combating cyberattacks is growing. Many CIOs and CISOs are making cybersecurity an integral part of their digital transformation journey. To understand the solutions that they implement and their future plans for cybersecurity, Infosys conducted an independent study. The report of which presents a holistic view of the cybersecurity landscape.

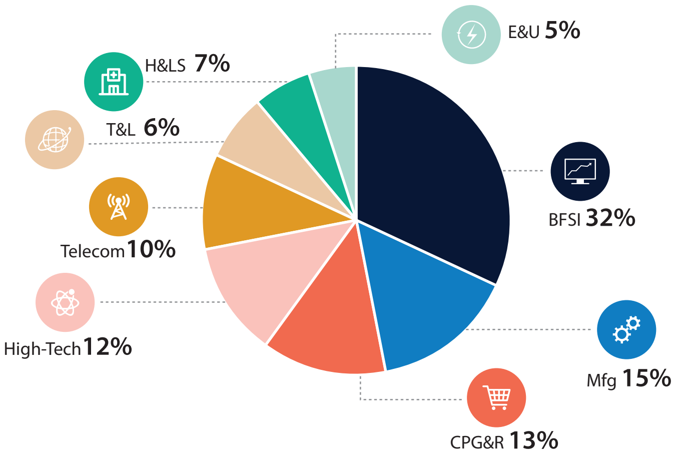
The main objective of this report is to explain the current global cybersecurity landscape and how organizations have geared up to take on the cyberthreat challenge. It considers inputs from a variety of sources:

1. A survey of 867 executives representing firms from 12 industries with annual revenues over $500 million across the United States, Europe, Australia and New Zealand. Over 60% of the responses were from leaders of companies with annual revenues of more than $1 billion. Respondents represented multiple industries that were grouped into eight industry clusters.
2. Insightful conversations with customers.
3. Practitioners' perspectives from Infosys subject matter experts.

Figure 1. Respondent geographies



Industries represented



E&U: Energy and Utilities

H&LS: Health Care and Life Sciences

Mfg: Manufacturing

Telecom: Telecommunications

BFSI: Banking, Financial Services and Insurance

CPG&R: Consumer Packaged Goods and Retail

T&L: Transportation and Logistics

EXECUTIVE SUMMARY

The need for a robust and pervasive cybersecurity program is established as businesses become increasingly connected and consequently expand the attack surface during their digital transformation journey.

Given this, cybersecurity is no longer restricted to the perimeter of an enterprise. Instead it should be an essential part of every transaction across stakeholders, inside and outside the organization.

With cybersecurity being central to digital transformation, are all enterprises treating it with the importance it deserves? Does it get attention from the highest levels in the company? What are enterprises concerned and challenged with, and how are they tackling them? Do enterprises have an eye on the future, and what are their plans? Answers to these questions can help enterprises review and benchmark the maturity of their cybersecurity program with global and industry peers.

The three biggest takeaways gleaned from the Infosys study are:

1. Cybersecurity is in the spotlight across enterprises

A significant 83% of respondents view cybersecurity as critical to their organization. Further, 66% had implemented a well-defined enterprisewide strategy reiterating the priority it is accorded. Only 4% of the surveyed firms were still working on their enterprisewide strategy, and hence, their implementation was ad hoc.

2. Cybersecurity starts at the top

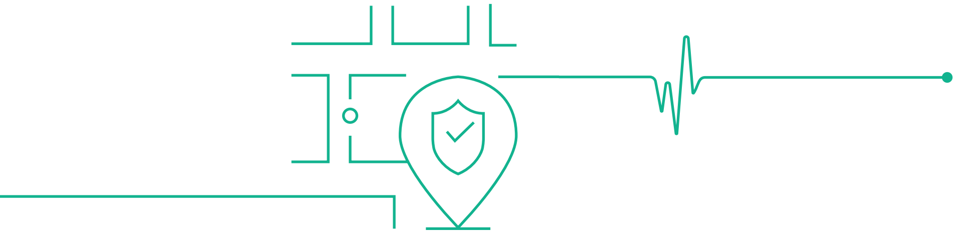
Cybersecurity is an enterprisewide responsibility with engagement required from the topmost levels. The survey shows that 48% of the board and 63% of business leaders are involved actively in cybersecurity strategy discussions. Their involvement is essential to ensure that the cybersecurity program is aligned with business objectives and to convey a powerful message across the organization.

3. A few concerns and challenges impede cybersecurity programs

Respondents indicated that hackers (84%), low awareness among employees (76%), insider threats (75%) and corporate espionage (75%) are the top concerns. To keep these threats at bay, enterprises deploy solutions such as security incident management (66%), risk and compliance (66%) and security awareness training (66%) the most. However, embedding security in the enterprise IT architecture (67%), shortage of skills (49%) and keeping pace with rapidly changing technologies (63%) pose challenges while designing a cybersecurity program.

While enterprises have devised some methods to overcome these challenges, considerable efforts are needed to make it more effective. Today, it implies having an enterprisewide security mindset right from the design stage and at every stage of the business lifecycle to augment visibility and reduce risk. It means having security integral to the scaling efforts to optimize costs and enhance reach as well as identify next-generation solutions and technologies to secure the future.

An organization must put its entire strength behind cybersecurity programs as it enables digital transformation by delivering an effective counterpunch to the myriad threats that bombard it anywhere, anytime.



DIVING INTO CYBERSECURITY

The year 2019 saw the occurrence of significant security breaches unleashing massive damage on the affected firms. The compromised information included social security numbers, credit card numbers, addresses, health information, usernames and emails, to name just a few. The methods that malicious actors use to obtain information vary. But the most common ones are phishing attacks, insider threats and hacking due to employee negligence. The damages from cyberattacks are not limited to financial losses. In a breach, a company also risks losing its reputation. In some cases, stiff penalties owing to noncompliance with regulatory requirements can cause severe disruption to the business.

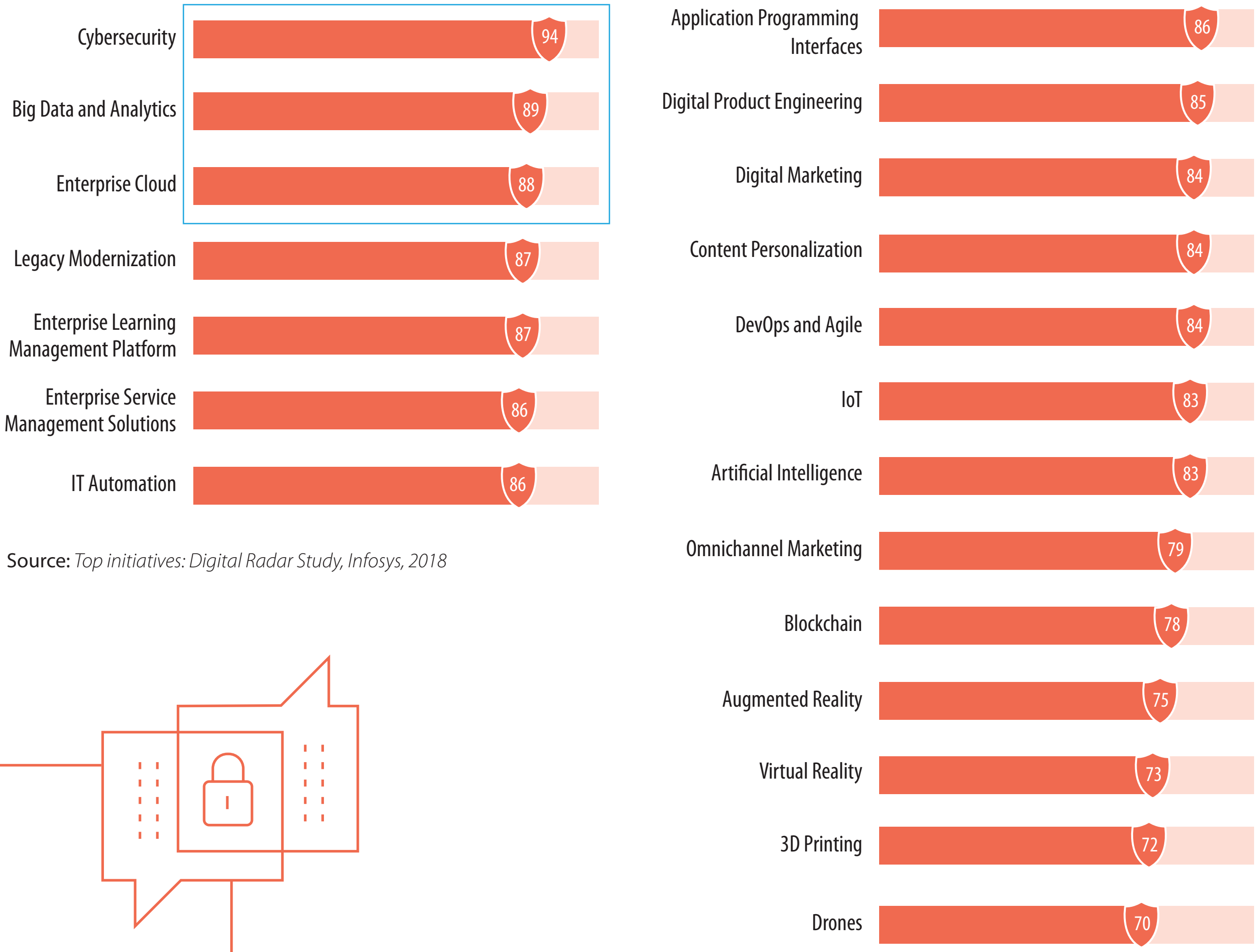
The need of the hour is to implement a well-defined, evolving cybersecurity strategy to maintain constant vigil and protect applications, data, networks and systems from the ever-changing cyberthreat landscape.

Enterprises acknowledge the role of cybersecurity in digital transformation

In 2018, Infosys surveyed 1,000 large enterprises to understand their digital transformation initiatives. The study revealed that many respondents experienced digital disruption. Figure 2 demonstrates that for 94% of the firms, cybersecurity is the top initiative in their digital transformation journey.

Figure 2. List of initiatives

Base - 1014

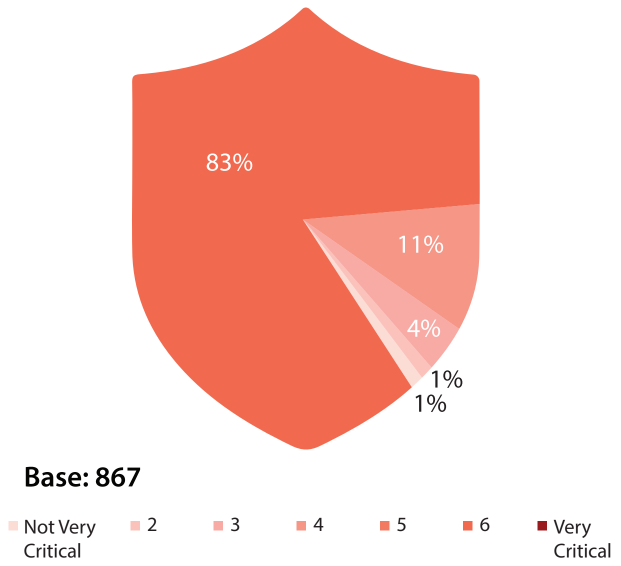


Source: *Top initiatives: Digital Radar Study, Infosys, 2018*

The 2019 Infosys cybersecurity study found that the respondents from the manufacturing (87%), the energy and utilities (85%) and the banking, financial services and insurance (83%) industries view cybersecurity as highly critical in their industries. (See Figure 3.) The companies in these industries are among the most attractive targets for cybercriminals due to the nature of their businesses, which demands a high degree of connectivity and sharing of information, thereby exposing more surface area to cyberattacks.

The need to prevent or reduce the impact of these attacks, so that companies can continue to realize value from digital transformation, has encouraged them to prioritize cybersecurity. It is evident that cybersecurity has now become mainstream and fundamental for the future of business. With boards now being held accountable for ensuring proper management of cybersecurity risks, it's no longer the issue of getting budgets, but the challenge has shifted to execution.

Figure 3. 83% of the respondents believe cybersecurity is viewed as highly critical in their organizations



Criticality	Overall	BFSI	Mfg	CPG&R	Hi-Tech	Telecom	H&LS	T&L	E&U
Base	***867***	***274***	***130***	***113***	***106***	***90***	***61***	***53***	***40***
High Criticality (%)	83	83	87	81	82	80	79	79	85
Low Criticality (%)	1	1	-	1	1	-	-	4	-

BFSI: Banking, Financial Services and Insurance | **Mfg:** Manufacturing | **CPG&R:** Consumer Packaged Goods and Retail | **Hi-Tech:** High-tech | **Telecom:** Telecommunications | **H&LS:** Health Care and Life Sciences | **T&L:** Transportation and Logistics | **E&U:** Energy and Utilities

Kumar MSSR,

Global Head -
Delivery and Operations,
Cybersecurity, Infosys

Expert View:
Significance and criticality of cybersecurity

Organizations are embarking on the digital transformation journey to expand their horizon, bring speed and agility in business processes and improve customer experience. During this journey, huge amounts of data are processed and transferred across enterprise boundaries. Interconnected devices, blockchains, IoT, artificial intelligence (AI), cloud-based services etc. make the ecosystem multifaceted, thus resulting in numerous challenges with respect to cybersecurity. Country-specific regulations add complexity to this transformation. Digital enterprises, thus, have an enhanced threat landscape and sophisticated threat actors to deal with. It is not a surprise that 94% of the survey respondents, across industries, listed cybersecurity as the top initiative in their digital transformation journey with a large number emphasizing its criticality.

Developing an enterprisewide cybersecurity strategy

Digital technologies are making boundaries disappear, not only within the enterprise, but also across organizations. At the same time, the sophistication, complexities and reach of cyberattacks are on the rise. These factors will encourage mature firms to choose an enterprisewide approach strategically aligned to business goals to ensure all angles of cyber defense are covered.

The good news, according to our study, is that all respondents recognize cybersecurity as an integral part of their business and acknowledge the necessity for an enterprisewide strategy. However, these enterprises are at varying levels of maturity in their implementation of cybersecurity programs.

Kishore Susarla
Delivery Manager, Cybersecurity, Infosys

Expert View:
Steps to follow while implementing a cybersecurity strategy

1. Align the cybersecurity goals to the business objectives of the organization.
2. Build a comprehensive short-term and long-term cybersecurity program.
3. Constant measurement and recalibration of the cybersecurity controls.
4. Deciding on the prioritization for implementation of the controls.

Figure 4. Most respondents have a well-defined enterprisewide strategy with an existing or already implemented road map

(%)	Overall	BFSI	Mfg	CPG&R	Hi-Tech	Telecom	H&LS	T&L	E&U
Base	***867***	***274***	***130***	***113***	***106***	***90***	***61***	***53***	***40***
Well defined enterprisewide strategy/roadmap exists, implemented	66	69	59	65	70	72	61	55	65
Enterprisewide strategy/ roadmap exists as a guideline, but implementation in progress	30	27	36	33	25	23	38	42	30
Enterprisewide strategy/roadmap is work in progress and therefore, implementations and operations are ad hoc	4	4	5	2	5	4	2	4	5
No defined framework or program	0	0	-	1	-	-	-	-	

BFSI: Banking, Financial Services and Insurance | **Mfg:** Manufacturing | **CPG&R:** Consumer Packaged Goods and Retai | **Hi-Tech:** High-tech industry | **Telecom:** Telecommunications | **H&LS:** Health Care and Life Sciences | **T&L:** Transportation and Logistics | **E&U:** Energy and Utilities

The communications and telecom industry had the most respondents (72%), while the transportation and logistics industry had the fewest respondents (55%). This is no surprise due to the heightened exposure these industries face in addition to the regulatory requirements.

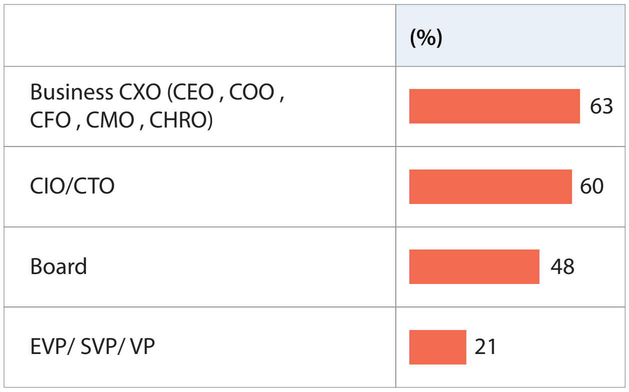
Higher board visibility increases the cybersecurity program's success rate

Support and sponsorship from the board and senior management are critical for an effective cybersecurity program. If traditionally the board's focus has been on setting the strategic direction of the company, today's dynamic business environment makes it essential for the board to be involved in a deeper cybersecurity discussion. Cybercrime can cost a business great amounts of money. But the risks are not only financial — they can completely destroy a business. To be aware of their companies' specific risks, board members need to be constantly updated on the current challenges, impending scenarios and remedial processes undertaken for securing their organization.

In many organizations, cybersecurity issues are handled entirely by in-house cybersecurity professionals. These expectations are changing as more privacy-focused issues appear. Hence, having the CIO or CISO solely responsible for the program without any involvement from the board and senior leaders is unlikely to produce the desired results.

The survey revealed that 48% of the board and 63% of business leaders are involved in the cybersecurity strategy discussions.

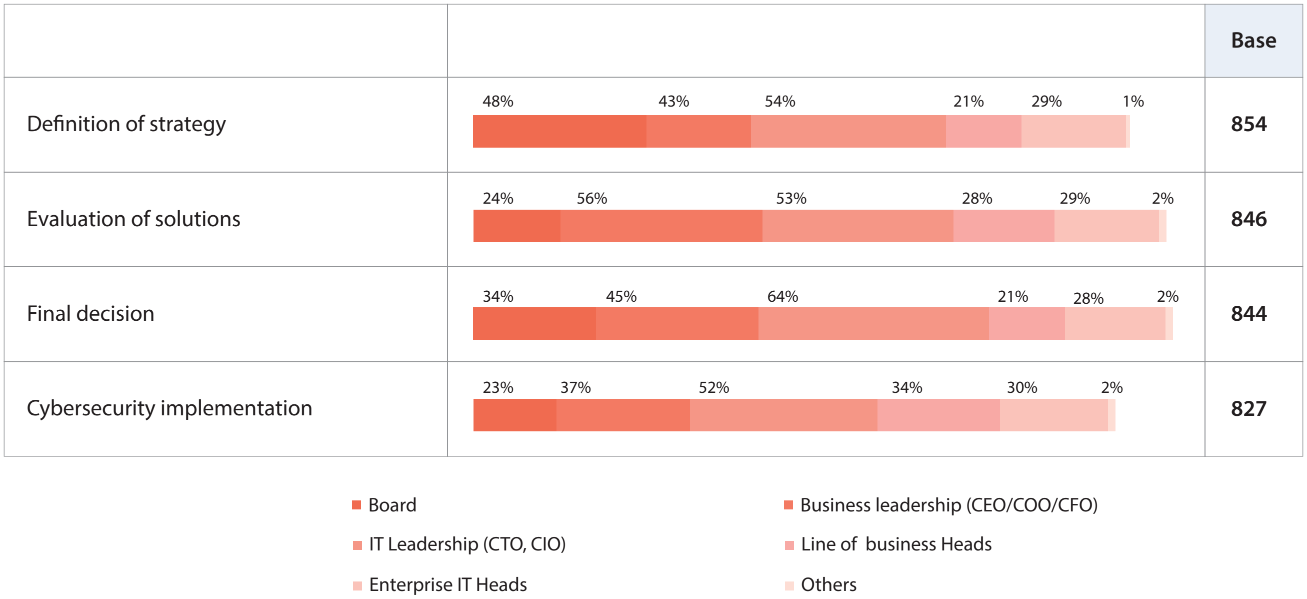
Figure 5. Almost 50% of the boards are involved in the cybersecurity strategy



Base: 867

The survey further showed that the board ensures the formulation of the cybersecurity strategy in 48% of the enterprises and aids with the final decision-making in 34%. Figure 6 shows that besides the board, business leaders stay engaged during the strategy formulation (43%), evaluation of solutions (56%) and final decision-making (45%) stages. When the senior leadership actively participates in cybersecurity initiatives, it sends a strong signal across the company and significantly improves the program's chances of success. The higher involvement of the board is definitely a positive sign and will help to further the cause of embedding cybersecurity into the organization's fabric.

Figure 6. 48% of boards are involved in the strategy definition and 34% in the final decision



Apart from the need to have active senior leadership involvement, a firm's CISO plays a crucial role in ensuring an effective cybersecurity program. The CISO's primary responsibility is to ensure that the direction of the company's cybersecurity initiatives stays aligned with its business priorities. To develop effective security controls, the CISO must understand the business context. Therefore, a modern day CISO must possess technical and domain expertise and also be business-savvy.

Figure 7 demonstrates that the percentage of CISOs reporting to the board (32%) is almost the same as those reporting to the CIO (34%). CISOs must maximize their access to the board and senior leaders to effectively posture the cybersecurity approach and gain the required resources to strengthen the defenses.

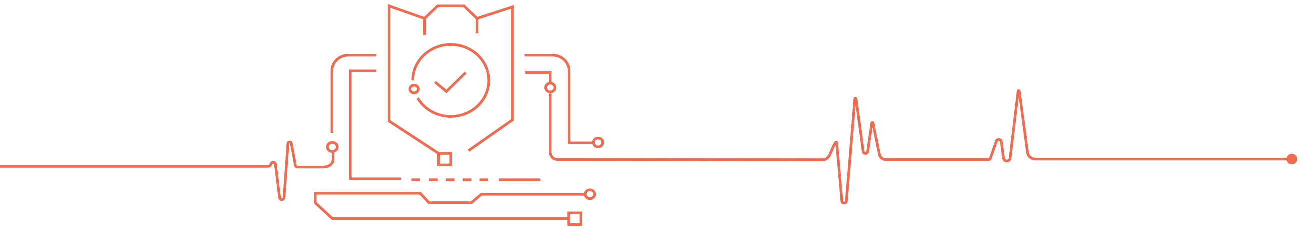
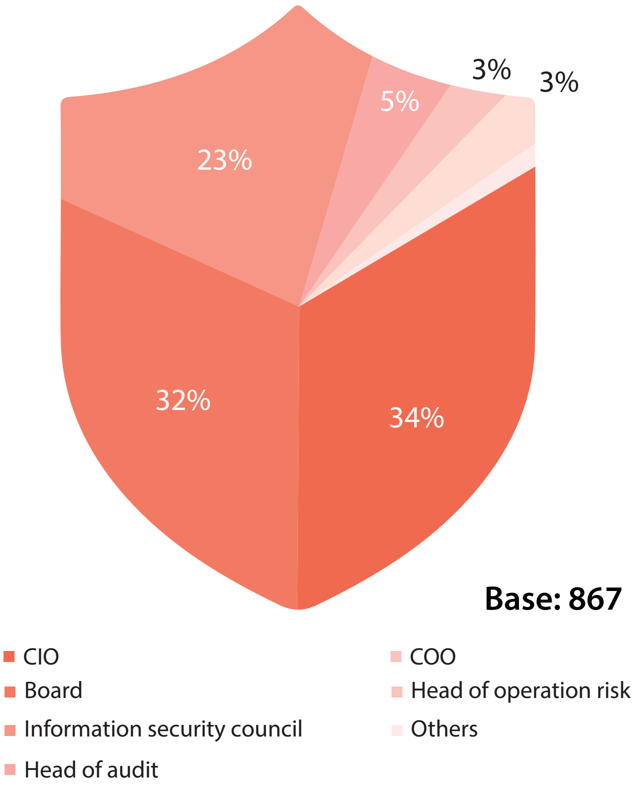


Figure 7. To whom does the CISO report?



To whom does the CISO report? (%)	Overall
Base	***792***
CIO	34
board	32
Information security council	23
Head of audit	5
COO	3
Head of operation risk	3

The cyberthreats enterprises are most concerned about

The existing cyber defense measures may trick enterprises into thinking that the myriad cyberthreats are under control. However, as attacks get more advanced, deceptive, and dangerous, businesses need to be always on their guard to protect themselves. Further exacerbating the situation are internal impediments such as unintended breaches, weak processes and under-equipped technology infrastructure.

Figure 8 shows that hackers (84%), low awareness among employees about security risks (76%) and corporate espionage (75%) are top concerns for the respondents. Today, the motivations of the malicious actors extend beyond profit-making. Hacktivists can be motivated by political, economic or social causes ranging from fighting for human rights to awakening a business to its vulnerabilities. We have also seen an increase in state-sponsored actors who interfere with computer systems to send a political message. Such attacks can compromise the business operations considerably, not to mention the costs incurred in the form of lost revenues, a blot on the company's reputation, financial penalties and increased regulation. Therefore, prioritizing and acting on these concerns is necessary to remain relevant in today's business environment.

Figure 8. Top cybersecurity concerns

	(%)
Hackers/hacktivists	84
Low awareness of potential security risks among employees	76
Corporate espionage	75
Insider threats	75
Organized crime	67
Nation-states	60
Uneven deployment of cybersecurity solution	60

Base: 867

The manufacturing (82%), consumer goods and retail (81%), and communications and telecom (80%) industries were significantly more apprehensive about corporate espionage. The three sectors operate in a hypercompetitive environment with ever-increasing pressure on business performance. Consequently, they are more susceptible to corporate espionage, which can be used to gain a foothold over the competition.

In addition to deliberate sabotage attempts, unaware employees can cause significant damage. By opening a suspicious attachment or visiting an unsecured website, employees can trigger major cyber incidents. Inadvertent security breaches by employees (76%) are standard in companies where a rigorous cybersecurity culture is absent.

Figure 9. Hackers and hacktivists are the top concern for companies across all geographies

(%)	U.S.	Europe	Australia and New Zealand
Hackers/hacktivists	85	82	88
Low awareness of potential risks of security incidents among employees	76	76	75
Corporate espionage	77	72	77
Insider threats	76	74	72
Organized crime	62	74	67
Nation-states	59	61	60
Uneven deployment of cybersecurity solution	62	57	57

THE ENTERPRISE IMPERATIVES

Securing your business is no longer about just securing the perimeter; it is about shifting the focus to users, devices and data. Increase in phishing, ransomware and zero-day attacks prove how easy it is to skirt traditional perimeter-based solutions. Organizations today are implementing solutions that cover risk and compliance, encryption, incident management, identity management, etc. to better address cybercrime. However, there are challenges where organizations are unable to have security embedded in their technology architecture, where they are battling with a shortage of skilled personnel, where keeping pace with technological advancements appears difficult. And the only way to address these are by embedding security in the nascent stage of the business lifecycle, building scalability and efficiency in the cybersecurity program and creating advanced solutions. This is an ongoing journey towards a secure digital future.

Umashankar Lakshmipathy

Head – Cloud, Infrastructure and Cybersecurity - Europe, Infosys

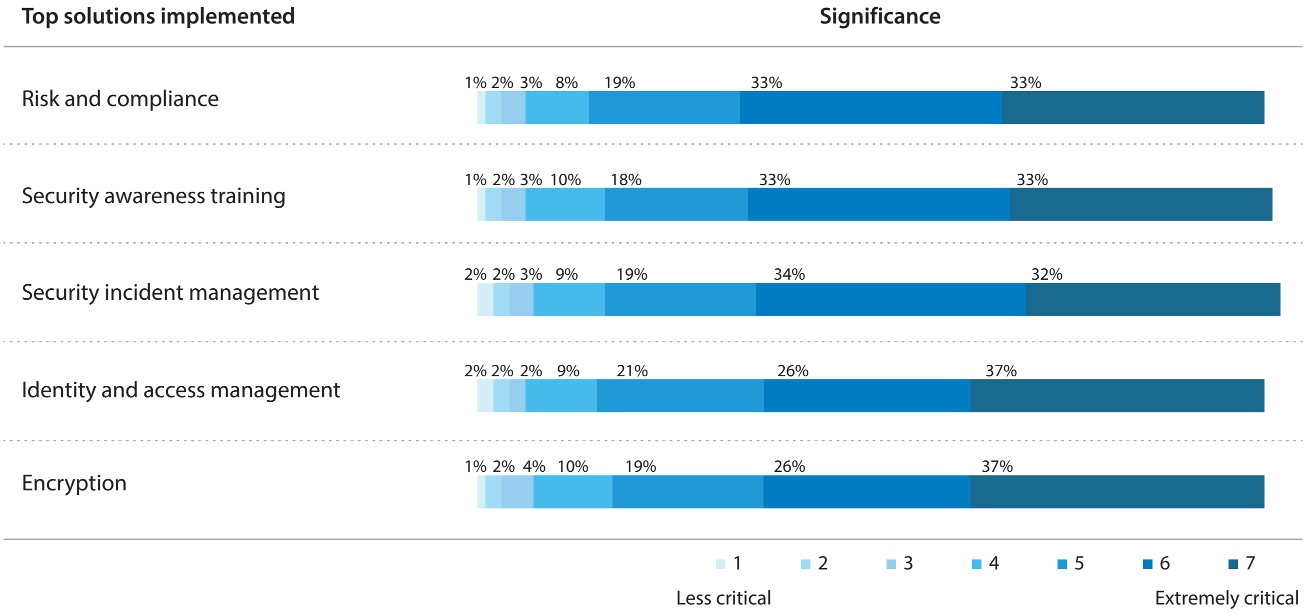
Expert View:
The need for an evolving cybersecurity strategy

Not very long ago, organizations deployed security strategies that focused on blocking and securing the perimeter by 'locking down' users, access and data. The new business environment has dissolved the perimeter. Today, users include not just employees but partners, vendors, suppliers and customers and the points of interaction are too many with data and applications residing on the cloud, on mobile devices, and even outside the network. To protect the digital enterprise, organizations must secure interactions between business-critical digital assets and protect the free-flow of information between all the stakeholders in, around and outside the enterprise and at the same time ensure speed and agility. Unfortunately, new threats are continuously emerging with ingenious malware and ransomware coming into play. Organizations are also exposed to the vulnerabilities in their IT infrastructure, both old and new. Therefore, establishing a comprehensive cyber security strategy is very critical to not only counter these threats but to also allow the new 'boundary less' businesses to exist and grow.

Top security solutions implemented today

Figure 10 shows that the five most critical components are risk and compliance (66%), security incident management (66%), security awareness training (66%), encryption (64%) and cloud access security brokers (64%). All survey respondents said their enterprise is implementing or has already implemented a suite of solutions.

Figure 10. Most common security solutions that are being implemented in organizations



While most of the solutions deployed point to standard tactics adopted by enterprises to prevent cyberattacks, risk and compliance and security awareness training are critical elements of effective cybersecurity programs.

Lakshminarayanan RS

Practice Head – Infrastructure Security, Cybersecurity, Infosys

Expert View:
Priority list of cybersecurity solutions

- Risk and compliance solutions are necessary to address the complex and changing regulatory and compliance requirements across regions and industries. Failure to comply with these requirements has harsh consequences. For instance, regulations like Europe's General Data Protection Regulation(GDPR) can levy penalties up to 4% of revenue if the organization cannot prove that it has taken adequate measures to protect customer and employee information.
- There is a mandate for reporting all incidents within 72 hours, making incident response a critical part of the security landscape.
- Encryption solves the problem of security at a fundamental level, protecting data and preventing it from being misused.

So, stringent data privacy related mandates with steep penalties and the realization that companies are vulnerable to breaches are all driving the implementation of these technologies.

Global companies must keep up with regulatory compliance requirements in all the countries in which they operate; otherwise, they risk receiving heavy penalties. An increasing focus on data privacy and regulations such, as the GDPR, the Australian Privacy Act and the California Consumer Privacy Act further add to the challenges. For this reason, risk and compliance solutions take priority.

Highly ranked in the survey, security awareness training programs help establish a cybersecurity-oriented culture across the organization. Employees can be the weakest link in an organization mainly due to lack of awareness of cyber risks and their roles in those risks. Therefore, instituting a security-first culture is an urgent and critical requirement today.

On the importance of security awareness training programs

It's crucial to establish and nurture a security-minded culture across the board, including employees, partners and even outside vendors. A company will not invest $2 million in a new CRM system only to leave out employee training. So, a company should not invest in the latest security technologies without giving stakeholders the tools necessary to maximize that investment. The most advanced firewalls and intrusion detection systems are no match for an administrative assistant who freely gives out passwords or a contractor who clicks on malware because the person didn't know what to look for. Simply put, most of the data being compromised today is because someone got duped — not because a sophisticated piece of malware thwarted defenses. Hence, convincing board members and employee training are crucial challenges.

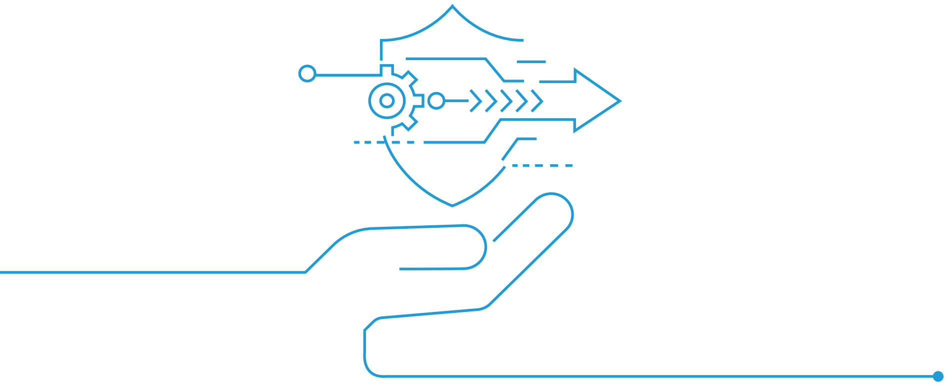
– CISO,
leading bank

The communications and telecom industry leads in the implementation of risk and compliance solutions (72%). The companies operating in this industry are custodians of confidential customer financial and personal information. Their focus primarily revolves around privacy and security, data breaches, fraud and data privacy laws.

The manufacturing and the banking, financial services and insurance have also been diligent about implementing security solutions. Manufacturers are getting more connected due to technological advances and therefore getting more exposed to cyberattacks. The solutions they have implemented, security incident management (72%), identity and access management (71%), intrusion prevention systems (71%) and IoT security (64%), highlight their efforts to contain such attacks.

The banking, financial services and insurance firms have always been under pressure to handle sensitive customer data and adhere to regulations. Consequently, they have invested in solutions such as risk and compliance, encryption, cloud access security broker, intrusion prevention systems and security incident management.

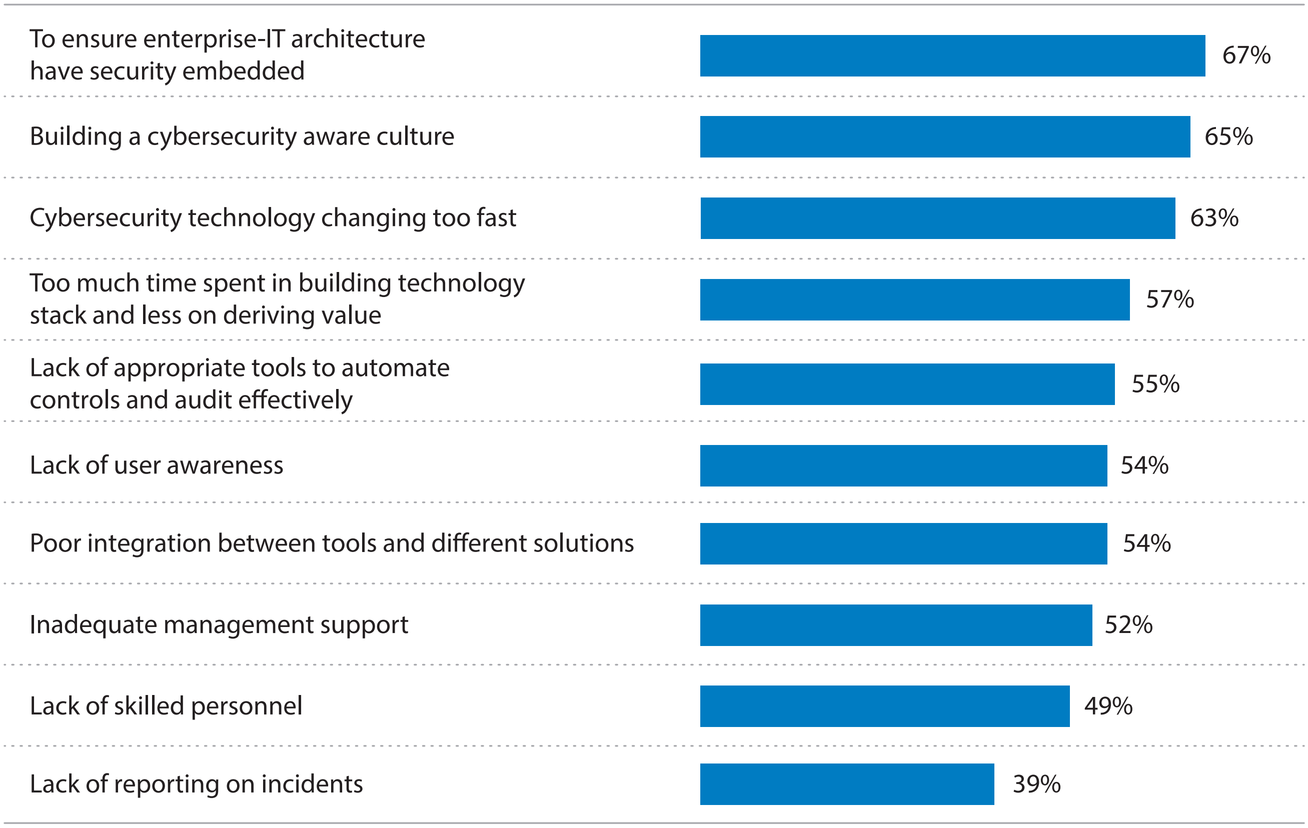
The survey results depict that organizations not only implement preventive controls but are also now making significant progress in building threat intelligence platforms and threat hunting.



Challenges galore

As can be expected, enterprises cited a few issues while navigating the cybersecurity path. The top challenges include embedding security in the enterprise IT architecture, fostering a security-first culture (65%) and keeping pace with cybersecurity technology changes (63%).

Figure 11. Top cybersecurity challenges



Base: 867

A significant number of enterprises continue to rely heavily on legacy systems. The legacy systems pose challenges to the process of embedding security in the IT architecture. This disrupts existing business operations and leads to large-scale systemic changes across the enterprise.

Any significant initiative should begin with a mindset change and educating employees. To prevent employee-triggered cybersecurity risks, enterprises must prioritize and invest more resources in developing a security-first culture.

Ajit Zanjad
Delivery Manager,
Cybersecurity, Infosys

Expert View:
Five steps to establish a security-first mindset

- Initiate a security awareness program with regular review and improvements.
- Perform a workforce survey to benchmark security programs, processes and awareness, and continuous improvement.
- Conduct social engineering simulation to review the effectiveness of a "security-aware culture" across the organization.
- Establish robust systems and processes for self-reporting security incidents.
- Initiate incentive programs to identify and report breaches in a timely manner.

Challenges also include lack of the right tools to automate controls, an integrated systems environment and a disproportionate amount of time spent on building the technology stack. These are exacerbated by insufficient know-how, lack of business orientation, and a shortage of skills. Overcoming these challenges is necessary to create an agile and resilient enterprise.

Beyond compliance: The pitfalls of a narrow approach to cybersecurity

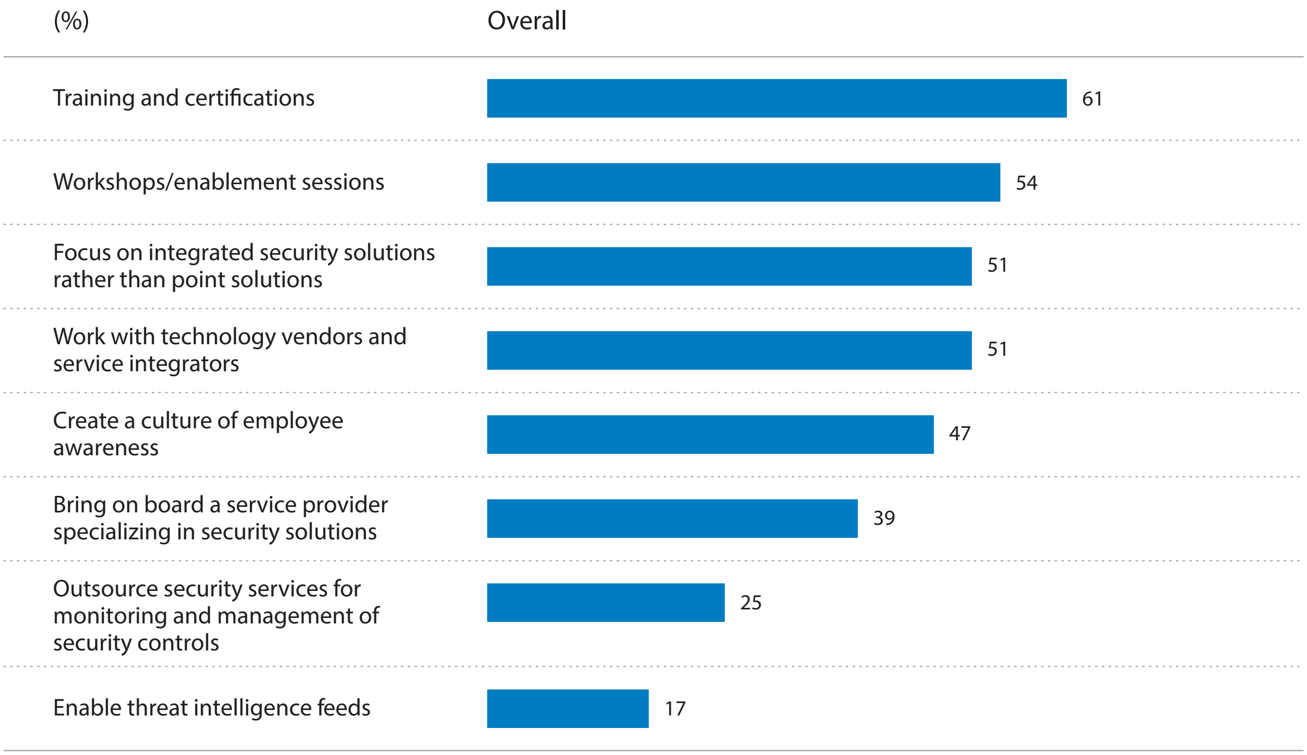
The challenge we face with cybersecurity is that what is happening now is something we've never seen before. And so, if you have only a compliance-focused approach, you will not be mindful of some of these other things that could hit your organization. For me, it's about resilience. It's about understanding better how to equip the organization to deal with a fast-moving environment, where things happen that you've never seen before. You can't possibly expect compliance to cover all those areas. CEOs need to focus on making investments that can ensure cyber resilience, rather than simply focusing on regulatory compliance. It will make sure that you are in line with what regulators or legislators understand today.

– MD,
Information Security Forum

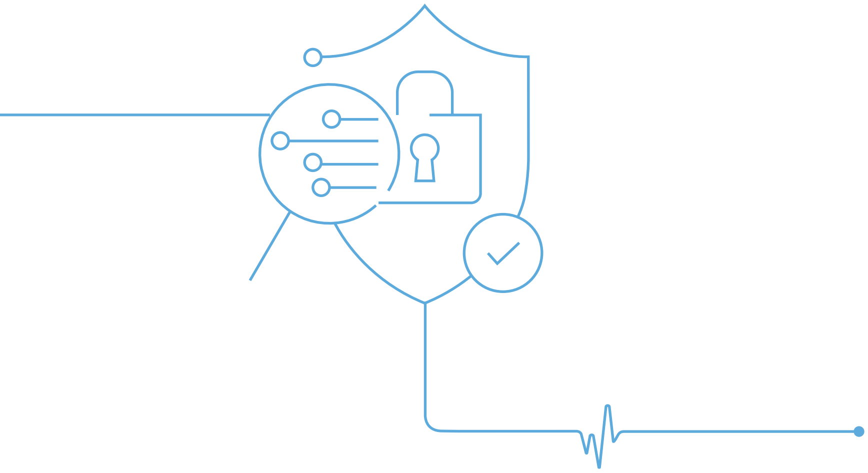
Overcoming the challenges using multiple methods

Organizations must find ways to embed security into the enterprise fabric, build scalable and efficient cybersecurity programs, and secure against the emerging threat scenario to counter the challenges.

Figure 12. Methods to overcome challenges



Respondent organizations rely on a series of "soft" measures such as workshops (54%), training and certification (61%), and spreading employee awareness (47%) to embed security into the very core of the enterprise. Awareness sessions are valuable in increasing preparedness of a company and creating a security-first culture necessary to fend off deliberate or inadvertent breaches.



Sujatha M

Practice Head – GRC, Vulnerability Management, Data Security, Cybersecurity, Infosys

Expert View:
Embedding security at the start

Organizations can embed security at the beginning and every stage of the business cycle by developing a culture of security across the organization and adopting the principles of secure by design and privacy by design. A few ways to enable these principles are:

- Using guidelines and gating – Have documented security guidelines at the enterprise level to be followed for every project and a checkpoint for validation of the security of the developed systems before they are approved for production deployment. It's also crucial to embed security into the enterprise architectures created and used within the organization.
- Ensuring secure software development life cycle – Implement this for every project, including those in the waterfall and agile execution modes. The same applies to DevOps.
- Safeguarding privacy – The increase in privacy-related regulatory mandates across geographies makes it more important to capture and manage the privacy-related aspects in every project.

To deliver expected scalability and efficiency, cybersecurity solutions must be able to seamlessly handle a larger volume of transactions, both in the cloud and on-premises. A scalable cybersecurity program involves instituting an enterprise mindset by consolidating siloed solutions (51%) and using intelligent solutions to detect and prevent incidents (17%). Integrating security solutions becomes a priority in this context.

Suhas Anandrao Desai,

Practice Head - Cloud Security and Emerging Technologies, Cybersecurity, Infosys

Expert View:
Focus on integrated solutions over point solutions

The main reason for an integrated solution is the lack of visibility of the threat landscape that escalates the cost of operations with limited intelligence sharing. Point solutions are unable to cope with changing technologies and sophisticated cybercrimes.

An integrated platform with behavior-based technologies and advanced analytics enables real-time proactive defense and predictive cyberthreat intelligence. It helps in getting a unified view of the security posture, predicting threats and responding to them appropriately, delivering risk identification and remediation. An integrated platform is a necessity to achieve security orchestration and remediation, and hence minimize the threat footprint.

Enhancing regulatory alignment is an additional, yet crucial, outcome of an integrated approach. Regulatory pressures likely compelled both the health care and life sciences (59%) and banking, Financial Services and Insurance (57%) respondents to prioritize integrated solutions.

By developing an ecosystem of competent technology vendors and service integrators (51%), enterprises are tapping into external expertise to ensure an updated and comprehensive cybersecurity program. Through a blend of spreading employee awareness and partnering with external service providers, enterprises prepare to counter emerging threats.

Figure 13. Training and certifications is the top solution for organizations in the U.S., Europe, Australia and New Zealand

Solutions to overcome challenges (%)	U.S.	Europe	Australia and New Zealand
Training and certifications	61	61	63
Workshops/enablement sessions	59	50	48
Focus on integrated security solutions rather than point solutions	52	52	46
Work with technology vendors and service integrators	50	50	53
Create a culture of employee awareness	48	45	45
Bring on board a service provider specializing in security solutions	38	41	35
Outsource security services for monitoring and management of security controls	24	23	31
Enable threat intelligence feeds	17	17	23

Pachaiyappan Varadhan

Delivery Head - North America, Cybersecurity, Infosys

Expert View:
Constantly innovating to deliver value to our customers – case in point

Infosys is providing managed security services to a large customer in North America. The client had problems managing the stability and standardized configurations of the identity and access management solution, endpoint protection and firewalls.

Infosys assessed the issues carefully and devised an approach to:

- Stabilize environments for smoother operations over the short term, reducing 80% of P1 and P2 situations.
- Consolidate all data centers and applications into a single hosted environment on Azure Cloud over the long term.

Infosys continues to innovate to add more value for the client.

Focus areas – next moves

We asked respondents about their focus areas to implement security solutions in the near term to medium term.

Figure 14. Respondents' plans in implementing security solutions

(%)	Overall	
	Implemented	Implementing
Network segregation	65	25
Threat intelligence platform	57	27
Advanced threat protection	55	31
Deception technologies	49	36
User and entity behavior analytics	48	29
DevSecOps	46	34
Security orchestration and automation response	46	34
Cloud access security broker	44	30

The top three focus areas where enterprises have implemented solutions are network segregation (65%), threat intelligence platform (57%) and advanced threat protection (55%). These areas reveal that enterprises are looking to optimize and increase efficiencies of cyber defense mechanisms and set the stage for intelligent monitoring of threats. Enterprises that have established a foundation for cyber defense by implementing foundational security solutions are now looking to cultivate them further.

The cybersecurity threat landscape is rapidly evolving as perpetrators figure out new ways to launch bigger attacks and inflict increasing damage. Use of orchestration, automation and threat intelligence platforms can counter such threats to a large extent. These trends allow quick and intelligent filtering through large volumes of information. They can identify high-potential threats to focus on, saving precious effort and time.

U.S. respondents have already implemented network segregation solutions (70%) and threat intelligence platforms (61%); more European respondents said they are in the process of implementing such solutions.

The communications and telecom industry has been at the forefront of implementing network segregation (78%) and advanced threat protection (64%) solutions. The high-tech (61%) and the consumer goods and retail (60%) industries have been progressive in implementing threat intelligence platforms.

Pulling out all stops to safeguard your enterprise

Deception technology is still at an early stage, and it would involve educating key stakeholders and overcoming myths to increase its foothold. Currently, it is used in a post-breach/incident scenario. It is most effective to build a proactive defense where technology helps to decoy, lure and defend a more evolved stage.

– VP Strategy
Cybersecurity firm

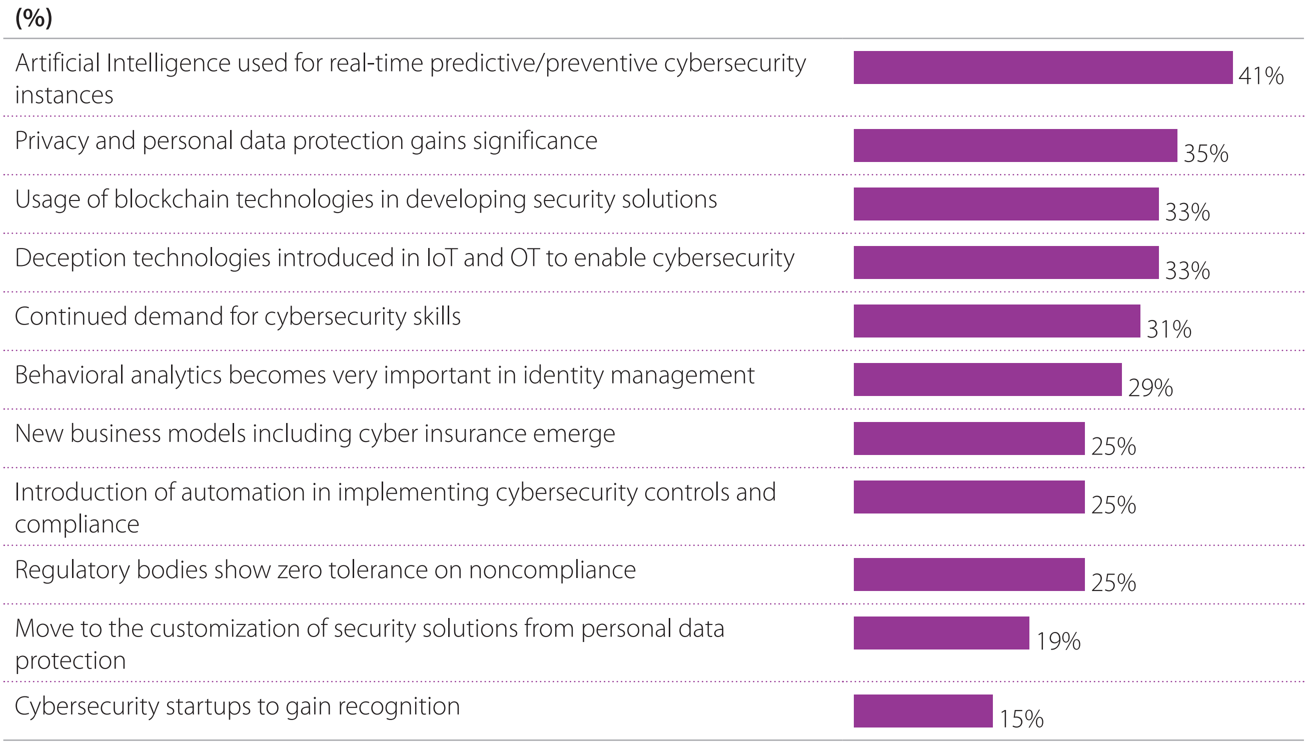
Unified threat management solutions are seeing a rise in terms of acceptance in the market. The main reasons can be attributed to the fact that malware currently use multiple paths to enter, and organizations increasingly also want a holistic view in terms of the security position which is obtained through a UTM. The downside of this is performance challenges, as it is challenging to become good at everything.

– Europe based security products firm

SHAPING CYBERSECURITY OF THE FUTURE WITH NEW TECHNOLOGIES

The goals of cyberattacks remain the same, but perpetrators are using sophisticated methods to execute the attacks. To be better prepared to handle these attacks, enterprises must be cognizant of the following trends.

Figure 15. Top 3 cybersecurity trends are artificial intelligence, blockchain and privacy and personal data protection



Artificial intelligence (41%) can play a pivotal role in helping enterprises quickly and accurately identify threats and generate action to prevent damage. Besides, they can handle massive volumes of data faster and better, allowing cybersecurity professionals to concentrate on more value-adding tasks.

The digital era has resulted in an explosion of data that is more freely available. While the surfeit of data has unlocked many benefits, it has also raised entirely justified concerns over privacy and protection (35%). In addition, regulations such as GDPR have come into play, and more are likely to follow.

The nature of blockchain technology (33%) enables it to safeguard data and prevent data breaches and cyberattacks. This technology can play a valuable role, mainly in securing edge devices.

Figure 16. Top 3 trends in cybersecurity are artificial intelligence, blockchain, and privacy and personal data protection

(%)	U.S.	Europe	Australia and New Zealand
AI used for real-time predictive/preventive cybersecurity instances	43	41	34
Privacy and personal data protection gains significance	33	38	33
Usage of blockchain technologies in developing security solutions	30	35	39
Deception technologies introduced in IoT and OT to enable cybersecurity	31	32	39
Continued demand for cybersecurity skills	32	32	27
Behavioral analytics becomes very important in identity management	28	28	33
New business models, including cyber insurance, emerge	25	25	27
Introduction of automation in implementing cybersecurity controls and compliance	25	25	26
Regulatory bodies show zero tolerance on noncompliance	26	22	28
Move to the customization of security solutions from standard	18	19	23
Cybersecurity startups gain recognition	18	14	11

EXTERNAL SERVICE PROVIDERS PLAY A VALUABLE ROLE

Survey respondents acknowledge the necessity of external partners through the security life cycle, from formulating the strategy to the maintenance of existing cybersecurity systems.

U.S. enterprises expressed the need for external help across the life cycle, whereas, enterprises from Europe, Australia and New Zealand preferred help during implementation and maintenance phases.

All respondents, except those from the energy and utilities and transportation and logistics industries, expressed a need for external partners most in the actual execution of the cybersecurity program and for maintaining and upgrading existing cybersecurity controls.

Figure 17. Key areas of partner support

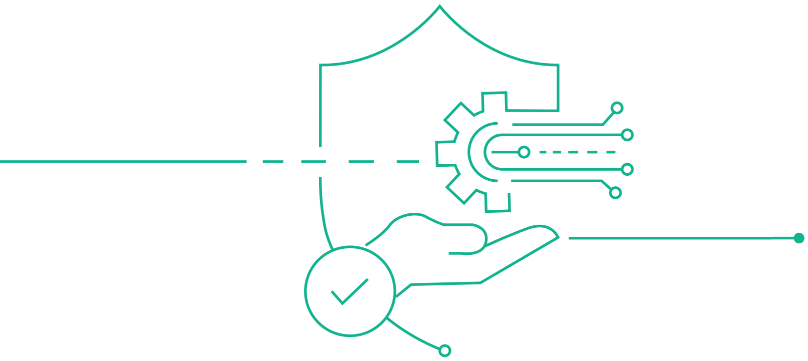
Key areas of partner support (%)	Overall	U.S.	Europe	Australia and New Zealand
Formulating strategy and advisory	59	65	54	49
Drawing execution roadmap for initiatives	61	67	55	52
Choice of technologies/tools required for the initiatives	62	69	56	53
Actual execution/implementation of the program	64	69	59	56
Maintenance and upgradation of existing cybersecurity controls	65	70	59	64

The responses revealed that enterprises expect external partners not only to help combat threats but also to help prepare for the future by providing the right security measures.

Figure 18. Key expectations from the partner

Key expectations from the partner (%)	Overall	U.S.	Europe	Australia and New Zealand
Assess, build and manage your cybersecurity capabilities and also enable you to respond to incidents and crises	69	75	60	68
End-to-end cybersecurity and protection	67	73	61	61
Helping you in your digital transformation journey by providing right security controls and measures	67	75	59	55
Ensure business resilience	66	74	59	56
Secure and grow your business confidently	65	74	56	57

The situation calls for help from a technology partner with both advisory and implementation capabilities. Not only that, the partner must exhibit a sound understanding of business and technology to generate confidence and add maximum value.



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 and solutions which are based on secure by design principles thereby making sure that security is embedded deeply and not as an afterthought. We adopt a defense-in-depth mechanism to ensure that it becomes extremely unlikely for threats to enter our clients' 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 cyberattacks. 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 modern, cutting-edge 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.

THE WAY FORWARD TO INSTILL DIGITAL TRUST – NAVIGATING TO A SECURE FUTURE

As enterprises adopt digital transformation, the significance and criticality of cybersecurity becomes crucial. Enterprises need to be able to defend and monitor their information technology assets and information systems to protect their businesses from the ever-changing cyberthreat landscape. The absence of a well-defined and robust cybersecurity program not only leads to grave financial losses but also reputation loss and diminished goodwill.

As this research uncovers, organizations are finding it increasingly challenging to embed cybersecurity into the enterprise IT architecture. Not just that, most enterprises are battling with lack of integrated solutions and shortage of skilled workforce, unable to cope with the fast-paced technological changes. To overcome these challenges, most organizations are focusing on devising means to incorporate security at an early stage of the business lifecycle, embedding secure by design principles to minimize risks. As businesses grow, adoption of integrated, modular and intelligent platforms optimize costs and is fundamental for increasing operational efficiency to secure by scale. Training and enablement sessions, creating employee awareness and collaborating with technology partners and service integrators are the primary focus areas to keep the workforce updated and abreast of the evolving cyber technologies. This ensures organizations are keeping pace with sophisticated and persistent cyberthreats that require modern, cutting-edge cybersecurity solutions such as multi-layered threat defense, advance threat intelligence, deep analytics and correlation, orchestration and automation, robust incident response and highly skilled and motivated team, that can prepare enterprises for any eventuality, helping them stay relevant and hence secure the future.

The success of a cybersecurity program is in devising a comprehensive strategy that involves the board and senior management, building a cybersecurity culture among employees, increased collaboration between technology partners and focusing on developing modern, cutting-edge solutions.

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