ASSURING DIGITAL-TRUST

BANKING, FINANCIAL SERVICES AND INSURANCE INDUSTRY VIEW

Infosys® | Knowledge Institute

Table of Contents

INTRODUCTION

Digital transformation is critical in the banking, financial services and insurance (BFSI) industries as organizations respond to shifting customer expectations, the pressure to deliver superior business results and increasing regulatory requirements. The banking segment leads in the adoption of digital programs, while insurance firms started slowly but are trying to catch up.

Mobile and digital initiatives backed by technologies such as artificial intelligence, blockchain, and cloud computing have supercharged two-way communication between BFSI firms and customers. These initiatives allow multichannel access and enable more personalized, insight-driven, and quicker interactions.

However, the increased connectivity has led to an unprecedented level of cybersecurity risks and threats. This industry bears the highest cost from cybercrimes; the nature and volume of transactions make it a natural target. Guarding and defending against these threats have assumed paramount importance.

Traditionally risk-averse, banks have invested significantly in cybersecurity to protect their business interests as well as safeguard customer privacy. But insurers have trailed in these initiatives. No financial institution can afford to lag in the cybersecurity investments needed to combat increasingly sophisticated and frequent attacks and comply with more stringent regulations.

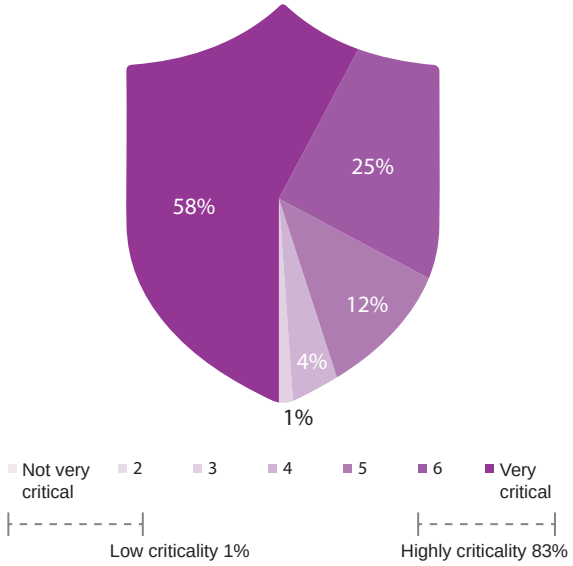
To investigate further, Infosys commissioned a study of 274 senior executives from BFSI organizations with revenues over $500 million and located across the U.S., Europe, Australia and New Zealand (ANZ). The study's objectives were to understand the industry's challenges, solutions, and plans for the future, and also to present a holistic view of the cybersecurity landscape.

Diving into cybersecurity

Malware, phishing, ransomware, and cryptojacking have been an enormous cause for concern among BFSI firms. A rise in the number and sophistication of attacks has led to widespread disruption, including financial losses, compromised customer data, damaged reputations, and increased regulations. Given the clear need for a robust cyber defense program, how critically are enterprises viewing cybersecurity?

Infosys research revealed that 83% of BFSI enterprises across all countries surveyed viewed cybersecurity as critical to their organizations.

Figure 1. How do organizations view cybersecurity?

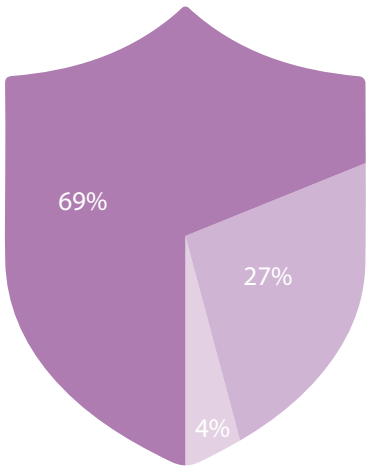


Criticality	Overall	BFSI	U.S.	Europe	ANZ
Base	***867***	***274***	***148***	***98***	***28***
High criticality (%)	83	83	89	80	64
Low criticality (%)	1	1	1	-	4

BFSI: Banking, Financial services and Insurance

Beyond considering it a top priority, enterprises must also put it into practice. A nearly unanimous 96% of respondents said they have a well-defined, enterprise-wide strategy that is either implemented or is being implemented. The study findings indicate that cybersecurity is an integral part of BFSI firms' digital agenda.

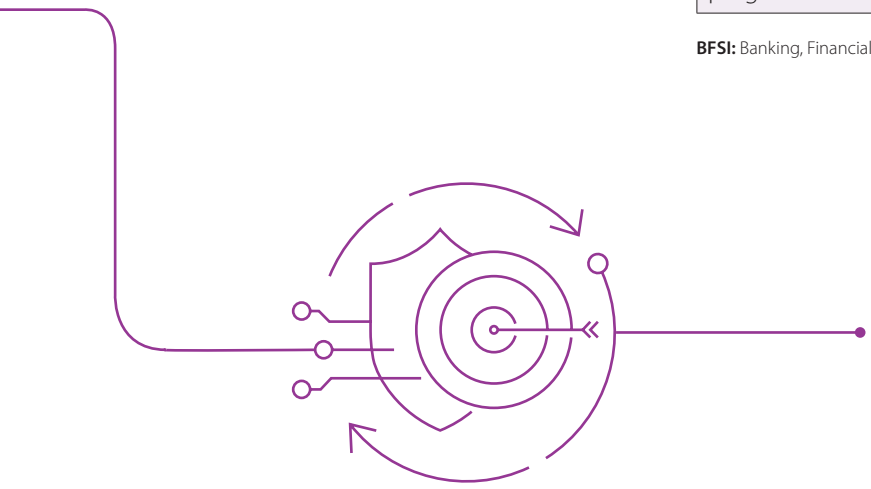
Figure 2. Maturity of your cybersecurity program



Base: 274

What is the current maturity of your cybersecurity program (%)	Overall	BFSI	U.S.	Europe	ANZ
Base	***867***	***274***	***148***	***98***	***28***
Well defined enterprisewide strategy/roadmap exists, implemented	66	69	72	66	57
Enterprisewide strategy/ roadmap exists as a guideline but implementation in progress	30	27	22	31	36
Enterprisewide strategy/ roadmap is work in progress and therefore implementation and operations are ad hoc	4	4	5	3	4
No defined framework or program	0	0	-	-	4

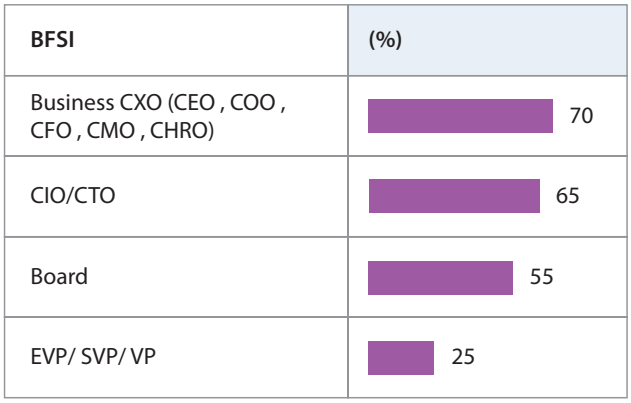
BFSI: Banking, Financial services and Insurance



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

Figure 3. Organizational levels that are discussing cybersecurity



U.S.	Europe	ANZ
148	***98***	***28***
74	63	68
68	59	64
55	52	61
33	13	25

Base: 274

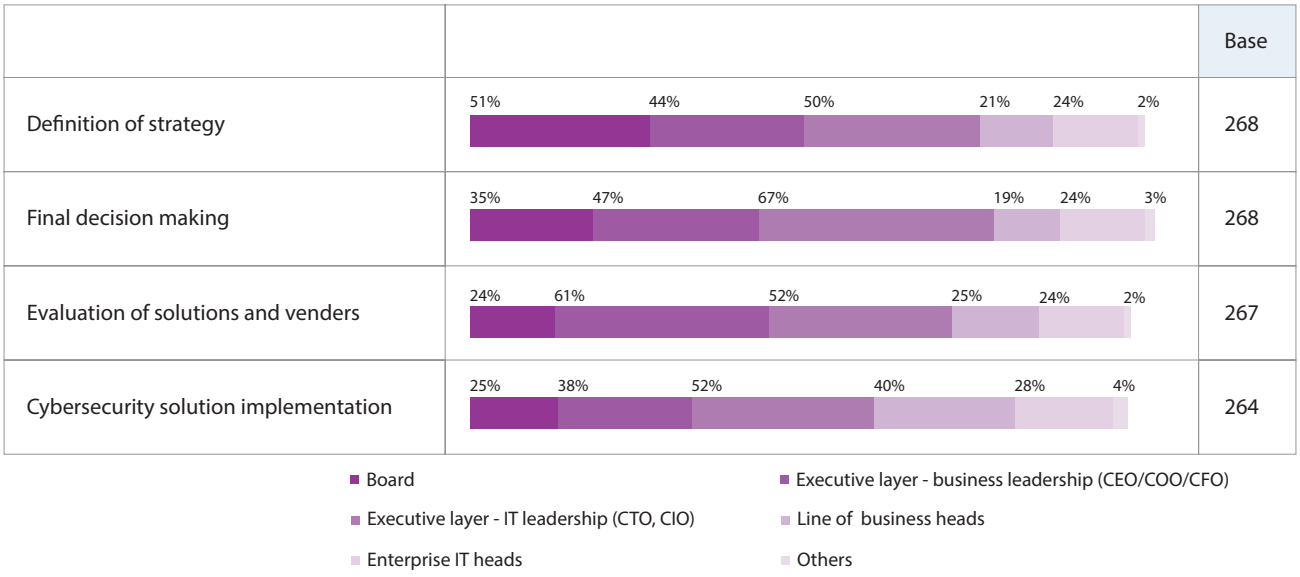
Respondents said that 55% of the board and 70% of business leaders are actively involved in setting the cybersecurity strategy. With this high participation rate, the BFSI industry is setting the benchmark for others.

European firms have the least involvement from the board and senior management compared with companies in the U.S., Australia and New Zealand.

While the board contributes the most at the strategy definition stage (51%), business leaders participate more in evaluating solutions and vendors (61%). Notice that more than half the respondents said IT leaders remained engaged during the entire life cycle. Attention from senior management and the board is warranted and will enable the enterprise to race forward on its cybersecurity journey.

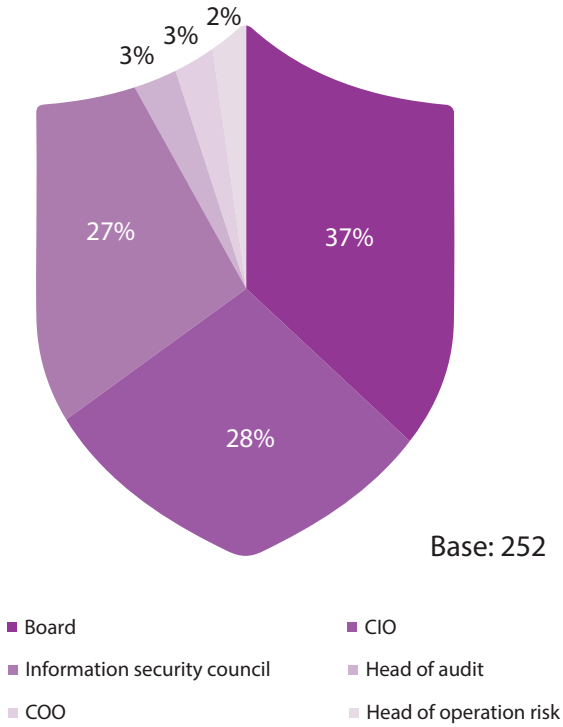
"Cybersecurity is on the way to becoming a key player in the boardroom, integrating business, compliance and technology concerns. This goes beyond traditional information security and cybersecurity and is an integral part of corporate governance. Business support functions, therefore, need to transform themselves into becoming enablers, supporting business leadership by ensuring that the security controls that have been put in place are not only adequate but also help businesses to grow." — *Chief information security officer (CISO) of a large leading Indian financial services firm*

Figure 4. Key participants in the cybersecurity journey



A key executive is the chief information security officer (CISO), who is responsible for protecting the digital sprawl across the enterprise and ensuring the cybersecurity program stays alignedwith the business strategy.

Figure 5. CISO reporting hierarchy



Where does the CISO organization report in to (%)	Overall	BFSI	U.S.	Europe	ANZ
Base	***792***	***252***	***136***	***91***	***25***
Board	32	37	33	41	40
CIO	34	28	28	24	40
Information security council	23	27	29	27	16
Head of audit	5	3	3	3	4
COO	3	3	4	3	-
Head of operation risk	3	2	3	1	-
Others	1	0	1	-	-

BFSI: Banking, Financial services and Insurance

In accordance with that role's importance, CISOs report to the board 37% of the time in the BFSI industry. Visibility and access to the highest levels in the company help amplify the reach across the organization.

The most pressing cyberthreats

With cyberthreats and attacks on the rise, respondents viewed hackers and hacktivists (83%), low awareness among employees (76%), corporate espionage (75%) and insider threats (75%) as the top concerns.

- Hackers/hacktivists — The growing sophistication of cyberattacks has made regular financial transactions, such as card processing and money transfers, and sensitive customer data more vulnerable. The nature of the business places these firms at heightened risk and makes them subject to many more attacks compared with firms in other industries.
- Low awareness of security incidents among employees — Often, ill-informed employees can pose a high risk by sharing confidential information inadvertently. For instance, cybercriminals use spear phishing and social engineering techniques to delude employees into handing over sensitive data.
- Insider threats — In an intensely competitive business environment, the prospect of insiders causing damage is a real possibility. Typically, this occurs through stealing and leaking of confidential information. Corporate espionage is another closely related concern.

Survey participants from Europe were the most worried about these threats.

Figure 6. Top cybersecurity concerns

What is your number one concern regarding threats(%)	Overall	BFSI	U.S.	Europe	ANZ
Base	***867***	***274***	***148***	***98***	***28***
Hackers/hacktivists	84	83	82	85	86
Low awareness on potential risks of security incidents among employees	76	76	76	79	71
Insider threats	75	75	74	78	68
Corporate espionage	75	72	77	61	82
Organized crime	67	68	66	74	61
Nation-states	60	63	64	62	61
Uneven deployment of cybersecurity solution	60	57	57	56	61

BFSI: Banking, Financial services and Insurance

THE ENTERPRISE IMPERATIVES

Enterprises must always be hyperalert to effectively counter cyberthreats. The appropriate defense should have touch points across technologies, 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 implemented today

Figure 7. Cybersecurity solutions

Top solutions implemented (%)	Overall	BFSI	U.S.	Europe	ANZ
Security incident management	66	72	78	68	56
Security awareness training	66	71	72	72	63
Risk and compliance	66	70	76	61	67
Encryption	64	68	73	63	64
Cloud access security broker	64	68	71	66	61
Tackling IoT security	60	67	73	62	57
Intrusion prevention systems	63	67	73	62	57
Identity and access management	63	64	73	55	50
Unified threat management	58	63	67	56	63
Application control on server workloads	58	62	70	51	54

BFSI: Banking, Financial services and Insurance

Protecting customers' data and safeguarding their interests are perhaps the biggest priorities for the BFSI industry. Failure to do so can threaten an organization's survival.

As one of the top strategies, security incident management (72%) helps identify, analyze, and mitigate incidents quickly and prevent damage.

Given that low employee awareness and corporate espionage are significant concerns, security awareness training (71%) is another critical option. An enterprise can avert potential damage by educating employees on various cyber scenarios and preparing them to handle those situations.

Also, the BFSI industry is highly regulated, so enterprises must steer through the complex web of rules and regulations with great care. The U.S. alone has created more than 30 cybersecurity regulations since 2014. Therefore, risk and compliance solutions (70%) are an essential part of an organization's cybersecurity strategy.

The U.S. has implemented these top three solutions significantly more than Europe, Australia and New Zealand.

"There are two important aspects in maintaining a fairly mature cybersecurity program in my organization. The first one involves streamlining of NSEW network flows, along with providing visibility of the flows by utilizing intrusion prevention systems along key points. The second one involves the implementation of an incident management platform, which continuously collects and reports on threat vectors that impact the landscape." — *Technology leader at a large U.S. multinational investment bank and financial services company*

Challenges galore

BFSI enterprises undergo multiple challenges as they establish a cybersecurity defense. The top three are building a cybersecurity aware culture (66%), embedding security into enterprise IT architecture (65%) and keeping pace with fast-changing cybersecurity technologies (63%).

Figure 8. Top cybersecurity challenges

(%)	Overall	BFSI	U.S.	Europe	ANZ
Base	***867***	***274***	***148***	***98***	***28***
Building a cybersecurity aware culture	65	66	61	73	68
To ensure enterprise IT architecture has security embedded in it	67	65	61	66	82
Cybersecurity technology changing too fast	63	63	65	60	64
Too much time spent in building technology stack and less on deriving value	57	62	61	63	61
Lack of appropriate tools to automate controls and audit effectiveness	55	61	59	62	68
Poor integration between tools and different solutions	54	52	46	57	64
Lack of user awareness	54	50	50	47	57
Inadequate management support	52	47	48	43	61
Lack of skilled personnel	49	46	43	49	50
Lack of reporting on incidents	39	43	47	37	50

BFSI: Banking, Financial services and Insurance

The survey findings repeatedly confirm that BFSI firms are acutely aware of the vulnerability of employees, both those who are unaware and those with malicious intent. Insider threats can pose a higher risk since employees have easier access to confidential information. However, building a cybersecurity-aware culture is not easy as it involves changing mindsets and processes.

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

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

European respondents felt the pain most in building a cybersecurity aware culture (73%), while respondents in Australia and New Zealand struggled most with embedding security in enterprise IT architecture (82%).

"All stakeholders need to be involved to ensure that the investment in cybersecurity is maximized. It is, therefore, critical that the organization invests to nurture and build a security-oriented culture across the board. This applies to all employees, partners, and even vendors. Everyone should realize that the most sophisticated system is no match for human errors and behavior that compromise organization security, including seemingly innocuous sharing of passwords or clicking on malware. Mostly we see that data breaches also stem from ignorance and errors more than sophisticated technology. Training, therefore, is critical for employees to meet these challenges." — *CISO for a mid-sized U.S. bank and member of the Federal Reserve, with more than 600 branches and 15,000-plus staff*

Overcoming the challenges using multiple methods

BSFI organizations must realize that simple perimeter defense is no longer adequate to secure the enterprise. They must instead take an enterprise-wide approach, starting at the design stage, taking it through growth and focusing on the future as well.

BFSI firms are taking initial steps towards such an approach through training and certifications (62%), workshop and enablement sessions (57%), and integrated security solutions (57%).

Figure 9. Cybersecurity approaches

Cybersecurity approaches	(%)	U.S.	Europe	ANZ
		148	*98*	*28*
Training and certifications	62	61	60	75
Focus on integrated security solutions rather than point sol	57	61	55	39
Workshops and enablement sessions	57	59	53	57
Creating a culture of employee awareness	46	47	46	36
Work with technology vendors and service integrators	45	47	43	43
Hire service provider specializing in security solutions	39	38	39	43
Outsource security cybersecurity monitoring and management	21	20	16	39
Enable threat intelligence feeds	16	18	10	25

Base: 274

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.

Interestingly, the views in all regions are aligned. Responses generally show that BFSI firms rely on technology providers and security solutions specialists more than integrated solutions to address their challenges.

Focus areas – next moves

BFSI firms are ready to move to the next level of cyber defense after establishing a solid foundation. The top three focus areas where firms have implemented solutions are network segregation (67%), threat intelligence platform (58%), and user and entity behavior analytics (UEBA) (53%).

Threat intelligence platforms and UEBA signal the intent to counter advanced attacks since they can predict and identify danger in advance and prevent damage even before it occurs.

The U.S. is ahead of other regions in implementing these solutions.

Figure 10. Next stages of cybersecurity

Next stages of cybersecurity	Implemented				
	Overall	BFSI	U.S.	Europe	ANZ
Network segregation	65	67	71	63	64
Threat intelligence platform	57	58	65	50	50
User and entity behavior analytics	48	53	54	53	46
Advanced threat protection	55	53	50	58	50
Deception technologies	49	47	43	56	39
Security orchestration and automation response	46	46	43	50	50
Cloud access security broker	44	46	49	43	44
DevSecOps	46	42	40	45	41

Next stages of cybersecurity	Implementing				
	Overall	BFSI	U.S.	Europe	ANZ
Network segregation	25	24	21	30	18
Threat intelligence platform	27	26	20	34	29
User and entity behavior analytics	29	26	24	30	21
Advanced threat protection	31	34	37	31	32
Deception technologies	36	41	46	34	36
Security orchestration and automation response	34	38	44	35	14
Cloud access security broker	30	31	30	33	30
DevSecOps	34	39	46	30	30

BFSI: Banking, Financial services and Insurance

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
		83	*33*	*14*
Deception technologies introduced in IoT and OT to enable cybersecurity	46%	34	42	50
Artificial intelligence used for real time predictive/ preventive cybersecurity instance	43%	36	42	29
Continued demand for cybersecurity skills	33%	31	24	43
New business models including cyber insurance emerge	30%	30	30	36
Privacy and personal data protection gains significance	30%	25	36	43
Usage of blockchain technologies in developing security solutions	28%	28	18	36
Behavioral analytics becomes very important in identity management	25%	22	36	14
Introduction of automation in implementing cybersecurity controls and compliance	25%	25	21	29
Move to customization of security solutions from standard	24%	19	30	21
Cybersecurity startups to gain recognition	14%	25	21	7
Regulatory bodies show zero tolerance on non-compliance	12%	23	12	21

BFSI: Banking, Financial services and Insurance

Respondents stated that artificial intelligence (39%), privacy and personal data protection (35%), and continued demand for cyber skills (34%) are likely to influence the future direction of cybersecurity.

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

The digital revolution has unleashed vast volumes of data, giving rise to concerns over privacy and protection. Consequently, regulations such as the European Union's General Data Protection Regulation have come into play, and more are likely to follow.

But there is a significant shortage of high-quality cybersecurity skills in the market today, making it challenging to run a cyber program optimally. cybersecurity professionals will also need to bring a business flavor to complement their technical expertise and ably address today's evolving demands.

"The security threat landscape has become all-encompassing through advanced targets and methods. It is not only the financial services sector that is at risk. No one is completely safe, including utilities, government, social media, and even smaller businesses." — *leader at a mid-size U.S. accounts receivable management and student loan servicing solutions company*

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

While the industry has made good progress in setting up a robust cybersecurity structure, more needs to be done to cope with the evolving cyberthreat landscape. As a natural target for cyberattacks since they process significantly valuable information, BFSI firms should fortify defenses by investing in advanced solutions such as orchestration and automation platforms.

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

Further, cybersecurity must be an integral part of every stage of the business life cycle. 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 senior leadership support, educating employees, and instituting a security-first mindset. The alternative to this path is to bear financial losses, damage to reputation, and loss of customer trust. It may even lead to a threat to the business's survival.

On the other hand, an effective cybersecurity program can enable a business to pursue its plans to strengthen operations, enhance customer loyalty by providing more meaningful and personalized services, and handle competition more confidently. Indeed, it is a game changer.

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