Aite Novarica

MAY 2023

CYBERSECURITY 2023

INFOSEC LEADERS PURSUE THE FUTURE OF FINANCIAL SERVICES

JOHN HORN

This report provided compliments of:

IMPACT REPORT

TABLE OF CONTENTS

LIST OF FIGURES

IMPACT REPORT

MAY 2023

CYBERSECURITY 2023

InfoSec Leaders Pursue the Future of Financial Services

JOHN HORN

LIST OF TABLES

SUMMARY AND KEY FINDINGS

Across the financial services (FS) market, senior information security (InfoSec) executives, including chief information security officers (CISOs), are elevating from cybersecurity technical leaders to executives managing business risk. InfoSec executives in FS operate in fast-paced environments, holding high value for actional cybersecurity intelligence and strategic insights for the future. Market vendors serve as important sources of information, but InfoSec executives need insights decoupled from security vendor biases. InfoSec executives desire perspectives from outside their corporate boundaries and direct experiences, especially from peers leading cybersecurity at other FS firms.

This Impact Report, driven by extensive Aite-Novarica Group surveys of 221 InfoSec executives in eight countries, is intended to provide these key insights for InfoSec executives at financial institutions (FIs), insurance carriers, or other FS firms. The key findings from this report follow:

- Artificial intelligence, defense against tomorrow's attacks, identity, and API security are the four top-of-mind enterprise defense challenges for the InfoSec executive. From the perspective of the FS InfoSec executive, these are the hottest, most important topics in the cybersecurity market. These are the solutions InfoSec executives value most, and they require the greatest need for outside assistance.
- Nonhuman actors or bots, Internet of Things (IoT), and the emerging digital workforce are the three technology trends InfoSec executives are most concerned about. As technology trends lead the FS market to new capabilities and business value, these specific technology trends are believed to create the most difficult cyber risk for InfoSec executives and their teams.
- Annual cybersecurity budgets for most FS InfoSec executives are increasing in 2023 and 2024. Given bear-market conditions and the highly competitive nature of financial services, an industry narrative existed (in some circles) that FS InfoSec executives would face flat or decreasing budgets. Yet, Aite-Novarica Group research found that 88% of surveyed InfoSec executives won increasing year-over-year (YoY) cybersecurity budgets for 2023 and 2024. These findings reflect how board and top-of-house executives better understand the critical nature of enterprise cybersecurity defenses in all market conditions.

- Malware/ransomware defenses, infrastructure security, cloud security, and API security are the top cybersecurity investments for FS InfoSec executives in 2023.
- Payments resiliency (or stand-in capability) has a strong InfoSec emphasis with a high need for external assistance (44%) and high-priority 2023 investment (51%).
- Most InfoSec executives in Germany (80%) are very interested in receiving outside assistance to defend against future attacks.
- Most InfoSec executives in Brazil (76%), Saudi Arabia/United Arab Emirates (UAE; 65%), Australia (60%), Germany (60%), and the U.S. (58%) believe much market innovation is needed for their enterprise use of artificial intelligence.
- Most InfoSec executives in Saudi Arabia/UAE (70%), Brazil (67%), and the U.S. (57%) believe much market innovation is needed for identity solutions enabling digital transformation.
- Ransomware defenses are the top 2023 cybersecurity investment for InfoSec executives in India.
- Malware defenses are the top 2023 cybersecurity investment for InfoSec executives in Germany, Saudi Arabia/UAE, and the U.K.
- API security is the top 2023 cybersecurity investment for InfoSec executives in the U.S.

INTRODUCTION

InfoSec executives have one of the most exciting and demanding executive leadership roles in all FS. No other executives at FIs, insurance carriers, or other FS firms are tasked with facing the relentless attacks of skilled criminal teams and nation-state attackers on the digital enterprise. No other executives have the breadth of solutions to design and operate, thus requiring deep technical acumen from InfoSec executives and their teams. No other executives must constantly modernize solutions like InfoSec executives. Innovation in the FS market often exposes gaps in existing security controls, which fuels dynamic innovation of new security products that InfoSec executives and their teams must select, integrate, and operate. And no other executives have more adjacent areas of the business to understand and manage.

Beyond traditional cybersecurity domains, CISOs and InfoSec executives are expected to own or partner extensively with executives responsible for operational resiliency, technology, identity, data, enterprise risk management, third-party risk management, and even human resources. As a result, the career of an InfoSec executive is complex, constantly evolving, and extremely satisfying for dynamic leaders.

In this dynamic context, it can be difficult for FS InfoSec executives to make strategic decisions and decide on their top investments. When defending against constant attacks, InfoSec executives can become vulnerable to narrow perspectives within their enterprise. For InfoSec executives worldwide, making similar priority and investment decisions for cybersecurity is critical, but finding actionable insights across these broader perspectives can be difficult. This report provides several key insights for InfoSec executives at FIs, insurance carriers, and other FS firms. Through this research, InfoSec executives identify their most critical enterprise defense challenges, most concerning technology trends, budget realities, and top investments for 2023.

METHODOLOGY

Commissioned by Mastercard, Aite-Novarica Group surveyed 221 InfoSec executives serving large and midsize FIs and large and midsize merchants in five geographical regions across eight countries: the U.S., the U.K., Germany, Brazil, Australia, India, Saudi Arabia, and the UAE. Of the 221 InfoSec executives, 111 serve FIs, and 110 serve merchants.

Midsize FIs are defined as holding assets of US$20 billion to less than US$100 billion. Large FIs are defined as holding assets of US$100 billion or greater.

Midsize merchants are defined as having annual sales of at least US$100 million but less than US$500 million with at least 15% in online sales, while large merchants are defined as having annual sales of US$500 million or greater with at least 10% in online sales.

These surveys focus on the most urgent enterprise defense challenges, most concerning technology trends, budget characteristics, and top 2023 investments. The surveys were conducted from December 2022 through January 2023. Information was also gathered from Aite-Novarica Group's Financial Institution CISO Research Council (April 2022 and February 2023) and Insurance CISO Special Interest Group (February 2023) to supplement this data.

The total sample of the study has a margin of error of 6.5 points at the 95% confidence level. Within FIs and merchants, the margin of error is 9.3 points at the 95% confidence level.

TOP-OF-MIND ENTERPRISE DEFENSE CHALLENGES

The ability to solve the greatest cybersecurity needs of the business is key to InfoSec success. In practice, identifying these top priorities can be difficult. Regular cyberattacks against the enterprise can create "whack a mole" dynamics for the InfoSec executive, wherein one resolved problem leads the next problem to surface. As operational teams move from one emergency to the next, and InfoSec executives run from one executive post-mortem to another, these leaders can fall into a trap of sorts, believing the latest fire is their highest-priority enterprise challenge.

Seasoned InfoSec executives must put significant time toward strategic outcomes, understanding that some enterprise defense challenges are more important to solve than others. Some challenges require new technology or new assets. Others require new kinds of security solutions or operational actions. Some enterprise challenges require a new kind of cybersecurity framework that helps transform the effectiveness of all other defenses.

The essential InfoSec question is, what really are the most urgent enterprise defense challenges at my firm right now? Internal risk perspectives form the base understanding for each firm. Aite-Novarica Group's research was designed to understand top-of-mind enterprise challenges across 221 firms. Table A details the four most urgent enterprise defense challenges identified by the research.

TABLE A: TOP-OF-MIND ENTERPRISE DEFENSE CHALLENGES

TOP FOUR CHALLENGES	DESCRIPTION
Artificial intelligence	**Artificial intelligence is technology.** Artificial intelligence and machine learning (ML) are not new concepts. The ability to rapidly analyze millions of data sets to detect cybersecurity patterns has been relished for years. Artificial intelligence/ML capability is found within many current security products. But in 2023, FS InfoSec executives need much more significant and practical value from Artificial intelligence/ML.

TOP FOUR CHALLENGES	DESCRIPTION
Defending against tomorrow's attacks	**Defending against attacks is an action.** InfoSec executives have always kept an eye toward future attacks in planning new defense solutions. But after enduring years of attacks against the enterprise, InfoSec executives in 2023 hold a more elevated value in gaining line of sight to new attack vectors and deploying more effective capabilities against attacks.
Identity	**Identity is a key asset.** User identity has traditionally functioned as a component of the legacy IT framework. In 2022, identity found the main stage in the cybersecurity industry. Modern identity structures are recognized as central to enabling digital transformation business outcomes and zero-trust security outcomes.
API security	**API security is a new class of solution.** As open banking/finance ecosystems disrupt traditional value chains and create new capabilities for consumers, attackers have become effective in beating legacy API systems. InfoSec executives urgently need zero-trust-based API security solutions to reduce risk and enable the business.

Source: Aite-Novarica Group

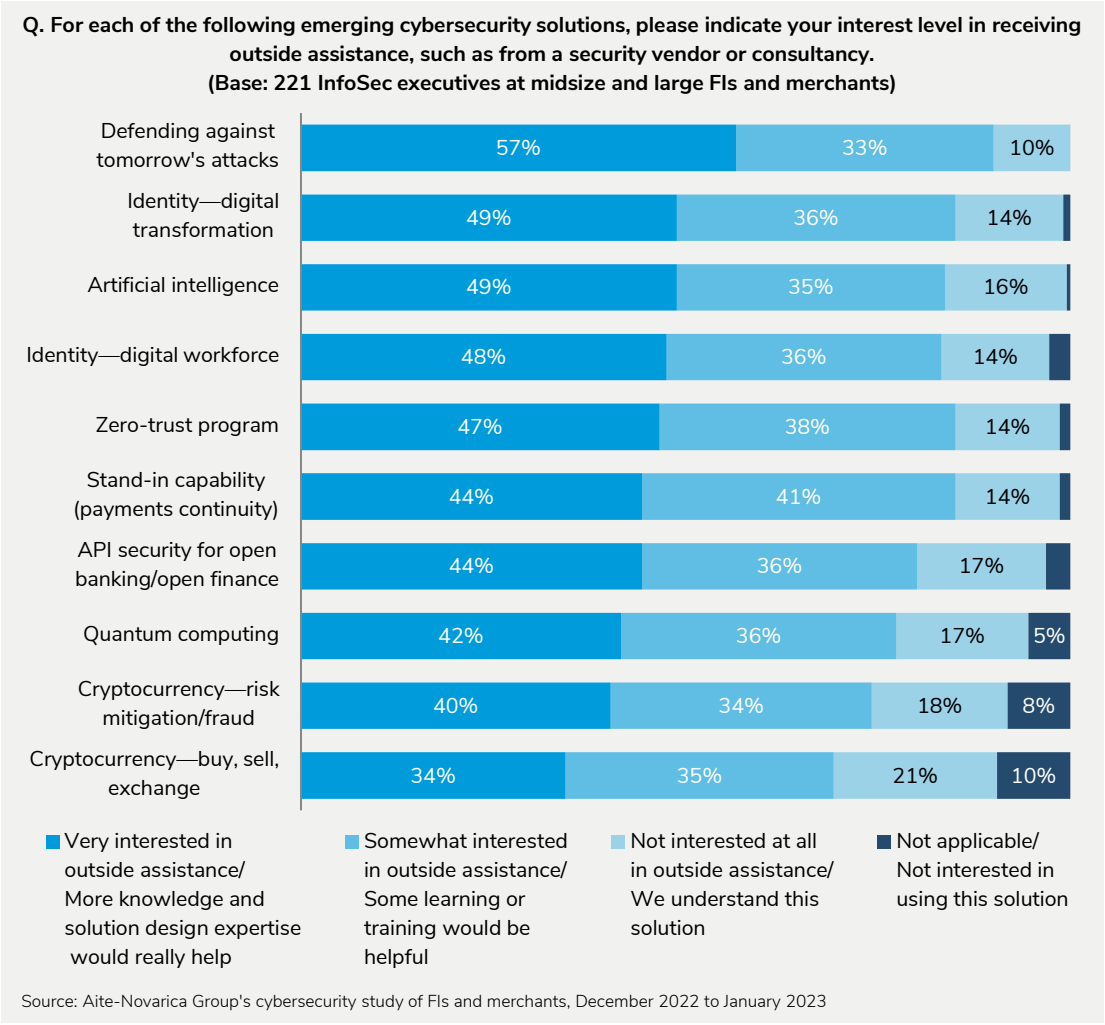
INFOSEC EXECUTIVE RESEARCH ANALYSIS

Responses to two specific survey questions help inform and identify the highest-priority enterprise defense challenges for InfoSec executives.

ENTERPRISE CHALLENGES MOST IN NEED OF OUTSIDE ASSISTANCE

The need for external assistance is a very strong indicator of the importance of an enterprise challenge for the FS InfoSec executive. Conversely, when an InfoSec executive shares an area that does not require outside assistance, they are indicating a lack of (relative) importance or affirming the ability of their staff to solve problems with existing talent, tools, and processes. Figure 1 presents the responses of InfoSec executives ranking the need for external assistance for several contemporary enterprise challenges.

FIGURE 1: PERCEIVED NEED FOR OUTSIDE ASSISTANCE



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2023

FI and merchant InfoSec executives responded similarly regarding enterprise challenges needing the most outside assistance. Both groups highlight defending against tomorrow's attacks as the challenge needing the most outside assistance, especially from InfoSec executives serving firms in Germany (80%). Criminal teams have become more resourced, more sophisticated, and broadly more agile than their counterparts at the FS firm. Add in pervasive talent gaps and operational processes at corporations, which tend to slow the deployment of cyber defenses, and it is no wonder that InfoSec executives believe they need massive external help for their teams to keep pace with modern attackers.

Identity efforts were also highlighted by both groups as needing significant outside assistance. InfoSec executives in Germany (65%) and the U.K. (55%) most strongly identify needing external help for identity-enabled digital transformation efforts. Both groups also emphasized stand-in capability as an important area needing external assistance resiliency (44%). Many InfoSec executives recognize that user identity can become a strategic asset for the firm, but modernization projects can be difficult. Many firms need to overcome significant identity tech debt tied to the legacy IT estate. Many also lack senior identity talent on staff. Modernization projects often must coordinate across multiple stakeholders at the firm. It makes sense that InfoSec executives need major external assistance to help transform identity into a key enabling asset for their firms.

FIs assert the need for outside help for API security challenges more so than their merchant counterparts. FIs generally hold liability risk and tend to operate many more APIs than merchants; it follows that FI InfoSec executives need more external assistance, which is what the research indicates. For FI InfoSec executives, the following are the top four enterprise defense challenges:

- Defending against tomorrow's attacks
- API security
- AI
- Identity—digital workforce

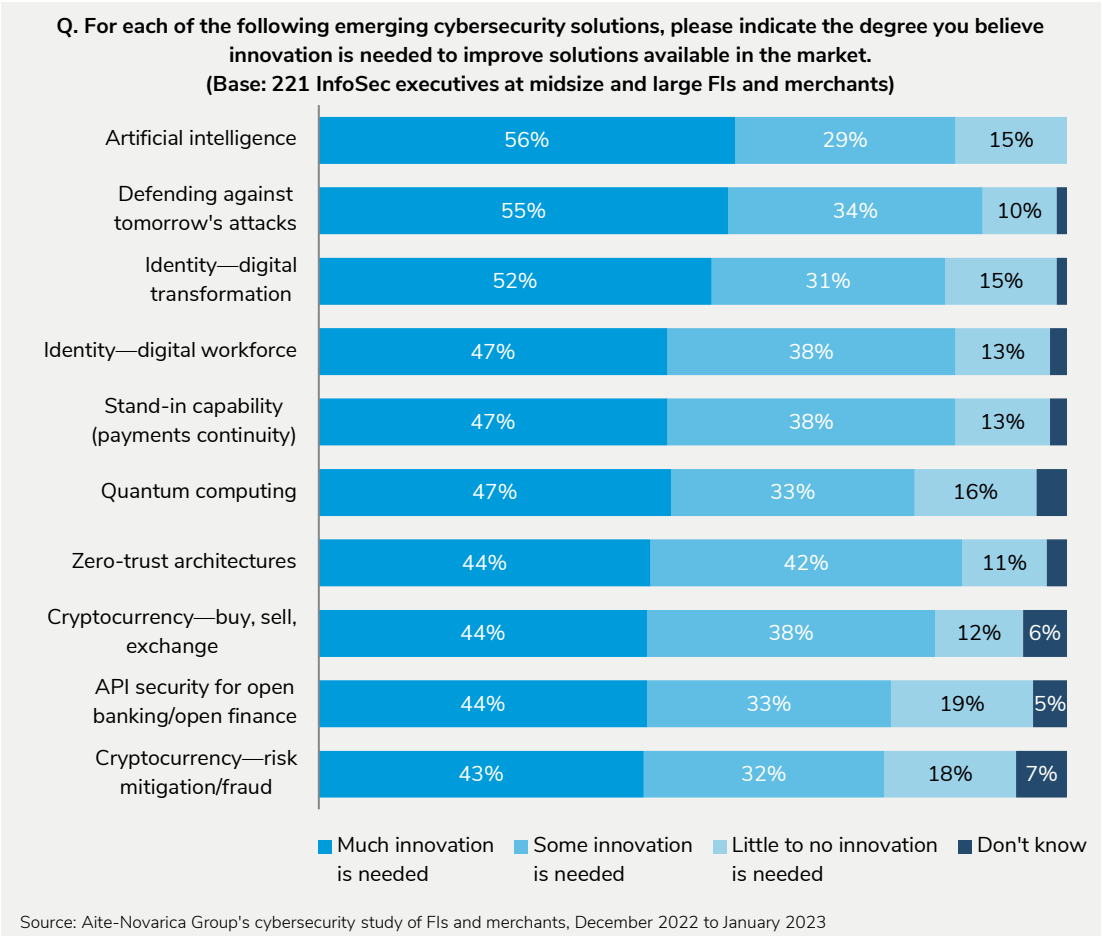
For merchant InfoSec executives, identity challenges rise near the top for workforce and business transformation outcomes. Merchants often have even fewer identity domain experts than FIs, which could explain this prioritization. Zero-trust programs rose to the fourth-highest need, indicating less maturity at present as compared to their FI counterparts. Artificial intelligence remains important but drops to the fifth priority. The following are the top four enterprise challenges for merchants:

- Defending against tomorrow's attacks
- Identity—digital transformation
- Identity—digital workforce
- Zero-trust program

ENTERPRISE CHALLENGES MOST IN NEED OF MARKET INNOVATION

The need for innovation is another strong indicator of the importance of an enterprise challenge for FS InfoSec executives. When identifying the need for innovation, they are indicating an importance ("I need to solve this challenge") and a real or perceived gap in available solutions ("I don't seem to be able to solve this challenge with available solutions"). Innovation is often required to solve more complex enterprise problems. It suggests the challenge is not adequately solved, perhaps due to solution shortcomings, lack of integration, or support gaps. Figure 2 presents the InfoSec executives' responses ranking the need for innovation in several enterprise defense challenges.

FIGURE 2: PERCEIVED NEED FOR MARKET INNOVATION



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2023

Most InfoSec executives favor using artificial intelligence/ML technology and are bullish regarding future capability. But the research highlights that FS InfoSec executives need more practical artificial intelligence value in 2023, which they express as a perceived innovation gap. This gap is especially highlighted by InfoSec executives serving firms in Brazil (76%), Saudi Arabia/UAE (65%), Australia (60%), Germany (60%), and the U.S. (58%).

Some perspective is important. Artificial intelligence is absolutely crucial to FS InfoSec executives as their teams solve enterprise defense challenges. Yet, artificial intelligence is on a journey. InfoSec executives understand this; they simply need more. Addressing issues critical to the business, most InfoSec executives view artificial intelligence as central to delivering more effective risk intelligence and real-time decisioning. In this mindset, FS InfoSec executives believe more innovation will lead artificial intelligence technology to achieve even greater value to their enterprise defenses.

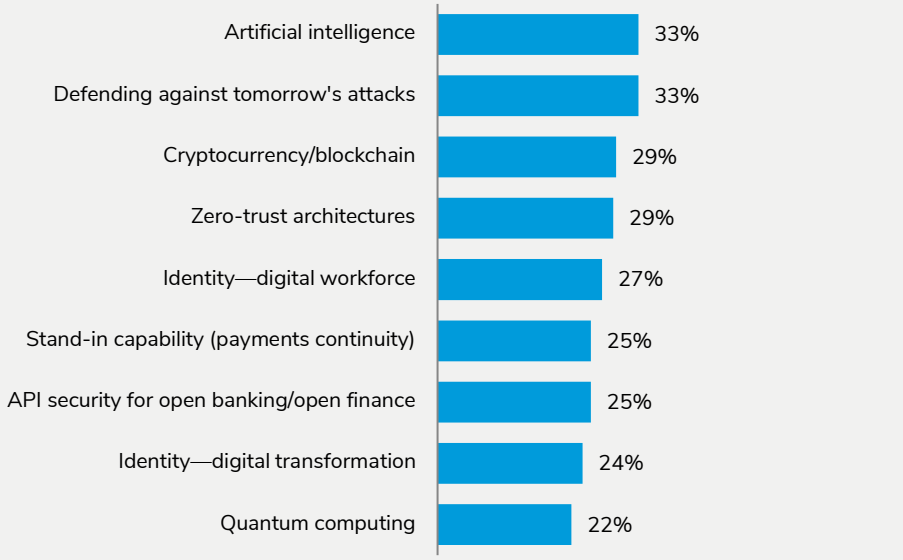
According to the research, most InfoSec executives believe greater market innovation can lead to important improvements in defending against future attacks. Innovation could lead to more cohesive visibility of attacks or potentially different solution models to improve the timeliness and precision of cyber defense mechanisms. In addition, the research shows InfoSec executives strongly perceive a need for innovation regarding identity, especially as a key enabler to digital transformation for the business. This is strongly emphasized by InfoSec executives serving firms in Saudi Arabia/UAE (70%), Brazil (67%), and the U.S. (57%). This need for innovation seems to reflect an exciting yet complex current market for identity solutions.

Implementing identity as an asset is difficult. The identity vendor market has exploded over the past five years. It now includes a diverse set of identity capabilities with traditional platforms, data fabrics, orchestration hubs, governance tools, and multifactor authentication features for enterprise and customer-facing services. InfoSec executives must evaluate and design multivendor identity ecosystems. Identity innovation may look like more packaged and pre-integrated solutions so the InfoSec executives can streamline the evaluation, procurement, and deployment process for their firm.

ENTERPRISE CHALLENGES MOST EXCITING TO THE INFOSEC EXECUTIVE

InfoSec executives have personal passions related to the enterprise defense challenges that their firms face. These aspects have much less material bearing on prioritization but are interesting, nonetheless. The research asked InfoSec executives where their greatest personal excitement lies across the many challenges they face. Figure 3 presents solutions InfoSec executives are most excited about.

FIGURE 3: SOLUTIONS THAT MOST EXCITE INFOSEC EXECUTIVES



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2023

In the area of excitement, both FI and merchant InfoSec executives respond strongly to defending against tomorrow's attacks and AI, occupying two of the top four solutions in each segment. Rounding out each group's top four, FI InfoSec executives also indicate excitement for API security and cryptocurrency/blockchain. In contrast, merchant InfoSec executives indicate excitement for identity (digital workforce) and stand-in capability. InfoSec executives are seasoned critical thinkers. They enjoy solving complex problems. Their personal passions come from a lifetime of career experiences and a drive to achieve a more secure digital future for their firms and society at large.

ANALYST PERSPECTIVES LOOKING AHEAD

The four enterprise defense challenges most InfoSec executives highlighted in this research (AI, defending against tomorrow's attacks, identity, and API security) bear significant attention. From the advisor chair, some interesting similarities and themes are observed across these four hot challenges and the current maturity of cybersecurity solutions in the market. Modern cybersecurity is steeped in highly technical solutions. Each of the InfoSec executives' most urgent challenges requires market solutions that harness and deliver technology more effectively. Market strategists may say similar things years from now. FS needs more. A secure digital future demands more.

FS InfoSec executives need practical value and operational simplicity in a world of digital complexity. Faced with expanding attack surface, complicated solutions, and pervasive cyber talent gaps, the practical desire of the InfoSec executive is often to reduce risk and streamline operations. For the four hot enterprise challenges highlighted by this research, responses suggest a perceived gap in practical understanding, risk reduction value, or support from available market solutions. InfoSec executives have developed significantly higher expectations for these solutions, as the distance between market promises and operational realities can feel like a chasm. They need more value, illustrated by the following:

- Significant progress has been made in solutions helping firms defend against modern cyber-attacks. Still, InfoSec executives need even more cohesiveness from these solutions. They need solutions that better represent worldwide cyber phenomena and cross-industry views, have less vendor-centric perspectives, and deliver greater timeliness.
- Nearly all FS InfoSec executives believe in the promises of artificial intelligence/ML and have invested budgets and personal reputations in this area. But they now need solutions that deliver substantially on those promises. Can the market deliver?
- Most FS InfoSec executives have come to understand the centrality of modern user identity to achieve zero-trust and digital transformation outcomes. But in taking stock of current solutions, InfoSec executives believe they need significant assistance and innovation to bring identity-enabled value to operational reality.

Security vendors providing solutions for any of these four enterprise challenges should view the research results as quite positive. FS InfoSec executives need what these vendors sell. Yet a more sobering realization is that InfoSec executives perceive they

need more from these strategic solutions. With a few exceptions, when InfoSec executives perceive they need more assistance, they are usually correct and will seek out providers who can deliver this help.

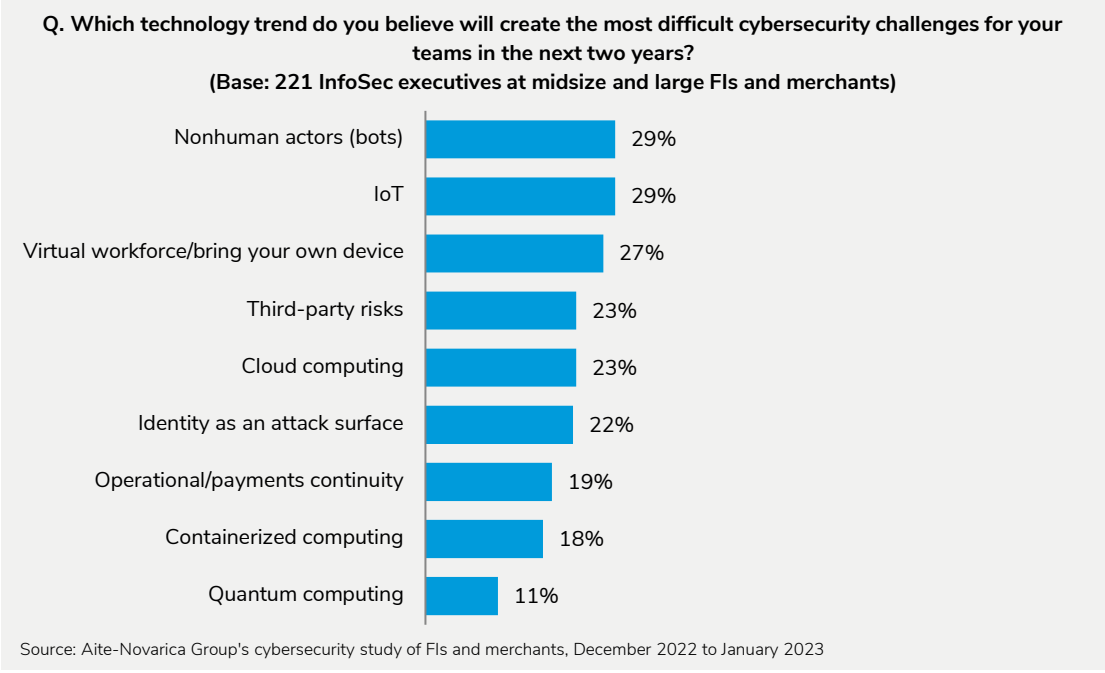
The impacts may be significant for security providers. It may have been enough in years past for a vendor to have an artificial intelligence or identity product in the market. The research suggests, however, that the season of possessing a solution in a desirable market category is giving way to a season wherein delivering practical security value is coming into focus for InfoSec executives.

TECHNOLOGY TRENDS—GREATEST INFOSEC CONCERNS

Several technology trends drive strategic direction in digital markets worldwide. Within FS, technology trends usually produce quality or efficiency advances for the business but create new cyber risks for InfoSec executives and their teams. Rarely does a technology trend include a drop-in security assurance component. Rather, market innovation is usually followed by efforts to secure or manage the new cyber risk created.

Not all technology trends are equal in the InfoSec executive's mind. This research asked InfoSec executives to identify the technology trends they believed would cause the most difficult risk challenges for their teams. Figure 4 presents the results.

FIGURE 4: TECHNOLOGY TRENDS CREATING THE MOST DIFFICULT CYBER CHALLENGES



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2023

Important observations can be made given these responses. First and foremost, InfoSec executives are greatly concerned about the growing prevalence of nonhuman actors (bots) and the proliferation of endpoints not under the control of human beings (IoT).

Bots have become commonplace in the current market. Several market tools are available for InfoSec executives to detect their presence and manage their risk.[1]

[1] See Aite-Novarica Group's report Aite Matrix: Leading Bot Detection and Management Providers, August 2022.

Firms are at various stages in deploying modern bot security tools. InfoSec executives expect cyber risk stemming from bots to worsen in the future. Similarly, as internet-connected computing devices become embedded into everyday objects at scale, InfoSec executives anticipate difficult cyber risks for their teams. Legacy security models, antiquated authentication mechanisms, and inadequate identity solutions will leave enterprises vulnerable to IoT-based cyber-attacks.

Neither of the top two concerns dominates compared to other InfoSec executives' responses. Rather, the top two rank highest among several high-ranking responses. InfoSec executives show concern for several other risks at nearly the same degree. Virtual workforce, third-party, and cloud risks represent significant risk concerns. With a degree of uncertainty, InfoSec executives are rightfully concerned about several technology trends.

Finally, in what may surprise some, InfoSec executives identified quantum computing as the lowest concern for cyber risk, even as cryptography supports data encryption—the most fundamental of all cybersecurity defenses. Post-quantum cryptography solutions continue to experience challenges[2]. With all this noted, the research results align with FS CISO discussions the past year, which reflect a broad assumption that quantum breaches of current cryptography algorithms are still some time off. Hence, the reasoning goes that risk at present is not as significant. This represents a large collective bet held across many in the cybersecurity market. Time will tell if this bet has been well played.

[2] See Aite-Novarica Group's blog Post-Quantum Cryptography Deconstructed, February 2023.

CYBERSECURITY BUDGET TRENDING

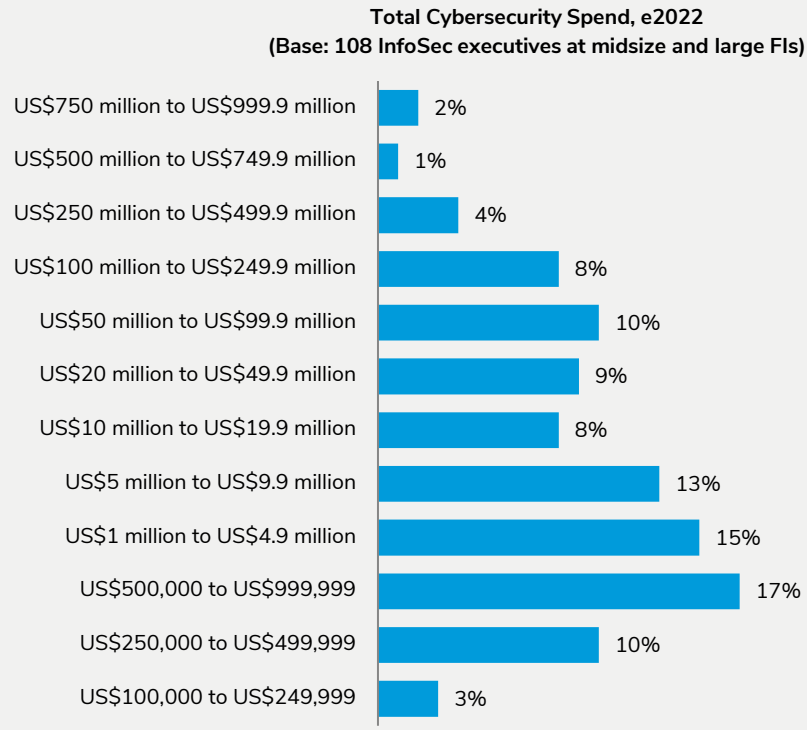
InfoSec executives work each year for cybersecurity budgets at their firms. Annual cybersecurity budgets have been rooted as a cost center, historically driven by regulatory compliance, operational resilience, staffing, solutions, and cyber underwriting. As cybersecurity has risen in importance, budgets have evolved, with InfoSec executives earning some allocation in support of revenue-generating businesses (e.g., customer identity, API security). The annual cybersecurity budget is influenced by the executive risk appetite of the FS organization. Awareness of cybersecurity budget realities at other FS firms has been challenging historically, as many viewed annual cybersecurity budgets as sensitive internal information.

In the summer of 2022, as InfoSec executives began formal 2023 budget planning, they did so in full awareness of bear-market expectations for 2023 and beyond. Peer discussions at industry events, such as RSA (June 2022), have been characterized by a common acknowledgment of unfavorable business conditions ahead and the need for financial belt-tightening across the cybersecurity market.

FS CYBERSECURITY BUDGET TRENDING—FIS

FI InfoSec executives across eight countries were asked to share their total cybersecurity spend for calendar year 2022. Figure 5 shows the distribution of responses.

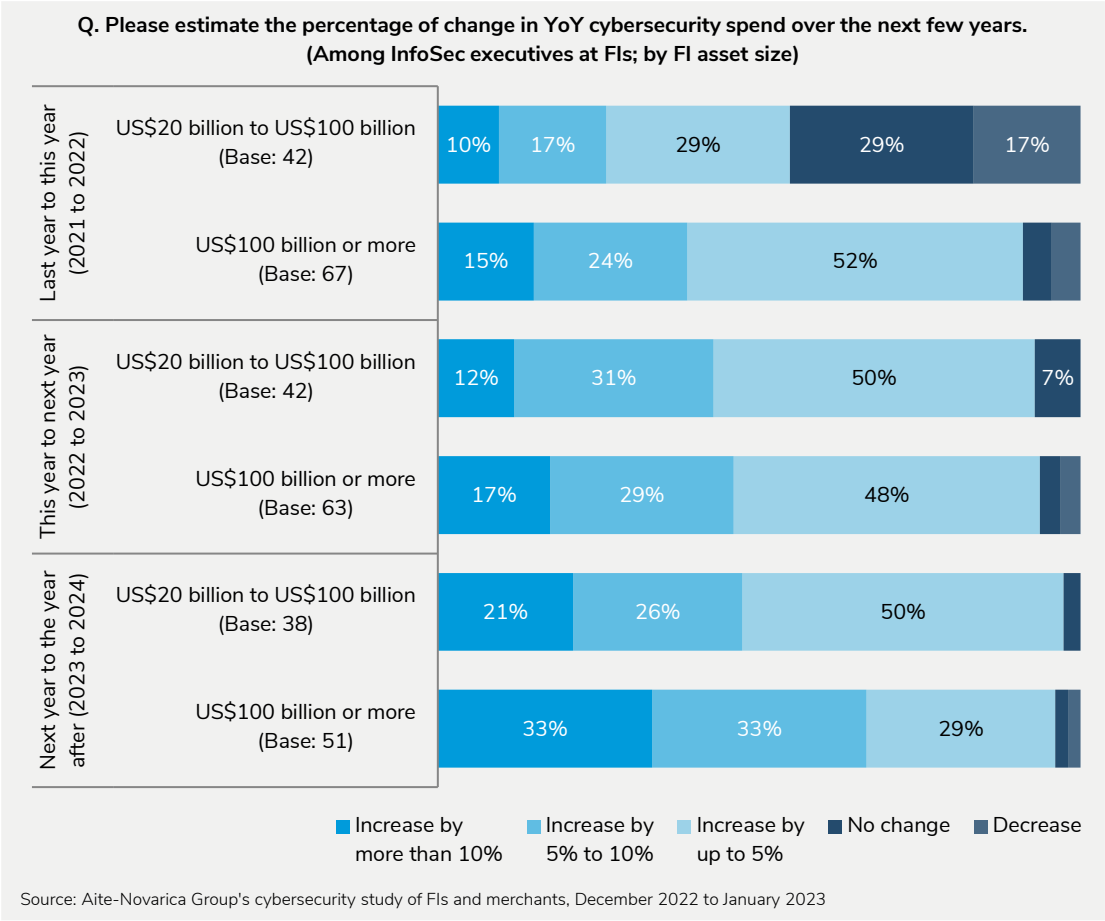
FIGURE 5: FIS' ESTIMATED CYBERSECURITY SPEND, 2022



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2022

These InfoSec executives were asked to compare their annual cybersecurity spending and budgets across four years to observe budget trending characteristics. Figure 6 provides these results, segmented by FI asset sizes.

FIGURE 6: FIS' YOY CYBERSECURITY SPEND AND BUDGET



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2023

Given current bear-market conditions, the survey results above are stunning. Overall, 93% of all FI InfoSec executives have earned increasing year-over-year (YoY) cybersecurity budgets for 2023, growing to 97% in 2024. Larger FIs exhibited the greatest YoY budget growth.

For midsize FIs, many InfoSec executives are operating with sizeable YoY cybersecurity budget increases:

- **Increases 5% or more:** 43% of FIs in 2023 (growing to 47% in 2024)
- **Increases 10% or more:** 12% of FIs in 2023 (growing to 21% in 2024)

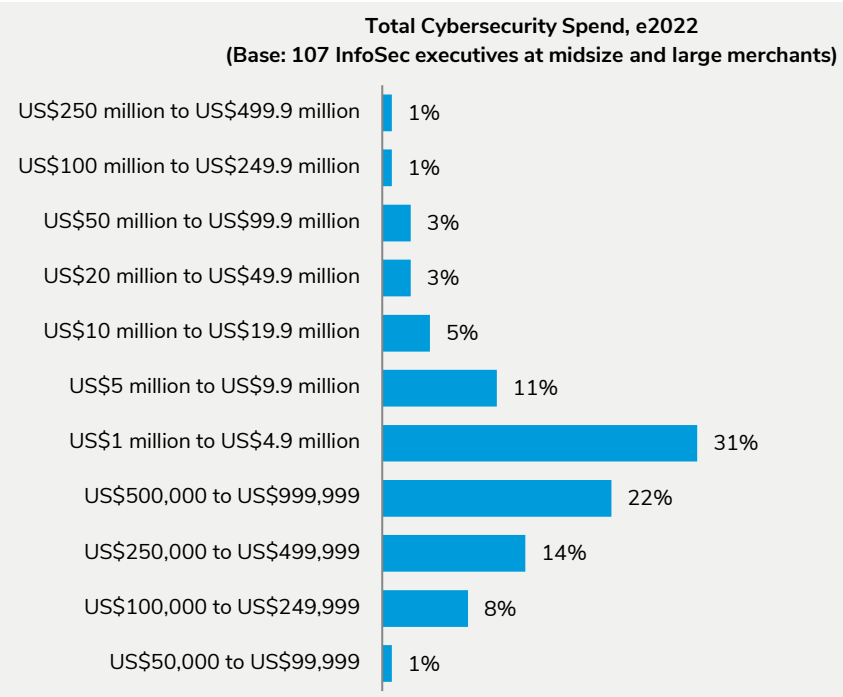
For large FIs, even more InfoSec executives are operating with sizeable YoY cybersecurity budget increases:

- **Increases 5% or more:** 46% of FIs in 2023 (growing to 66% in 2024)
- **Increases 10% or more:** 17% of FIs in 2023 (growing to 33% in 2024)

FS CYBERSECURITY BUDGET TRENDING—MERCHANTS

Merchant InfoSec executives respondents were asked to share their total cybersecurity spend for calendar year 2022. Figure 7 shows the distribution of responses.

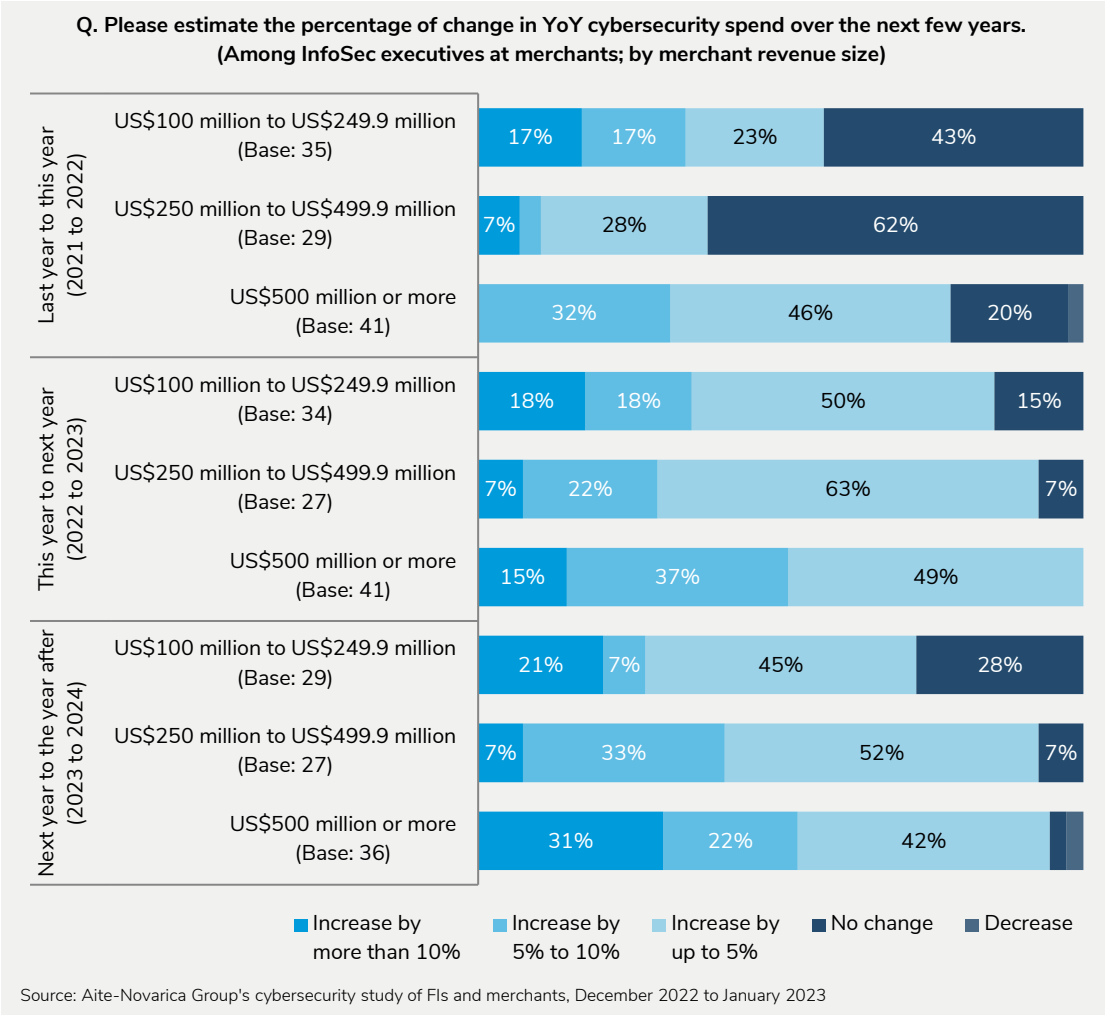
FIGURE 7: MERCHANTS' ESTIMATED CYBERSECURITY SPEND, 2022



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2022

Next, merchant FI InfoSec executives were asked to compare their annual cybersecurity spending and budgets across four years to observe budget trending characteristics. Figure 8 provides these results, segmented by merchant revenue segments.

FIGURE 8: MERCHANTS' YOY CYBERSECURITY SPEND AND BUDGET



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2023

In bear-market conditions, merchant cybersecurity budgets are strongly growing YoY. Merchant budget growth rates trail FI budget growth rates for 2023 and 2024. Overall, 93% of all merchant InfoSec executives have earned increasing YoY cybersecurity budgets for 2023. Based on 2024 forecasts, 87% of merchants will operate with an increased YoY budget next year.

Significantly, 100% of large merchants are operating with increased YoY budgets in 2023. Over half (52%) of large merchants are operating with at least 5% more cybersecurity budget this year than last year. In 2024, almost one in three large merchants (31%) forecast growing budgets by 10% or more.

FS CYBERSECURITY BUDGET TRENDING—ANALYST PERSPECTIVES

Increased cybersecurity budget for FIs and merchants is a positive development. But when InfoSec executives are earning increasing YoY cybersecurity budgets during bear-market conditions as other parts of the organization are operating flat (or reduced) budgets, it means InfoSec executives are doing something right. CISOs and InfoSec executives have helped boards better understand the critical nature of cybersecurity to the success of the business. This is good news for FS.

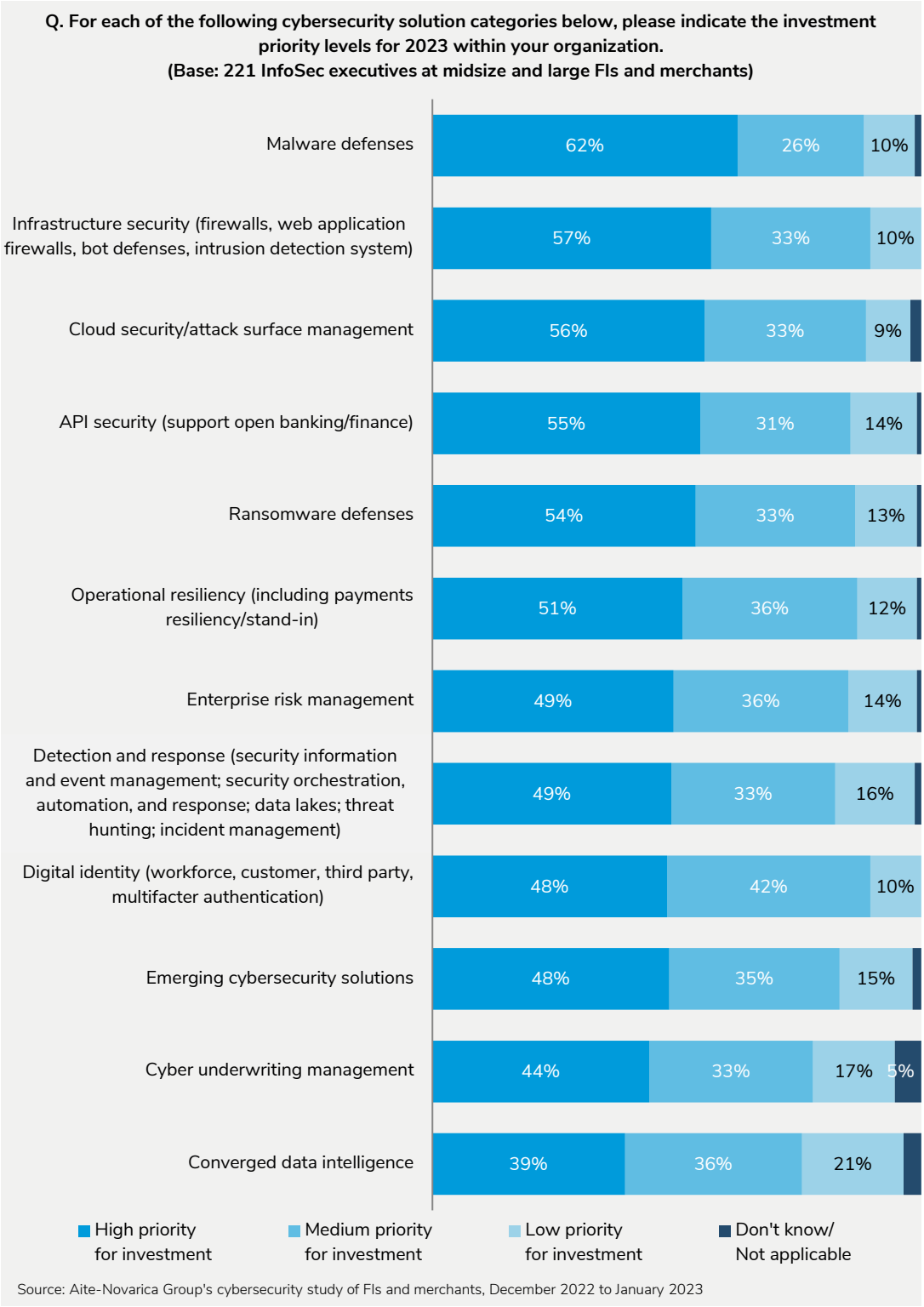
None of this suggests that InfoSec executives have arrived at some kind of "easy street" financially. They will always be forced to make difficult decisions between investments, and their teams will continue to complete security improvements each year. But they are doing so with expanded budgets, which helps considerably.

TOP CYBERSECURITY SOLUTION INVESTMENTS 2023

InfoSec executives and their teams continue to execute against planned and emergent work in 2023. Aite-Novarica Group asked InfoSec executives to indicate priority levels to improve solutions in several categories. High-priority investments were defined as those most urgent for the business, with funded projects and no dependencies. Medium-priority projects were defined as important for the business, but some dependencies or funding matters still need to be resolved.

Figure 9 summarizes the responses from 221 InfoSec executives.

FIGURE 9: TOP 2023 CYBERSECURITY INVESTMENTS



Source: Aite-Novarica Group's cybersecurity study of FIs and merchants, December 2022 to January 2023

Responses reflect a robust 2023 for cybersecurity improvements at FIs and merchants. Several interesting observations stem from these responses:

- Malware defenses are the top investment in 2023. Driven partly by the need to deploy improved ransomware defenses (the fifth-highest investment area), improvements to better defend against malware attacks are primary this year. High-priority malware defense investments are especially noteworthy for firms in Saudi Arabia/UAE (85%), Germany (80%), Brazil (71%), and the U.K. (70%).
- The next set of highest-priority investments includes infrastructure security, cloud security/attack surface management, API security, ransomware defenses, and operational resiliency (including stand-in payments capability). InfoSec executives and their teams are working on these critical areas. Aite-Novarica Group's regular discussions with FS InfoSec executives continue to affirm these solution types as a high priority for 2023 investment.
- API security is the top cybersecurity investment for InfoSec executives in the U.S.
- Cloud security/attack surface management investments are especially strong for InfoSec executives in Brazil (81%), Saudi Arabia/UAE (70%), and Australia (65%).
- Digital identity investments tell an interesting story. The research shows that high-priority investment is strong across all InfoSec executives (48%) and is especially strong for InfoSec executives in Brazil (62%) and the U.K. (58%). Regulatory pressures may be causing firms in these countries to prioritize identity improvements. From a different perspective, digital identity holds the highest percentage of medium-priority investment (42%) for all InfoSec executives, with funding or some other dependency still unresolved at the time of the survey—more so than for any other category. What is getting in the way of identity improvements at these firms? According to the research, an unmet need for outside assistance is a strong possibility, as 48% of InfoSec executives indicate identity as one of their top needs for external assistance (Figure 1). Supplemental research with Aite-Novarica Group's FI Cybersecurity Council indicates that identity projects are being impeded by gaps in external assistance, internal stakeholder alignment, and a lack of senior identity talent on staff.
- The big-picture view of 2023 CISO investments is quite encouraging. Ten solution types hold high-priority investment (funded, no dependencies) from at least 48% of InfoSec executives. In 2023, CISOs and InfoSec executives are overseeing security

improvements across the entire enterprise through plans and increased budgets, as seldom seen before. FS CISOs and InfoSec executives are commended for achieving this level of planning and funding support.

Table B presents the top 2023 cybersecurity investment for each country.

TABLE B: TOP 2023 CYBERSECURITY INVESTMENT BY COUNTRY

COUNTRY	TOP 2023 CYBERSECURITY INVESTMENT CATEGORY
Australia	Cloud security/attack surface management (65%)
Brazil	Cloud security/attack surface management (81%)
Germany	Malware defenses (80%)
India	Ransomware defenses (55%)
Saudi Arabia/UAE	Malware defenses (85%)
The U.K.	Malware defenses (70%)
The U.S.	API security (58%)

Source: Aite-Novarica Group

CONCLUSION

InfoSec executives at FIs and FS organizations:

- Seek and partner with distinguished cybersecurity vendors and analyst firms to address enterprise challenges in AI, defense against future threats, identity, and API security. Especially in these four areas, some market vendors may be unable to extend beyond industry hype and opaque value statements. Find the kind of high-value partners that hold true domain expertise, practical insights, and return on investment for your enterprise and can help your team achieve results.
- Find cybersecurity vendors and analyst firms with deep insights into cyber risks associated with market trends, such as bots, IoT, and digital workforce.
- Continue to improve cybersecurity budget planning for your enterprise, including for adjacent areas of the business wherein shared responsibility exists. Though you cannot plan for all attacks, a strong budget helps de-risk your firm and avoid the unplanned tactical spend that often comes with reactionary measures.
- Continue to elevate the vision for cybersecurity assurance across the enterprise.

Security vendors:

- For providers in the security domains of artificial intelligence, defense against future threats, identity, and API security, your company has a tremendous opportunity and a significant responsibility. Many FS InfoSec executives need considerable domain assistance and greater evidence of practical value from their security vendors. Consider enterprise-centered enterprise case studies and ROI models.
- InfoSec executives have strong budgets this year and for 2024. Expect InfoSec executives to leverage their funds judiciously to maximize value from chosen cybersecurity solutions.

RELATED AITE-NOVARICA GROUP RESEARCH

API Security: Market Landscape, March 2023

Top 10 Trends in Cybersecurity, 2023: A Sea of Change for the Industry, January 2023

Attack Surface Management: Avoiding Device Whack-a-Mole, October 2022

Aite Matrix: Leading Bot Detection and Management Providers, August 2022

Open Banking, Open Finance, Open Economy: The New Identity of Finance, May 2022

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

CONTACT

Research, consulting, and events:
sales@aite-novarica.com

Press inquiries:
pr@aite-novarica.com

All other inquiries:
info@aite-novarica.com

Global headquarters:
6 Liberty Square #2779
Boston, MA 02109
www.aite-novarica.com

AUTHOR INFORMATION

John Horn
+1.330.312.3302
jhorn@aite-novarica.com

Research Design & Data:
Sonia Kundal
skundal@aite-novarica.com