Infosys®
Navigate your next

ASSURING DIGITAL-TRUST

HEALTH CARE AND LIFE SCIENCES INDUSTRY VIEW

Infosys® | Knowledge Institute

Table of Contents

INTRODUCTION

The healthcare and life sciences (H&LS) industry is facing monumental challenges as it moves toward a value-based model from a fee-based model to appeal to savvy customers. The key issues include intense competition, new business and care delivery models, changing demographics of customers with increasingly sophisticated expectations, and increased regulatory scrutiny. To survive, H&LS firms must constantly innovate and redefine their old, familiar ways of conducting business.

By capitalizing on digital technologies such as artificial intelligence (AI), blockchain, big data, robotics, and cloud computing, H&LS organizations can aim to provide more accessible, affordable, and intelligent services.

The resulting surge of new data and increased connectivity to growing business and technological ecosystems, however, creates opportunities and threats. These newly transformed enterprises offer more targets for cyber attackers. Thus, a sound cybersecurity strategy and effective implementation are essential to digital transformation.

To investigate further, Infosys commissioned a study of 61 senior-level executives from H&LS organizations with revenues over $500 million located across the United States, 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.

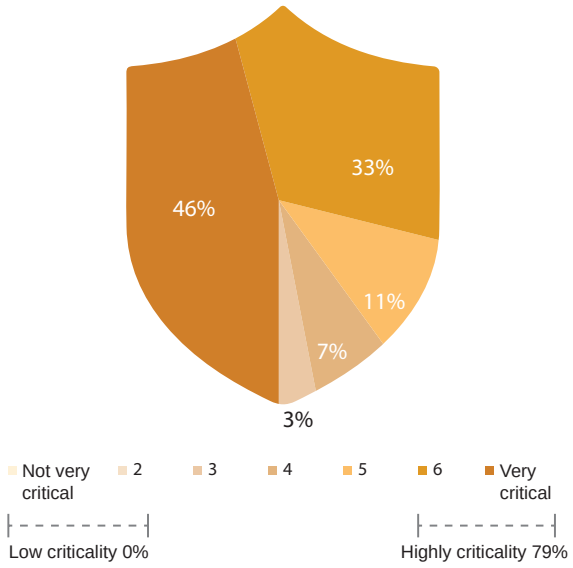
Diving into cybersecurity

Over the years, healthcare firms have collected valuable patient data through electronic health records and other methods. Meanwhile, life sciences companies store sensitive information on new drug development. Cybercriminals can cause havoc if they lay their hands on this information. Also, cyberattacks are now targeting connected medical devices and health data gathering apps. In fact, the H&LS industry reported the highest volume of cybersecurity breaches among all industries in 2018, according to BakerHostetler's 2019 Data Security Incident Response Report (Bryant, 2019).

cybersecurity must be viewed as a top priority industrywide.

However, only 79% of those surveyed consider cybersecurity to be highly critical. All respondents from Australia and New Zealand share that concern, followed by 83% of U.S. participants. Europe trails significantly at 56%.

Figure 1. How do organizations view cybersecurity?

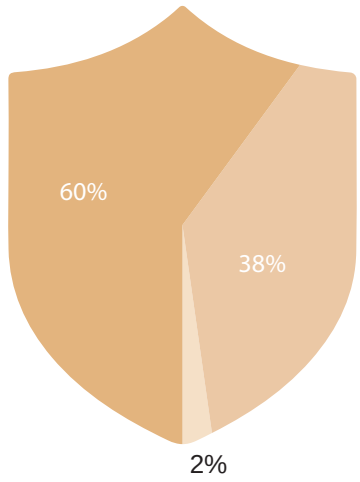


Criticality	Overall	H&LS	U.S.	Europe	ANZ
Base	***867***	***61***	***36***	***16***	***9***
High criticality (%)	83	79	83	56	100
Low criticality (%)	1	10	0	0	0

H&LS: Health Care and Life Sciences

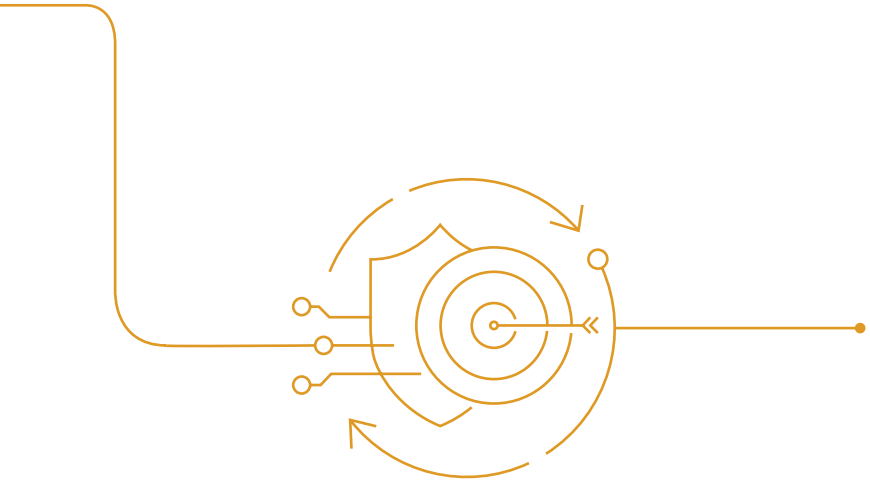
While many H&LS firms rank cybersecurity as a top priority, this appraisal has not always translated into tangible action. Almost all respondents (98%) had a well-defined enterprisewide strategy, but only 61% said they had implemented it. Australia and New Zealand (67%) and Europe (63%) were ahead in that effort.

Figure 2. Maturity of your cybersecurity program



What is the current maturity of your cybersecurity program (%)	Overall	H&LS	U.S.	Europe	ANZ
Base	***867***	***61***	***36***	***16***	***9***
Well defined enterprisewide strategy/ roadmap exists, implemented	66	60	58	63	67
Enterprisewide strategy/roadmap exists as a guideline but implementation in progress	30	38	42	38	22
Enterprisewide strategy/ roadmap is work in progress and therefore implementation and operations are ad hoc	4	2	-	-	11
No defined framework or program	0	-	-	-	-

H&LS: Health Care and Life Sciences



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-level 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

H&LS	(%)
CIO/CTO	62
Business CXO (CEO , COO , CFO , CMO , CHRO)	59
Board	36
EVP/ SVP/VP	25

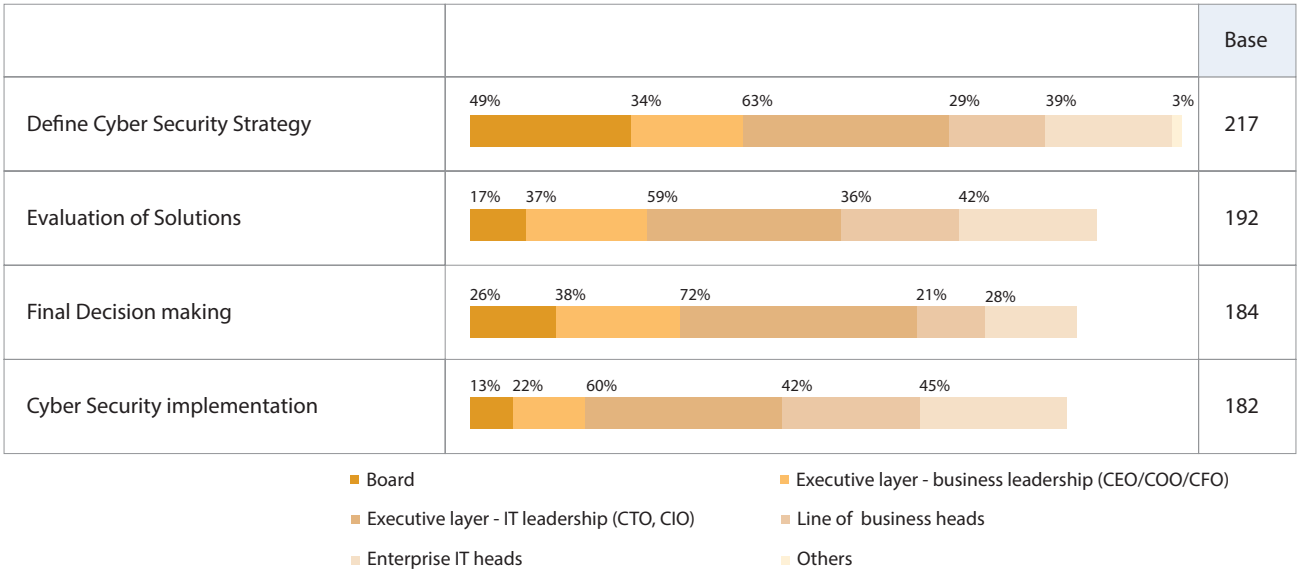
U.S.	Europe	ANZ
36	***16***	***9***
67	44	78
58	56	67
31	38	56
25	13	44

Base: 61

But the survey results show that only 36% of boards are involved in strategy discussions. Senior-level IT leaders (62%) and business leaders (59%) are more actively involved. It is likely that a focus on traditional business outcomes and inadequate understanding of cybersecurity's impact prevent greater participation from the board.

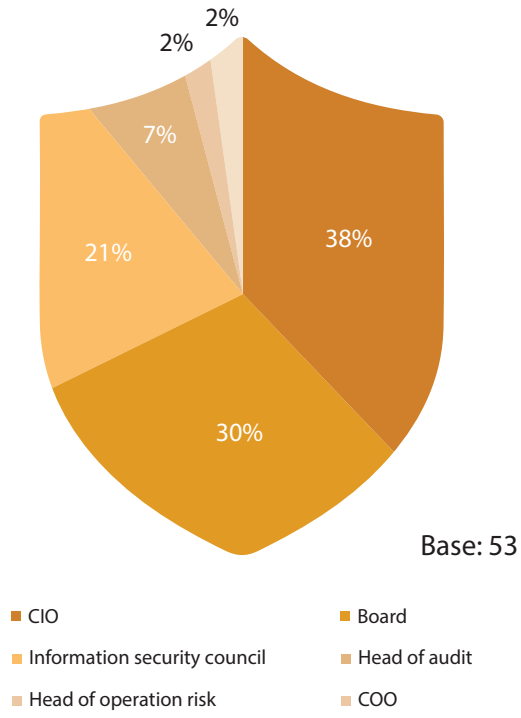
Predictably, boards contribute the most in defining the cybersecurity strategy (49%), whereas business leaders were most involved in making the final decision (38%) and evaluating solutions (37%). On the other hand, IT leaders are actively engaged through the journey.

Figure 4. Key participants in the cybersecurity journey



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

Figure 5. CISO reporting hierarchy



Where does the CISO organization (Chief Information Security Officer) report in to	Overall	H&LS	U.S.	Europe	ANZ
Base	***792***	***53***	***29***	***16***	***8***
CIO	34	38	38	38	38
Board	32	30	31	25	38
Information security council	23	21	21	25	13
Head of audit	5	8	3	13	13
COO	3	2	3	-	-
Head of operation risk	3	2	3	-	-

H&LS: Health Care and Life Sciences

The survey showed that CISOs in the H&LS industry mostly report to the chief information officer (38%). Firms in Australia and New Zealand have the highest number of CISOs reporting to the board (38%), while European respondents are the least likely to report to the board (25%).

The H&LS industry must consider increasing the influence of the CISO, given that cybersecurity is woven into an organization's digital journey.

The most pressing cyberthreats

As cybersecurity risks and threats grow exponentially in the H&LS industry, respondents are chiefly concerned about hackers and hacktivists (85%), insider threats (80%) and low awareness about security risks among employees (80%).

Figure 6. Top cybersecurity concerns

What is your number one concern regarding threats(%)	Overall	H&LS	U.S.	Europe	ANZ
Base	***867***	***61***	***36***	***16***	***9***
Hackers/hacktivists	84	85	86	81	89
Insider threats	75	80	83	81	67
Low awareness of potential security risks among employees	76	80	69	100	89
Nation states	60	77	72	88	78
Corporate espionage	75	67	78	44	67
Organized crime	67	59	53	63	78
Uneven deployment of cybersecurity solution	60	44	47	44	33

H&LS: Health Care and Life Sciences

Firms worry that hackers might steal personal consumer information, company financial data or even intellectual property. The consequences could be severe financial damage, decline in reputation, and loss of customer trust. Further, it can attract regulators that may levy stiff penalties.

The H&LS industry must also pay more attention to insider threats, whether it is employees selling confidential data to competing firms or sloppy computer security practices, such as poorly secured mobile phones and other devices.

For European firms, low employee security awareness is a unanimous cybersecurity concern (100%), while hackers topped the list in the U.S. (86%). In Australia and New Zealand, 89% of respondents cited hackers as their top concern. European companies are also worried about the role of nation-states (88%), which can cause havoc for political gains.

THE ENTERPRISE IMPERATIVES

Enterprises must always be hyperalert to effectively counter cyberthreats. The appropriate defense should have touchpoints across technology, processes, and people to address all concerns and imminent threats. Besides, cyber defense must have enterprisewide access to ensure maximum protection.

Top security solutions today

To counter threats and attacks, enterprises have deployed solutions such as encryption (68%), intrusion prevention systems (68%), identity and access management (66%) and risk and compliance (66%).

Figure 7. Cybersecurity solutions

Top solutions implemented (%)	Overall	H&LS	U.S.	Europe	ANZ
Intrusion prevention systems	64	68	69	63	78
Identity and access management	63	68	67	60	89
Cloud access security broker	63	66	74	44	78
Security awareness training	66	66	72	50	67
Risk and compliance	66	61	56	56	89
Security incident management	66	61	61	50	78
Tackling IoT security	58	59	61	44	78
Unified threat management	64	57	56	50	78
Application control on server workloads	60	57	56	50	78
Encryption	58	49	50	44	56

H&LS: Health Care and Life Sciences

In data-rich enterprises, encryption is imperative since it provides a high level of protection and effectively mitigates risk. Also, intrusion prevention systems and identity and access management solutions are key parts of a cybersecurity strategy that targets insider threats and corporate espionage.

Regulatory factors, such as Europe's General Data Protection Regulation, and customer concerns about privacy and data usage, compel H&LS companies to implement risk and compliance solutions.

Australia and New Zealand are ahead in the implementation of all solutions, while U.S. firms are most likely to use identity and access management solutions (74%).

Challenges galore

E&U industry executives said they are most challenged by the rapid changes in cyber technologies (68%), inadequate management support (65%), lack of user awareness (63%) and the difficulty of embedding cybersecurity in the enterprise IT architecture (63%).

Figure 8. Top cybersecurity challenges

(%)	Overall	H&LS	U.S.	Europe	ANZ
Base	***867***	***61***	***36***	***16***	***9***
Building a cybersecurity aware culture	65	75	83	56	78
To ensure enterprise it architecture has security embedded in it	67	67	69	75	44
Poor integration between tools and different solutions	54	66	53	81	89
Cybersecurity technology changing too fast	63	57	67	44	44
Lack of user awareness	54	54	47	56	78
Too much time spent in building technology stack and less on deriving value	57	49	47	56	44
Lack of skilled personnel	49	49	56	44	33
Inadequate management support	52	46	42	63	33
Lack of appropriate tools to automate controls and audit effectiveness	55	46	42	56	44
Lack of reporting on incidents	39	39	47	31	22

H&LS: Health Care and Life Sciences

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

U.S. firms struggle the most to build a cybersecurity aware culture (83%), while European companies (56%) were least challenged by it. On the other hand, European organizations have a harder time embedding security into enterprise IT (75%), whereas Australia and New Zealand (44%) do not consider it as significant. Respondents from Australia and New Zealand (89%) and Europe (81%) regard poor integration between tools and solutions as a high-priority issue.

Overcoming the challenges using multiple methods

A study of the responses shows that H&LS firms need to do more to overcome the challenges. The top methods employed currently are as follows: training and certifications (61%), focusing on integrated solutions over point solutions (59%), workshops (49%) and creating a culture of employee awareness (49%).

Australia and New Zealand lead in actively using multiple methods to address the challenges, while the U.S. trails in most areas.

Figure 9. Cybersecurity approaches

Cybersecurity approaches	(%)	U.S.	Europe	ANZ
		36	*16*	*9*
Training and certifications	61	58	63	67
Focus on integrated security solutions rather than point solutions	59	56	63	67
Workshops and enablement sessions	49	42	56	67
Creating a culture of employee awareness	49	56	38	44
Work with technology vendors and service integrators	46	47	31	67
Hire service provider specializing in Security solutions	34	22	56	44
Outsource security cybersecurity monitoring and management	20	17	19	33
Enable threat intelligence feeds	18	11	13	56

Base: 61

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

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

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

Focus areas — next moves

The top three focus areas where enterprises have implemented solutions are network segregation (65%), threat intelligence platform (57%), and advanced threat protection (55%).

Figure 10. Next stages of cybersecurity

Next stages of cybersecurity (%)	Implemented				
	Overall	H&LS	U.S.	Europe	ANZ
Advanced threat protection	55	61	64	50	67
Network segregation	65	55	60	38	67
Threat intelligence platform	57	54	58	38	67
Deception technologies	49	49	56	44	33
User and entity behavior analytics	48	44	56	31	22
Cloud access security broker	44	41	42	44	33
Security orchestration and automation response	46	39	42	38	33
Devsecops	46	38	41	20	56

Next stages of cybersecurity (%)	Implementing				
	Overall	H&LS	U.S.	Europe	ANZ
Advanced threat protection	31	21	19	25	22
Network segregation	25	33	29	44	33
Threat intelligence platform	27	25	25	38	-
Deception technologies	36	31	31	31	33
User and entity behavior analytics	29	34	22	50	56
Cloud access security broker	30	25	28	31	-
Security orchestration and automation response	34	41	36	38	67
Devsecops	34	33	32	40	22

H&LS: Health Care and Life Sciences

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

The U.S., Australia and New Zealand are all ahead in implementing solutions in these top three focus areas compared with respondents in Europe.

THE INFOSYS PERSPECTIVE – SCALE WITH ASSURANCE

Infosys ensures enterprises become SECURE BY DESIGN by helping them imbibe the concept of security at the very early stage of their business lifecycle. Our focus is to drive an enterprise mindset to build systems, platforms & solutions which are based on "secure by design" principles thereby ensuring that security is embedded deeply and not as an afterthought. We adopt defense-in-depth mechanism to ensure that it becomes extremely unlikely for threats to enter our client's network. We strive to provide visibility of the threats, vulnerabilities and incidents on our clients network using comprehensive dashboards while ensuring compliance with industry standards, policies and processes. We help our clients in embedding 'secure by design' at an early stage to reduce the attack surface and minimizes risks. We help organizations to build a mindset that incorporates security in everything that they do.

Infosys is committed to building a resilient cybersecurity program and drive our customers to operate at scale, while increasing operational efficiency and reducing costs. Our scalable, AI-ML based managed detection and automated incident response platform enables integrated incident monitoring and orchestration helps prevent, detect and respond to advanced cyber-attacks. With our strong team of security experts, best practices, automation, deep industry insights and actionable intelligence, commercial flexibility and frictionless delivery of operations through global cyber defense centers, we are ready to scale our customers' digital journey and amplify security, hence the promise of SECURE BY SCALE. Boosting our ability to deliver at scale and providing our customers access to the best talent, is our collaboration with Ivy League universities like Purdue, to reskill and upskill employees globally.

Infosys helps enterprises SECURE THE FUTURE by continuously adopting newer technologies and keeping pace with changing times. Our clients also have access to advanced threat-hunting capabilities, forensics, malware analysis and the latest in technology innovations incubated in the Infosys Security R&D Labs. Nurturing the culture of innovation and research to co-create solutions, deepens the value we deliver for enhanced protection against known and unknown threats. With the advent of newer technologies like Blockchain and IoT, security has become the need of the hour with enterprises seeking new age cybersecurity solutions that can help overcome enterprise security challenges. Infosys prepares enterprises for the future by catering to this need and helping them stay ahead of these threats.

Shaping cybersecurity of the future – trends to watch

The sustainable cybersecurity approach is the one that takes care of today's needs and anticipates tomorrow's requirements. Given the pace at which the business environment is changing, it would be myopic to ignore building future capabilities.

Figure 11. Cybersecurity trends

H&LS	(%)	U.S.	Europe	ANZ
		36	*16*	*9*
Artificial intelligence used for real time predictive/ preventive instances	44%	44	31	67
Behavioral analytics becomes very important in identity management	41%	42	31	56
Privacy and personal data protection gains significance	34%	39	25	33
New business models including cyber insurance emerge	33%	33	38	22
Deception technologies introduced in IoT and OT	31%	31	25	44
Move to customization of security solutions from standard solutions	30%	28	19	56
Regulatory bodies show zero tolerance on non-compliance	28%	25	38	22
Continued demand for cybersecurity skills	28%	33	25	11
Usage of blockchain technologies in developing security solutions	23%	11	50	22
Introduction of automation in implementing cybersecurity controls	20%	11	38	22
Cybersecurity startups to gain recognition	13%	17	13	-

H&LS: Health Care and Life Sciences

The survey points out that H&LS firms consider AI (44%) and behavioral analytics (41%) as the top two cybersecurity trends.

With AI, enterprises can more accurately identify threats and trigger action to prevent damage. Moreover, it can enable faster and better handling of massive volumes of data.

Standard identity management solutions operate with basic information and seldom have a holistic view of access-related risks. By collecting data from various sources on how users spend their time and adding an analytics layer, firms can generate a comprehensive picture of their customers. Behavioral analytics promises to analyze user activity and detect inconsistencies. This intelligent solution is necessary for a smarter future..

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

The H&LS industry is grappling with significant changes as it attempts to meet the high expectations of demanding customers and settle into a value-based model. Having embarked on the digital journey to handle these demands, H&LS firms with their wealth of information have become a popular target for cyberattacks. In this scenario, cybersecurity plays a vital role in protecting critical business assets and earning the trust of customers.

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

Further, cybersecurity must be an integral part of every stage of the business lifecycle. Infosys recommends that enterprises adopt security at each phase, including design and scale, to build a holistic defense.

However, this path is challenging and demands significant changes, both systemic and cultural. It requires senior leadership support, educating employees, and instituting a security-first mindset. The alternative to this path is to bear financial losses, damage to reputation, loss of customer trust, and may even lead to a threat to the business' survival.

On the other hand, an effective cybersecurity program can enable H&LS firms to focus on new value-based delivery models and provide personalized services and enhance customer engagement. 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