SECURING THE BOUNDS OF DIGITAL TRANSFORMATION

Infosys®
Navigate your next

Infosys® | Knowledge Institute


Username
Password
LOGIN

Contents

Introduction 4
Executive summary 5
Cyber-risk strategy should complement digital transformation 6
Enterprisewide strategy is important across the board 7
Confidentiality and integrity of data 8
The main challenges firms are facing 10
What do CISOs look for in vendors or service providers? 11
Conclusion 14
Survey methodology 16

Introduction

Edward Snowden, Cambridge Analytica, Huawei, the U.S. presidential election … the hearts of cyber professionals miss a beat when such buzzwords are traded around. In today's digitally connected world, no area of life is safe from the rising threat of cyberwarfare.

Back in 2015, the costs of constantly defending, securing and predicting this risk was $3 trillion. By 2021, the costs will rise to $6 trillion globally. [1]

But unless enterprises transform themselves to take advantage of digital technologies and compete in this age of the always-on, always-transacting marketplace, they will fall behind those that do.

Firms across industries need to constantly disrupt their business, investing in technologies such as prescriptive analytics, internet of things (IoT), cloud, edge computing and interconnected platforms, while securing the core and periphery of their ecosystem against threats. Many firms are heavily investing in premium security services offered as a bundle and yet are still in crisis mode.

As attackers get more sophisticated in their methods of cyberattacks, security solutions at most enterprises fall short. Often, the security landscape at incumbent firms is a hodge-podge of "point solutions," each one solving a different problem in isolation. Solution design is reactive, lagging far behind the real source of attack.

Despite all the well-publicized cybersecurity attacks over the past few years, just how seriously are firms taking cyber-risks? How many have a trusted plan in place? What are the main technologies and solutions they are employing to straighten up their security posture and ensure digital transformation runs smoothly in the next decade?

In addition, what main challenges do digital natives and incumbent firms face, how much money are they spending, and what's their appetite for partnering with external providers to secure their ecosystem from both internal and external threats? Finally, what are the expectations around these partner relationships?

To find out, Infosys commissioned research through an independent agency, between January and March 2019, with 867 senior executives and cyber CXOs taking part in the survey. Ninety percent of the respondents represented companies with at least $800 million in annual sales. Twelve industries, including the high-tech space and communications industries, were accounted for, with the respondents hailing from Australia, Europe, New Zealand and the United States.

The findings are presented in this report.

Executive summary

Fifty-three percent of the leaders say that cybersecurity is very critical to their organization, while 30% acknowledge that it is critical. Leaders from the U.S. are even more concerned, with 88% citing its use as paramount to enterprise health.

Sixty-six percent of the respondents say that their organization has implemented a well-defined, enterprisewide security strategy. Another 30% say their security implementation is in progress, with the remainder saying they have an ad-hoc plan in place.

Almost 50% of company boards are involved in cybersecurity discussions around strategy, with the business CXO emerging as the main conduit (63%). Business CXOs are even more prevalent in cyber strategy discussions in the banking, financial services and insurance (BFSI) industries.

Ensuring security embedded within IT architecture, speed of change in cybersecurity technology and lack of user awareness are the highest-ranked challenges that leaders face when implementing security in the enterprise.

Network segregation (65%), threat intelligence platforms (57%) and advanced threat protection (55%) are the most implemented security technologies.

Identity and access management and encryption are the two most popular security solutions. Intrusion prevention systems are a close third.

Enterprises demand a lot from cybersecurity service providers, including end-to-end protection, increases in business resilience, and help to improve security capabilities and response to incidents.

Cyber-risk strategy should complement digital transformation

Digital natives and disruptive incumbents across industries are doubling down on certain digital features to win big in a market where nimble upstarts are swallowing market share. These features include stellar analytics capabilities, a flexible and potent core on which to build digital technologies, and a customer- and employee-centric operating model that achieves 24/7 low latency and straight-through processing of requests from anywhere in the world.

According to our research, the top four trends related to cybersecurity are the use of artificial intelligence (AI), specifically for real-time predictive and preventive cybersecurity instances (41% name it among their top three); the rise of privacy and data regulations across the board (35%); and the use of both blockchain (33%) and deception technologies (33%) to secure transactions and the edge of the enterprise (Figure 1).

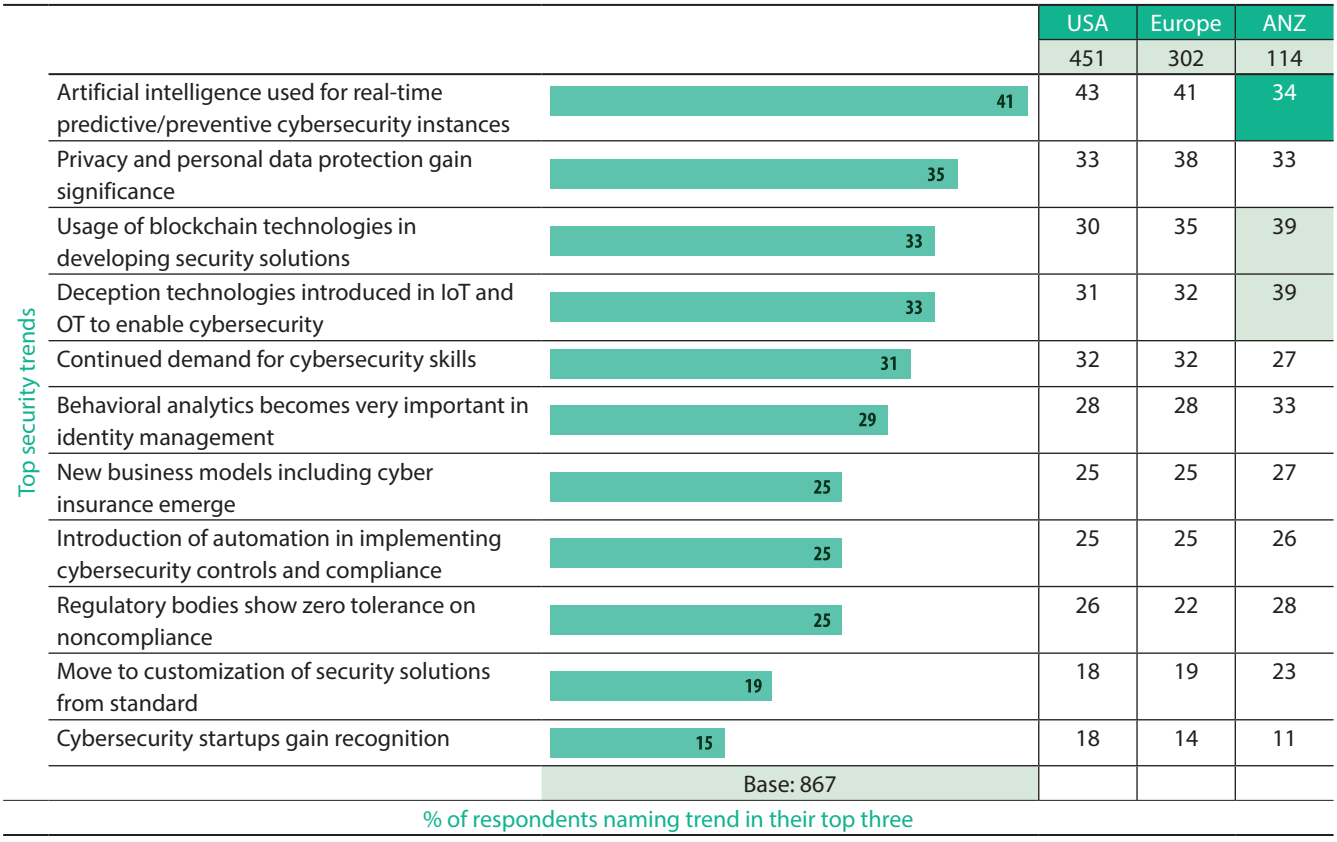
Perhaps the greatest risk to enterprises as they transform is in not taking cyber-risk seriously enough. Many of the world's top consultancies have looked into this dilemma, and the wide-reaching consensus is that securing the perimeter is seen as immensely critical in a firm's bid for survival, both to meet regulations and deter hefty fines, and to ensure that customers don't defect and go elsewhere (nowadays, consumers are not short on options; switching brands is as easy as downloading a new app).

But cyber-resilience and threat deterrence isn't just about making the firm's IT infrastructure secure by design or ensuring that customers and employees know exactly how and where data is collected. Neither is it just about understanding what enterprises do with that data.

By investing in hard-and-fast cyber technologies, while remembering that people and processes must also be aware, agile and part of the overarching cyber strategy, businesses can increase their chances of not only upholding trust, but also driving digital transformation — enhancing their brand in the process.

With this in mind, a security approach must be developed that ensures the enterprise is secure, while also allowing it to evolve. The new posture must move away from archaic network security to a vendor-savvy environment, where a flexible operating model dovetails with secure access to data and applications created at breakneck speed. In this new privacy and data-centric landscape, employees, partners and customers should be able to tap into the company resources from anywhere, anytime. Security product vendors can implement a wide variety of security mechanisms that automate diagnosis, prevention and management of data breaches.

Figure 1. Artificial intelligence, data protection, blockchain and deception technologies are the top security trends.



Source: Infosys Knowledge Institute, 2019

Enterprisewide strategy is important across the board

Cyber-risk is one of the top 10 global business risks[2], and threatens the ability of an enterprise to succeed in other endeavors, including everything from core modernization to the development of customer-centric business and operating models. Because of the possible fatal repercussions, both monetary and reputational, that come with this risk, it must not only be the concern of a chief information security officer (CISO), but it must also be top of mind in the boardroom.

Members of the board brought into these discussions must have a strong understanding of risk management, and the overall risk profile of the enterprise. This might mean bringing in security experts specifically for this purpose, though having a high-level stakeholder with a keen eye on the rest of the business strategy is not to be taken lightly. Board members — and others involved in these discussions — must flesh out the firm's appetite for risk, and put a plan in place that at once identifies, prioritizes and mitigates it. This goes for risk in general, but especially in the cyberspace, where particularly lethal malware attacks can 1) cause death in severe cases (an autonomous car crashing, for instance) and 2) raise a reputational red flag when customers stop trusting the product or service after a breach and either stop buying for a significant time period, or worse, defect to a competitor.

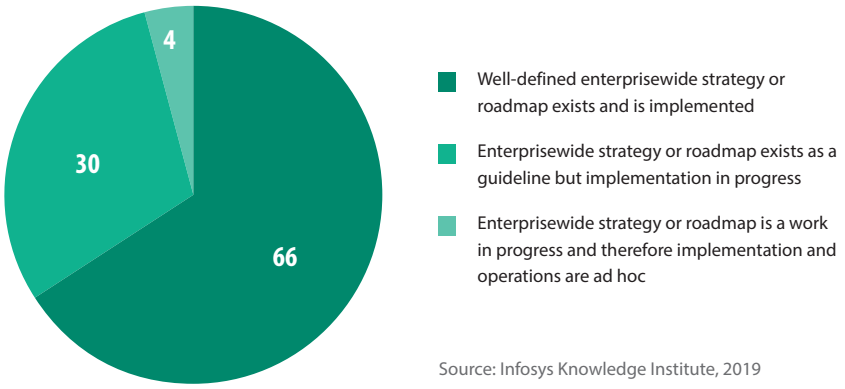
Most organizations do realize this. Of the firms surveyed in our study, 83% said that cyber-risk is viewed as mission critical in their organization, with only 1% saying that it was not critical.

Further, 100% said that, at the least, they had a plan in place to mitigate cyber-risk, with 66% saying that a trusted cybersecurity plan has been implemented in the organization, and 30% saying that implementation of a cybersecurity plan was in progress (Figure 2).

The enterprisewide strategy should include threat deterrence, a plan to circumvent corporate espionage and secure the perimeter of systems using advanced technologies, and a plan to educate the workforce on mission critical cyber-risks. With that in mind, 91% of the leaders said that their enterprise has carved out a special accountability structure for cyberwarfare and resilience, designating a CISO reporting to the board in most cases.

The CISO is tasked with implementing the end-to-end cybersecurity strategy, either by building capabilities in-house or working with a partner firm or a service provider.

Figure 2. Two-thirds of leaders say that a trusted cyber plan has been implemented, while almost a third are currently implementing an enterprisewide strategy.



Source: Infosys Knowledge Institute, 2019

Case study

24x7 monitoring and management services with Infosys Security Operations Center

One American multinational retailer was dealing with a heterogeneous IT security infrastructure managed by multiple vendors, leading to higher costs and operational inefficiencies.

The Infosys Security Operations Center (ISOC) enabled automated access provisioning, AI-driven security operations, and a common SOC monitoring solution to ensure data segregation for compliance and regulatory needs.

The retailer has seen a 99% success rate in monitoring of critical and high-severity incidents and cost reductions as a result of a scalable and affordable federated SOC.

Confidentiality and integrity of data

To combat cybercrime and make the surface of the organization resilient to cyberattacks, the organizations surveyed are investing in sophisticated technology solutions (Figure 3) such as:

- Network segregation — segregating sensitive information makes it difficult for an adversary to gain access to a firm's most sensitive data.
- Threat intelligence platforms that detect threats and alert customers to potential cyberattacks, while scouring the web to provide automatic threat intelligence in real time.
- Advanced threat protection and intrusion prevention systems.
- The use of a cloud access security broker (CASB) — a control point for visibility and management of data used and shared by SaaS applications.

With these technologies on the implementation agenda in strategic cyberdefense, firms are making gains in their war on cybercrime. Only one in eight cyberattacks caused significant disruption to enterprise assets in 2018, compared with one in three in 2017.[3]

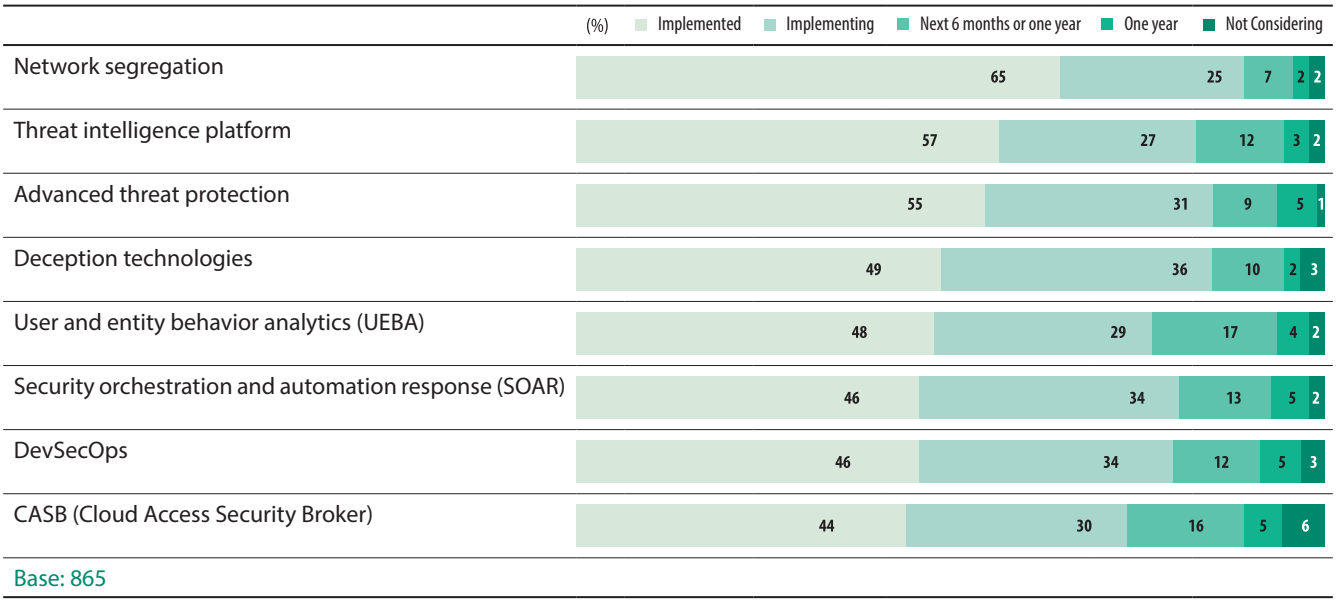
However, the battle is fierce. Threats and intrusions such as ransomware and SQL injection attacks have become commonplace and highly sophisticated in nature, causing system outages, with systems coming back online only after significant delays and reputational damage has been done. Evolved ransomware technologies, such as Cerber and Bad Rabbit, are wide-reaching strains of malicious code that have infected organizations around the world, impacting millions of users.

These malicious actors will only get more exacting, using streetwise technologies in innovative ways, exploiting weaknesses in software, hardware and edge computing, a problem made ever more prevalent with the rise of IoT. To stay secure, vigilant and resilient, firms must devise recovery plans before the event occurs, predict at which points in the system weaknesses are likely to arise, and ensure that the system has backup availability in the event of a breach.

Firms should also devise a carefully synchronized "impact analysis" process that develops a detailed plan for the graceful shutdown of mission-critical services. The decision-making criteria, key stakeholders involved and information sources to be included should be outlined, along with an estimation of the impact and cost that shutting down the system will incur. Here, the onus is on avoiding analysis paralysis by granting key strategic decision-making power to a few high-level experts who can balance reputational risk damage with the need to act fast.

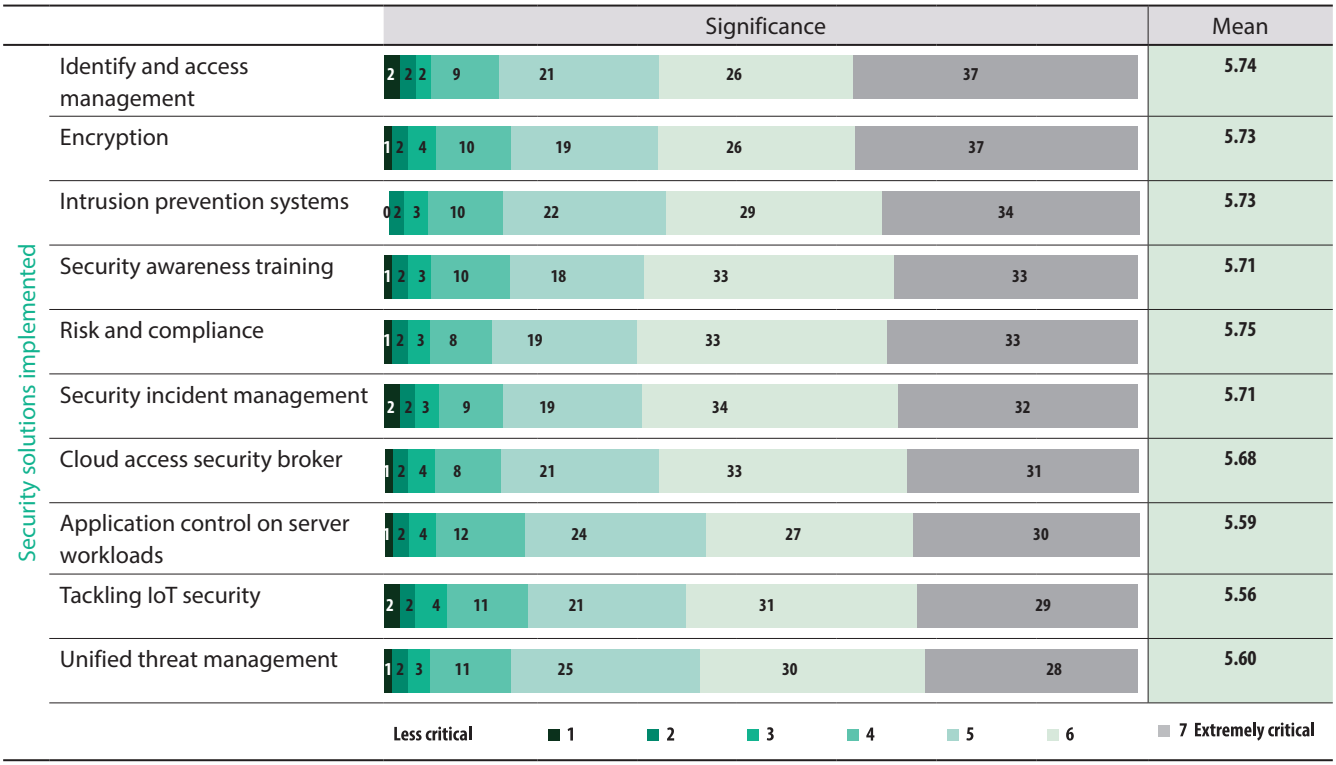
With confidentiality of data in mind, security solutions (rather than single technologies) on the agenda at enterprises include identity and access management (37% of the respondents named this as an extremely critical solution), security incident management (32% said it is extremely critical) and security awareness training (33% said it is extremely critical). The latter two solutions are quite popular in the banking and financial industry, with security incident management also finding favor in the manufacturing industry, given the high cost structures and reputational risks prevalent in these industries.

Figure 3. Network segregation, advanced threat protection and threat intelligence platform are the top implemented technology solutions.



Source: Infosys Knowledge Institute, 2019

Figure 4. Identity and access management, and encryption, are the top two security solutions implemented.



Source: Infosys Knowledge Institute, 2019

Case study

Identity and access management solution for an American financial services corporation

Onboarding clients was very time-consuming at a multinational financial services firm due to multiple provisioning systems. Data integrity was also an issue due to multiple databases and an unsatisfactory end-user experience.

Infosys worked with the client to ensure all user IDs were managed consistently across the network on one platform and adequate controls were in place for continued security and integrity of company data. This led to superior governance processes and an optimized user experience.

The new solution achieved an 80% reduction in onboarding time, reduction in infrastructure cost and improved security through a near-real-time account provisioning and de-provisioning process for users.

The main challenges firms are facing

According to our research, the top five IT security threats organizations face are:

- Hackers (84%)
- Low employee awareness on potential security risks (76%)
- Corporate espionage (75%)
- Insider threats (75%)
- Organized crime (67%)

These threats have both an external and internal element. Individual actors are getting more sophisticated as AI and the use of IoT and edge computing go mainstream. Here, perimeter protection is not enough. Malicious individuals compromise weak links in the ecosystem, and gain deep access to a firm's data, systems and networks. The threat of competitive espionage is also on the rise as monetary and political rewards increase. On the other hand, there is a growing gap between the impact these threats can actually have and the preparedness of the workforce.

Wargaming, an innovative new simulation exercise, is often used as part of a firm's incident management protocol, exposing loopholes in the security perimeter. Here, employees are immersed in a simulated cyber-risk incident, after which lessons are learned on what worked and what didn't. This exercise exposes some of the fears that employees have about taking the initiative in major breaches, clarifies roles and responsibilities across the value chain, and helps inform a culture where leaders quickly learn when a threat is at crisis level.

When the respondents were asked what challenges they faced while implementing cybersecurity in the organization, security-by-design, speed of technological change and lack of user awareness were the top-ranked frustrations of senior executives (Figure 5).

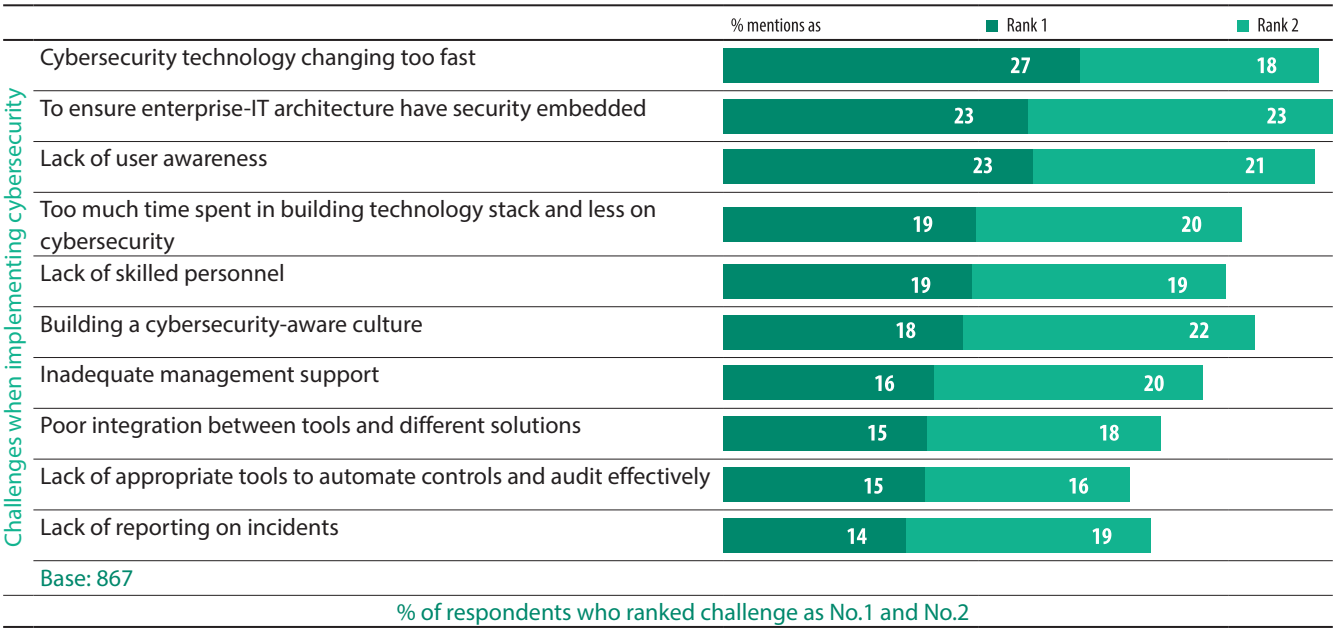
In the survey, 23% of the leaders said ensuring security-embedded enterprise-IT architecture is their No. 1 challenge, with a further 23% ranking it as No. 2. In this landscape, cyber-risks are created by connected, intelligent and autonomous systems. The focus of CISOs, and the board, should stretch outward so that security is embedded in business processes, product design and the daily work of employees as they go about their job.

Building security into products and processes should be the new normal if firms want to win the war against cyberattacks.

Organizations can tap into agile solutions and processes that harness the ingenuity and creativity of employees, rather than rely on scripted actions devised by siloed business units. This happens only when the workforce is alert and aware to security risks in the first place. In this case, decision support systems are the scaffolding that allow employees to form potent and expedient decisions. Coupled with automation, these frameworks can equip employees with the tools to sustain affected areas of the business.

For all these implementation challenges to be circumvented, the CISO should be brought into discussions well before a business opportunity has been devised by top management. Future risks and needs are to be factored in by stakeholders when allocating money for cybersecurity, not only to placate regulators but also as a boon to digital transformation initiatives. According to a recent cybersecurity report, CISOs from organizations that invest in future needs are more likely to confer with business leaders on strategic topics such as protecting newly adopted technologies, incorporating cybersecurity into new business initiatives, and investing in security-related data and insights.[4]

Figure 5. Security-by-design, a fast-changing technological security landscape and lack of user awareness were the top-ranked challenges when implementing cybersecurity.



Source: Infosys Knowledge Institute, 2019

What do CISOs look for in vendors or service providers?

The cybersecurity talent crunch

While the CISO is growing in importance, information security councils are set up and boards are ever more vigilant around confidentiality and security of company data — there is a dearth of talent in the cyberspace. This, even when companies are investing more in cybersecurity than ever before. According to our survey, companies are using between 4% and 12% of their IT budget for dedicated cybersecurity initiatives and programs, with an average of 8% across industries. The number was even higher in the communications and telecom space, spending an average of 1.55% more than transport and logistics companies (Figure 6).

This may seem small, but when you consider that cyber resilience used to be an afterthought, with experts largely absent when business units developed new products, services and processes, the numbers are significant.

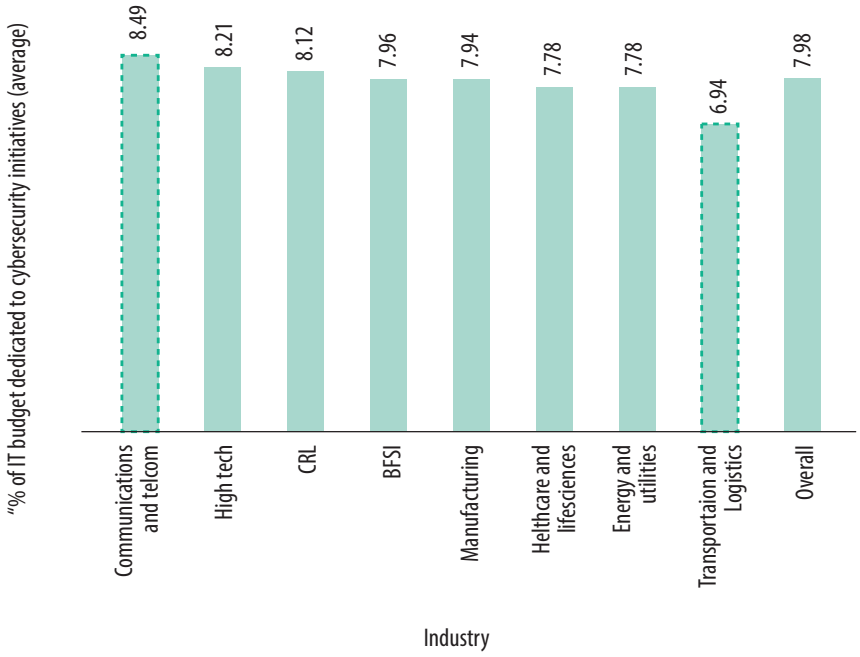
The critical challenge for the CISOs is to work closely with business units to ensure growth initiatives envisioned by top leadership don't collapse through lack of capable employees. In our research, one in three CISOs is committed to increase investment both in the underlying cyber technologies and the people element, with over half having a growth plan in place for extending their cyber teams.

According to the CyberSeek jobs tool[5], as of August 2018, 313,000 cybersecurity roles in the U.S. remained open.

Another report projects this number to exceed 1.8 million by 2022, underscoring just how far organizations and universities need to go to close the gap.[6] They can do this through "upskilling" the workforce (hands-on experience is even more sought after than standard security certifications and traditional degrees), paying higher salaries and/or hiring outside the box.

Another way for enterprises to get out of this conundrum is to partner with service providers or vendors that can help not only with external-facing cyberthreats but also with the culture within the firm itself. When asked what their expectations were from vendors or service providers, 55% of the senior executives said that the ability of the third party to help secure and grow the business confidently was either critical or extremely critical (Figure 7).

Figure 6. Average spend on cybersecurity is 8% of overall budget, though the numbers were higher in communications and telecom and lower in transportation and logistics.



Source: Infosys Knowledge Institute, 2019

Figure 7. End-to-end cybersecurity and protection and managing cyber capabilities are the key asks from a service provider.

Source: Infosys Knowledge Institute, 2019

A good partner increases cybersecurity — the cyber-risk strategy dovetailing with the increasing threat landscape of emerging technologies — and makes an enterprise more vigilant, monitoring systems, people, applications and the external environment to increase incident detection. Additionally, the right partnership improves the working culture of the organization to become more prepared, addressing cyber incidents as they escalate. This reduces the downtime and the risk of exposure to further incidents, ensuring that monetary and reputational liabilities are kept to a minimum.

Premium security services

Security as a service, a bundled offering, facilitates CISOs in their integration of their plans with the enterprise so that they can focus on delivering the bottom line while, at the same time, building customers' trust. These services often bring the advantages of the best-of-breed partnerships, domain expertise, deep industry insights and commercial flexibility for navigating the digital journey with more assurance.

These partners increasingly share information about the threats and cyber-risks that proliferate across industries, as well as best measures to combat them. Sharing this threat information and security intelligence enables firms to devise end-to-end cybersecurity and protection strategies (67% said this was either a critical or highly critical expectation from a service provider) along with keeping a more critical eye on business resilience.

Along with their expectations from service providers, the leaders in our research were asked which areas of their business were most ripe for vendor support (Figure 8).

Thirty-five percent of the respondents said that partners had high involvement maintaining and upgrading existing cyber controls. Firms also saw high partner involvement in formulating the cyber strategy and assistance in choosing the right technologies and tools for cyber initiatives (both 33%). In the wealth management space, partners are used by incumbents to onboard clients and remain compliant through the use of AI and robotic process automation. In the manufacturing industry, AI is increasingly used to standardize and streamline a wide array of business processes both in the front and back offices.

Use cases for bundled offerings also include incident management, secure access for digitally connected vehicles and data encryption. The choice of service provider ultimately comes down to what the firm's risk tolerance is and how much they have to spend, along with how well the vendor can ascertain and transform the enterprise security footprint. Does the vendor have a platform-based shared services delivery model? Is the prepackaged or bundled offering available via a subscription-based model? Is an automated incident response system for early detection and remediation in place? Companies with a wide geographic footprint should also ascertain whether the partner can serve them through a local or near-shore hub in different locations.

Selecting the right partner, offering premium services or not, should be done with caution. According to a recent study, only 7% of the consumer products companies conduct third-party risk assessments on a quarterly basis, and just 40% do so twice a year.[7] Without these assessments, firms are opening their door to an ecosystem that might be riddled with vulnerabilities.

Figure 8. Maintaining and upgrading cyber controls, formulating strategy and assistance in choosing technologies are the main areas for vendor support.

Source: Infosys Knowledge Institute, 2019

Case study

Security "as a service" solution at a beverage manufacturer

For incumbent organizations, security as a service eliminates operational overheads and reduces the costs that go into overseeing a portfolio of point solutions. The Infosys Cybersecurity platform is one such integrated offering. With AI-driven automation at its core, the platform helps transition clients from fragmented, reactive security architectures to a managed-security services model guided by a customized strategy.

A beverage manufacturer used the platform to bring together an optimized tool suite, and leveraged its predictive technologies to defend against advanced threats. The platform also provides 24/7 security monitoring along with identity and access management services for the company's more than 40,000 users and over 500 applications.

Conclusion

By 2021, there will be 3.5 million cyber job openings globally.[8] NASSCOM forecasts that this demand will grow greater as cyberattacks become more sophisticated in nature, culling $6 trillion off global GDP by 2021.[9]

Segregating sensitive information, automatic threat intelligence platforms and intrusion prevention systems are some ways firms in our research are fighting back. More vulnerable firms are also devising synchronized "impact analysis" processes for the shutdown of mission critical services in the event of a breach. Identity and access management solutions are also used to improve security through near real-time account provisioning, ensuring that bots don't compromise company data.

Firms also need to link security to their business strategy, a theme we have explored in this paper. Two-thirds of the respondents said that they have implemented a well-defined, enterprise wide strategy to meet this requirement, with 30% saying a plan is in progress. This is encouraging news. So too is the fact that 91% of executives said that their enterprise has carved out a special accountability structure for cyberwarfare and resilience, designating a CISO reporting to the board in most cases.

It is also telling that organizations are looking for end-to-end security solutions from service providers.

By articulating where the gaps are across people, processes and technology, a solid partner can help implement a concrete strategy that gets board approval.

Using premium security services is another option that leverages best-of-breed partnerships, domain expertise and commercial flexibility.

How to defend the perimeter from internal and external threats and organized crime can only be answered once appetite for risk and money-to-spend has been determined. Firms in telecom and media are spending the most on cyber resilience, with transport and logistics trailing further behind. Even in these more immature industries, end-customers must now take center stage, with products and services made secure by design.

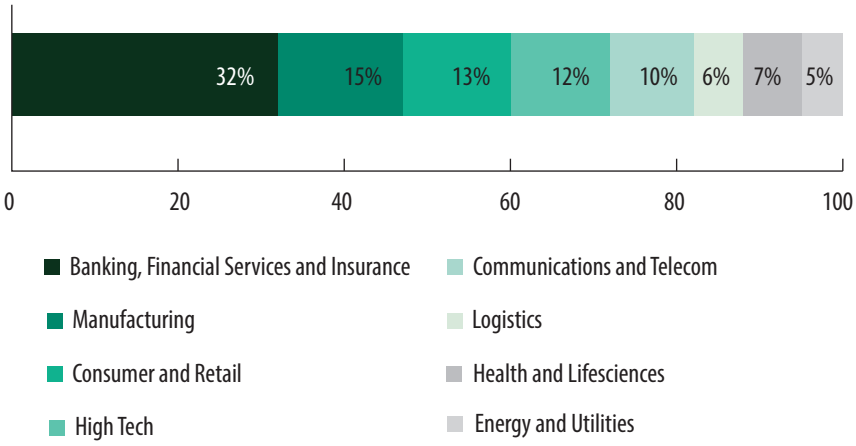
Stronger teams, better technology, clearer policies and trustworthy security vendors that gain a bird's-eye view of the entire enterprise ecosystem will speed this transformation, fueling the fire for further digital innovation.

References

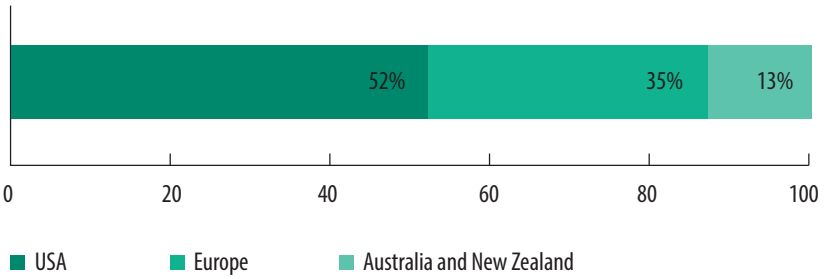
1. 2019 Official Annual Cybercrime Report, Cybersecurity Ventures
2. Global risk management report 2019, Forbes/AON
3. State of Cyber Resilience Report 2018, Accenture
4. Ibid
5. CyberSeek Jobs Tool
6. Center for Cyber Safety and Education Report, Booz/Allen/Hamilton
7. Cyber Risk in Consumer Business Report, Deloitte
8. 2019 Official Annual Cybercrime Report, Cybersecurity Ventures
9. Ibid

Survey methodology

Between January and March 2019, Infosys commissioned an independent market research firm to conduct an online survey that attracted responses from 867 senior executives and leaders involved in cybersecurity initiatives of companies with annual sales of at least US$500 million. Respondents represented multiple industries and hailed from Australia, Europe, New Zealand and the United States.



Coverage by industry



Coverage by region

Authors

Vishal Salvi
CISO & Head of Delivery Cyber Practice – Infosys
vishal.salvi@infosys.com

Harry Keir Hughes
Senior Consultant – Infosys Knowledge Institute
harrykeir.hughes@infosys.com

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

Notes

For more information, contact askus@infosys.com

Navigate your next