Infosys®
Navigate your next

# ASSURING DIGITAL-TRUST

## CONSUMER PACKAGED GOODS AND RETAIL INDUSTRY VIEW

Infosys® | Knowledge Institute

# Table of Contents


# INTRODUCTION

The consumer packaged goods and retail (CPG&R) industry has undergone a metamorphosis in the past decade. Power is shifting toward savvy customers and away from brick-and-mortar stores to online outlets. The CPG&R industry must now deal with omnichannel sales and fickle customers as well as, the usual business pressures to grow revenue and margins.

Digital technology assumes a crucial role in this new playing field and can help enhance customer experience and drive better business outcomes. 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 CPG&R companies to compete in an increasingly complex marketplace.

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

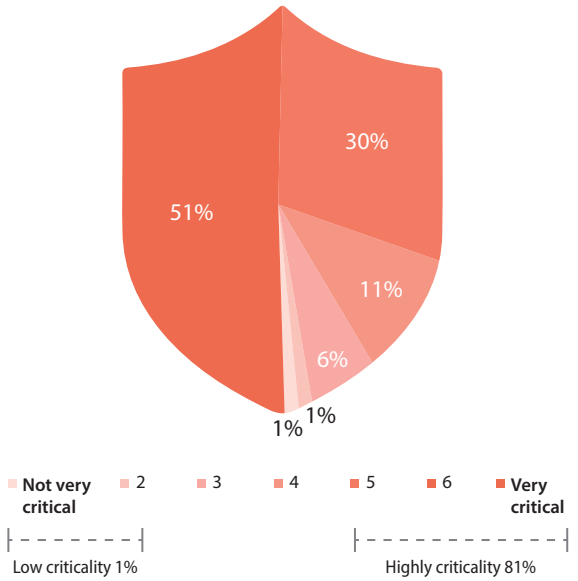
To investigate this issue further, Infosys commissioned a study of 113 senior-level executives from CPG&R organizations with revenues of over $500 million and located across the U.S., Europe, Australia and New Zealand (ANZ). The study's objective is to understand the industry's challenges, solutions and plans for the future and also to present a holistic view of the cybersecurity landscape.

# DIVING INTO CYBERSECURITY

Data-driven technology and the accelerated transition to electronic payments have created mountains of sensitive data in the CPG&R industry. That valuable information, which resides in the supply chain, point-of-sale terminals and other locations, has become an irresistible target for cybercriminals. Given the clear need for a robust cyber defense program, how critically are enterprises viewing cybersecurity?

According to the Infosys study, 81% regard cybersecurity as highly critical to their organizations. U.S. respondents were the most serious about cybersecurity, at 96%, while Europe was far behind, at 68%.

**Figure 1. How do organizations view cybersecurity?**

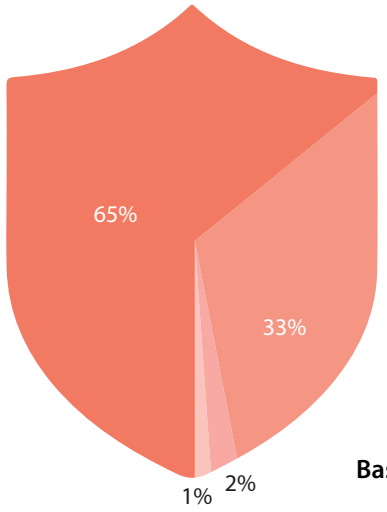



| Criticality | Overall | CPG&R | U.S. | Europe | ANZ |
|---|---|---|---|---|---|
| ***Base*** | ***867*** | ***113*** | ***45*** | ***44*** | ***24*** |
| High criticality (%) | 83 | 81 | 96 | 68 | 79 |
| Low criticality (%) | 1 | 1 | - | 2 | 0 |

**CPG&R:** Consumer Packaged Goods and Retail

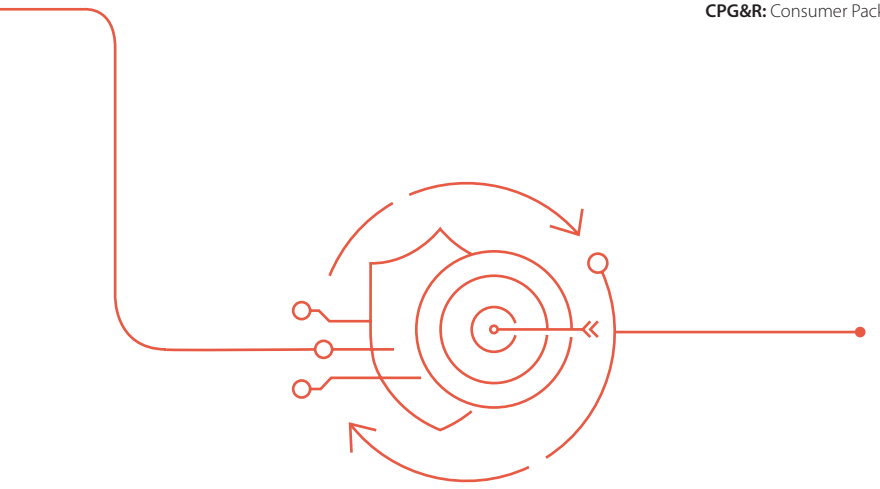
The Infosys study found that 98% have implemented or are implementing a well-defined enterprisewide strategy. Again, U.S. companies led the way with at 76% having completed implementation.

**Figure 2. Maturity of your cybersecurity program**




| What is the current maturity of your Cybersecurity program (%) | Overall | CPG&R | U.S. | Europe | ANZ |
|---|---|---|---|---|---|
| ***Base*** | ***867*** | ***113*** | ***45*** | ***44*** | ***24*** |
| Well defined enterprisewide strategy/ roadmap exists, implemented | 66 | 65 | 76 | 57 | 58 |
| Enterprisewide strategy/roadmap exists as a guideline but implementation in progress | 30 | 33 | 24 | 39 | 38 |
| Enterprisewide strategy/ roadmap is work in progress and therefore implementation and operations are ad hoc | 4 | 2 | - | 2 | 4 |
| No defined framework or program | 0 | 1 | - | 2 | - |

**CPG&R:** Consumer Packaged Goods and Retail



# 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. These initiatives can also benefit from the varied experiences of board members and senior leaders.

**Figure 3. Organizational levels that are discussing cybersecurity**

| CPG&R | (%) |
|---|---|
| CIO/CTO | 62 |
| Business CXO (CEO , COO , CFO , CMO , CHRO) | 56 |
| Board level | 50 |
| EVP/ SVP/ VP | 21 |

| U.S. | Europe | ANZ |
|---|---|---|
| ***45*** | ***44*** | ***24*** |
| 69 | 64 | 46 |
| 58 | 57 | 50 |
| 51 | 39 | 71 |
| 29 | 16 | 17 |

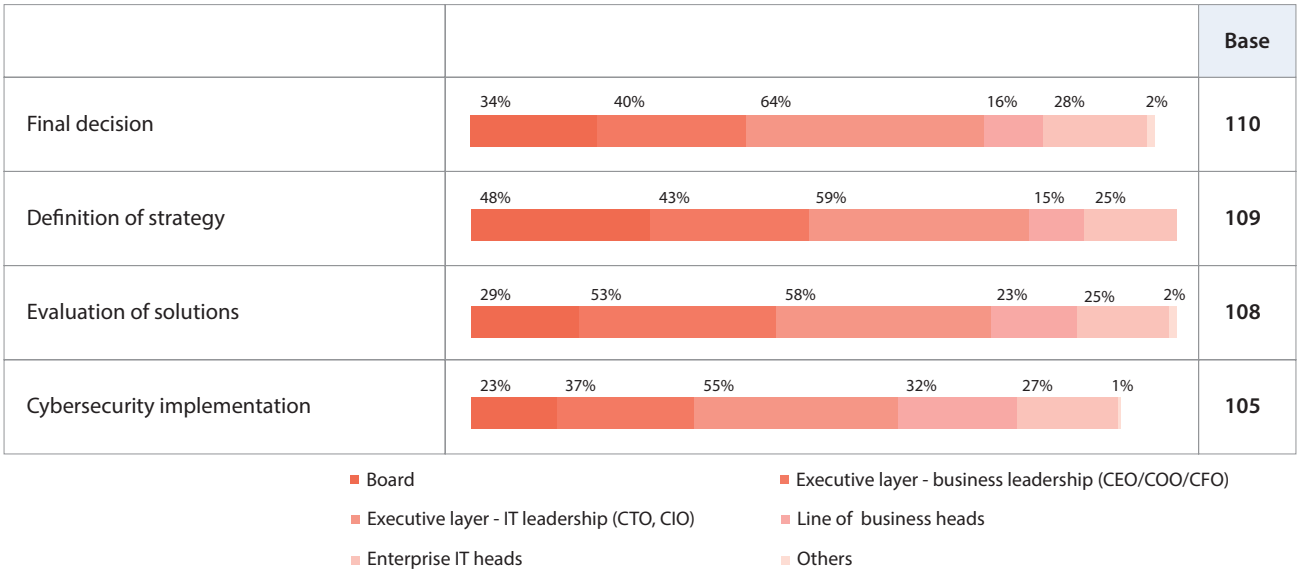
**Base: 113**

Respondents said the board (50%) and business leaders (62%) are actively involved in setting the cybersecurity strategy. In Australia and New Zealand, 71% of the boards are engaged in the cybersecurity program. European companies trailed, with only 39% of the boards involved.

However, both U.S. (58%) and European (57%) business leaders are actively engaged.

Predictably, the boards' most significant contribution is defining the strategy (48%), while IT leaders stay engaged through the cybersecurity lifecycle.

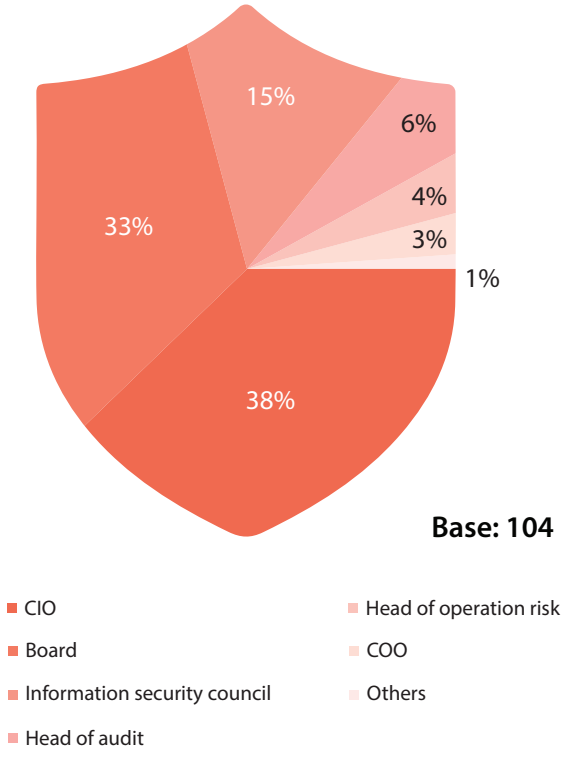
## Figure 4. Key participants in the cybersecurity journey




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

Among CPG&R firms, the survey showed that 38% of CISOs report to the chief information officer (CIO), while the proportion of CISOs reporting to the board trailed, at 33%. Respondents from Australia and New Zealand had the highest number of CISOs reporting to the board, at 48%. Europe had the highest number of CISOs reporting to the CIO (48%).

## Figure 5. CISO reporting hierarchy




| Where does the CISO organization report in to (%) | Overall | CPG&R | U.S. | Europe | ANZ |
|---|---|---|---|---|---|
| ***Base*** | ***792*** | ***104*** | ***41*** | ***42*** | ***21*** |
| CIO | 34 | 38 | 37 | 48 | 24 |
| Board | 32 | 33 | 27 | 31 | 48 |
| Information security council | 23 | 15 | 17 | 7 | 29 |
| Head of audit | 5 | 6 | 2 | 12 | - |
| Head of operation risk | 3 | 4 | 10 | - | - |
| COO | 3 | 3 | 5 | 2 | - |
| Others | 1 | 1 | 2 | - | - |

**CPG&R:** Consumer Packaged Goods and Retail

CPG&R firms must consider increasing the influence of the CISO given that cybersecurity is woven into an organization's digital journey.

# The most pressing cyberthreats

A rising wave of cybercrimes has the CPG&R industry concerned chiefly about hackers and hacktivists (83%), corporate espionage (81%) and insider threats (74%).

**Figure 6. Top cybersecurity concerns**

| What is your number one concern regarding threats(%) | Overall | CPG&R | U.S. | Europe | ANZ |
|---|---|---|---|---|---|
| ***Base*** | ***867*** | ***113*** | ***45*** | ***44*** | ***24*** |
| Hackers/hacktivists | 84 | 83 | 82 | 77 | 96 |
| Corporate espionage | 75 | 81 | 89 | 77 | 75 |
| Insider threats | 75 | 74 | 76 | 75 | 71 |
| Low awareness on potential risks of security incidents among employees | 76 | 74 | 82 | 70 | 67 |
| Organized crime | 67 | 69 | 58 | 77 | 75 |
| Nation-states | 60 | 58 | 56 | 61 | 54 |
| Uneven deployment of cybersecurity solution | 60 | 58 | 56 | 57 | 63 |

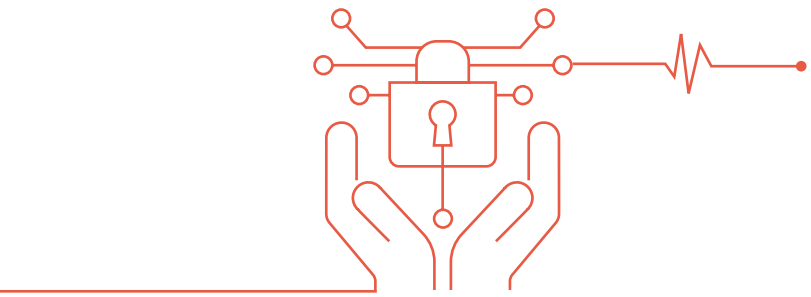
**CPG&R:** Consumer Packaged Goods and Retail

The CPG&R industry maintains vast stores of confidential information, such as payment data and personal information, that could facilitate identity theft. Hackers stand to benefit greatly if they can access that data through malware, exploiting vulnerabilities in IoT devices, or other means. This explains the recent waves of attacks on leading CPG&R companies.

Also, competition is brutal in the CPG&R industry, which incentivizes another type of criminal behavior: corporate espionage. And high employee turnover and frequent use of seasonal workers make the industry vulnerable to internal attacks.

Almost all respondents from Australia and New Zealand were highly concerned about hackers (96%) and U.S. executives were most worried about corporate espionage (89%). European respondents also expressed concerns about organized crime (77%).

It's clear that enterprises face serious challenges as they seek to address multiple concerns that threaten their business interests.



# 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. Cyber defense must also have enterprisewide access to ensure maximum protection.

## Top security solutions today

To counter threats and attacks, enterprises have resorted to security awareness training (68%), security incident management solutions (66%) and risk and compliance solutions (63%).

Security awareness training is an effective way to educate employees and minimize employee-led incidents. Security incident management solutions help enterprises identify, analyze and quickly manage breaches to prevent damage. With the advent of the European Union's General Data Protection Regulation, CPG&R firms must protect consumer data or face stiff penalties of up to 4% of their annual revenue.

The U.S. was well ahead of the other two regions in implementing a host of solutions to contain damage, whereas Europe trails.

**Figure 7. Cybersecurity solutions**

| Top solutions implemented (%) | Overall | CPG&R | U.S. | Europe | ANZ |
|---|---|---|---|---|---|
| Security awareness training | 66 | 68 | 84 | 55 | 64 |
| Security incident management | 66 | 66 | 80 | 55 | 63 |
| Risk and compliance | 66 | 63 | 84 | 45 | 54 |
| Cloud access security broker | 64 | 62 | 70 | 50 | 67 |
| Identity and access management | 63 | 61 | 80 | 43 | 58 |
| Encryption | 64 | 59 | 69 | 45 | 67 |
| Intrusion prevention systems | 63 | 58 | 76 | 45 | 46 |
| Tackling IoT security | 60 | 57 | 73 | 43 | 52 |
| Unified threat management | 58 | 56 | 76 | 36 | 54 |
| Application control on server workloads | 58 | 54 | 71 | 40 | 50 |

**CPG&R:** Consumer Packaged Goods and Retail

# Challenges galore

The top three problems that enterprises face are embedding security in the enterprise IT architecture (73%), building a security-first culture (72%) and keeping pace with fast-changing cyber technologies (64%).

**Figure 8. Top cybersecurity challenges**

| Challenges that you face while implementing cybersecurity (%) | Overall | CPG&R | U.S. | Europe | ANZ |
|---|---|---|---|---|---|
| ***Base*** | ***867*** | ***113*** | ***45*** | ***44*** | ***24*** |
| To ensure enterprise it architecture has security embedded in it | 67 | 73 | 67[2] | 82[1] | 67[2] |
| Building a cybersecurity aware culture | 65 | 72 | 76[1] | 64[3] | 79[1] |
| Cybersecurity technology changing too fast | 63 | 64 | 67[2] | 64[3] | 58 |
| Lack of user awareness | 54 | 63 | 62[3] | 66[2] | 58 |
| Poor integration between tools and different solutions | 54 | 63 | 62[3] | 61 | 67[2] |
| Inadequate management support | 52 | 58 | 58 | 57 | 63[3] |
| Lack of appropriate tools to automate controls and audit effectiveness | 55 | 58 | 67[2] | 55 | 46 |
| Too much time spent in building technology stack and less on deriving value | 57 | 57 | 56 | 57 | 58 |
| Lack of skilled personnel | 49 | 48 | 47 | 50 | 46 |
| Lack of reporting on incidents | 39 | 33 | 40 | 32 | 21 |

**CPG&R:** Consumer Packaged Goods and Retail

It's no longer enough to protect the perimeter. Efforts must start at the design stage, especially as the enterprise becomes more connected. However, well-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.

Safeguarding against damage caused inadvertently by unaware employees, as well as those with malicious intent, should be a top priority. Insider threats can pose a higher risk than external attacks because employees have easier access to confidential information. However, building a cybersecurity aware culture is not easy; it involves changing both mindsets and processes.

Rapid evolution in digital technologies must be met with corresponding modifications to the cybersecurity approach. However, this is a demanding task, especially given the pace of change and the advanced skills sets required.

European firms (82%) are at the forefront of embedding security in enterprise IT architecture. Australia and New Zealand (79%) and the U.S. (76%)were ahead in their attempts to build a cybersecurity aware culture.

# Overcoming the challenges using multiple methods

Analyzing the responses, it appears that CPG&R firms overall have invested little in overcoming these cybersecurity challenges. The top solutions are as follows: working with technology vendors and service providers (56%), training and certification (50%) and workshops and enablement sessions (48%).

The U.S. was most active in conducting workshops and enablement sessions (67%), while Australia and New Zealand focused more on training and certifications (58%).

**Figure 9. Cybersecurity approaches**

| Cybersecurity approaches | (%) | U.S. | Europe | ANZ |
|---|---|---|---|---|
| | | *45* | *44* | *24* |
| Work with technology vendors and service integrators | 56 | 58 | 57 | 50 |
| Training and certifications | 50 | 44 | 50 | 58 |
| Workshops and enablement sessions | 48 | 67 | 36 | 33 |
| Focus on integrated security solutions rather than point sol | 46 | 49 | 43 | 46 |
| Creating a culture of employee awareness | 46 | 42 | 39 | 67 |
| Hire service provider specializing in security solutions | 40 | 51 | 36 | 25 |
| Outsource security cybersecurity monitoring and management | 29 | 31 | 25 | 33 |
| Enable threat intelligence feeds | 21 | 20 | 20 | 25 |

**Base: 113**

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.

# Focus areas – next moves

CPG&R firms 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 advanced threat protection.

Network segregation can provide better security to sensitive data and drastically reduce damage inflicted through attacks by restricting the breach. Threat intelligence platforms signal the intent to counter advanced attacks since they can predict and identify danger in advance and prevent damage even before it occurs. Advanced threat protection solutions help guard sensitive data by providing real-time visibility and contextual alerts, thereby detecting trouble early and enabling swift responses.

Companies in the U.S., Australia and New Zealand have been quick to implement solutions in these top three focus areas.

**Figure 10. Next stages of cybersecurity**

| Next stages of cybersecurity (%) | Implemented | | | | |
|---|---|---|---|---|---|
| | Overall | CPG&R | U.S. | Europe | ANZ |
| Network segregation | 65 | 64 | 78 | 41 | 79 |
| Threat intelligence platform | 57 | 60 | 71 | 45 | 67 |
| Advanced threat protection | 55 | 58 | 58 | 52 | 71 |
| Security orchestration and automation response | 46 | 54 | 49 | 48 | 75 |
| Deception technologies | 49 | 50 | 53 | 43 | 54 |
| DevSecOps | 46 | 46 | 47 | 37 | 61 |
| User and entity behavior analytics | 48 | 42 | 49 | 30 | 50 |
| Cloud Access Security Broker | 44 | 40 | 52 | 27 | 42 |

| Next stages of cybersecurity (%) | Implementing | | | | |
|---|---|---|---|---|---|
| | Overall | CPG&R | U.S. | Europe | ANZ |
| Network segregation | 25 | 23 | 16 | 36 | 13 |
| Threat intelligence platform | 27 | 24 | 20 | 34 | 13 |
| Advanced threat protection | 55 | 58 | 58 | 52 | 71 |
| Security orchestration and automation response | 34 | 28 | 42 | 25 | 8 |
| Deception technologies | 36 | 31 | 40 | 25 | 25 |
| DevSecOps | 34 | 32 | 36 | 35 | 17 |
| User and entity behavior analytics | 29 | 33 | 36 | 39 | 17 |
| Cloud Access Security Broker | 30 | 31 | 27 | 41 | 21 |

**CPG&R:** Consumer Packaged Goods and Retail

# 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 |
|---|---|---|---|---|
| | | *45* | *44* | *24* |
| Artificial intelligence used for real time predictive/ preventive | 46% | 56 | 48 | 25 |
| Usage of blockchain technologies in developing security solutions | 43% | 44 | 41 | 46 |
| Behavioral analytics becomes very important in identity management | 33% | 33 | 25 | 46 |
| Privacy and personal data protection gains significance | 30% | 31 | 39 | 13 |
| Deception technologies introduced in IoT and OT to enable cybersecurity | 30% | 29 | 27 | 38 |
| New business models including cyber insurance emerge | 28% | 36 | 25 | 21 |
| Introduction of automation in implementing Cybersecurity controls and compliance | 25% | 24 | 20 | 33 |
| Continued demand for cybersecurity skills | 25% | 24 | 27 | 21 |
| Regulatory bodies show zero tolerance on non-compliance | 24% | 27 | 20 | 25 |
| Move to customization of security solutions from standard solutions | 14% | 13 | 9 | 25 |
| Cybersecurity startups to gain recognition | 12% | 9 | 16 | 8 |

**CPG&R:** Consumer Packaged Goods and Retail

The survey points out that CPG&R firms consider artificial intelligence and blockchain technologies as the top two approaches.

Enterprises can use artificial intelligence to help accurately identify threats and trigger action to prevent damage.

Moreover, it can help manage and prioritize the massive volumes of point-of-sale data faster and better.

Blockchain's inherently secure nature and distributed ledger technology make it another top option to boost cybersecurity programs.

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

The CPG&R industry is in the throes of significant and exciting change as companies embrace omnichannel and technology-led interactions to deliver personalized and fulfilling experiences to demanding consumers. In this scenario, cybersecurity plays a vital role in protecting critical business assets and earning the trust of customers. This trust will go a long way in retaining CPG&R customers who are quick to switch brands.

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 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 CPG&R businesses to respond more agilely to market feedback and deliver customer-relevant solutions to the market in quick time. 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