Prioritizing Security for Success: Analyzing Organizational Security Structures

Insight report produced by Accenture in collaboration with The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC)

February 2024

accenture

RETAIL & HOSPITALITY ISAC

Contents

Introduction

In the bustling realm of today's digital landscape, where data reigns supreme and cyber threats loom ever larger, safeguarding sensitive information has become an imperative for organizations worldwide. Amid this backdrop, Accenture in partnership with RH-ISAC, embarked on a research exercise, delving into the cybersecurity organizational structures by analyzing the Security Organograms of 66 companies across the Consumer Goods & Services (CG&S), Retail, and Travel & Hospitality industries (See "About the Research" for more information on our approach and methodology). Our goal: to understand how these companies are organized from a security standpoint and discern the security functions that they prioritize amidst the evolving threat landscape.

The top leadership is fully aware of the threats to their business from cyberattacks. Yet, our recently published research - The Cyber-Resilient CEO - shows most lack confidence in their organization's ability to avert or minimize such attacks[1]. They learn how to be cyber-resilient only after their organization experiences a breach. Within this landscape, organizational structure emerges as the backbone of cybersecurity efforts, dictating how resources are allocated, strategies devised, and risks managed. Since the digital world connects everything, ensuring its security is essential, as digital exposure and vulnerabilities continues to expand.

Picture a vast network of interconnected entities, each bearing the weight of immense responsibility in protecting their digital assets from malicious actors. This **Cybersecurity Organogram Analysis dives** into the organizational intricacies of cybersecurity functions, highlighting key functions that are paramount. First, prioritizing cybersecurity involves integrating it into organizational strategy and culture, requiring a clear understanding of risks and their potential business impact. This also highlights the importance of leadership endorsement in securing adequate resources and support for cybersecurity initiatives. Second, optimizing efficiency becomes possible by uncovering organizational inefficiencies or bottlenecks, enabling companies to streamline processes,

allocate resources effectively and enhance operational efficiency. Third, examination of cybersecurity organizational layouts aids in identifying and mitigating potential security risks, allowing proactive measures to address vulnerabilities and shield against cyber threats.

Moreover, analysis of cybersecurity team structures enables informed decisions regarding resource allocation, including staffing levels, required skill sets, and necessary technologies to combat current and emerging threats. The comparative analysis of cybersecurity structures across industries provide valuable benchmarks and insights into best practices, empowering organizations to adopt proven strategies and bolster their cybersecurity posture. We believe, a clear understanding of cybersecurity organizational structures facilitates seamless communication and collaboration within the cybersecurity team and across other departments, instrumental in mounting effective responses to security incidents and implementing robust security measures across organization.

In our findings, several key messages emerge. Firstly, there is a notable opportunity for senior leadership, including CEOs, to be more directly involved in cybersecurity, as the majority of reporting lines lead to the CIO. Secondly, while companies prioritize Cyber Protection functions, there is a significant gap in attention given to Cyber Resilience and Cyber-Physical security. Moreover, Cyber Strategy focus predominantly revolves around regulatory and compliance aspects. Thirdly, majority of organizations are not adequately organized to address challenges arising out of emerging trends such as GenAI. Lastly, higher-performing companies exhibit a more mature focus on cybersecurity, emphasizing the importance of strategic security practices in achieving excellence.

In the pages that follow, we invite you to read through the analysis that delves into the very essence of cybersecurity preparedness. Together, let us unravel the intricacies of cybersecurity organizational structures, uncover hidden vulnerabilities, and pave the way for a future where organizations stand resilient against the ever-present tide of cyber threats.

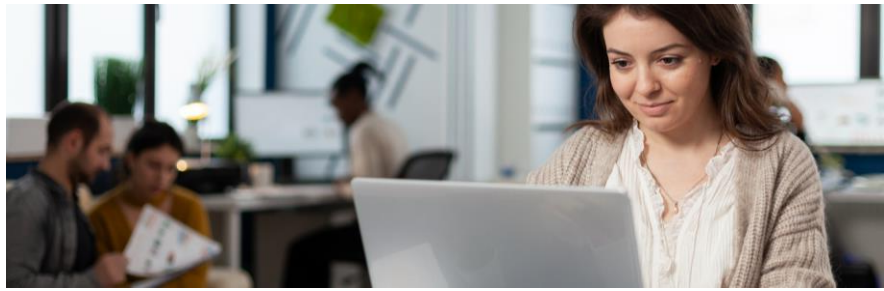
"Cybersecurity excellence is achieved not by chance but by deliberate design – a well-thought-out structure that is proactive, adaptive, and resilient."

Key Findings: Security Structure Priorities

The following section presents the key findings from our analysis of how companies across industries and sizes prioritize and structure their cybersecurity functions. We shed light on crucial aspects like reporting lines of the Chief Information and Security Officers (CISOs), reveal which security capabilities and their related functions are deemed most critical by enterprises and how they align with trends in the ever-evolving threat landscape. We also turn our lens to high-performing organizations, uncovering the security function priorities that set them apart. By examining these security trends, focused areas and leader best practices, this section aims to help organizations benchmark their own approach to optimize their cybersecurity posture and gain a competitive edge.

Decoding CISO Reporting Lines

In our initial analysis, we examined the reporting structure of CISOs to determine their hierarchical placement within organizations. Unsurprisingly, our findings reveal that the predominant reporting line for cybersecurity functions lies with the Chief Information Officer (CIO) or similar roles, constituting one-third of the cases. Notably, in smaller retail enterprises, we observed a positive trend where 2% of CISOs report directly to the Chief Executive Officer (CEO), underscoring a top-down approach to cybersecurity governance within these organizations. This direct involvement of senior leadership in cybersecurity decision-making is a promising indication of the importance placed on security measures at the highest levels of management. Additionally, within larger Consumer Goods & Services (CG&S) companies, 3% of cybersecurity functions fall under the purview of the Chief Financial Officer (CFO). This alignment suggests a strategic integration of security considerations into overall financial planning, potentially leading to more targeted investments in security budgets aligned with the strategic vision of top management.



Security Checkdown: Examining Security Capabilities

One of the key findings of our analysis involved comparing and analyzing the focus of the various reported security functions, which we grouped into four essential security capabilities by industry and company size (Figure 1). These capabilities include Cyber Protection, Cyber Resilience, Cyber Strategy, and Cyber-Physical security which enabled us to assess the extent to which key elements for securing an enterprise's security posture are adopted and the level of maturity achieved.

Our research revealed that most companies universally prioritize Cyber Protection as a central security capability. This includes functions aimed at protecting core enterprise and platforms by hardening environments and improving monitoring, testing, and controls. Functions such as Identity and Access Management (IAM) and Data Security, among others fall under this domain. However, Cyber Resilience and Cyber-Physical Security received comparatively less attention across industries. Cyber Resilience, consisting of functions that enable organizations to swiftly identify, respond,

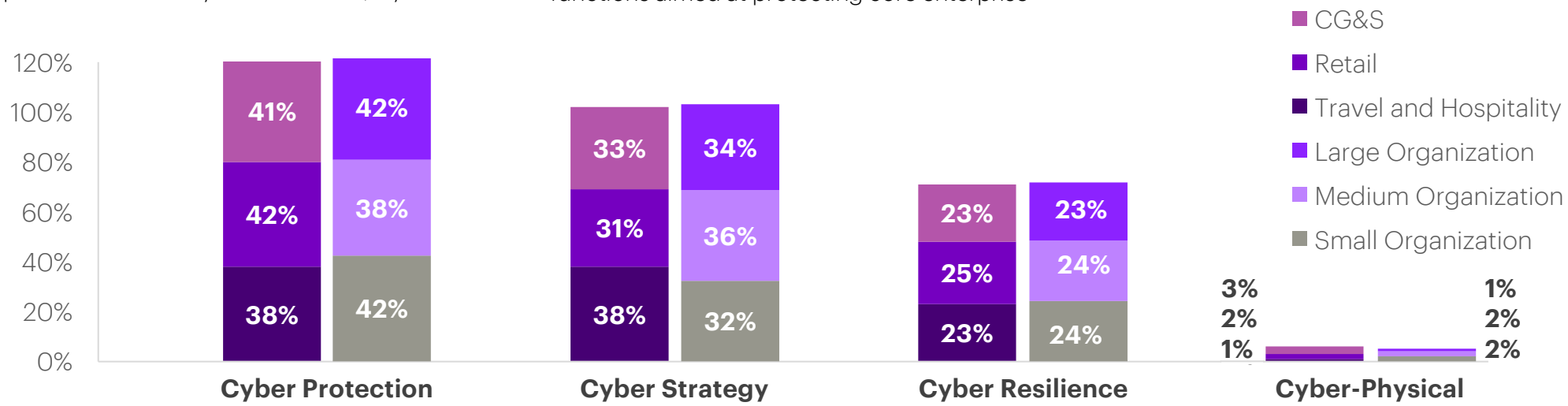


Figure 1: Security Capability Focus by Industry and Company Size

and recover from IT security incidents; and Cyber-Physical security, focusing on securing cyber-physical environments such as IT/OT Convergence and Product Security.

In the realm of Cyber Strategy, our analysis highlighted a predominant focus on compliance and risk management functions across most organizations. This emphasis aligns with the findings of the recently published Cyber Resilient CEO study by Accenture, where 95% of CEOs consider cybersecurity a compliance and regulatory requirement. This highlights the importance that executives are placing with regards to alignment with regulatory standards and frameworks as well as planning and managing security risks.

Furthermore, our research revealed a notable increase in discussions about cybersecurity among G2000[2] executives in Consumer Goods and Services, Retail, and Travel & Hospitality sectors over the last two years. This surge in interest, evidenced by a 50% increase in cybersecurity-related discussions during earnings calls was driven by Cyber Strategy related topics indicating a growing awareness and focus on Cyber Strategy-related topics within these industries.

> "Over the last 2 years, G2000 executives in Consumer Goods and Services, Retail, and Travel & Hospitality industries have increased mentions of cybersecurity by 50% during earnings calls, particularly focusing on Cyber Strategy"

Diving Deeper: Insights into Security Function Prioritization

Next, we took a close look into the capabilities by examining the various functions that companies prioritize across each security capability (Figure 2). It is important to note, however, that the data from our analysis is purely based on reported functions by organizations of our sample size. Some companies may group or combine functions, potentially impacting individual adoption rates from our analysis. For example, "Cloud Security" (30%) might be included under "Infrastructure Security" in some organizations.

Across all industries, our research identified several prioritized functions, including Security Engineering, Security Operations Center (SoC), Compliance, Security & Risk Management, Identity and Access Management (IAM), and Security Architecture. Notably, from a **Cyber Protection** perspective, Identity and Access Management emerged as a significant focus, with 64% of companies placing emphasis on this crucial area. Conversely, Digital Security and Active Directory were found to be the least prioritized functions, with only 9% of companies allocating resources to address these aspects of cybersecurity.

Within the **Cyber Resilience** capability, our analysis revealed that Threat Detection, Vulnerability Management & Forensics, Security Operations and Security Engineering were the primary areas of focus with adoption rates by over half the companies for all three functions. In contrast, Cyber Resilience and Response Management received lower attention, with only 36% of companies demonstrating prioritization in this domain.

As previously indicated, under the **Cyber Strategy** capability, Regulatory and Compliance Risk Management emerged as a top priority for over 80% of companies. However, it was concerning to note that only 9% of the companies had a Business Continuity Planning, Management & Reporting and a dedicated Cyber Strategy function in place, indicating potential gaps in strategic planning and preparedness.

When examining the **Cyber-Physical Security** capability, our analysis found that this area received minimal attention, with less than 10% of companies focusing on functions such as IT/OT Convergence and Product Security.

Interestingly, smaller, and medium-sized companies showed a heightened emphasis on Security Architecture, while larger peers led in Threat Detection and Forensics functions. These findings highlight the diverse approaches taken by organizations of different sizes in prioritizing cybersecurity functions to address their unique security challenges and requirements.

Focused Security Functions

>= 50% Focus | Between 20% - 49% Focus | < 20% Focus | No Focus

L Large Company | M Medium Company | S Small Company | C CG&S | R Retail | T Travel and Hospitality

Cyber Protection

Protection against cyber incidents & attacks	L	M	S	C	R	T	Overall
Identity & Access Management	64%	73%	59%	78%	56%	63%	**64%**
Security Architecture	43%	73%	59%	50%	63%	63%	**59%**
Cloud Security	21%	33%	32%	44%	31%	13%	**30%**
Application Security	43%	47%	41%	39%	44%	44%	**42%**
Information Security	36%	47%	46%	39%	44%	50%	**44%**
Infrastructure Security	36%	27%	16%	33%	13%	31%	**23%**
Data Security (incl. data engineering)	36%	27%	19%	39%	22%	13%	**24%**
Network Security	29%	27%	27%	33%	28%	13%	**27%**
Endpoint Security	7%	13%	22%	17%	22%	6%	**17%**
Fraud Management	21%	20%	5%	11%	13%	13%	**12%**
Payment Security	21%	20%	5%	11%	9%	19%	**12%**
Digital Security	14%	7%	8%	6%	13%	6%	**9%**
Active Directory	21%	7%	5%	28%	3%		**9%**

Cyber Resilience

Business and IT resilience	L	M	S	C	R	T	Overall
Threat Detection, Vulnerability Management & Forensics	64%	80%	43%	78%	53%	38%	**56%**
Security Operations (Incl. SOC)	64%	67%	57%	61%	59%	63%	**61%**
Security Engineering	43%	73%	73%	61%	63%	81%	**67%**
Cyber Resilience and Response (Incl. Cyber Insurance, Incident Mgt response)	50%	47%	27%	50%	38%	19%	**36%**

Cyber Strategy

Regulatory & Compliance Risks	L	M	S	C	R	T	Overall
Security Risk & Privacy Management	79%	87%	84%	89%	78%	88%	**83%**
Compliance (Incl. SOX IT)	79%	93%	76%	89%	75%	81%	**80%**
Loss of customer trust	**L**	**M**	**S**	**C**	**R**	**T**	**Overall**
Assurance and Audits	21%	27%	22%	22%	22%	25%	**23%**
Business Continuity Planning and Disaster Recovery (BCP/DR)	7%	13%	8%	6%	9%	13%	**9%**
Cyber Strategy	14%	13%	5%	11%	6%	13%	**9%**
Cybersecurity Control Framework Standardization	21%	20%	3%	22%	6%	6%	**11%**
Management and Reporting	7%	27%	3%	11%	9%	6%	**9%**
Program and Project Management	14%	40%	24%	28%	16%	44%	**26%**
Security Training and Awareness	29%	27%	24%	33%	25%	19%	**26%**
Supply Chain risks	**L**	**M**	**S**	**C**	**R**	**T**	**Overall**
Vendor/ Third Party Cyber Risk Management	50%	40%	19%	44%	22%	31%	**30%**

Cyber- Physical Security

Cybersecurity Incidents & attacks	L	M	S	C	R	T	Overall
IT/OT Convergence		7%	14%	28%	3%		**9%**
Product Security	7%	13%	5%		13%	6%	**8%**

Figure 2: Security Function Focus by Organizations

Note:
Compliance function could also reside outside the CISO organization but for the analysis we have considered it under cyber strategy.
Vendor/third party cyber risk management is not limited to Cyber Strategy capability but for analysis we grouped it under cyber strategy

Mapping Security Capabilities to Evolving Threats

Driven by the surge in sophisticated cyber threats, we mapped trends with companies' security function adoption and priorities. Our analysis reveals six crucial trends, highlighting the urgent need for organizations to strengthen their cybersecurity posture. These insights illuminate the evolving threat landscape and pinpoint areas where enhanced security measures are essential for effective risk mitigation.

- **Fraud Management:** Despite a 25% increase in digital payments fraud over the last 3 years[3], only 12% and 9% allocate teams for Payment Security & Fraud Management or Digital Security.
- **Data Security:** Right data strategy and data accuracy are two of the top 3 cited risks in the adoption of GenAI[4], yet only 24% of organizations have a focused function for Data Security.
- **Cloud Security:** On current trends, many organizations have started their journey to the cloud, in fact 86% of companies reported an increase in the volume and/or scope of their cloud initiatives since 2020[5], yet only 30% of organizations have a dedicated Cloud Security function.
- **Workforce Vulnerabilities:** 69% of employees have bypassed their organization's cybersecurity guidance in the past 12 months and 74% of employees would be willing to bypass cybersecurity guidance to achieve a business objective[6]. Yet only 26% have a dedicated function for Security Training and Awareness.
- **Supply Chain Security:** CEOs rank supply chain disruptions as the second highest among external risks that has reshaped the cyber threat landscape[1], while 41% of organizations that suffered a material impact from a cyberattack said it originated from a 3rd party[7], yet Vendor/3rd Party Cyber Risk Management function is present in just 30% of organizations, despite a rise in these attacks.
- **IT/OT Convergence:** The Global IT/OT convergence market is anticipated to grow at 14.3% to reach $281bn by 2030[8], yet IT/OT Convergence function sees a low focus (9%), with CG&S companies leading at 28%.

Securing the Future: Preparing for GenAI

As we continue our analysis, a crucial area of concern emerges: the security posture of organizations in the context of generative AI (GenAI) adoption. Despite the growing influence of GenAI technologies, our findings suggest that many organizations are not adequately prepared to secure GenAI initiatives, thus exposing themselves to potential risks and vulnerabilities. Consider that a staggering 56% of organizations believe that GenAI will provide an overall advantage to attackers within the next two years[7]. This alarming statistic underscores the urgent need for organizations to bolster their cybersecurity defenses in anticipation of evolving cyber threats enabled by GenAI. Our research reveals that 67% of CEOs recognize security as a major consideration for the adoption or implementation of GenAI[1]. This acknowledgment indicates the critical importance of integrating security measures into GenAI initiatives from the outset, rather than treating security as an afterthought. Furthermore, the potential impact of GenAI on workforce productivity cannot be overlooked.. Our analysis indicates that a significant proportion of working hours could be potentially transformed with GenAI adoption: 43% in Consumer Goods & Services (CG&S), 53% in Retail, and 50% in Travel & Hospitality[9]. While this technology holds promise for enhancing operational efficiency and driving innovation, organizations must ensure that adequate security measures are in place to safeguard against potential risks and mitigate any adverse impacts on productivity.

> "56% of organizations believe that GenAI will provide an overall advantage to attackers within the next two years"

> "67% of CEOs recognize security as a major consideration for the adoption or implementation of GenAI"

GenAI Security Preparedness Lags Behind: Our analysis reveals a concerning lack of focus on GenAI-critical security functions across industries (Figure 3). Take Cloud Security, essential for protecting GenAI infrastructure: most organizations in all three industries (CG&S: 44%, Retail: 31%, Travel & Hospitality: 13%) prioritize it minimally or not at all. Data, the lifeblood of GenAI, fares similarly: Data Security focus remains low (CG&S: 39%, Retail: 22%, Travel & Hospitality: 13%). These figures indicate widespread under-preparedness for securing GenAI initiatives.

Key Functions Needed to Secure GenAI

Securing Responsible AI	C	R	T
Cloud security	44%	31%	13%
Data Security	39%	22%	13%
Identity & Access Controls	78%	56%	63%
Application Security	39%	44%	44%
Cyber Resilience	C	R	T
Threat Intelligence	78%	53%	38%
Security Monitoring	61%	59%	63%
Cyber Resilience and Response	50%	38%	19%
Security & Governance Framework	C	R	T
Training & Awareness	33%	25%	19%
Cybersecurity Control Framework Standardization (AI usage Policy)	22%	6%	6%
Compliance	89%	75%	81%
Security Risk & Privacy Management (For RAI Risk Assessment)	89%	78%	88%
Vendor/ Third Party Cyber Risk Management	42%	22%	31%

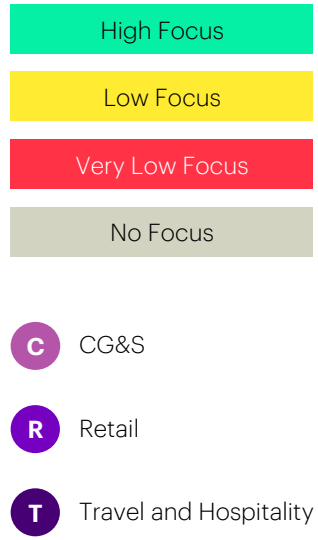


Figure 3: Key functions to secure GenAI

Benchmarking Success: Lessons from High-Performing Companies

We conducted a financial analysis of the 66 companies to discern the top performers in terms of profitability. Among them, we identified a total of 15 companies that have consistently demonstrated strong EBIT margins over the past three years compared to their peers. Our examination of the organizational structures within these top-performing companies revealed that their CISO organizations have higher adoption rates across the threat trends as outlined in the earlier sections. Additionally, our analysis (Figure 4) uncovered several other key findings:

- **Identity and Access Management** emerges as a top priority function across all industries, indicating its critical importance in ensuring secure access to resources. Remarkably, high-performing companies demonstrate a 34% greater emphasis on this foundational area, highlighting its significance in tightly controlling who accesses sensitive data and resources, thereby minimizing attacks and potential breaches.
- Despite being relatively low-priority areas across industries, high-performing companies exhibit a considerable focus on **Security Training and Awareness,** with a 12% higher adoption rate, and **Vendor/Third-Party Risk Management,** with a notable 32% increase. This underscores the proactive approach of top performers in mitigating potential risks associated with workforce vulnerabilities and external partnerships.
- In the era of cloud migration, high-performing companies demonstrate a 15% higher likelihood of prioritizing **Cloud Security.** Particularly in the CG&S and Travel & Hospitality sectors, top performers exhibit an even stronger focus, with adoption rates 22% and 25% higher, respectively. This suggests a strategic alignment with industry threat trends and a proactive stance towards securing cloud environments.

Focused Security Functions: High Performers vs the Rest

>= 10% Focus than rest	< 0% Focus	Between 1% - 10% Focus than rest	No Focus	C CG&S	R Retail	T Travel and Hospitality

Cyber Protection

	C	R	T	Overall
Identity & Access Management	+31%	+38%	+5%	+34%
Security Architecture	-14%	-25%	+46%	-3%
Cloud Security	+22%	-3%	+25%	+15%
Application Security	+2%	-1%	-54%	-8%
Information Security	-26%	+17%	-21%	-2%
Infrastructure Security	+37%	-16%	+2%	+7%
Data Security (incl. data engineering)	-26%	+9%	-15%	-4%
Network Security	+57%	+1%	-15%	+18%
Endpoint Security	+5%	+9%	+33%	+14%
Fraud Management	-15%	+39%	-15%	+11%
Payment Security	-15%	+6%	+18%	+2%
Digital Security	-8%	+39%	-8%	+15%
Active Directory	+17%	-4%		+6%

Cyber Resilience

	C	R	T	Overall
Threat Detection, Vulnerability Management & Forensics	-25%	+23%	+36%	+18%
Security Operations (Incl. SOC)	+26%	-21%	+5%	+4%
Security Engineering	-2%	+30%	-25%	+12%
Cyber Resilience and Response (Incl. Cyber Insurance, Incident Mgt response)	-42%	+25%	+18%	+7%

Cyber Strategy

	C	R	T	Overall
Security Risk & Privacy Management	-12%	+28%	+15%	+19%
Compliance (Incl. SOX IT)	+15%	+14%	+23%	+22%
Assurance and Audits	-31%	-10%	-31%	-19%
Business Continuity Planning and Disaster Recovery (BCP/DR)	-8%	-12%	-15%	-11%
Cyber Strategy	+12%	-8%	+25%	+6%
Cybersecurity Control Framework Standardization	-3%	-8%	-8%	-4%
Management and Reporting	-15%	+6%	-8%	-2%
Program and Project Management	-11%	-20%	-13%	-14%
Security Training and Awareness	-18%	+23%	+18%	+12%
Vendor/ Third Party Cyber Risk Management	-6%	+27%	+85%	+32%

Cyber- Physical Security

	C	R	T	Overall
IT/OT Convergence	+45%	-4%		+15%
Product Security		+2%	+33%	+8%

Figure 4: Security Function Focus: High Performers vs the Rest of Organizations

Note:
**Top performers are the companies that have EBIT margins in the 3rd and 4th quartile of the industry group in last 3 years

**Top performers: Overall n = 15; CG&S: n= 5; Retail: n= 7; T&H n= 3;

Note: Compliance function could also be outside the CISO organization but for the analysis we have considered it under cyber strategy

Vendor/third party cyber risk management is not limited to Cyber Strategy capability but for analysis we have clubbed it under cyber strategy

- High-performing CG&S companies show a remarkable 57% higher focus on **Network Security** and a 45% higher emphasis on **IT/OT Security** compared to their industry peers.
- In the Travel & Hospitality sector, high-performing companies are 33% more likely to have a dedicated function for **Endpoint Security,** reflecting their commitment to ensuring the security of customer-facing systems, applications and data.
- Despite being a critical area for fraud prevention, only 13% of Retail companies have a dedicated Fraud Management function. However, high-performing retailers exhibit a significant 39% higher adoption rate, indicating their proactive approach to combatting digital fraud and safeguarding financial transactions.
- In an increasing digital world, **Digital Security** is recognized as another key focus area for high-performing retailers, with a notable 39% higher adoption rate compared to their industry peers.

Organization chart based on high performers

Overall, high performers invest strategically in key security functions, demonstrating a proactive approach to managing risk and building resilience in the face of evolving threats (Figure 5). They understand the value of a comprehensive security posture and prioritize functions that align with their industry-specific needs and vulnerabilities.

CISO

Cyber Protection	Cyber Strategy	Cyber Resilience	Cyber Physical Security
Identity & Access Management	Vendor/3rd party cyber risk Management	Threat Detection & Management	IT/OT Convergence
Network Security	Compliance	Security Engineering	Product Security
Cloud Security	Security Risk & Privacy Management	Cyber Resilience & Response	
Digital Security	Security Training & Awareness	Security operations	
Endpoint Security	Cyber Strategy		
Fraud Management			
Infrastructure Security			
Active Directory			
Payment Security			
Information Security			
Security Architecture			
Data Security			
Application Security			

Note - The suggested org chat is built by studying the top performing companies' structure, industry risks, and Accenture Experience
Compliance function could also be outside the CISO organization but for the analysis we have considered it under cyber strategy
Vendor/third party cyber risk management is not limited to Cyber Strategy capability but for analysis we have clubbed it under cyber strategy

Figure 5: Organization Chart based on high performers is constructed based on analysis of top-performing companies' organizational structures. Highlighted cells indicate functions aligned to security threat trends.

Conclusion

Our Cybersecurity Organogram Analysis underscores three critical takeaways for organizations aiming to fortify their security posture in an increasingly digital world.

First, it is imperative for companies to strengthen security across the board. Beyond traditional compliance and risk management measures, organizations must broaden their focus to encompass key areas such as fraud, supply chain security, cloud security, data protection, workforce training, and cyber-physical defense. By addressing these multifaceted aspects of security, companies can establish a robust defense mechanism against evolving cyber threats.

Second, the analysis highlights the pressing need for organizations to secure GenAI initiatives effectively. Despite the growing influence of GenAI technologies, many companies lack the necessary organizational security functions to mitigate associated risks adequately. This underscores the urgent need for companies to adapt and enhance their security frameworks to safeguard GenAI initiatives effectively, ensuring long-term success and resilience.

Lastly, our findings emphasize that security maturity drives excellence. High-performing companies distinguish themselves by showcasing mature organizational security functions. By strategically positioning themselves to navigate modern threats and challenges, these companies demonstrate resilience and readiness to tackle cybersecurity risks effectively.

In essence, our analysis serves as a clarion call for organizations to prioritize cybersecurity, broaden their security focus, secure GenAI initiatives effectively, and strive for security maturity. By embracing these takeaways, organizations can fortify their security posture, mitigate risks, and thrive in an increasingly digital landscape.

About the Research

We took a multi-method approach to conduct the analysis, integrating organizational structure analysis, data science-driven NLP risk assessment, and financial performance evaluation. Our methodology involved three key approaches aimed at understanding how companies are organized from a security standpoint and discerning the prioritized security functions within their structures.

First, we conducted a meticulous examination of security organizational structures within 66 global companies spanning the Consumer Goods & Services (CG&S), Retail, and Travel & Hospitality industries. This involved studying the hierarchical arrangement of cybersecurity functions within these organizations to gain insights into how they approach and prioritize cybersecurity.

Second, utilizing advanced data science techniques, we employed the Accenture Research GenAI tool to extract and distil insights from the security risks outlined in companies' annual reports and earnings releases. By leveraging natural language processing (NLP), this data-driven approach allowed us to uncover the top security concerns directly from the sources that companies deem critical for disclosure. This enabled us to gain a deeper understanding of the cybersecurity landscape and the key challenges faced by organizations across industries.

Furthermore, we adopted a financial analysis methodology to complement our findings. We identified a cohort of 15 high-financial performers based on their profitability over the last three years. By scrutinizing the security practices of these top performers, we aimed to delineate prioritization patterns in contrast to their peers. This comparative analysis provided valuable insights into how companies with strong financial performance prioritize and allocate resources to cybersecurity, shedding light on effective cybersecurity practices that contribute to business success.

Overall, our multi-faceted approach allowed us to gain a comprehensive understanding of cybersecurity organizational structures and priorities across industries, providing valuable insights for organizations seeking to enhance their cybersecurity posture.

Acknowledgments

Lead Authors:

Piyush Jain
Global Industry Cybersecurity Lead: Retail and Travel & Hospitality, Accenture

Yusof Seedat
Global Cybersecurity Research Lead, Accenture

Kristen Dalton
Director of Strategic Cyber Engagement, Research & Analytics , RH-ISAC

Contributors:

Accenture:

Manav Saxena (Cybersecurity Research Project Co-Lead),

Shweta Baidya (Cybersecurity Research Project Co-Lead),

Arlene Lehman (Cybersecurity Senior Research Analyst)

Tamara Karelidze (Cybersecurity Consultant)

Bala Periasamy (Retail Industry Cybersecurity Lead)

Sid Srivastava (Consumer Goods Industry Cybersecurity Lead)

Jennifer Graham (Travel Industry Cybersecurity Lead)

Lars Zywietz (EMEA Products Industry Cybersecurity Lead)

Michelle DeLiberty (North America Products Industry Cybersecurity Lead)

RH-ISAC:

RH-ISAC CISO Benchmarking Task Force

References

1. The Cyber Resilient CEO, Accenture 2023
2. G2000 includes the largest 2000 companies in the world ranked by size.
3. One big idea to turn payments fraud from risk to opportunity, Accenture 2023
4. Pulse of Change: October 2023, Accenture
5. The race to cloud: Reaching the inflection point to long sought value, Accenture 2023
6. Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025, Gartner 2023
7. Global Cybersecurity Outlook 2024, WEF & Accenture 2024
8. Global IT/OT Convergence Market, Virtue Market Research 2023
9. A new era of generative AI for everyone, Accenture 2023

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth, and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 733,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise, and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners, and communities.

Visit us at **www.accenture.com**

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data science led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value, and deliver on the power of technology and human ingenuity.

For more information, visit **www.accenture.com/research**

About RH-ISAC

The RH-ISAC was formed in 2014 as the home of the Retail and Hospitality Information Security and Analysis Center (ISAC) and operates as a central hub for sharing sector-specific cyber security information and intelligence. The association connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other – all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC currently serves companies in the retail, hospitality, gaming, travel and other consumer-facing entities.

https://rhisac.org/