BEHIND THE FIREWALL:

Assessing Cyber Resilience in U.S. Manufacturing

MxD Survey of U.S. Manufacturers

Produced by APCO

Letter from the CEO

The digital thread weaves through our manufacturing organizations and supply chains, connecting every process and operation to enhance efficiency, boost productivity, and fuel continuous improvement. However, with the knowledge that 86% of the cybersecurity threats facing the manufacturing sector are targeted, this connectivity can also become a weakness.

The manufacturing sector continues to be the most-targeted sector for cyber-attacks. This unfortunate reality comes at a time when American manufacturers are turning to a wide range of digital tools as they prioritize greater resilience in their post-pandemic supply chains.

As the recognized National Center for Cybersecurity in Manufacturing by the Department of Defense, MxD stands at the forefront of working with the U.S. manufacturing sector to prepare and protect America's supply chains against cybersecurity threats through our programs, partnerships, and strategic initiatives.

With our ecosystem of manufacturers, solution providers, government stakeholders, and academic partners, MxD drives economic prosperity and supports national security by leading digital innovation and adoption in U.S. manufacturing to deliver a resilient and revitalized supply chain. We tackle critical manufacturing challenges, particularly those faced by global manufacturing primes and the defense industrial base that meets the needs of the Pentagon, by empowering a skilled workforce, modernizing supply chains, and securing U.S. manufacturing operations.

To continue focusing our efforts where manufacturers need the most support, MxD conducted a comprehensive survey to establish a baseline of cybersecurity in manufacturing and to provide a compass pointing toward preparedness and resilience. It identifies key areas where manufacturers can benefit from additional resources in strengthening their cybersecurity infrastructure and will guide future investment by MxD.

Creating a more secure manufacturing sector requires collaboration. This report provides us with a starting point and signpost for the right direction, but it is up to us to work together and implement the much-needed improvements in cyber preparedness, resilience, and optimizing U.S. manufacturing for a digital future.

Berardino Baratta,
CEO

Overview

MxD has partnered with APCO Insight, the strategic research consultancy arm of APCO, to examine cybersecurity readiness within the U.S. manufacturing sector, a critical component of the nation's economic and security infrastructure.

As prime targets for cyber-attacks, manufacturers confront risks that threaten their operations and supply chains. For small and medium-sized manufacturers, the challenge is intensified by the cost of implementing effective cybersecurity measures. Within the sector, decision-makers weigh the balance between risk, cost, and the significant business advantages of cybersecurity investment, from safeguarding operations to bolstering brand reputation.

This survey offers insights into the current state of cybersecurity preparedness among manufacturers and identifies key areas where they can benefit from additional guidance and support in strengthening their cybersecurity infrastructure. We further investigate variations in cybersecurity preparedness among small-medium manufacturers and large manufacturers, as well as differences across manufacturing sectors of interest—aerospace and defense, defense industrial base and chemicals.

Approach

APCO Insight conducted a poll of 750 manufacturers in the United States.

The poll was conducted between November 30 and December 15, 2023. To qualify for the poll, participants were required to be senior-level cybersecurity decision-makers at a manufacturing company that conducts business in the U.S. For the purposes of our analysis, we segmented respondents based on manufacturing sector and size of the company. Respondents represent a broad variety of manufacturing sectors including aerospace and defense, chemicals and materials, medical devices, plastics and rubber, food and beverage, industrial machinery and equipment, textiles and apparel, automotives and components, energy and utilities, pharmaceutical preparations, and semiconductors. These were categorized into four groups—aerospace and defense, defense industrial base (DIB), chemicals, and other manufacturing sector (Other Mfg)-to draw a distinction between discrete manufacturing versus process manufacturing as well as the stringent requirements that aerospace and the DIB sectors face. These sectors align well with the MxD ecosystem and markets MxD serves. We define the size of a manufacturer by the number of employees. Small-medium manufacturers have 500 or fewer employees, and large manufacturers have more than 500 employees.

Respondent Profile		
Sector	Aerospace and Defense	106
	Defense Industrial Base (DIB)	102
	Chemicals	137
	Other manufacturing sectors (Other Mfg)	405
Company Size	Small-medium manufacturers (500 or fewer employees)	630
	Large manufacturers (more than 500 employees)	120
	Total	**750**

Disclaimers

This study was sponsored by MxD. The responses in this report reflect the opinions of the survey respondents and do not necessarily represent the views of MxD. If you have questions, you can contact APCO Insight at cybersecuritymfgsurvey@APCOworldwide.com.

Executive Summary

The state of cybersecurity within the U.S. manufacturing sector signals an imperative for reinforced defensive strategies, especially for small to medium manufacturers (SMMs) who encounter unique challenges compared to their larger counterparts.

Although a remarkable 76% of manufacturers report a high level of confidence in their cybersecurity capabilities, closer inspection reveals a discrepancy between this confidence and the actual execution of cybersecurity protocols.

The survey highlights a striking gap in dedicated talent, with only 43% of manufacturers employing a cybersecurity leader—a figure that drops to 35% among SMMs, calling attention to the need for focused cybersecurity oversight. The readiness gap extends to policy comprehensiveness, with just 16% of manufacturers boasting extensively detailed cybersecurity policies. While 76% of large manufacturers adhere to moderately comprehensive policies, only 42% of SMMs meet this standard. This disparity is more pronounced among the smallest SMMs, those with 100 employees or fewer, who display a weaker cybersecurity posture than SMMs with larger workforces. In sectoral comparison, the aerospace and defense sector leads in preparedness, likely reflecting more stringent cybersecurity requirements of their customers.

The survey also sheds light on the intricacies of vendor management and supply chain cybersecurity: 68% of manufacturers have embedded cybersecurity requirements in contracts, yet only 31% rate these as comprehensive. This underscores the necessity for heightened contractual cybersecurity stipulations and proactive vendor audits, given 64% of manufacturers possess the provisions to conduct such checks.

Cybersecurity emerges as a shared investment focus across the manufacturing industry, with a consensus of 82% planning to raise cybersecurity spending in the upcoming budget cycle. This highlights an industry-wide acknowledgment of cybersecurity's integral part in maintaining a competitive edge. Common practices across manufacturers include adherence to basic cybersecurity policies, mandated training, usage of essential tools like multi-factor authentication, and the capability to detect and manage cyber-attacks. Yet, a considerable 74% of manufacturers acknowledge facing moderate difficulty in meeting the cybersecurity requirements of customer RFPs and contracts.

The insights conveyed call upon manufacturing leaders to fortify their cybersecurity posture strategically. This includes enhancing leadership engagement, augmenting internal capabilities, and harmonizing cybersecurity readiness with comprehensive business continuity planning. As manufacturing faces an evolving cyber threat environment, decision-makers should prioritize reinforcing cybersecurity not just as a safeguard but as a fundamental pillar supporting business growth and sustainability.

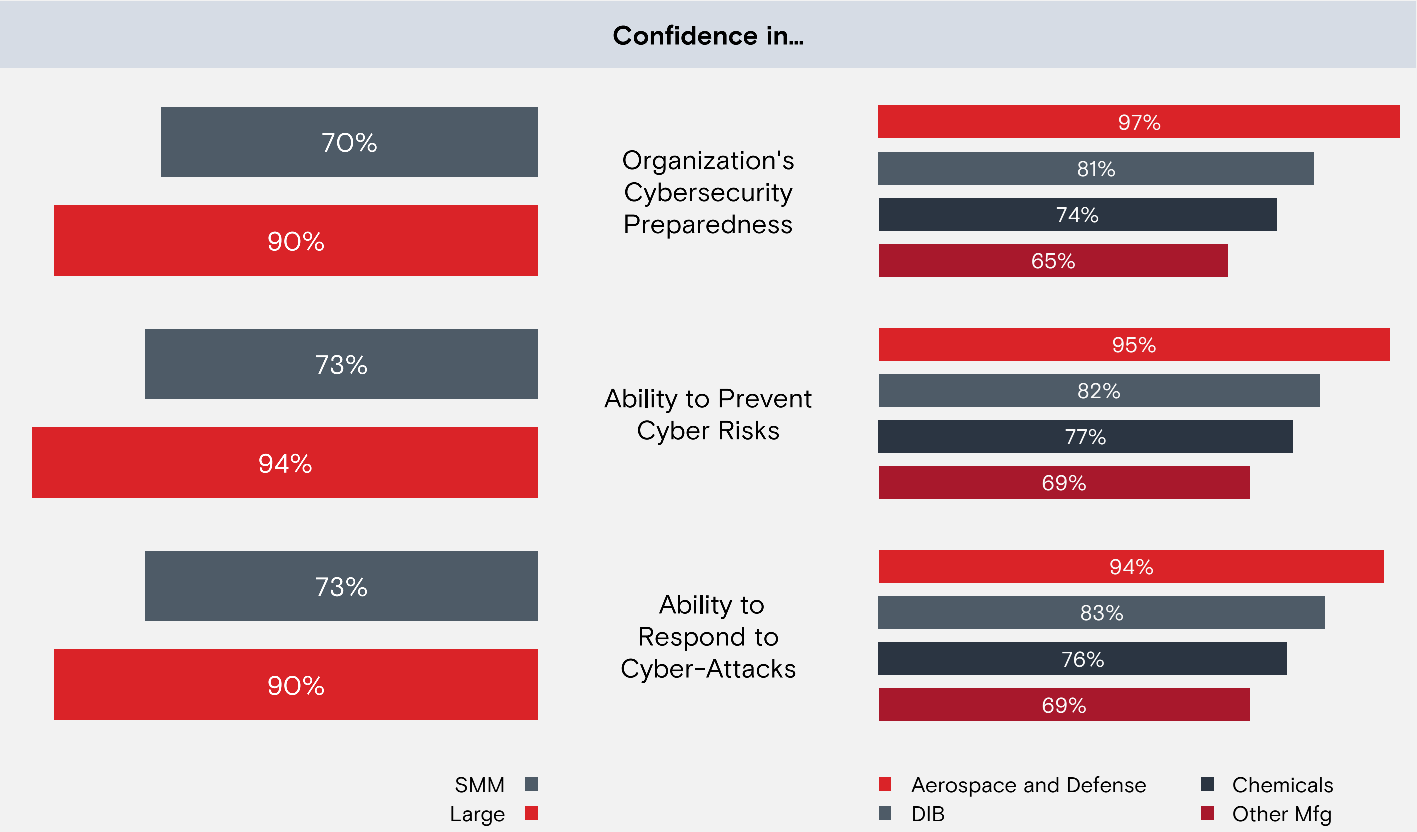
CHAPTER 1

Cybersecurity Preparedness Practices

Perceived Preparedness

Manufacturers’ ability to detect and mitigate cyber-attacks shows a considerable degree of confidence, though it may not fully align with established preparedness metrics. Around 76% of manufacturers express confidence in their organization's capacity to both prevent cyber risks and respond to cyber-attacks, with 73% confident in their overall cybersecurity preparedness. Large manufacturers and global manufacturers outpace their SMMs and domestic counterparts in confidence levels, which may reflect greater resources and experience in dealing with cyber threats. Despite this overall confidence, there is an indication of potential overconfidence, particularly among SMMs, suggesting the need for a reality-aligned perception of cybersecurity capabilities.

Figure 1. Confidence in Preparedness, Risk Prevention and Response
By Company Size and Sector

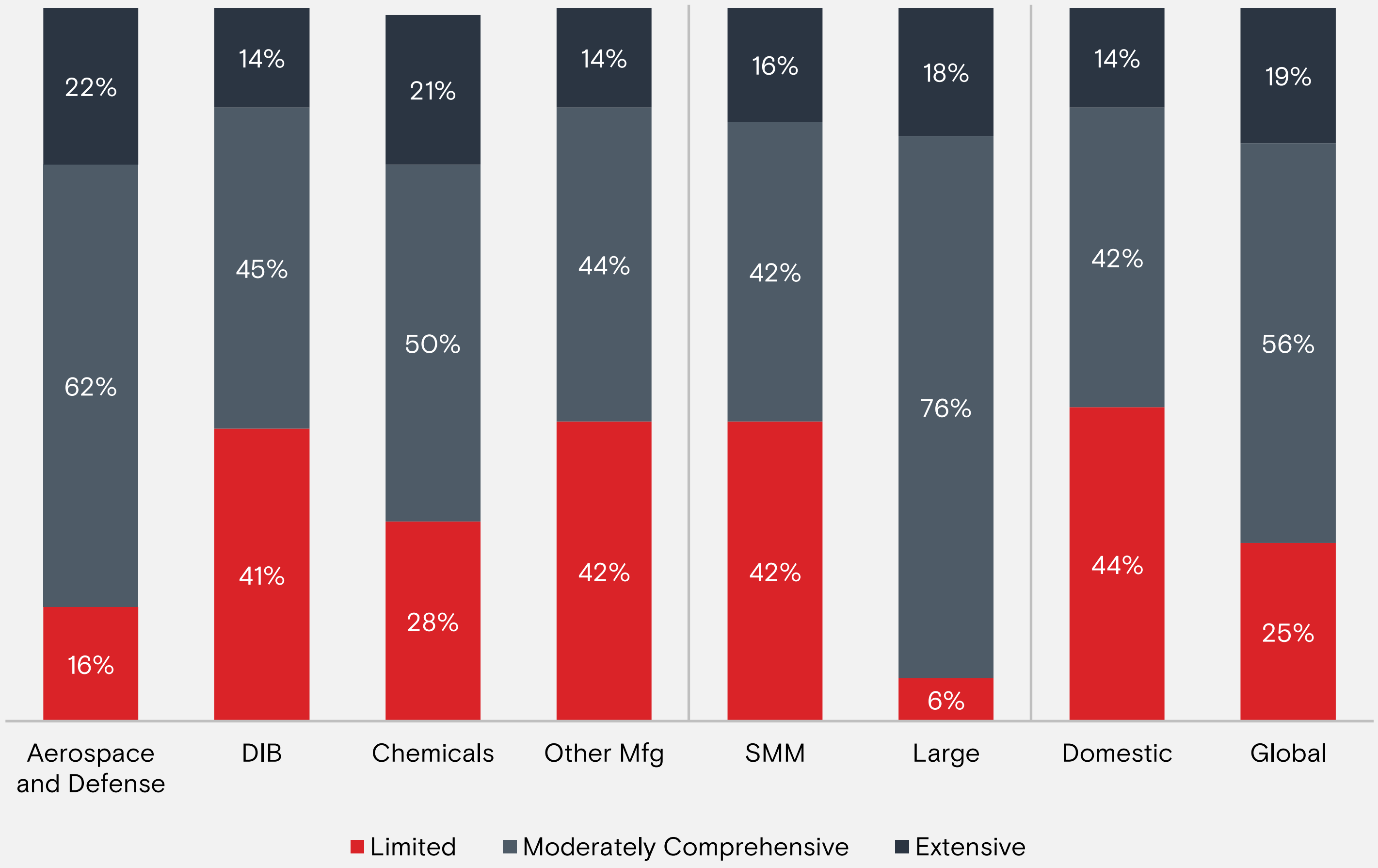


Q17. How confident are you in - Confident (7-10)

Policies & Procedures

Manufacturers' cybersecurity policies reveal a spectrum of comprehensiveness, laying the groundwork for the industry's varied capabilities in safeguarding digital assets. While every manufacturer maintains some level of documentation, it's the extent of these policies that differs: 48% report having a moderately comprehensive policy, whereas only a leaner 16% describe theirs as extensively detailed, highlighting potential for further development in policy depth. Sector-wise nuances emerge, with the aerospace and defense sector having more robust policies—encompassing a wider range of cybersecurity topics—than the defense industrial base, chemicals, or other manufacturing sectors. This disparity in policy depth is amplified by size and reach; 76% of large manufacturers have moderately comprehensive policies, surpassing the 42% of SMMs. Similarly, 56% of global manufacturers exceed the 42% of domestic-only operators in having moderately comprehensive policies. These differences highlight a considerable gap in cybersecurity standardization across sectors and geographies, emphasizing the industry's urgent need for uniform preparedness and policy depth.

Figure 2. Comprehensiveness Cybersecurity Policy
By Company Sector, Size, and Reach



Q05. How comprehensive is your organization's formal, documented cybersecurity policy?

Preparedness Practices

For manufacturers, implementing thorough and regular cybersecurity training is essential, as their employees, from the factory floor to the executive suite, are often the primary line of defense against cyber threats like email phishing. The heartening news—73% of manufacturers require annual training; the caveat—over half (54%) restrict it to specific roles, thereby inadvertently stratifying the cybersecurity knowledge landscape. While IT staff and engineering/R&D roles are predominantly covered, with 88% and 61% respectively being required to complete training, the numbers hint at unguarded entry points in organizations where only select roles are mandated to train. Less than half of manufacturers require finance (41%), manufacturing/plant (32%), legal (30%), executive leadership (26%), and sales (10%) teams to undergo cybersecurity training, areas where security awareness is equally imperative to cultivate a resilient cybersecurity posture organization wide. Operational readiness appears stronger in large manufacturers and the aerospace and defense sector, where across-the-board training is more likely to be required. This highlights an area where SMMs in particular may benefit from enhanced guidance to leverage their entire workforce to strengthen their cybersecurity defenses.

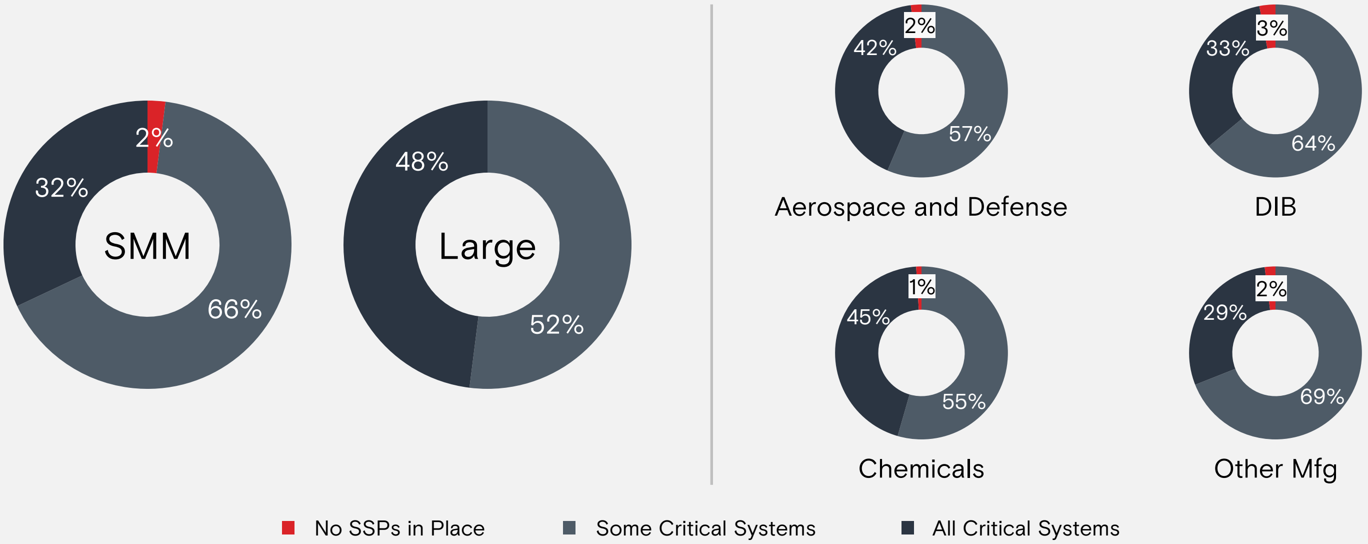
Figure 3. Employee Roles Required to Complete Cybersecurity Awareness Training
By Company Sector

	Aerospace and Defense	DIB	Chemicals	Other Mfg
Sales	8%	8%	4%	13%
Executive Leadership	19%	34%	21%	27%
Legal	42%	60%	17%	27%
Manufacturing/Plant Floor	42%	40%	32%	28%
Finance	39%	44%	47%	38%
Engineering/R&D	64%	56%	72%	58%
IT	86%	88%	83%	89%

Q06c. Which roles are required to complete cybersecurity awareness training?

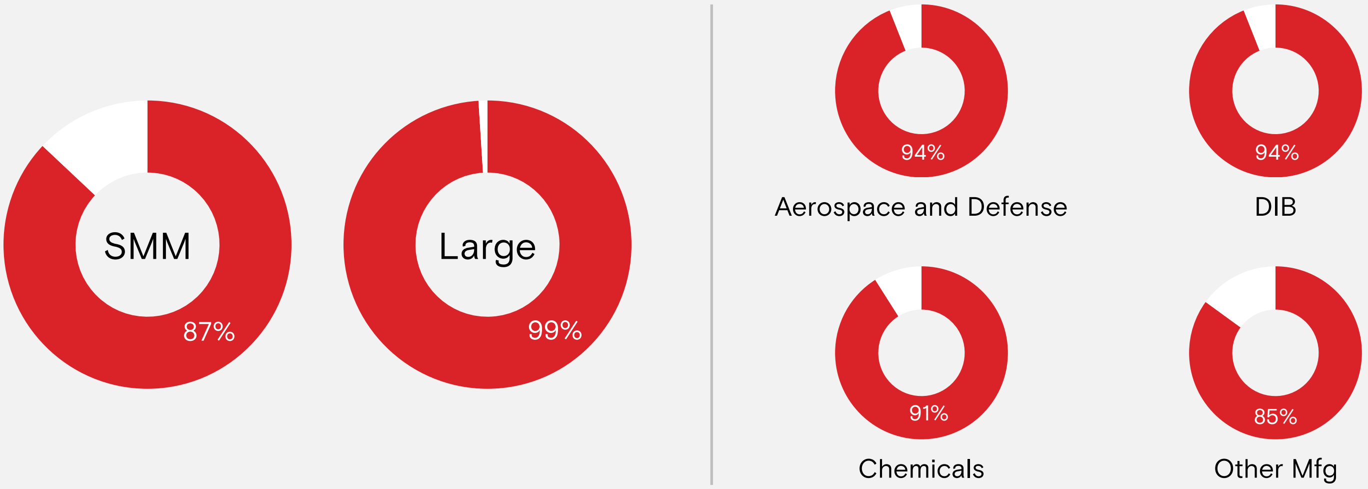
The maintenance of System Security Plans (SSPs) and the deployment of multi-factor authentication (MFA) further chart a checkered readiness field. Only 34% of manufacturers have comprehensive SSPs in place, evidencing a dissonance between perceived security and actual preparative action. MFA, on the other hand, enjoys wide acceptance (89%), marking a significant positive step.

Figure 4. System Security Plans (SSPs) in Place for Critical IT Systems
By Company Size and Sector



Q07. Does your organization maintain System Security Plans (SSPs) for critical IT systems and environments?

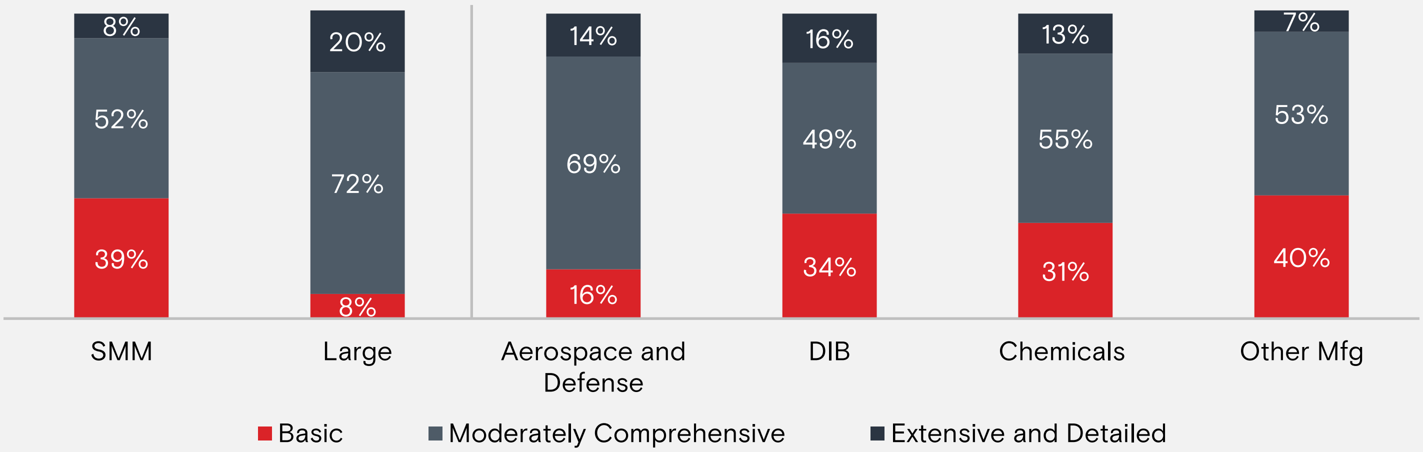
Figure 5. Company Uses Multi-factor Authentication for Access to Networks and Systems (% Yes)
By Company Size and Sector



Q08. Does your organization use multi-factor authentication for access to networks and systems?

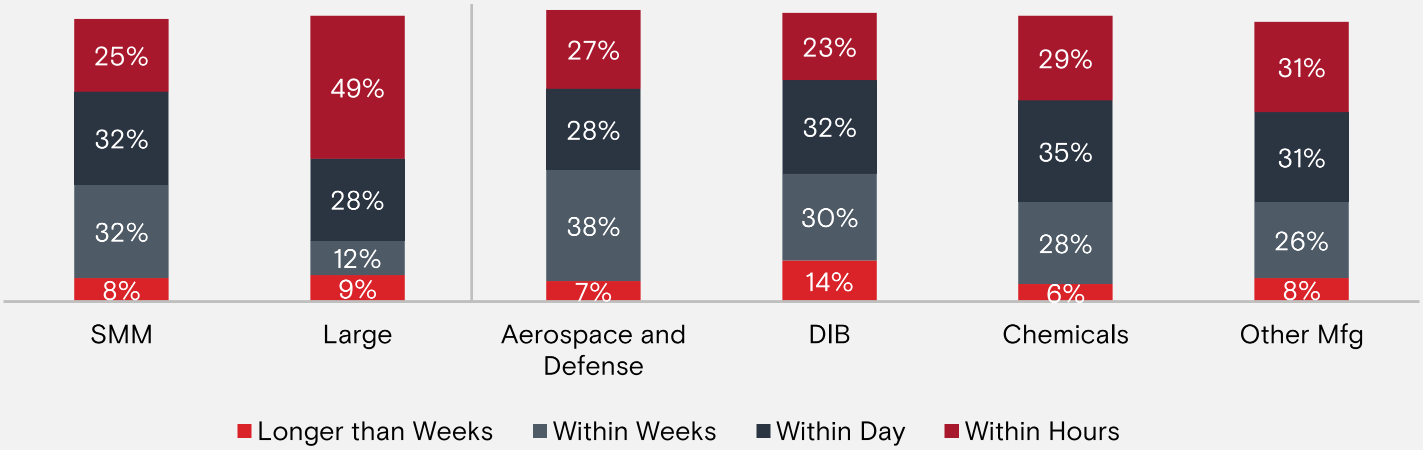
On the matter of keeping cybersecurity mechanisms current, the majority (58%) review and update controls like firewall rules and access controls annually, but a proactive subset (32%) engages in this essential maintenance on a quarterly basis, with large manufacturers (51%) more diligent in this regard than SMMs (28%). Likewise, the frequency of hands-on training exercises such as simulations or tabletop exercises follows a similar pattern, conducted annually by most manufacturers (66%), suggesting an industry norm of bolstering preparedness this way at least once a year. Large manufacturers again take the lead in having either moderate or extensive incident response plans, with SMMs more likely to only have a basic plan in place.

Figure 6. Comprehensiveness of Incident Response Plan
By Company Size and Sector



Q10. How comprehensive is your organization's cybersecurity incident response plan?
Percentages may not add to 100% due to rounding.

Figure 7. Time to Detect and Contain a Cyber-attack
By Company Size and Sector



Q12. On average, how quickly can your team detect and contain a cyber-attack on your systems?
Percentages may not add to 100% due to rounding.

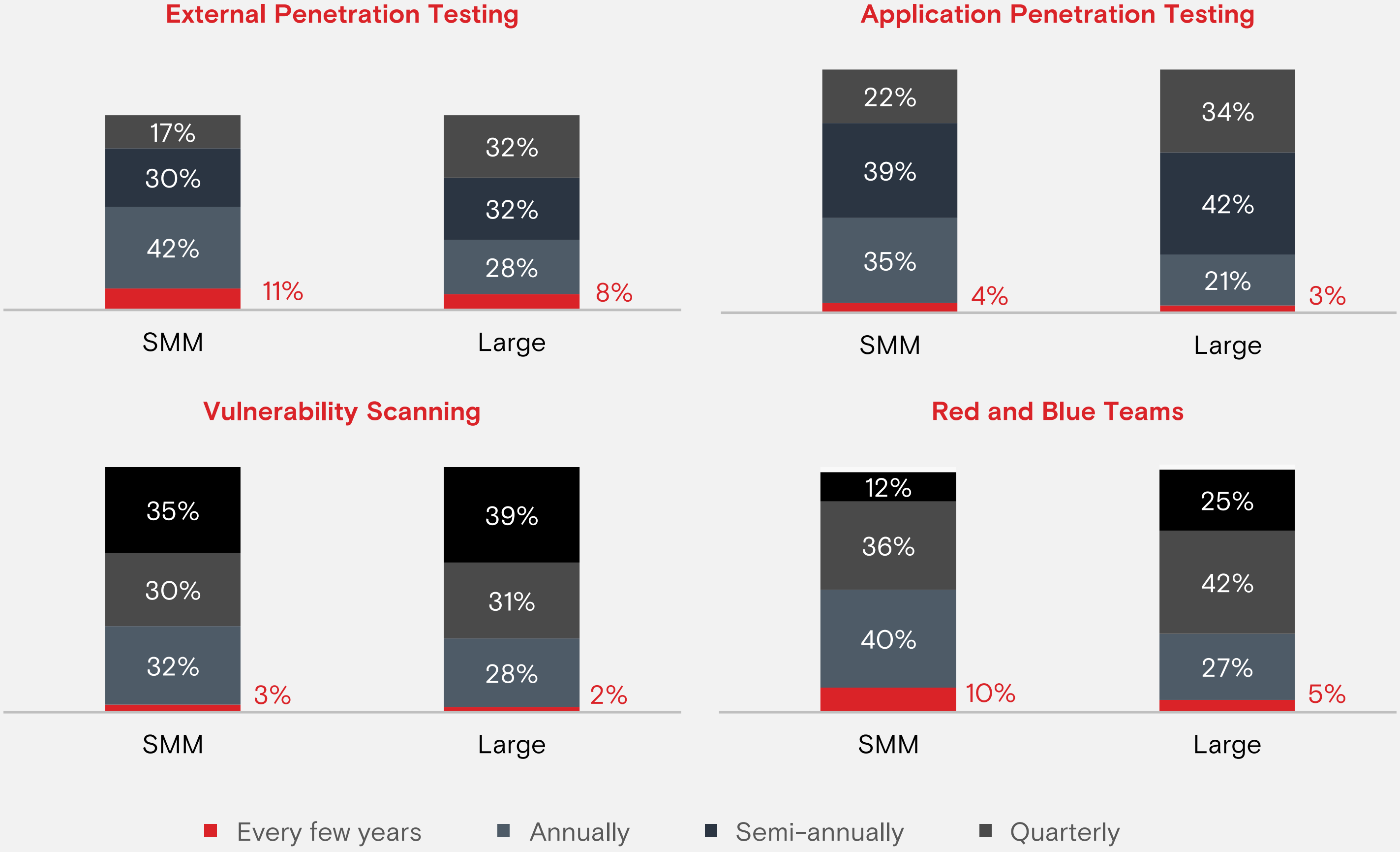
Penetration Testing

Penetration testing and vulnerability assessments serve as the proving grounds for a manufacturer's cybersecurity defenses, with the frequency of these exercises painting a vivid picture of industry readiness.

The frequency of security testing among U.S. manufacturers varies significantly based on company scale. While 40% undertake annual external penetration testing to assess their cyber fortifications, a deeper look reveals that large manufacturers double down on preparedness: 32% conduct these crucial checks quarterly, compared to the 17% of SMMs who do the same. Application penetration tests, targeting software vulnerabilities, are conducted semi-annually by 39% of all manufacturers, with large firms again taking the lead—34% perform these tests quarterly versus 22% of SMMs.

Red and blue team assessments, which simulate cyber-attacks to test response procedures, show that 37% of manufacturers conduct these annually or semi-annually. However, large manufacturers are more diligent, with 25% holding these assessments quarterly, demonstrating an elevated commitment to cybersecurity vigilance. These discrepancies not only illuminate the proactive stance of large organizations but also highlight a critical opportunity for SMMs to intensify their testing to fortify against evolving cyber threats.

Figure 8. Frequency Manufacturers Conduct Assessments
By Company Size

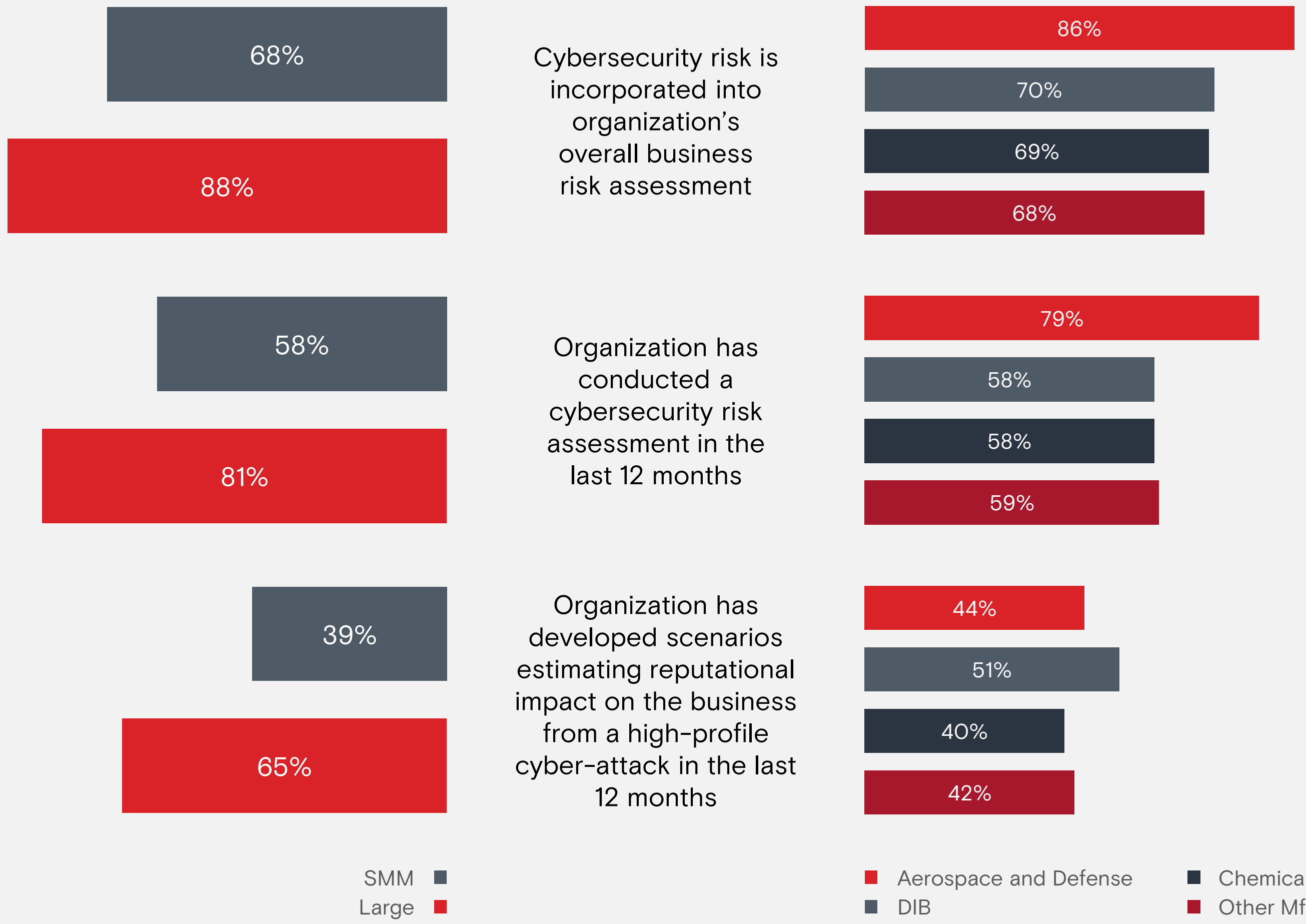


Q18. How frequently does your organization conduct each of the following assessments?
Percentages may not add to 100% due to rounding.

Business Risk Assessment

Integrating cybersecurity risk into broader business risk assessments is a practice adopted by a majority (71%) of manufacturers, acknowledging the significance cybersecurity holds in their organizational strategy. Again, large manufacturers are at the forefront (88%), compared to 68% of SMMs. Manufacturers in the aerospace and defense sector are notably more likely to integrate cybersecurity risk into their overall business risk assessments, emphasizing how critical robust cybersecurity preparedness is for this sector. Furthermore, while 62% of manufacturers conduct risk assessments to estimate potential financial losses from various cyber-attack scenarios, more than half (56%) have not explored scenarios that estimate reputational damage, an aspect critical to post-incident recovery. Only a fraction (6%) fully integrate cyber risk into business continuity and disaster recovery plans, an opportunity area for enhancing enterprise resilience, with large manufacturers and SMMs integrating these aspects at rates of 38% and 15%, respectively.

Figure 9. Business Risk Assessments
By Size of Company and Sector



Q13. Is cybersecurity risk incorporated into your organization's overall business risk assessment? Yes
Q15. In the last 12 months, has your organization conducted a cybersecurity risk assessment to estimate potential financial losses from different attack scenarios? Yes
Q16. In the last 12 months, has your organization developed scenarios estimating reputational impact on the business from a high-profile cyber-attack? Yes

Spotlight on Aerospace and Defense

The aerospace and defense sector stands out in terms of cybersecurity preparedness compared to the other three sectors, DIB, chemicals, and other manufacturing sectors.

This sector outperforms others in incorporating cybersecurity risk into its overall risk assessments and demonstrates a more robust approach when it comes to cybersecurity training, controls, and incident response.

Aerospace and defense manufacturers prioritize cybersecurity training, requiring all staff to complete cybersecurity awareness training at a higher rate (59%) compared to other sectors such as DIB (51%), chemicals (43%), and other manufacturing sector (41%). Furthermore, they demonstrate a proactive approach in reviewing and updating cybersecurity controls, with 42% of aerospace and defense manufacturers engaging in this practice compared to only 27% of chemicals and 31% of other manufacturing sector.

In terms of incident response planning, aerospace and defense manufacturers exhibit greater preparedness, with 69% having moderately comprehensive incident response plans. This surpasses the preparedness levels of DIB (49%), chemicals (55%), and other manufacturing (53%) sectors. The aerospace and defense sector also outdoes other sectors in conducting cybersecurity training simulations or tabletop exercises, with 36% engaging in these exercises compared to chemicals (23%) and other manufacturing (21%) sectors.

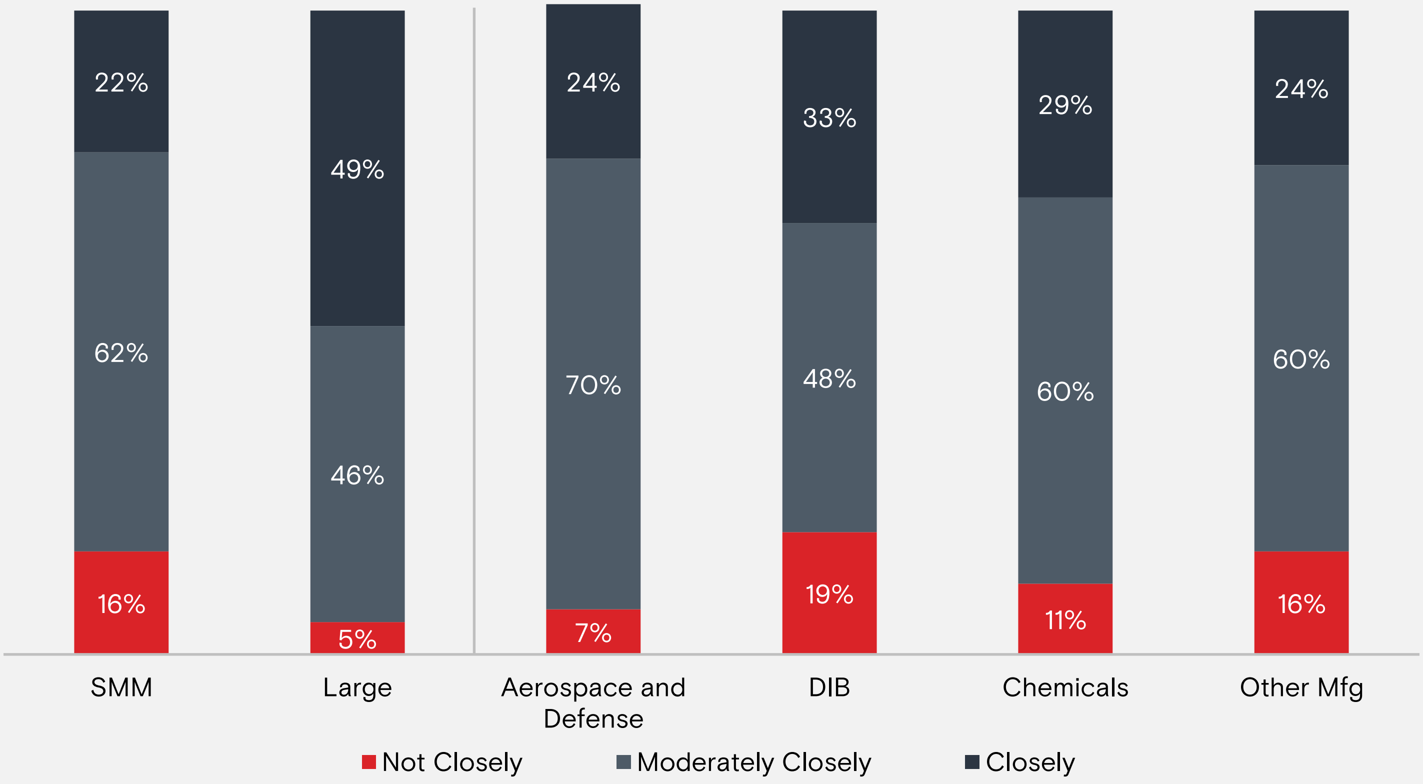
Importantly, the study reveals that aerospace and defense manufacturers (86%) significantly outperform other sectors (DIB 70%, chemicals 69%, and other manufacturing sector 68%) when it comes to incorporating cybersecurity risk into their organization's overall business risk assessment. This demonstrates their understanding of the critical role cybersecurity plays in overall business operations. Lastly, aerospace and defense manufacturers (79%) show a higher likelihood of conducting cybersecurity risk assessments to estimate potential financial losses from different attack scenarios, outpacing DIB (58%), chemicals (58%) and other manufacturing sector (59%). This indicates their proactive approach in assessing the potential impact of cybersecurity incidents and mitigating financial risks.

Regulatory Compliance and Audit Frequency

Monitoring of Laws and Regulations

Staying abreast of cybersecurity laws and regulations is key for manufacturers. Fifty-nine percent of manufacturers follow updates moderately closely, evidencing an industry-wide moderate dedication to compliance tracking. Nevertheless, when dissecting this data by size, 49% of large manufacturers monitor regulatory changes very or extremely closely, contrasting with just 22% of SMMs who maintain the same level of scrutiny. Unsurprisingly, SMMs with 100 employees or fewer are least likely to closely follow legal and regulatory developments. When comparing sectors, the aerospace and defense sector more proactively tracks cybersecurity laws and regulations (70%). This gap suggests a disparity in prioritization of regulatory compliance or a potential difference in resources available for such efforts.

Figure 10. How Closely Organization Monitors for New or Updated Cybersecurity Laws and Regulations
By Company Size



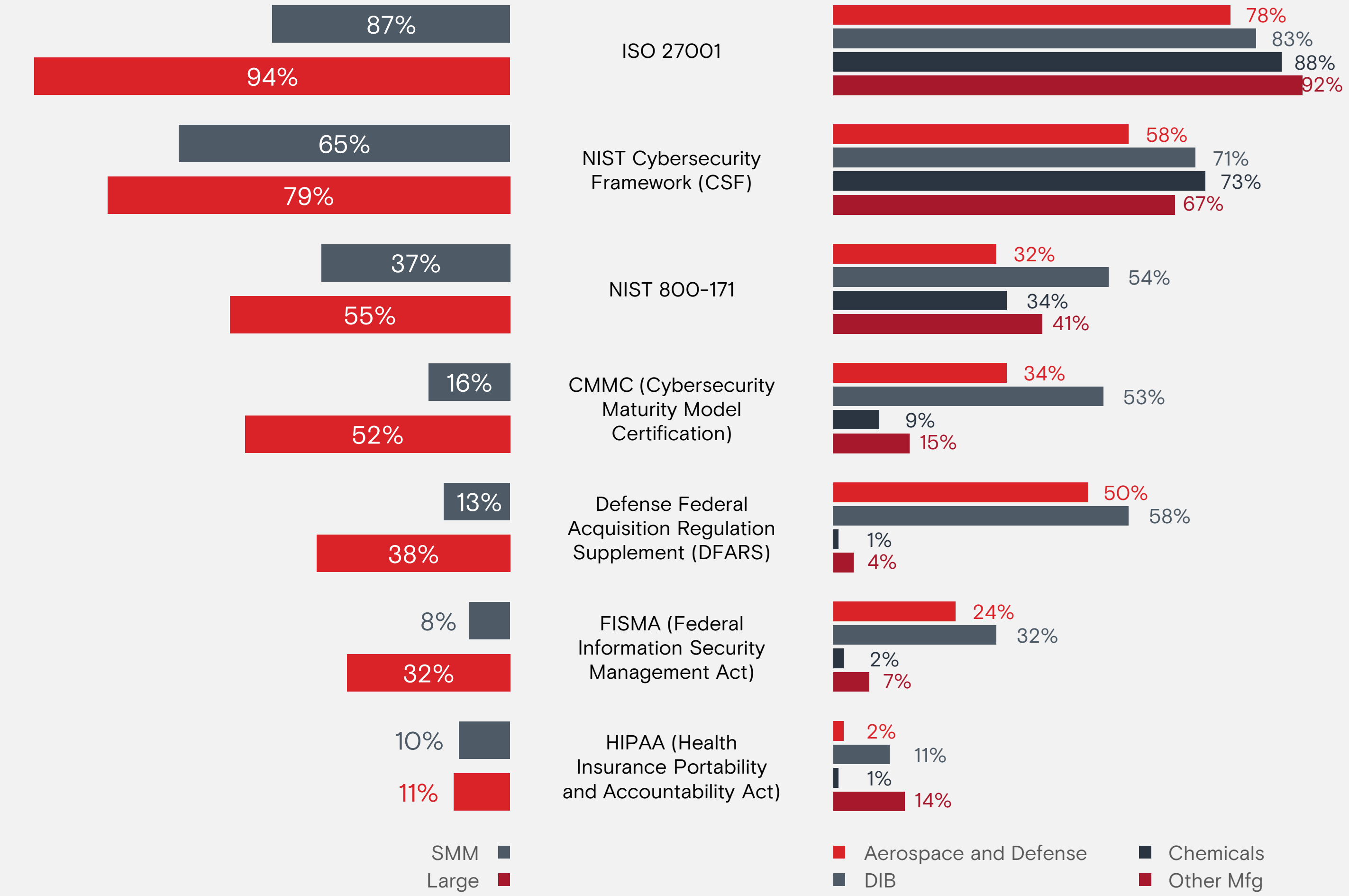
Q19. How closely does your organization monitor for new or updated cybersecurity laws and regulations?

Internal Compliance Audits

Internal audits for industry standards serve as a crucial measure of cybersecurity readiness. Our survey shows a solid dedication to compliance, with 88% of manufacturers having conducted audits against ISO 27001 standards and 67% against the NIST Cybersecurity Framework in the past year. It's primarily the larger manufacturers that frequently perform these audits across a wider range of standards, suggesting they have more comprehensive compliance frameworks and likely face more regulatory pressures.

The frequency of compliance standard assessments reveals varying levels of diligence among manufacturers, with a tendency towards annual or semi-annual audits. Specifically, 43% of firms conduct annual CMMC audits, and 31% perform DFARS compliance checks semi-annually. Large manufacturers are particularly vigilant, with 26% carrying out quarterly audits for NIST frameworks, compared to only 11% of SMMs—a difference that highlights disparities in compliance monitoring's frequency and robustness. In sectors that bear significant security implications, such as the defense industrial base, the commitment to rigorous compliance is even more pronounced; 58% of these manufacturers undertake at minimum annual audits for DFARS.

Figure 11. Organization Performed Internal Cybersecurity Audits Against the Following Compliance Standards in the Past 12 Months
By Company Size and Sector

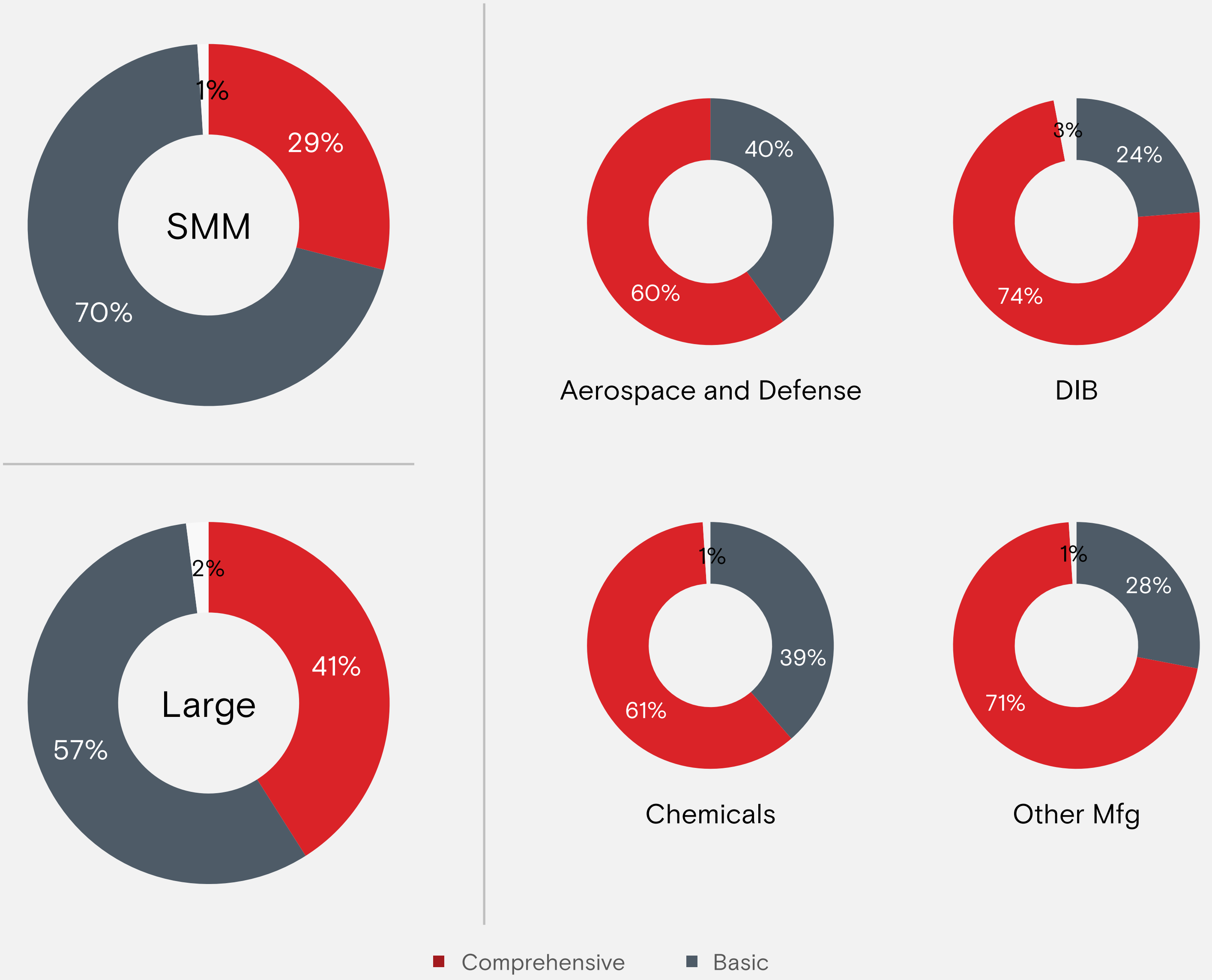


Q20. In the past 12 months, has your organization performed internal cybersecurity audits against any of the following compliance standards? - Yes

Vendor and Supplier Cybersecurity Posture

The incorporation of cybersecurity requirements in vendor and supplier contracts is a nuanced area within the manufacturing sector, recognizing supply chain security as a crucial aspect of overall cyber defenses. The data indicate that while 68% of manufacturers have some level of cybersecurity requirements in their contracts, only 31% describe these as comprehensive. This distinction is more pronounced among large manufacturers, where 41% include extensive cybersecurity stipulations, compared to 29% of SMMs, potentially due to the broader resources at their disposal and potential risks. Among SMMs, those with 100 employees or fewer tend to have basic, rather than comprehensive requirements in their vendor and supplier contracts, while manufacturers with over 100 employees tend to have comprehensive requirements.

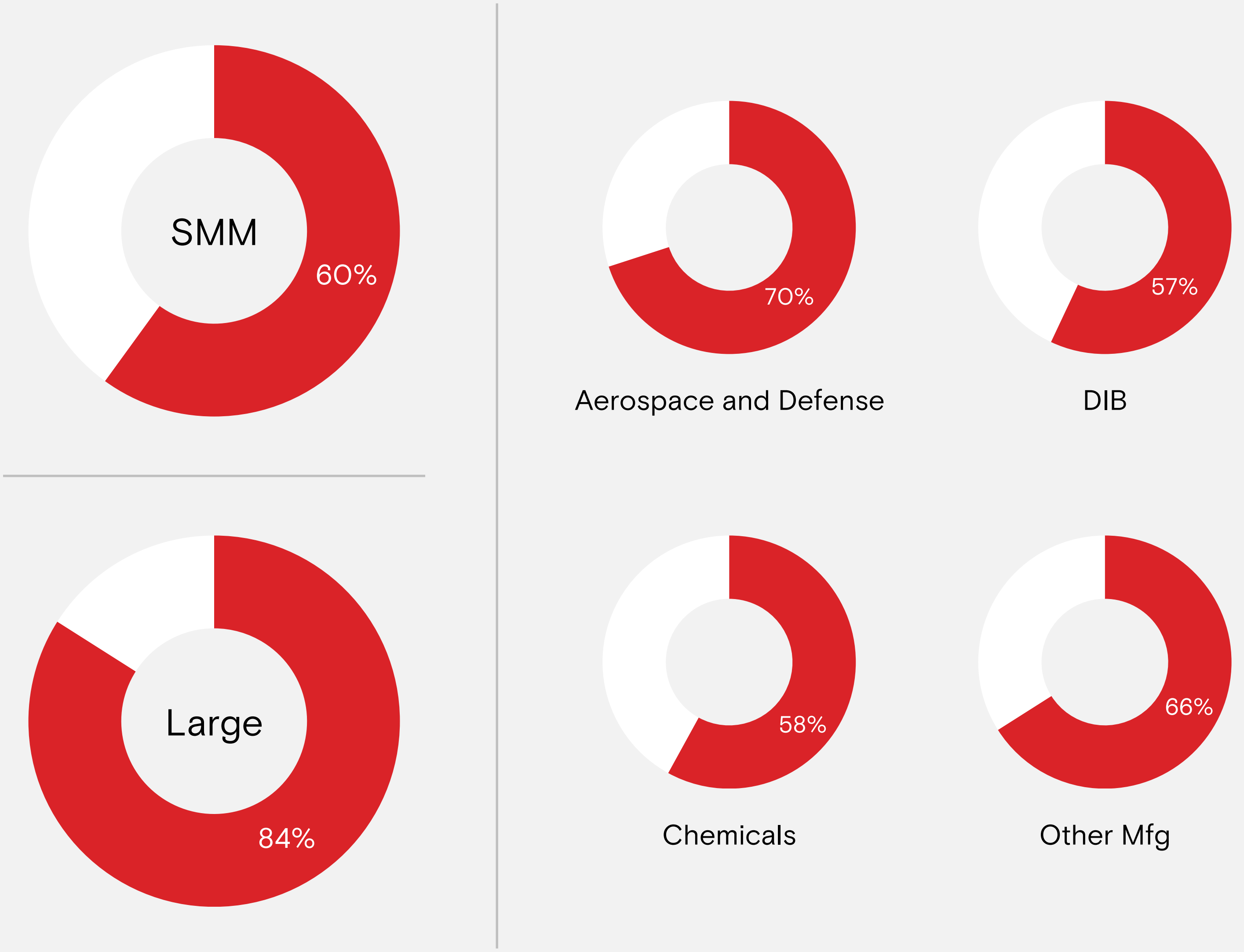
Figure 12. Cybersecurity Requirements in Vendor & Supplier Contracts
By Company Size and Sector



Q22. Does your organization include cybersecurity requirements in vendor and supplier contracts?

The ability to execute cybersecurity audits on vendors—a critical extension of internal cybersecurity practices—is reported by 64% of manufacturers, which points to a relatively high level of proactivity in managing third-party cyber risks. Large manufacturers take the lead, with 84% having the contractual provisions to audit vendors, nearly 25% higher than SMMs. Among SMMs, those with over 100 employees lead in adding provisions. This control difference could be pivotal in the event of a supply chain cyber incident. Termination of vendor relationships due to unresolved cybersecurity concerns underscores the importance of these provisions, with 21% of all manufacturers having done so. Large manufacturers, who tend to have more vendor relationships, are more likely than SMMs to have taken such a decisive action, 33% and 19%, respectively. SMMs with 100 employees or fewer are even less likely to terminate a vendor relationship. These figures underscore not only the vigilance but also the readiness to mitigate risk through strong contractual relationships and the potential need for SMMs to develop more robust vendor cybersecurity assessment capabilities.

Figure 13. Vendor Audit Provisions in Contracts, "Yes"
By Company Size and Sector



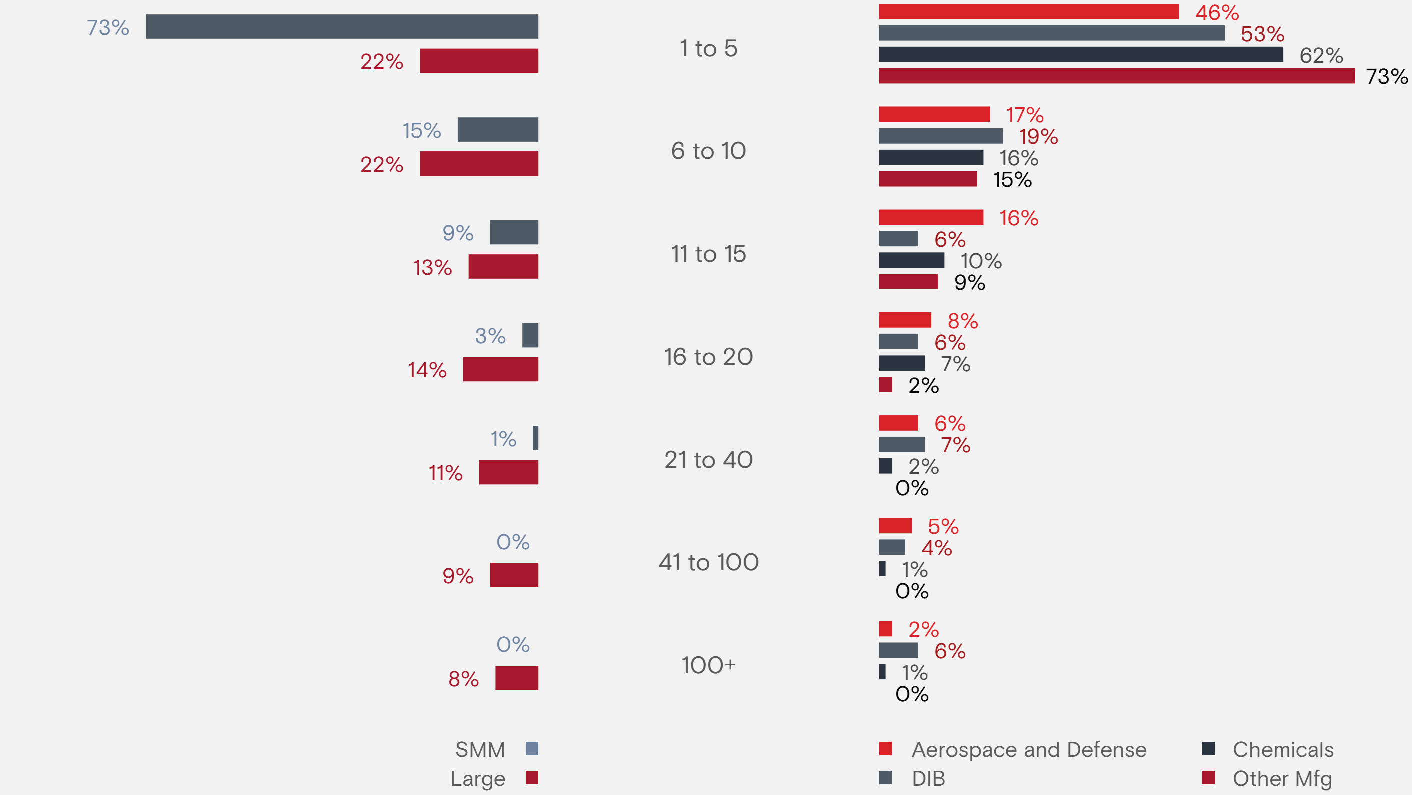
Q23. Do your contracts with vendors and suppliers contain provisions allowing your organization to audit their cybersecurity controls?

Barriers to Cybersecurity Preparedness

Staffing

A manufacturing company with a dedicated cybersecurity leader ensures there is focused oversight and strategic direction in protecting critical infrastructure and sensitive data from the ever-increasing and sophisticated cyber threats. Across U.S. manufacturers, the presence of a cybersecurity leader and dedicated teams to support them varies notably by the company size and sector. Just 43% of all manufacturers have a dedicated cybersecurity leader such as a CISO or Director of Cybersecurity with the defense industrial base sector leading the way at 56%. The disparity is stark when compared by size: a robust 88% of large manufacturers have assigned such leaders, in contrast to 35% of small-medium manufacturers (SMMs). However, nearly half (47%) of SMMs with 101 to 500 employees have a cybersecurity leader. This discrepancy delineates a critical gap in cybersecurity leadership, which is amplified further when considering the number of full-time employees dedicated to this function. Seventy-three percent of SMMs employ a team of five or fewer full-time cybersecurity employees, whereas 71% of larger manufacturers have teams of up to 20 full-time cybersecurity professionals. Again, this disparity is most pronounced for manufacturers with 100 or fewer employees, with almost all (97%) declaring having between one and five employees dedicated to cybersecurity.

Figure 14. Number of Full Time Staff Dedicated to Cybersecurity
By Company Size and Sector



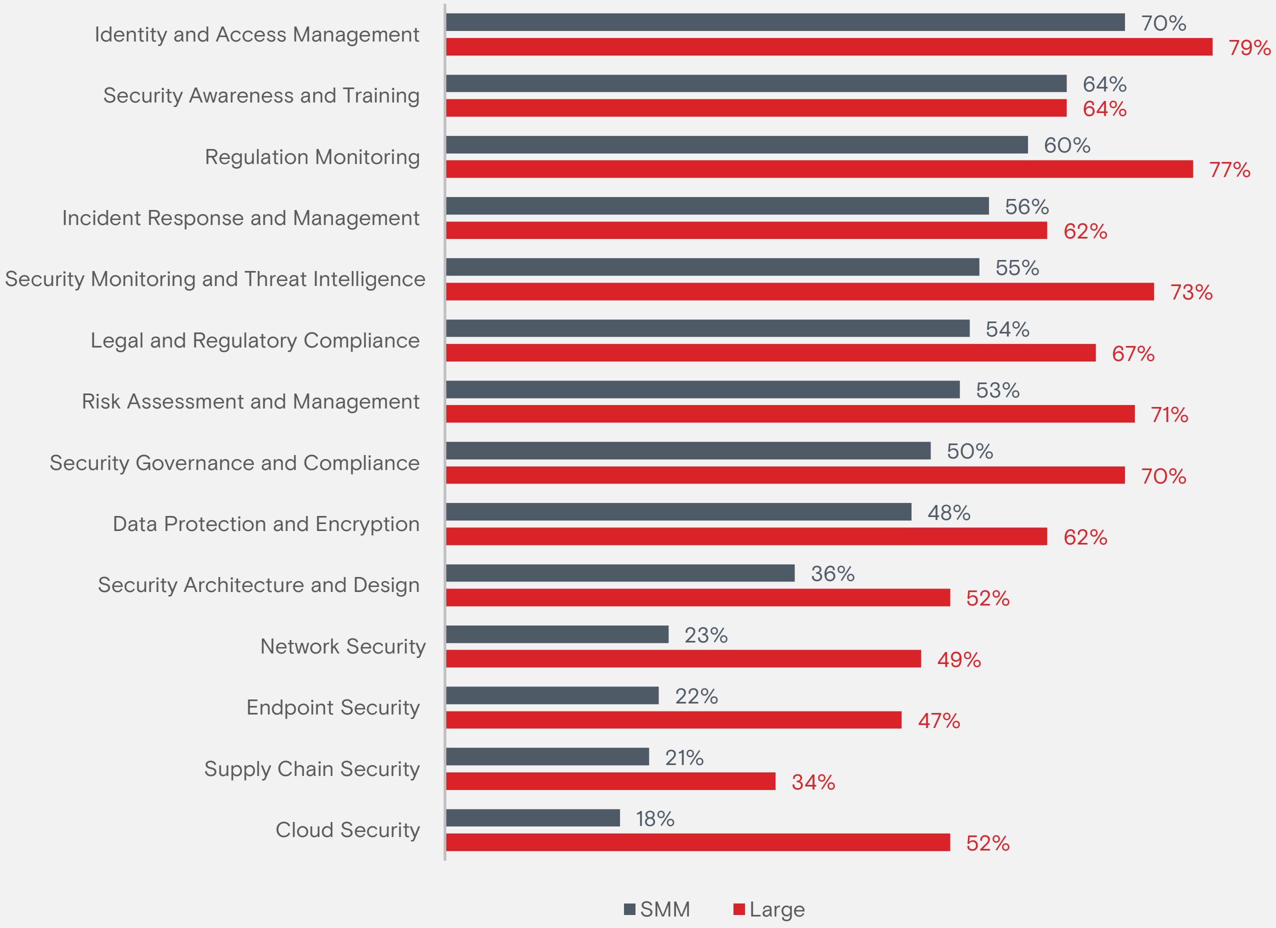
Q03. Approximately how many full-time staff are dedicated to cybersecurity roles in your organization?

Internal Capabilities and Expertise

The trend extends to internal capabilities for cybersecurity functions, with large manufacturers relying less on external vendors for key tasks such as security architecture, network, endpoint security, cloud security, and supply chain security compared to SMMs. This potentially paints a picture of larger enterprises having a more self-sufficient, robust structure to contend with cyber threats, whilst many SMMs, perhaps resource-constrained, lean on external partnerships to manage their cybersecurity needs. Although there are few discrepancies across sectors, aerospace and defense, as well as DIB, tend to rely less on external vendors for risk assessment and management, network, endpoint, and cloud security, suggesting these sectors are more self-reliant as it pertains to these cybersecurity protections.

Hiring cybersecurity experts is one the challenges manufacturers face that impede the strengthening of their internal capabilities. Specifically, 63% of manufacturers indicate moderate difficulty in recruiting cybersecurity talent, with SMMs being more likely than large manufacturers to find it difficult, especially those with 100 employees or fewer. This reflects a broader industry trend of talent scarcity that disproportionately affects smaller players who may not have the same resources to attract and retain top-tier professionals as larger companies do.

Figure 15. Cybersecurity Functions Handled Internally
By Size of Company

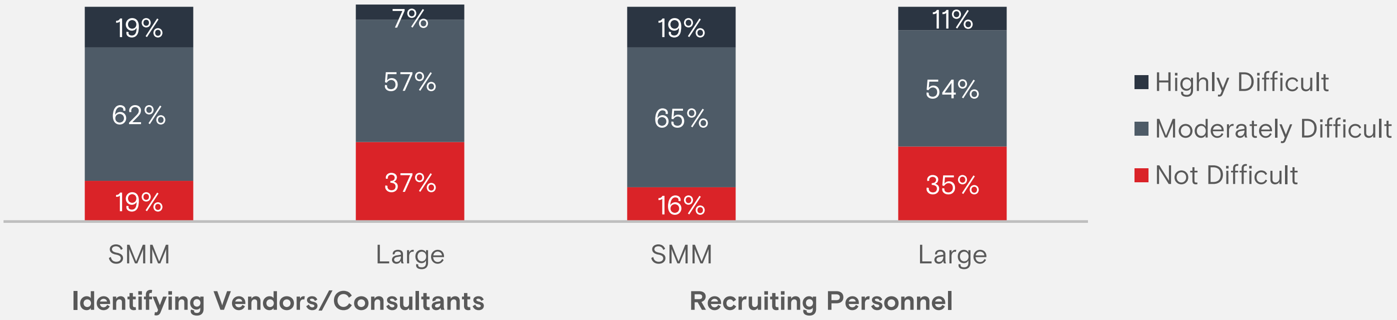


Q04. For each of the cybersecurity functions below, please indicate if your organization handles this internally with your own staff, if you rely on an external vendor or service provider, or if this function is not applicable to your organization. Handled internally by our own staff.

Qualified Vendors

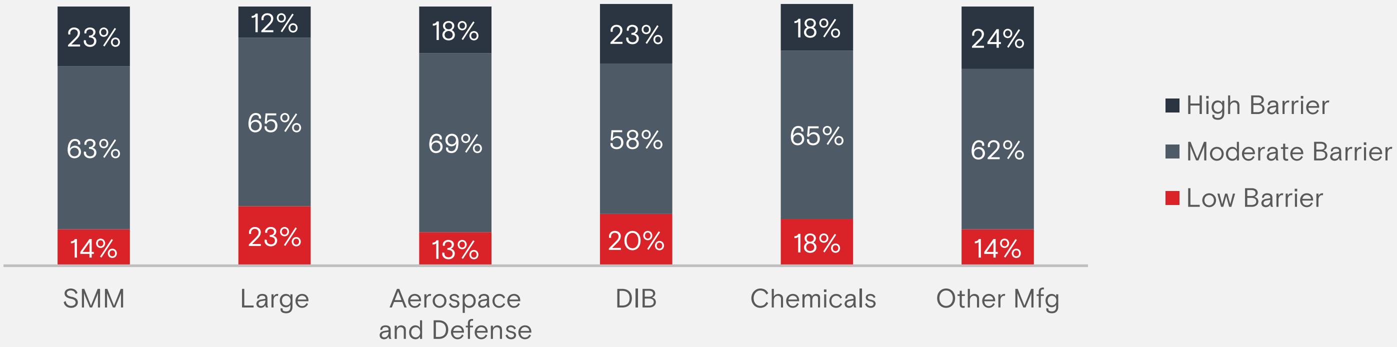
Similarly, the selection of qualified vendors to support cybersecurity needs presents as moderately challenging for 61% of respondents, accentuating the importance of dependable partnerships in the cybersecurity ecosystem. This is especially relevant for SMMs, of which 19% report finding qualified vendors to be more challenging than large manufacturers at 7% with companies 100 or fewer employees finding it slightly more difficult at 22%. Aging IT infrastructure is identified as a moderate barrier by 63% of manufacturers, with SMMs again being more likely than large manufacturers to report it as a barrier. Integration of upgraded cybersecurity controls into legacy manufacturing equipment is a moderate challenge for 60% of manufacturers; 27% of SMMs note this is a difficult challenge, compared to 14% of large manufacturers.

Figure 16. Barrier: Vendor Identification & Cybersecurity Talent Acquisition
By Company Size



Q26. How difficult is it for your organization to identify qualified external vendors or consultants to support your cybersecurity needs?
Q25. How difficult is it for your organization to recruit personnel with needed cybersecurity expertise?

Figure 17. Barrier: Aging/Legacy IT Systems
By Company Size and Sector



Q27. On a scale of 1-5, how much of a barrier are aging or legacy IT systems (computers, software, networks, etc.) to improving cybersecurity in your manufacturing environment?

Leadership Support

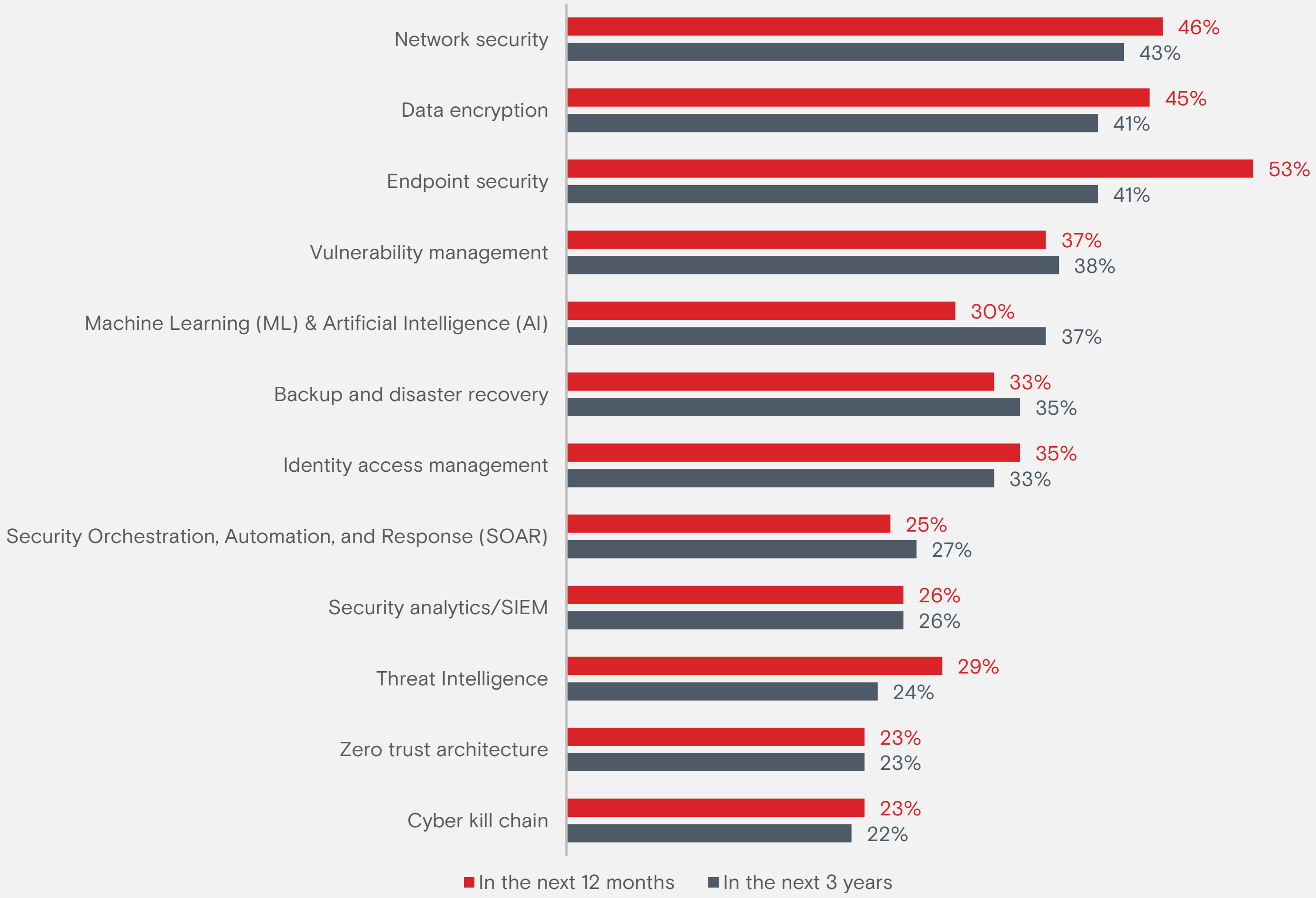
Senior leadership's buy-in is crucial for advancing cybersecurity measures, and the majority (57%) regard enhancing cybersecurity posture as a moderate priority. Encouragingly, very few (5%) perceive it as a low priority, reflecting widespread recognition of cybersecurity's strategic importance. Leaders in the chemical sector distinguish themselves by prioritizing the enhancement of their cybersecurity posture, indicating a strong inclination towards making improvements within the industry. Even so, the modest priority level suggests a potential disconnect between the urgency of cyber threats and the prioritization at the leadership level, underlining the need for more compelling advocacy for robust cybersecurity investments.

Outlook for Cybersecurity Investments

Planned Investments in Cybersecurity Capabilities

The manufacturing sector's dedication to advancing cybersecurity is driven by strategic investment and staffing plans, with trends unfolding differently in various industry segments. As manufacturers plot their course for the coming years, their focus for the next 12 months consolidates around investments in endpoint security (53%), network security (46%), and data encryption (45%). This prioritization is consistent with industry imperatives to safeguard critical data and infrastructure. Over a more extended horizon of the next three years, the investment priorities remain largely similar, although the percentage of firms aiming to invest in these areas slightly decreases. Large manufacturers signal a more robust forward investment strategy, particularly in endpoint security and network security, suggesting a sustained commitment to foundational cybersecurity technologies.

Figure 18. Outlook: Investments in Cybersecurity Technologies
All manufacturers



Q30a. Which of the following cybersecurity technologies will your organization prioritize investing in over the next 12 months?
Q30b. Which of the following cybersecurity technologies will your organization prioritize investing in over the next three years?

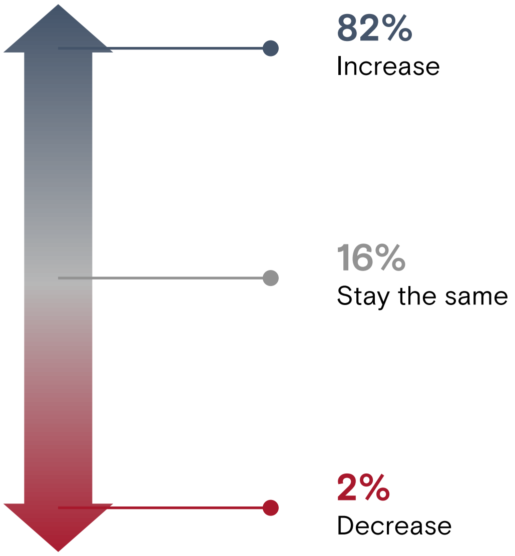
Cybersecurity Budget Outlook

Considering the budgetary landscape, a striking 82% of manufacturers forecast an increase in their cybersecurity budgets in the next planning cycle, indicative of the high priority placed on cyber resilience across the board.
Notably, this outlook is uniform across manufacturer sizes and sectors, demonstrating a universal recognition of the importance of financial allocation to combat emerging cyber threats.

Planned Investments in Cybersecurity Staff

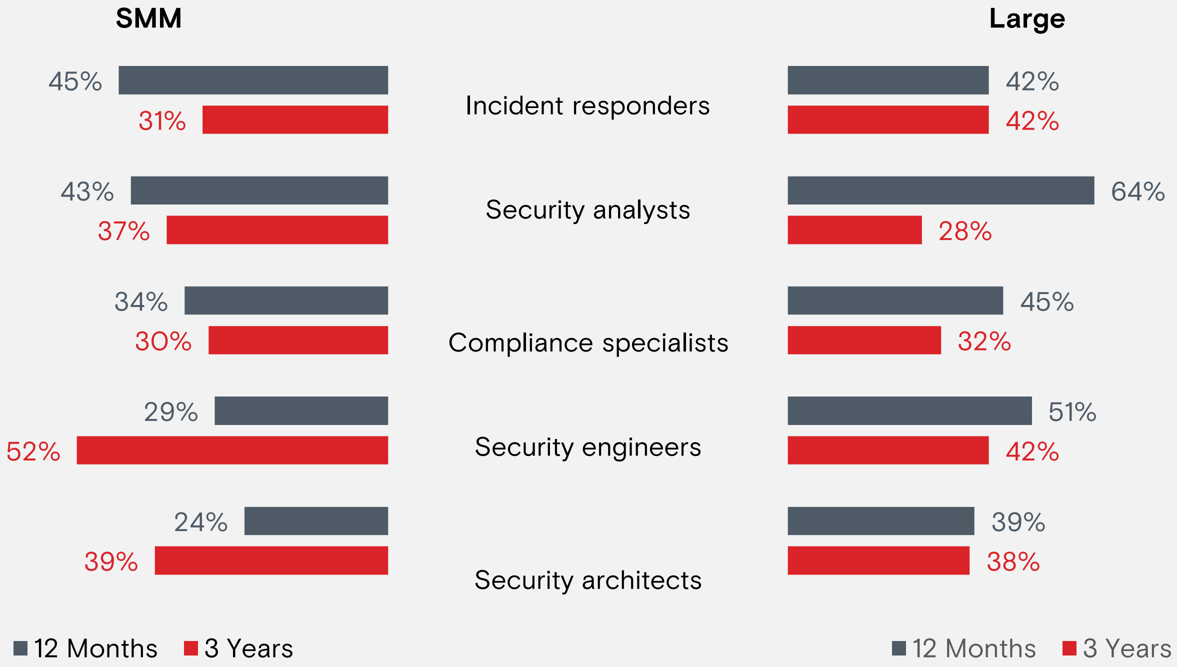
The staffing outlook reveals that cybersecurity roles are set to expand within the industry, with large manufacturers more inclined to add staff. Over the next year, 64% of large manufacturers plan to hire security analysts, compared to 43% of SMMs, and 51% of large manufacturers anticipate recruiting security engineers, significantly outpacing the 29% of SMMs with similar intentions. The defense industrial base, a sector with heightened security imperatives, shows a particular propensity to strengthen its teams with security architects (39%) and compliance specialists (52%), bolstering their strategic cyber defense capacities.

Figure 19. Outlook: Cybersecurity Budget Changes
All manufacturers



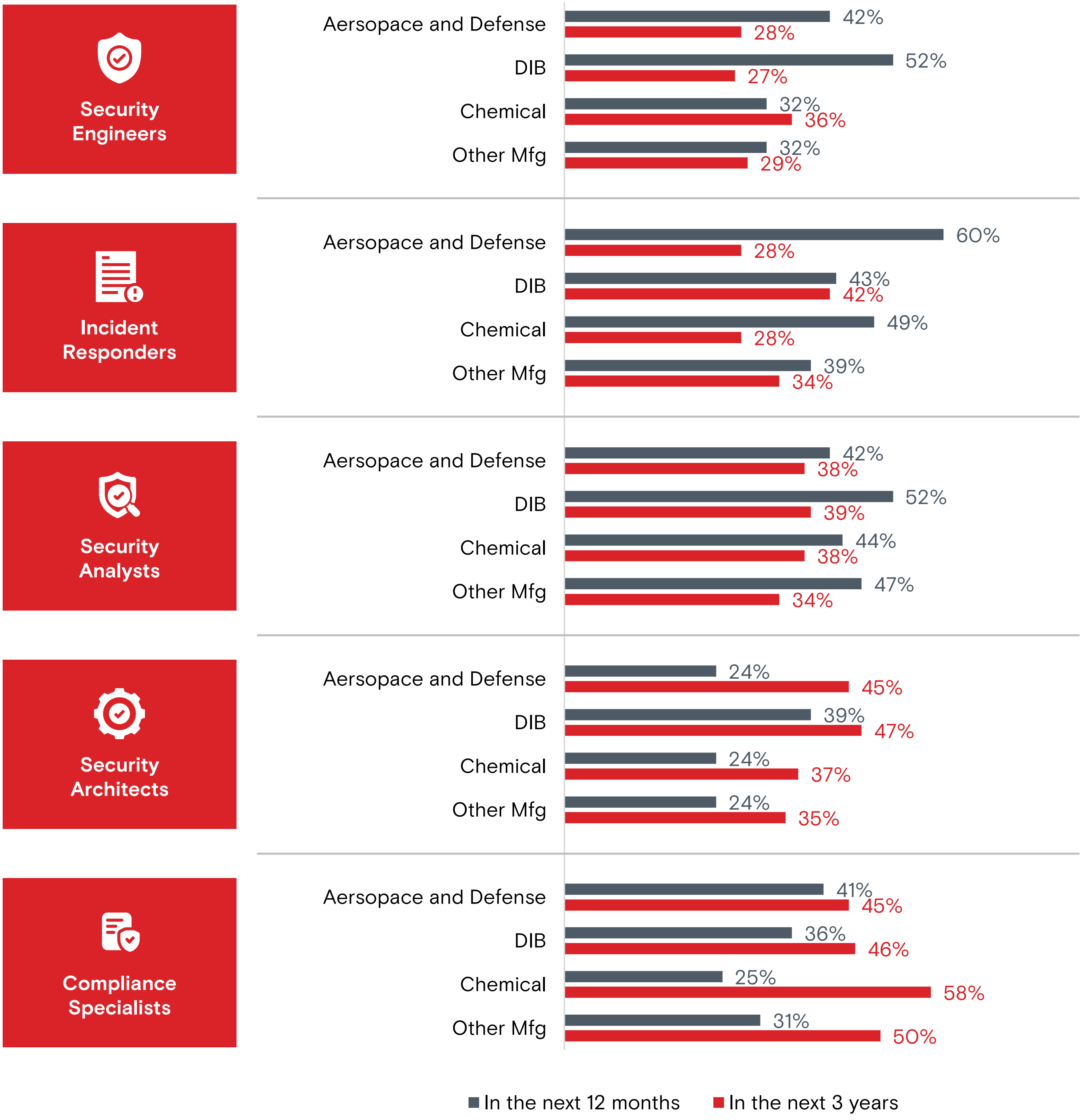
Q31. In your next budget planning cycle, do you predict that your budget for cybersecurity preparedness will increase, decrease, or stay the same?

Figure 20. Outlook: Cybersecurity Staffing
By Company Size



Q32. Does your organization plan to add more staff dedicated to any of the following cybersecurity roles? - Yes, over the next 12 months
Q32. Does your organization plan to add more staff dedicated to any of the following cybersecurity roles? - Yes, over the next three years

Figure 21. Outlook: Cybersecurity Staffing
By Sector



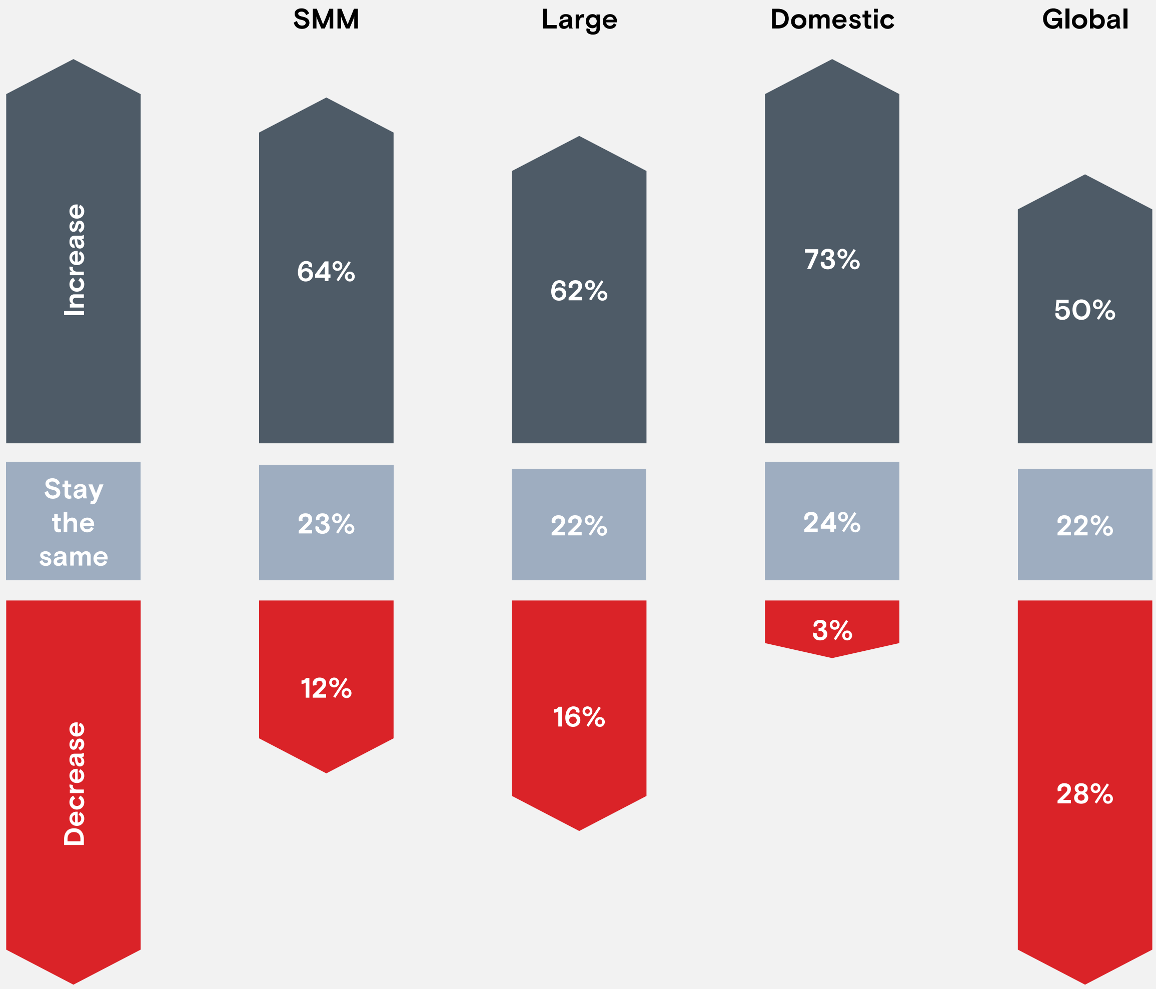
Q32. Does your organization plan to add more staff dedicated to any of the following cybersecurity roles? - Yes, over the next 12 months
Q32. Does your organization plan to add more staff dedicated to any of the following cybersecurity roles? - Yes, over the next three years

Outlook on Vendor Reliance

Looking ahead, the manufacturing industry's reliance on external cybersecurity service providers is anticipated to undergo substantial growth: 64% of manufacturers predict an increase in their engagement with cybersecurity vendors over the next three years. This trend is especially pronounced among domestic manufacturers, where a notable 73% forecast an uptick in reliance on external cybersecurity services, as opposed to 50% of global manufacturers. When dissecting by size, the reliance is relatively even, with 64% of SMMs and 62% of large manufacturers expecting to increase usage of these services, suggesting a common trajectory for enhanced third-party support.

In terms of specific cybersecurity services, manufacturers are preparing to direct their investments most significantly towards network security, endpoint security, and supply chain security services. Unique differences emerge when addressing the future investment in various cybersecurity services. For instance, large manufacturers are poised to invest in identity and access management, at 31% compared to 19% for SMMs, as well as in risk assessment and management services, at 34% against 19% for their smaller peers. Such differences may reflect large manufacturers' wider scope of operations and increased exposure to diverse cybersecurity risks that necessitate a broad array of sophisticated services.

Figure 22. Use of External Cybersecurity Consultants Over the Next Three Years
By Company Size and Sector



Q33. Over the next three years, do you predict that your organization's use of external cybersecurity service providers will increase, decrease, or stay about the same?

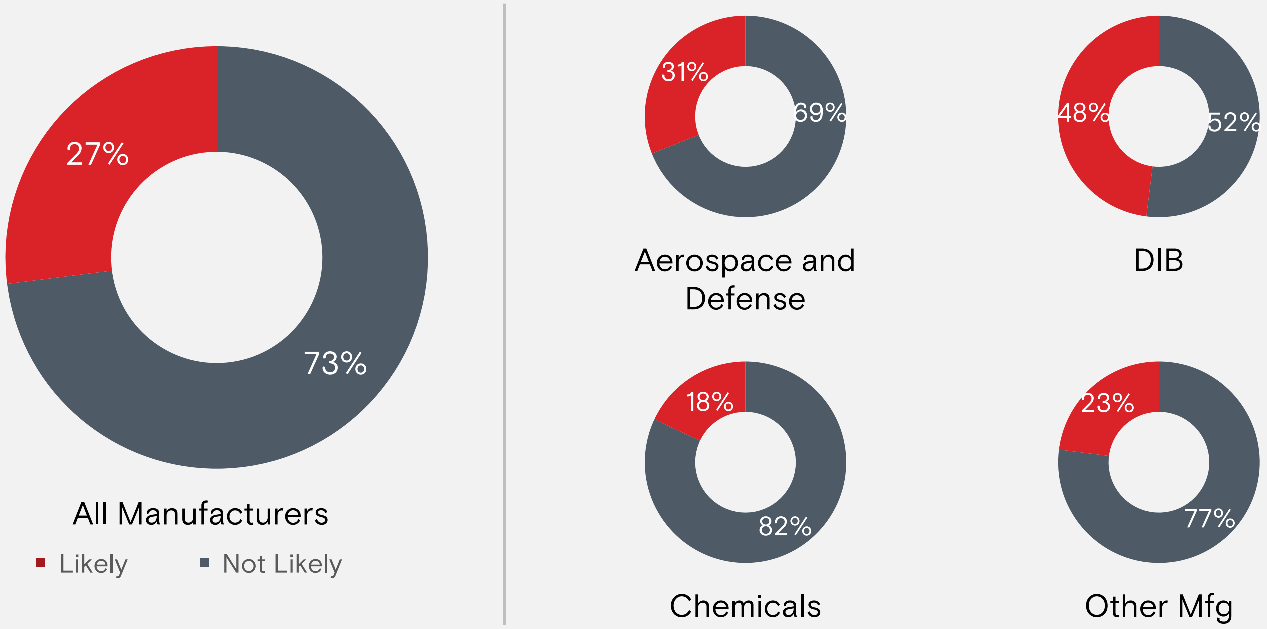
Impact of Cybersecurity on Competitiveness

Planned Investments in Cybersecurity Capabilities

Manufacturing customers are demanding a strong cybersecurity posture: 78% of manufacturers report they sometimes encounter cybersecurity requirements in customer RFPs. This underscores the need for robust cyber defenses in routine business operations. The frequency of these encounters varies considerably by company size; large manufacturers report "frequently" facing cybersecurity requirements in 22% of RFPs, double the 11% reported by SMMs. When broken down by sector, 17% of defense industrial base manufacturers often encounter these conditions, higher than the overall average of 14% across sectors.

Meeting cybersecurity criteria within RFPs is a moderate challenge for 74% of manufacturers, indicating that while meeting these requirements demands effort, the industry appears to be keeping pace with the mandates without insurmountable difficulty. However, 27% of manufacturers acknowledge that their contracts can be terminated over cybersecurity concerns. Specifically, the defense industrial base and aerospace and defense sectors are feeling the pressure more profoundly—48% of DIB and 31% of aerospace and defense manufacturers say it is likely that their contracts would be terminated due to cybersecurity concerns.

Figure 23. Likelihood that Customers Would Terminate a Contract Due to Cybersecurity Concerns
By Sector



Q37. In your experience, how likely is it that customers would terminate a contract with your organization due to cybersecurity concerns?

Restrictions on Vendor Collaborations

Cybersecurity criteria set forth by customers shape the ability of manufacturers to forge partnerships with technology vendors. Most manufacturers (65%) feel that their customers' cybersecurity mandates bring reasonable restrictions that impact their vendor collaboration to a noticeable degree. This factor is particularly influential in sectors with stringent security needs, such as aerospace and defense, where 15% of respondents report that such requirements considerably limit their ability to forge technological partners/hips. In comparison, only 4% of manufacturers in the chemicals sector perceive these cybersecurity demands as having a major or severe impact, pointing to varying degrees of influence across different manufacturing industries.

Taken together, these findings demonstrate that cybersecurity concerns are shaping business opportunities, contractual obligations, and the prospects of industry collaborations. The ability to meet these cybersecurity criteria is an important factor in maintaining and securing new contracts, stressing the importance of robust cybersecurity measures for manufacturers.

CHAPTER 6

Behaviors That Increase Confidence in Preparedness

Key Drivers of Confidence

- Our examination of the behaviors that bolster manufacturers' confidence in their cybersecurity preparedness has identified several key practices. We have ranked these behaviors by their impact on respondents' confidence levels. The findings reveal that comprehensive approaches to cybersecurity policy, training, integrating cybersecurity risk into the larger business strategy, and staying up to date on regulations are significantly correlated with heightened confidence.

- Each manufacturing sector has a behavior in which they are at least 10 points below the average . These behaviors are identified as potential areas for standardization in the industry. The aerospace and defense and DIB manufacturers demonstrate specific risks, with only 23% of the confident aerospace and defense manufacturers actively monitoring cybersecurity regulations, and a mere 30% of DIB manufacturers having extensive cybersecurity requirements for vendors. The chemical sector also shows opportunity for improvement, as only 36% of those confident in their cybersecurity review and update their controls on a quarterly basis.

- The data show a clear gap between perceived and actual cybersecurity readiness. This calls for a critical reassessment of cyber defenses across the manufacturing sector, especially for those in high-risk areas like the aerospace and defense and DIB sectors. As it stands, a sense of overconfidence could be masking underlying vulnerabilities. It's crucial that the industry recalibrates its security practices to more accurately reflect the dynamic and evolving nature of cyber threats.

- Respondents that stay up to date on external cybersecurity trainings and frequently update their own cybersecurity controls are more confident in their organization's cybersecurity preparedness, suggesting that knowing what is required of your organization increases respondent's confidence in meeting these requirements. Finally, we see that integrating cybersecurity risks into business continuity and disaster recovery plans is associated with an increase in overall cybersecurity confidence.

Figure 24. Key Drivers of Confidence in Cybersecurity Preparedness

Ranking	Behavior
1	At least moderately comprehensive formal documented cybersecurity policy
2	Mandatory cybersecurity training conducted at least quarterly
3	At least a moderately compressive incident response plan
4	All employees required to complete cybersecurity training
5	Comprehensive cybersecurity requirements in vendor and supplier contracts
6	System Security Plans (SSPs) in place for all critical IT systems and environments
7	Organization monitors for new or updated cybersecurity laws and regulations closely
8	Cyber-risks largely/fully integrated into business continuity and disaster recovery plans
9	Review and update cybersecurity controls like firewall rules and access controls at least quarterly
10	Cybersecurity training simulations or tabletop exercised conducted at least annually

Exploring Overconfidence in Cybersecurity Preparedness

Our analysis also illustrates the overconfidence manufacturers have in their cybersecurity preparedness and highlights key behaviors for which there is great variance in adoption. Figures 25 and 26 compare the key behaviors to the percentages of highly confident participants who engage in the behavior.

- Among manufacturers who are highly confident in their organization's cybersecurity preparedness, fewer than half are engaging in six of the 10 key drivers for confidence. For example, only 9% of highly confident manufacturers are mandating quarterly cybersecurity trainings and only three in 10 have fully integrated cyber-risks into their business continuity and disaster recovery plans.

- The overconfidence in cybersecurity preparedness is even more pronounced when we look at the data by manufacturer size and sector. Even though 70% of SMMs and 65% of manufacturers in the other sectors are highly confident in their cybersecurity preparedness, they have below average rates of behavior adoption for almost all the key behaviors identified.

- Each manufacturing sector has a behavior in which they are at least 10 points below the average. These behaviors are identified as potential areas for standardization in the industry. The aerospace and defense and DIB manufacturers demonstrate specific risks, with only 23% of the confident aerospace and defense manufacturers actively monitoring cybersecurity regulations, and a mere 30% of DIB manufacturers having extensive cybersecurity requirements for vendors. The chemical sector also shows opportunity for improvement, as only 36% of those confident in their cybersecurity review and update their controls on a quarterly basis.

- The data show a clear gap between perceived and actual cybersecurity readiness. This calls for a critical reassessment of cyber defenses across the manufacturing sector, especially for those in high-risk areas like the aerospace and defense and DIB sectors. As it stands, a sense of overconfidence could be masking underlying vulnerabilities. It's crucial that the industry recalibrates its security practices to more accurately reflect the dynamic and evolving nature of cyber threats.

Figure 25. Relationship Between Cybersecurity Confidence and Adoption of Key Behaviors Among Highly Confident Manufacturers (by manufacturer size)

		% Of Highly Confident Manufacturers Who Engage In Behavior			
Ranking	Behavior	All Manufacturers	Manufacturer Size		
			SMMs	Large	Variance
1	At least moderately comprehensive formal documented cybersecurity policy	77%	73% (-4)	96% (+19)	23
2	Mandatory cybersecurity training conducted at least quarterly	9%	2% (-7)	36% (+27)	34
3	At least a moderately compressive incident response plan	77%	73% (-4)	93% (+16)	20
4	All employees required to complete cybersecurity training	57%	57% (0)	55% (-2)	2
5	Comprehensive cybersecurity requirements in vendor and supplier contracts	40%	39% (-1)	43% (+3)	4
6	System Security Plans (SSPs) in place for all critical IT systems and environments	41%	39% (-2)	52% (+11)	13
7	Organization monitors for new or updated cybersecurity laws and regulations closely	33%	28% (-5)	53% (+20)	25
8	Cyber-risks largely/fully integrated into business continuity and disaster recovery plans	30%	25% (-5)	50% (+20)	25
9	Review and update cybersecurity controls like firewall rules and access controls at least quarterly	46%	41% (-5)	69% (+23)	28
10	Cybersecurity training simulations or tabletop exercised conducted at least annually	98%	98% (0)	98% (0)	0

Figure 26. Relationship Between Cybersecurity Confidence and Adoption of Key Behaviors Among Highly Confident Manufacturers (by manufacturing sector)

% Of Highly Confident Manufacturers Who Engage In Behavior								
Ranking	Behavior	All Manufacturers	Manufacturing Sector					
			Aerospace & Defense	DIB	Chemicals	Other Mfg	Variance
1	At least moderately comprehensive formal documented cybersecurity policy	77%	85% (+8)	69% (-8)	86% (+9)	73% (-4)	17
2	Mandatory cybersecurity training conducted at least quarterly	9%	18% (+9)	24% (+15)	5% (-4)	2% (-7)	22
3	At least a moderately compressive incident response plan	77%	83% (+6)	72% (-5)	84% (+7)	73% (-4)	12
4	All employees required to complete cybersecurity training	57%	68% (+11)	52% (-5)	55% (-2)	54% (-3)	16
5	Comprehensive cybersecurity requirements in vendor and supplier contracts	40%	40% (0)	30% (-10)	50% (+10)	39% (-1)	20
6	System Security Plans (SSPs) in place for all critical IT systems and environments	41%	42% (+1)	36% (-5)	55% (+14)	37% (-4)	19
7	Organization monitors for new or updated cybersecurity laws and regulations closely	33%	23% (-10)	40% (+7)	37% (+4)	32% (-1)	17
8	Cyber-risks largely/ fully integrated into business continuity and disaster recovery plans	30%	29% (-1)	41% (+11)	35% (+5)	24% (-6)	17
9	Review and update cybersecurity controls like firewall rules and access controls at least quarterly	46%	53% (+7)	58% (+12)	36% (-10)	44% (-2)	22
10	Cybersecurity training simulations or tabletop exercised conducted at least annually	98%	98% (0)	98% (0)	99% (+1)	98% (0)	1

Discussion

The survey results present a clear directive for manufacturing decision-makers: there is a pressing need to strengthen cybersecurity measures across the board. The reported confidence in cybersecurity capabilities, particularly among SMMs, juxtaposes with the demonstrable gaps in leadership, comprehensive policies, and the frequency of training and assessments. This misalignment suggests an area ripe for enhancement, where decision-makers must recognize the value of strategic cybersecurity investments not only as a defensive measure but also as an enabler of operational continuity and competitive advantage.

Decision-makers are encouraged to consider a more integrated approach to risk management, ensuring that cybersecurity is woven into the larger tapestry of their business models and operational strategies. This involves a higher degree of engagement with vendors, pressing for robust cybersecurity requirements in contracts as a standard industry practice, thereby securing the entire supply chain. This also includes championing education and training initiatives, facilitating knowledge-sharing across sectors, and advocating for uniform preparedness protocols to safeguard the industry against an evolving digital threat landscape.

Appendix

Respondent Profile

			Size		Reach	
		Total	SMM	Large	Domestic	Global
Sector	Aerospace and Defense	**106**	76	30	49	57
	Defense Industrial Base (DIB)	**102**	72	30	56	46
	Chemicals	**137**	107	30	74	63
	Other manufacturing sectors	**405**	375	30	270	135
Total		**750**	**630**	**120**	**449**	**301**

Definitions

Size:

- SMM (small and medium manufacturers, 500 or fewer employees)
- Large (more than 500 employees)

Reach:

- Domestic (company operates within one country)
- Global (company operates in multiple countries)

Industries:

- Aerospace and Defense
  - Aerospace and Defense is the industry classification that best represents the principal activity of manufacturing company.
  - Primary business activity is either developing space technologies and components or manufacturing civilian aircraft, engines, or related components.
- Defense Industrial Base (DIB)
  - Aerospace and Defense is the industry classification that best represents the principal activity of manufacturing company.
  - Primary business activity is developing/integrating military communications, electronics, or cybersecurity systems or manufacturing military aircraft, vehicles, weapons, or related components, or providing maintenance, repair, or overhaul (MRO) services for military equipment.
- Chemicals
  - Chemicals and Materials is the industry classification that best represents the principal activity of manufacturing company.
- Other Sectors
  - The industry classification that best represents the principal activity of the manufacturing company is one of the following:
    - Automotives and components, building and construction, consumer products, energy and utilities, food and beverage, industrial machinery and equipment, other manufacturing, medical devices, metals and mining, oil and gas, pharmaceutical preparations, plastics and rubber, semiconductors, technology and electronics (including consumer electronics and information/communications technology), textiles and apparel, or transportation equipment.

About MxD

As the recognized National Center for Cybersecurity in Manufacturing by the Department of Defense, MxD stands at the forefront of working with the U.S. manufacturing sector to prepare and protect America's supply chains against cybersecurity threats through our programs, partnerships, and strategic initiatives.

With our ecosystem of manufacturers, solution providers, government stakeholders and academic partners, MxD drives economic prosperity and supports national security by leading cybersecure digital innovation and adoption in U.S. manufacturing to deliver a resilient and revitalized supply chain.