Infosys
Navigate your next

ASSURING DIGITAL-TRUST

MANUFACTURING INDUSTRY VIEW

Infosys | Knowledge Institute

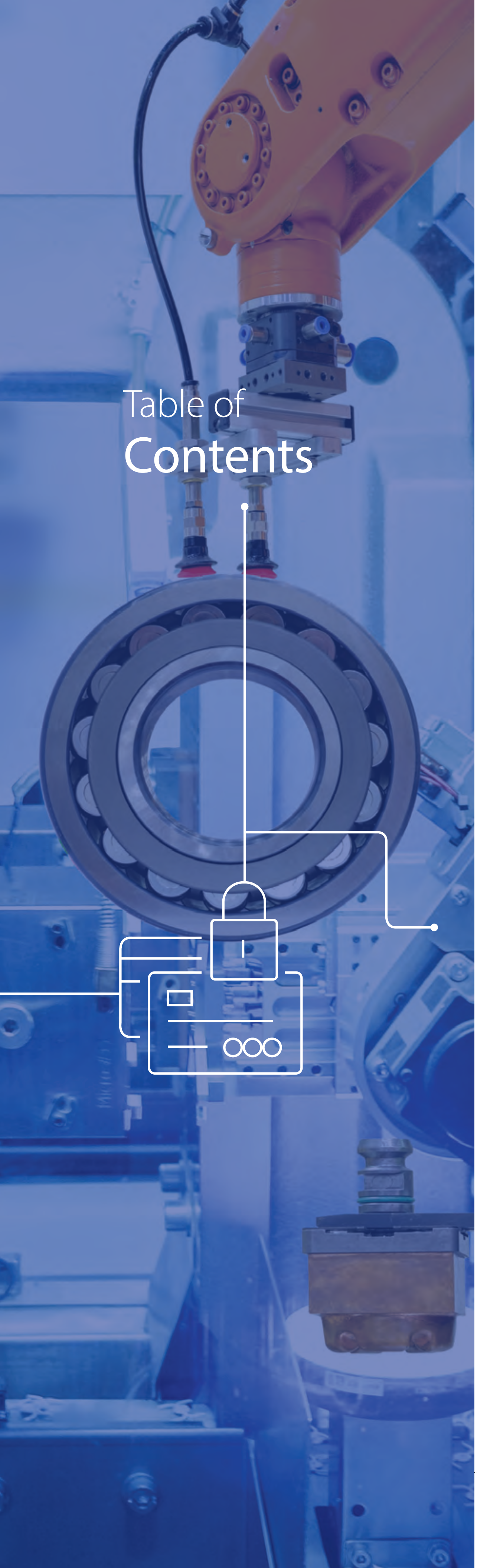


Table of Contents

Introduction 4

Diving into cybersecurity 5

- Higher the board's involvement, the better the chances of cybersecurity success 7
- The most pressing cyberthreats 9

The enterprise imperatives 10

- Top security solutions implemented today 10
- Challenges galore 11
- Overcoming the challenges using multiple methods 12
- Focus areas – next moves 13

The Infosys perspective – scale with assurance 14

Shaping cybersecurity of the future – trends to watch 15

The way forward to instill digital trust and navigate to a secure future 16

INTRODUCTION

As manufacturers find their footing in the fourth industrial revolution, they must urgently overhaul existing systems and processes and replace them with more advanced approaches. Digital transformation, bolstered by the internet of things (IoT), cloud computing, big data and analytics, robotics, and artificial intelligence (AI), is the most effective way for manufacturers to compete in an increasingly complex marketplace. That digital path can help firms in their quest for greater efficiency and lower costs, and it can help boost business performance by increasing connectivity and making shop floors smarter.

The downside of these interconnected technologies is the increased vulnerability to data breaches and other cyberattacks. Creating and implementing an effective cybersecurity strategy is imperative.

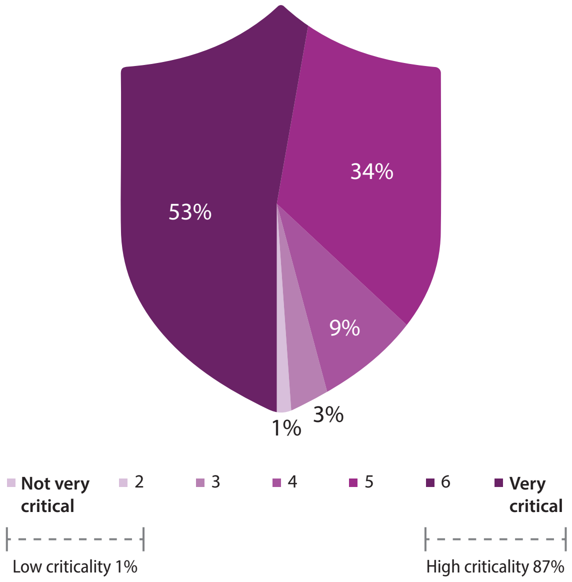
To investigate further, Infosys commissioned a study of 130 senior-level executives from manufacturing organizations with revenues over $500 million and located across the U.S., Europe, Australia and New Zealand (ANZ). The study's objectives were to understand the industry's challenges, solutions and plans for the future, and also present a holistic view of the cybersecurity landscape.

DIVING INTO CYBERSECURITY

As manufacturing operations become increasingly global and connected, the cybersecurity threats increase along with the business opportunities. Ransomware and email attacks have caused significant disruption to U.S. and European manufacturers. Given the clear need for a robust cyberdefense program, how critically are enterprises viewing cybersecurity?

Infosys research revealed that 87% of enterprises across all countries surveyed viewed cybersecurity as critical to their organization.

Figure 1. How organizations view cybersecurity?



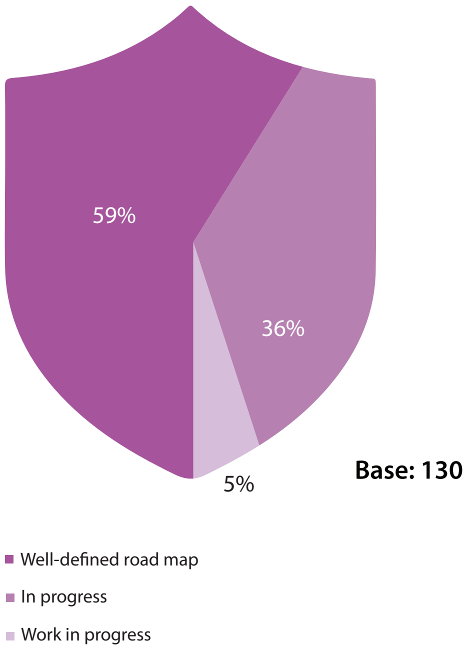
Criticality	Overall	Mfg	U.S.	Europe	ANZ
Base	***867***	***130***	***83***	***33***	***14***
High criticality (%)	83	87	87	88	86
Low criticality (%)	1	1	1	1	1

Mfg: Manufacturing

While 95% of respondents have a well-defined enterprisewide strategy, however, only 59% said they have implemented the strategy. Manufacturers must deal with the growing sophistication of threats and an expanding attack surface to stay ahead of danger. They may even hamper the implementation of an enterprisewide strategy.

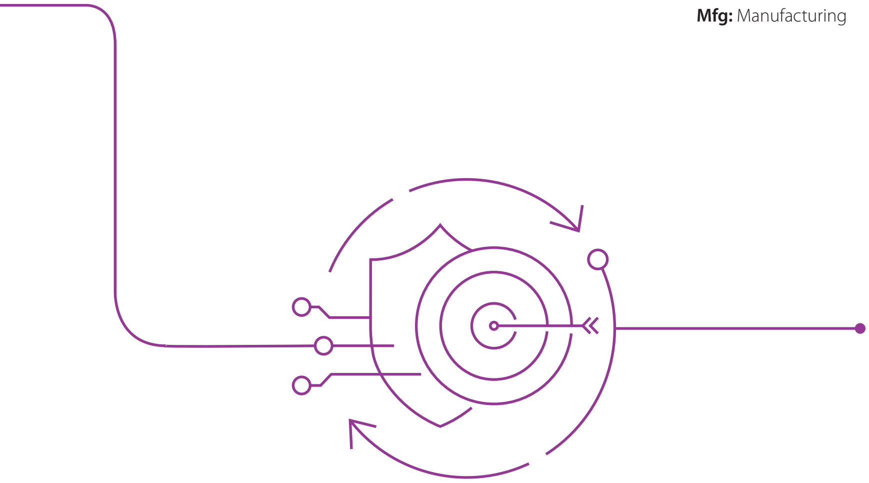
In the Infosys study, the U.S. is ahead in implementing an enterprisewide strategy compared with Europe, Australia and New Zealand.

Figure 2. Maturity of your cybersecurity program



What is the current maturity of your cybersecurity program? (%)	Overall	Mfg	U.S.	Europe	ANZ
Base	***867***	***113***	***45***	***44***	***24***
Well-defined enterprisewide strategy/roadmap exists, implemented	66	59	64	55	43
Enterprisewide strategy/ roadmap exists as a guideline but implementation in progress	30	36	33	42	43
Enterprisewide strategy/ roadmap is work in progress and therefore implementation and operations are ad hoc	4	5	4	3	14
No defined framework or program	-	-	-	-	-

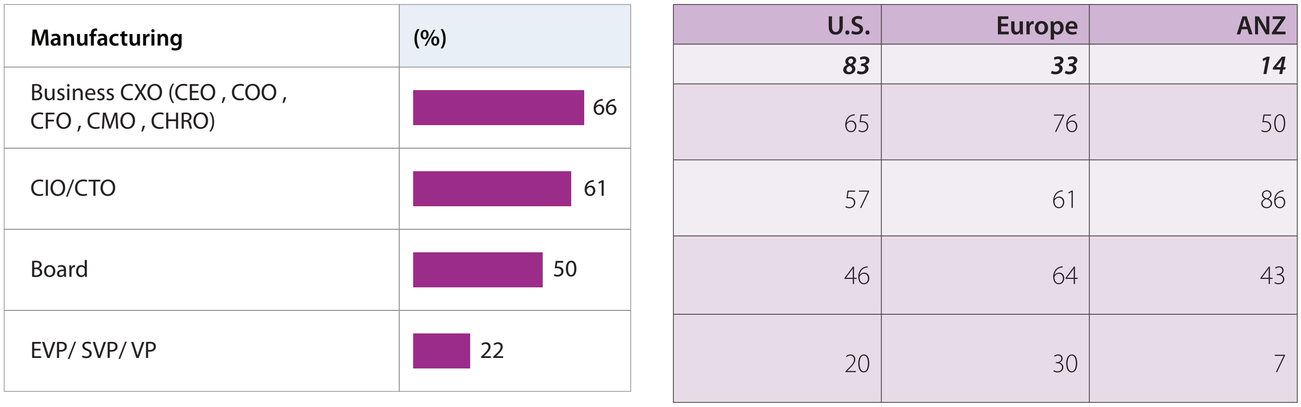
Mfg: Manufacturing



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

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

Figure 3. Organizational levels that are discussing cybersecurity



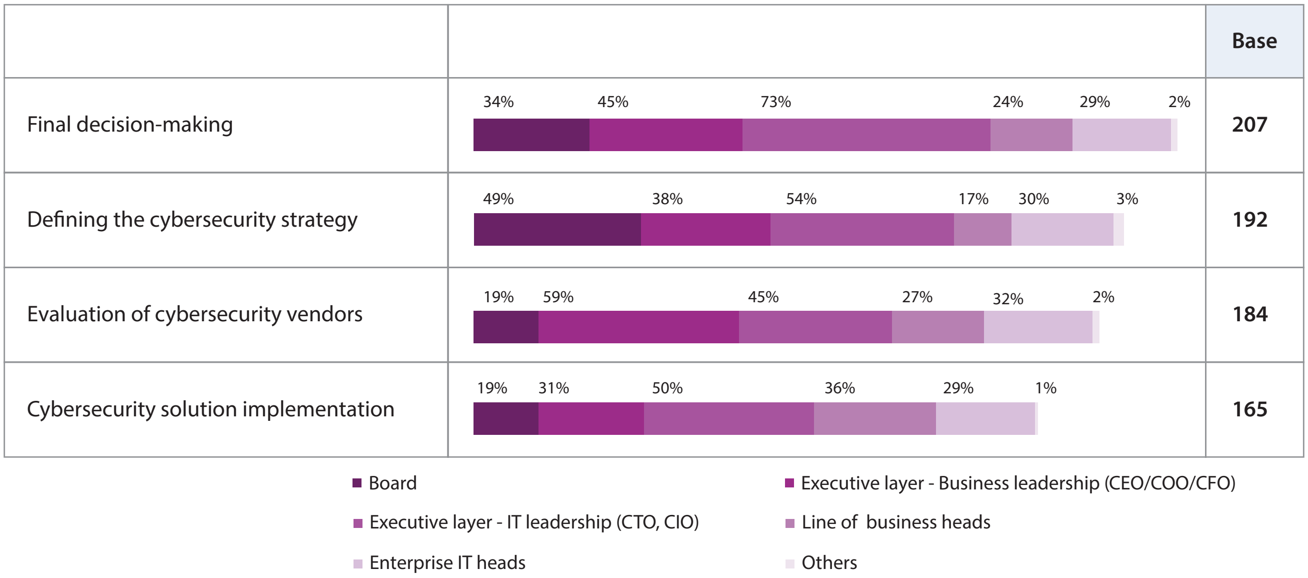
Manufacturing	(%)	U.S.	Europe	ANZ
		83	***33***	***14***
Business CXO (CEO , COO , CFO , CMO , CHRO)	66	65	76	50
CIO/CTO	61	57	61	86
Board	50	46	64	43
EVP/ SVP/ VP	22	20	30	7

Base: 130

Respondents said 50% of the board and 66% of business leaders are actively involved in setting the cybersecurity strategy. European business leaders and their boards are the most actively engaged in this area. Comparatively, board members from other countries surveyed play a lesser role.

While the board contributed the most at the strategy definition stage (49%), IT leaders were active throughout the journey and especially in the final decision-making (73%) stage.

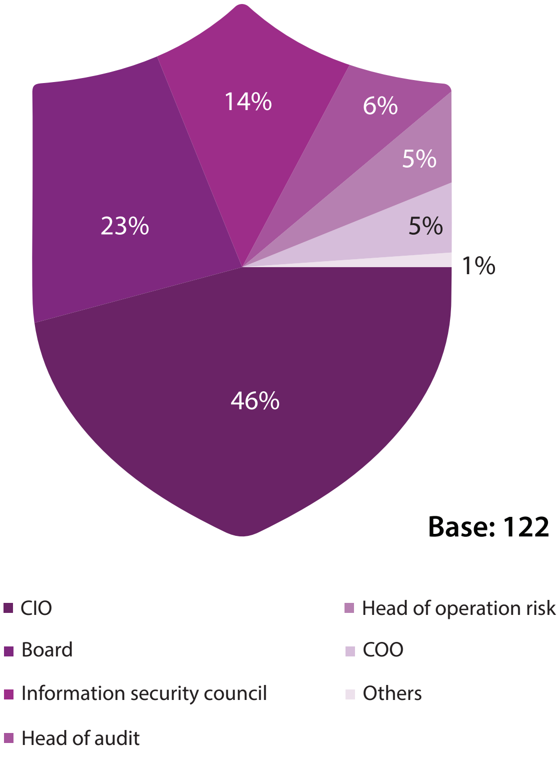
Figure 4. Key participants in the cybersecurity journey



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

Nearly half of manufacturing CISOs report to the CIO (46%), while less than a quarter report to the board (23%). Those results show that manufacturers trail global best practices, where the role is elevated by having CISOs report to the board.

Figure 5. CISO reporting hierarchy



Where does the CISO report? (%)	Overall	Mfg	U.S.	Europe	ANZ
Base	***792***	***122***	***79***	***30***	***13***
CIO	34	46	51	43	23
Board	32	23	18	37	23
Information security council	23	15	16	7	23
Head of audit	5	6	5	3	15
COO	3	5	4	7	8
Others	3	5	5	3	8

Mfg: Manufacturing

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

The most pressing cyberthreats

With cyberthreats and cyberattacks on the rise, respondents viewed hackers and hacktivists (85%), corporate espionage (82%) and insider threats (72%) as the top concerns.

By integrating new products and services into the manufacturing process as part of automation, enterprises introduce vulnerabilities that make it easier for hackers to penetrate the defenses.

Further, in a continually evolving and highly competitive environment, intellectual property (IP) can make the difference between success and failure. At the same time, IP is a natural target for espionage and insider threats.

Firms in Australia and New Zealand are significantly more concerned about corporate espionage (93%) and insider threats (79%) than firms in the U.S. and Europe.

Figure 6. Top cybersecurity concerns

What is your number one concern regarding threats? (%)	Overall	Mfg	U.S.	Europe	ANZ
Base	***867***	***130***	***83***	***33***	***14***
Hackers/hacktivists	84	85	86	85	86
Corporate espionage	75	82	78	85	93
Insider threats	75	72	72	70	79
Low awareness of potential risks among employees	76	70	69	79	57
Uneven deployment of cybersecurity solution	60	65	72	52	57
Organized crime	67	61	60	64	57
Nation-states	60	60	58	64	64

Mfg: Manufacturing

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 enterprisewide access to ensure maximum protection.

Top security solutions implemented today

Cybercriminals frequently look for IP-related or sensitive company information when attacking manufacturing firms. Security incident management solutions help identify, analyze, and manage incidents quickly to prevent damage. Also, intrusion prevention systems and identity and access management solutions are part of a cybersecurity portfolio that will allay concerns about corporate espionage and insider threats.

U.S. manufacturers are ahead of the others in implementing the top three solutions.

Figure 7. Cybersecurity solutions

Top solutions implemented (%)	Overall	Mfg	U.S.	Europe	ANZ
Security incident management	66	72	77	61	71
Intrusion prevention systems	63	71	76	58	79
Identity and access management	63	71	74	67	64
Security awareness training	66	71	73	70	64
Risk and compliance	66	70	75	63	57
Cloud access security broker	64	65	68	58	64
Encryption	64	65	67	55	71
Tackling IoT security	60	64	69	52	64
Application control on server workloads	58	64	71	45	64
Unified threat management	58	60	61	55	64

Mfg: Manufacturing

Challenges galore

Manufacturers said they are challenged when trying to embed security in the enterprise IT architecture (67%), keep pace with fast-changing cyber technologies (66%) and build a security-first culture (57%).

Figure 8. Top cybersecurity challenges

(%)	Overall	Mfg	U.S.	Europe	ANZ
Base	***867***	***130***	***83***	***33***	***14***
To ensure enterprise it architecture has security embedded in it	67	67	66	67	71
Cybersecurity technology changing too fast	63	66	67	64	64
Building a cybersecurity aware culture	65	57	55	61	57
Too much time spent in building technology stack and less on deriving value	57	55	53	42	93
Lack of skilled personnel	49	54	53	61	43
Poor integration between tools and different solutions	54	52	49	55	64
Lack of user awareness	54	51	43	70	50
Lack of appropriate tools to automate controls and audit effectiveness	55	47	47	48	43
Inadequate management support	52	42	35	58	50
Lack of reporting on incidents	39	40	42	36	36

Mfg: Manufacturing

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 skills sets required.

Manufacturers must safeguard against damage caused inadvertently by unaware employees as well as by 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 since it involves changing mindsets and processes.

European respondents voiced the most concern over lack of user awareness (70%), while those in the U.S., Australia and New Zealand don't view it as a major issue.

An overwhelming 93% of respondents in Australia and New Zealand are apprehensive about the disproportionate time spent building the technology stack compared with time spent deriving value. Surprisingly, the other two regions do not view this as a significant concern.

Overcoming the challenges using multiple methods

Manufacturers must take an enterprisewide approach, starting at the design stage, taking it through growth and focusing on the future as well.

These initial steps are underway. Respondents said they employ methods such as training and certifications (67%), workshop and enablement sessions (60%) and collaboration with technology vendors and service providers (57%) to overcome existing challenges.

Figure 9. Cybersecurity approaches

Cybersecurity approaches	(%)	U.S.	Europe	ANZ
		82	*33*	*14*
Training and certifications	67%	65	73	71
Workshops and enablement sessions	60%	57	64	71
Work with technology vendors and service integrators	57%	52	67	64
Focus on integrated security solutions rather than point solutions	52%	50	55	57
Creating a culture of employee awareness	51%	48	58	57
Bring on board a service provider specializing in security solutions	42%	38	55	36
Outsource security services for monitoring and management	27%	24	36	21
Enable threat intelligence feeds	19%	12	27	43

Base: 129

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

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

Respondents from Europe, Australia and New Zealand are exerting significantly more effort in overcoming these challenges compared with those in the U.S.

Focus areas — next moves

Manufacturers need to evolve to the next stage of cyber defense as they focus on more advanced technologies to safeguard their enterprises. The top three areas are network segregation, threat intelligence platforms, and DevSecOps.

Network segregation can provide better security for sensitive data by restricting access between network segments, thereby limiting impact of incidents and slowing down attacks. Threat intelligence platforms can predict and identify danger in advance and prevent damage. DevSecOps aims to insert security into every part of the application development life cycle, enabling rapid development and reduced frequency of incidents.

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

Figure 10. Next stages of cybersecurity

Next stage of cybersecurity(%)	Implemented				
	Overall	Mfg	U.S.	Europe	ANZ
Network segregation	65	63	66	64	43
Threat intelligence platform	57	57	59	55	57
DevSecOps	46	52	58	48	29
Deception technologies	49	51	58	42	29
Advanced threat protection	55	48	48	48	43
Cloud cccess security brokers	44	45	51	42	21
Security orchestration and automation response	46	45	42	52	43
User and entity behavior analytics	48	43	51	28	29

Next stage of cybersecurity(%)	Implementing				
	Overall	Mfg	U.S.	Europe	ANZ
Network segregation	25	28	27	27	43
Threat intelligence platform	27	30	30	24	43
DevSecOps	34	35	34	36	43
Deception technologies	36	35	33	36	50
Advanced threat protection	31	38	40	36	36
Cloud cccess security brokers	30	35	33	36	50
Security orchestration and automation response	34	37	41	24	43
User and entity behavior analytics	29	33	28	44	36

Mfg: Manufacturing

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

Mfg	(%)	U.S.	Europe	ANZ
		83	*33*	*14*
Deception technologies introduced in IoT and OT to enable cybersecurity	46%	34	42	50
AI used for real time predictive/preventive cybersecurity	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 solutions	24%	19	30	21
Cybersecurity startups to gain recognition	14%	25	21	7
Regulatory bodies show zero tolerance for non-compliance	12%	23	12	21

Mfg: Manufacturing

According to the survey, the top two trends to consider are deception technologies introduced in IoT and operational technology (OT) (38%) and AI for preventive cybersecurity (37%).

Manufacturing firms are increasingly integrating OT and IT environments in their quest to become more connected. However, this also exposes them to more risks and threats as cybercriminals can easily infiltrate the relatively less secure OT networks. The need for deception technologies is evident in this scenario.

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

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

Manufacturers globally are keen on becoming more digitized, intelligent and personalized in response to demanding market conditions and to survive intense competition. As they go through both strategic and operational transformation, 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-level management must 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 manufacturing firms to navigate the digital economy better and deliver increased operational efficiencies, competitiveness and business performance. 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