



# **MxD SMM Cyber Security Survey Results & Analysis: Spring 2026**

**DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.**

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

# Introduction

# Survey Background

MxD is seeking to better understand the cybersecurity posture, challenges, and decision-making processes of small and medium-sized U.S. manufacturers (SMMs). As digital technologies become more deeply embedded in manufacturing operations, these organizations face increasing risks from cyber threats, particularly those working in Aerospace, Defense, and the Defense Industrial Base (DIB).

The goal of this project is to capture insights from both technical decision-makers and organizational leaders. MxD seeks to identify how these organizations perceive cybersecurity risks, what barriers limit adoption of stronger practices, and what resources or support they need to improve resilience.

The findings from this research will enable MxD to design targeted programs, tools, and interventions that directly address manufacturers' most pressing cybersecurity needs, helping to safeguard critical industries while strengthening the competitiveness and security of the U.S. manufacturing base.

## **MxD Objectives**

- Assess cybersecurity awareness and readiness among small and medium-sized manufacturers (SMMs) across the U.S.
- Understand decision-making roles and responsibilities related to IT and cybersecurity, whether managed by dedicated personnel or by senior leadership in smaller firms.
- Identify key barriers and challenges manufacturers face in adopting stronger cybersecurity practices, including cost, expertise, compliance, and resource constraints.
- Gauge sector-specific needs, with particular attention to Aerospace, Defense, and the Defense Industrial Base (DIB), where cybersecurity is critical to national security.
- Inform the design of MxD programs, tools, and resources that directly support manufacturers in improving their cybersecurity posture and resilience.

# Survey Overview

## Methodology:

Mixed Quantitative & Qualitative Survey  
Questionnaire

Survey conducted February 20 – March  
30 2026

34 Questions

Average Time: 8 mins / response

## Sample:

Respondents employed in U.S.-based  
manufacturing entities with 2-499  
employees

700 Total Respondents

Must have a role in cybersecurity  
decision-making

+/- 3.7% margin of error at 95%  
confidence level

# Initial Key Takeaways

- **Significant Exposure to Cyber Incidents:** A substantial portion of the SMM community is actively dealing with threats, evidenced by 479 out of 700 respondents reporting a cyber incident within the past 24 months
- **Reliance on External Support:** Many SMMs, particularly those without a formal internal IT function, rely heavily on Third-party Managed Service Providers (**MSPs**) or hybrid models to manage their cybersecurity posture. Nonetheless, SMMs that rely primarily on MSPs and MSSPs are the least confident in their preparedness
- **Importance of Culture:** The biggest barriers revolve around culture. Beyond technical hurdles, a lack of organizational urgency and general inertia serve as significant internal barriers to adopting stronger security postures
- **Critical Impact on Operations:** For those who experienced an incident, **operational downtime** and the resulting halt in production were identified as primary impacts, highlighting the high cost and direct threat to the U.S. manufacturing base's competitiveness.
- **Compliance Complexity & Cost:** Small manufacturers face difficulty with CMMC/NIST compliance due to complex documentation and requirements, compounded by a shortage of specialized consultants to guide them
- **Supply Chain Vulnerability:** There is a notable need for improved supply chain risk management, as many firms are not yet performing rigorous audits or requiring specific certifications from their own sub-tier suppliers

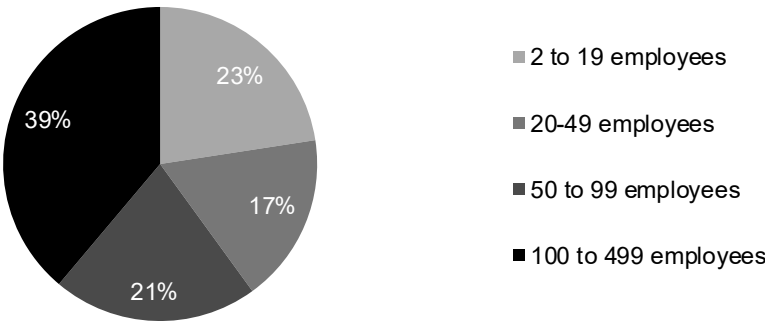
# Moving Forward

- **Focus on Culture:** A key hurdle highlighted by IT experts at SMMs is the lack of urgency and organizational misalignment over cybersecurity. IT and cybersecurity are viewed as cost centers and urgency is rarely proactive; it is born from near misses or costly incidents.
- **Develop Targeted Compliance Toolkits:** Based on the identified barriers, MxD should prioritize creating simplified CMMC/NIST compliance guides and cost-effective resource templates specifically tailored for firms with fewer than 50 employees
- **Invest in AI Agentic Support:** Complexity is the main barrier for firms of all sizes. Rather than rely on a limited number of consultants, an AI agent that can navigate the complexities of CMMC or NIST certifications with personalized advice and guidance for SMMs.
- **Creation of a Consultant Directory:** Establish a directory of consultants with transparent, SMM tailored costs can drive SMM engagement with MxD and help smaller firms quickly find experts and answers.
- **Consider OT-Specific Training Programs:** Design and deploy **hands-on workshops for factory floor staff** that focus on isolating compromised machinery without shutting down entire production lines, addressing a key area of low confidence

# Firmographic Overview

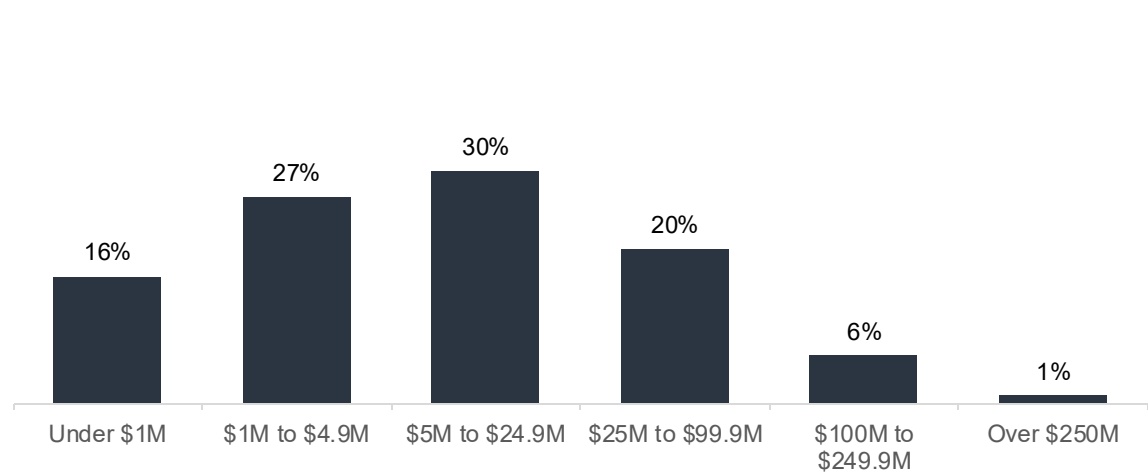
# Company Overview

## Company Size



Approximately how many full-time equivalent employees (FTEs) work for your business across all locations?

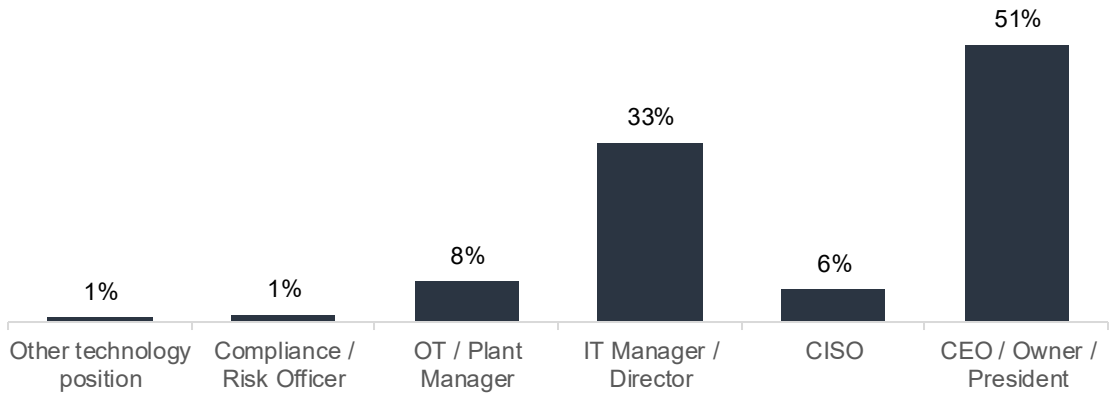
## Company Revenue



What was your company's total annual revenue for the most recent fiscal year?

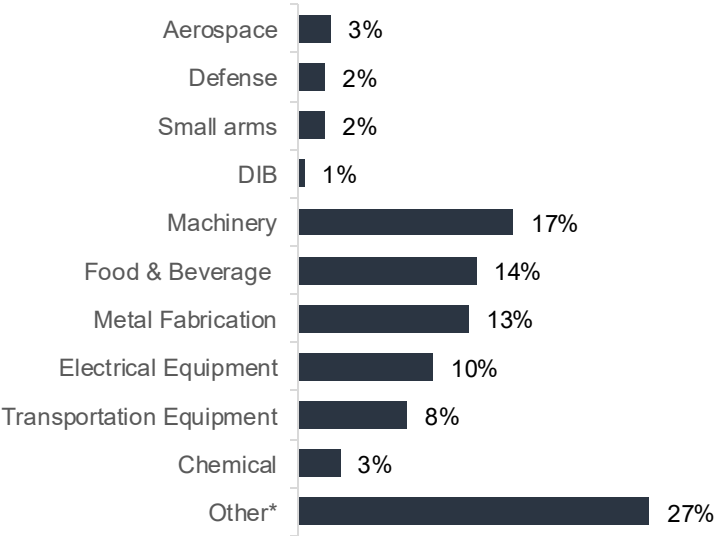
Base: n = 700 (all respondents)

## Professional Role



Which of the following best describes your primary professional role and relationship to your company's technology and security?

## Primary Output

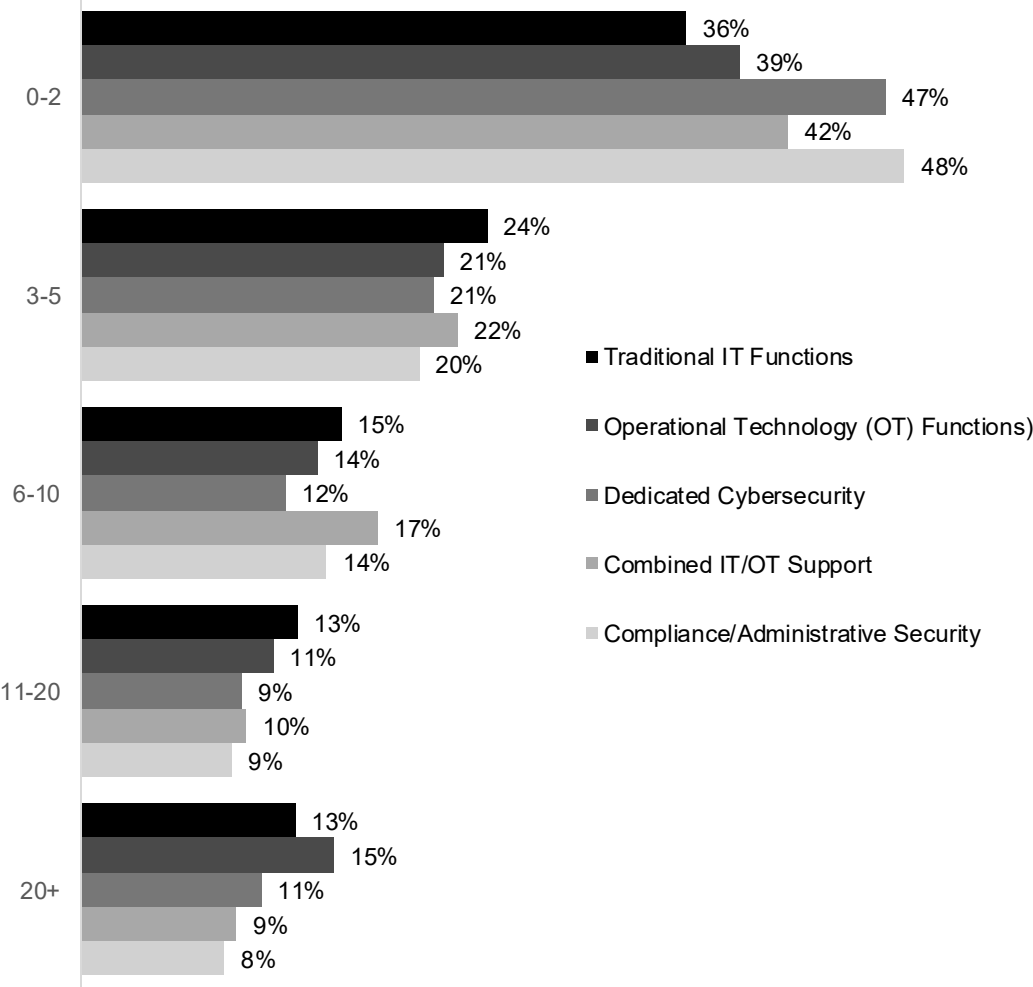


\*Other common industries include construction, technology, finance/professional/business services, manufacturing, and healthcare

Which of the following industries best describes your company's primary output?

# IT Overview

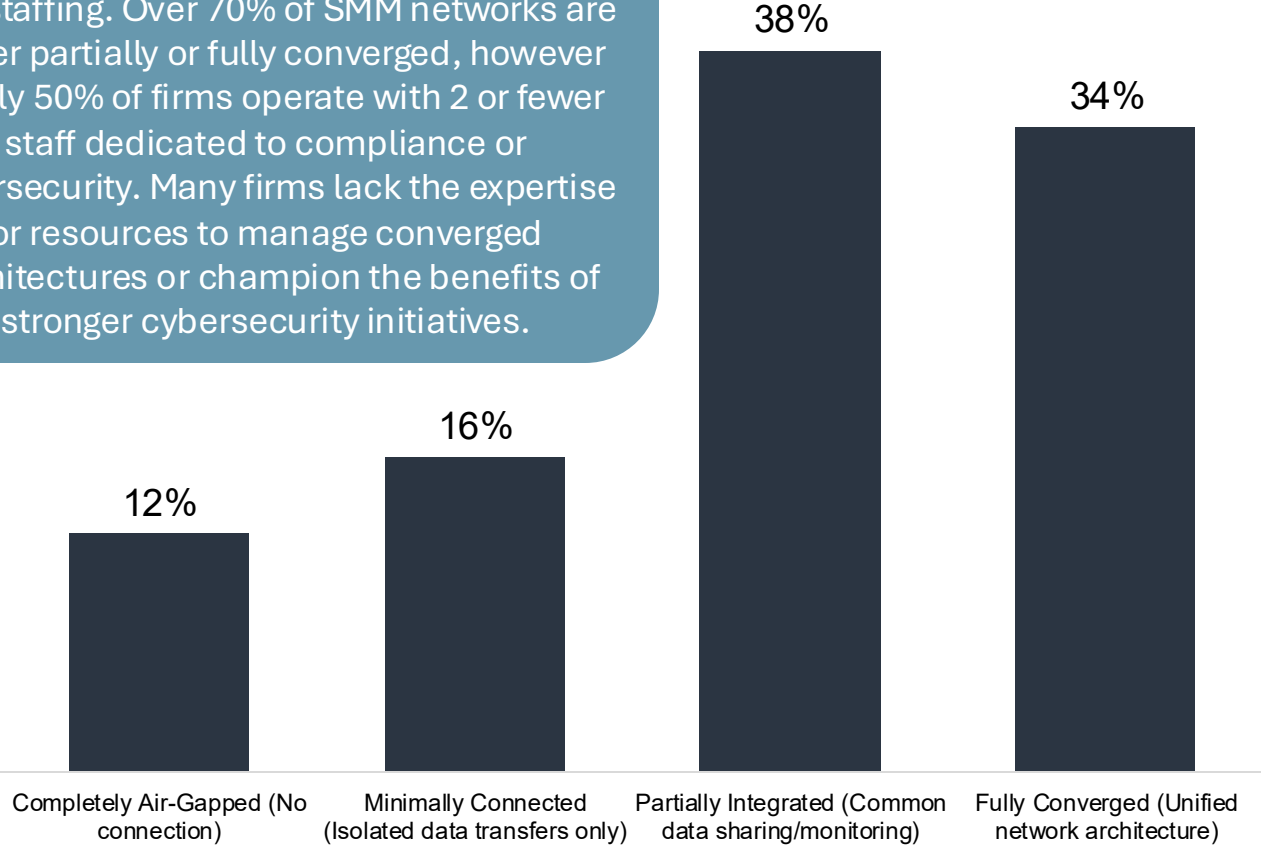
## Dedicated Employees



How many employees are dedicated to the following functions?  
Base: n = 700 (all respondents)

## Integration Level

There is a potential gap between complexity and staffing. Over 70% of SMM networks are either partially or fully converged, however nearly 50% of firms operate with 2 or fewer staff dedicated to compliance or cybersecurity. Many firms lack the expertise or resources to manage converged architectures or champion the benefits of stronger cybersecurity initiatives.

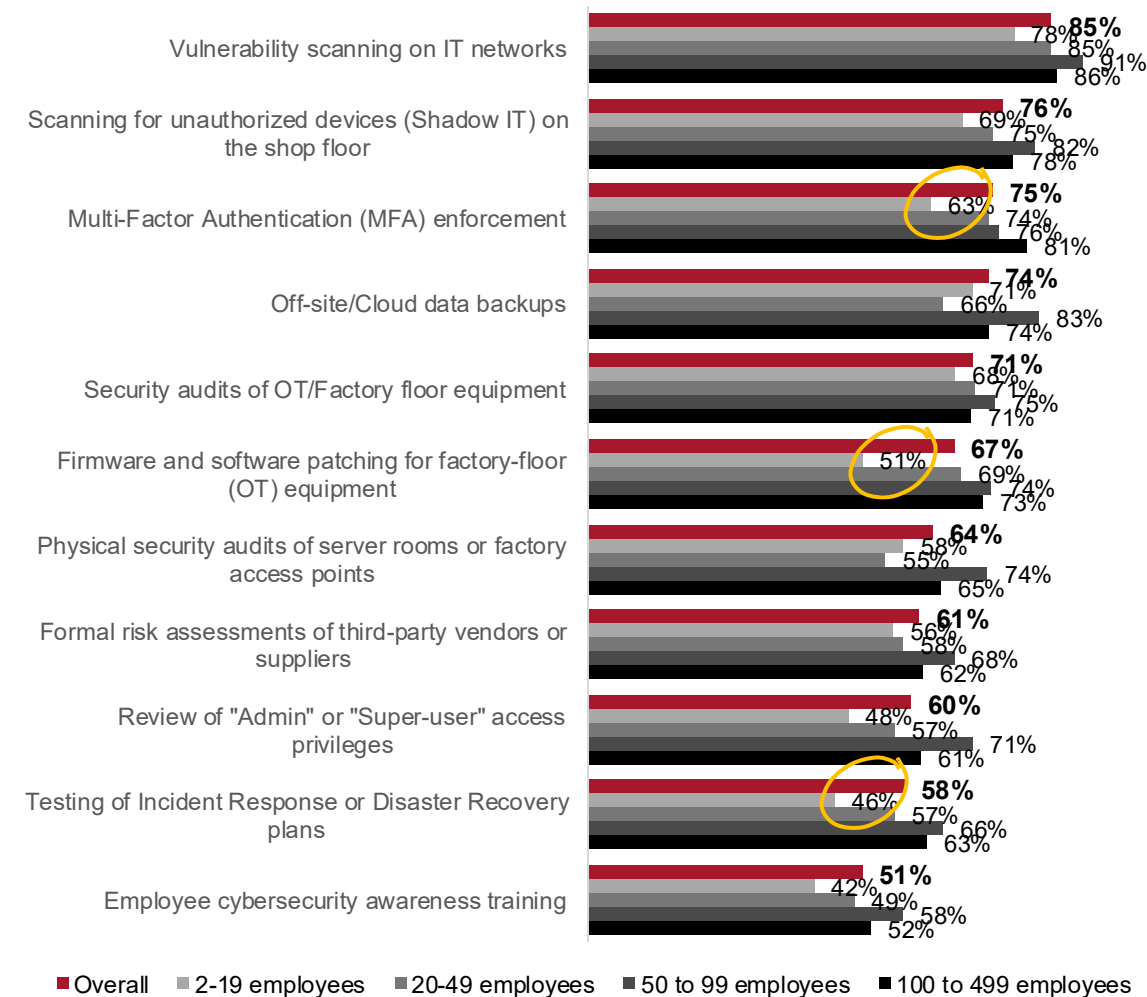


How would you describe the integration level between your IT (Office) and OT (Factory Floor) networks?

# Current Cybersecurity Practices

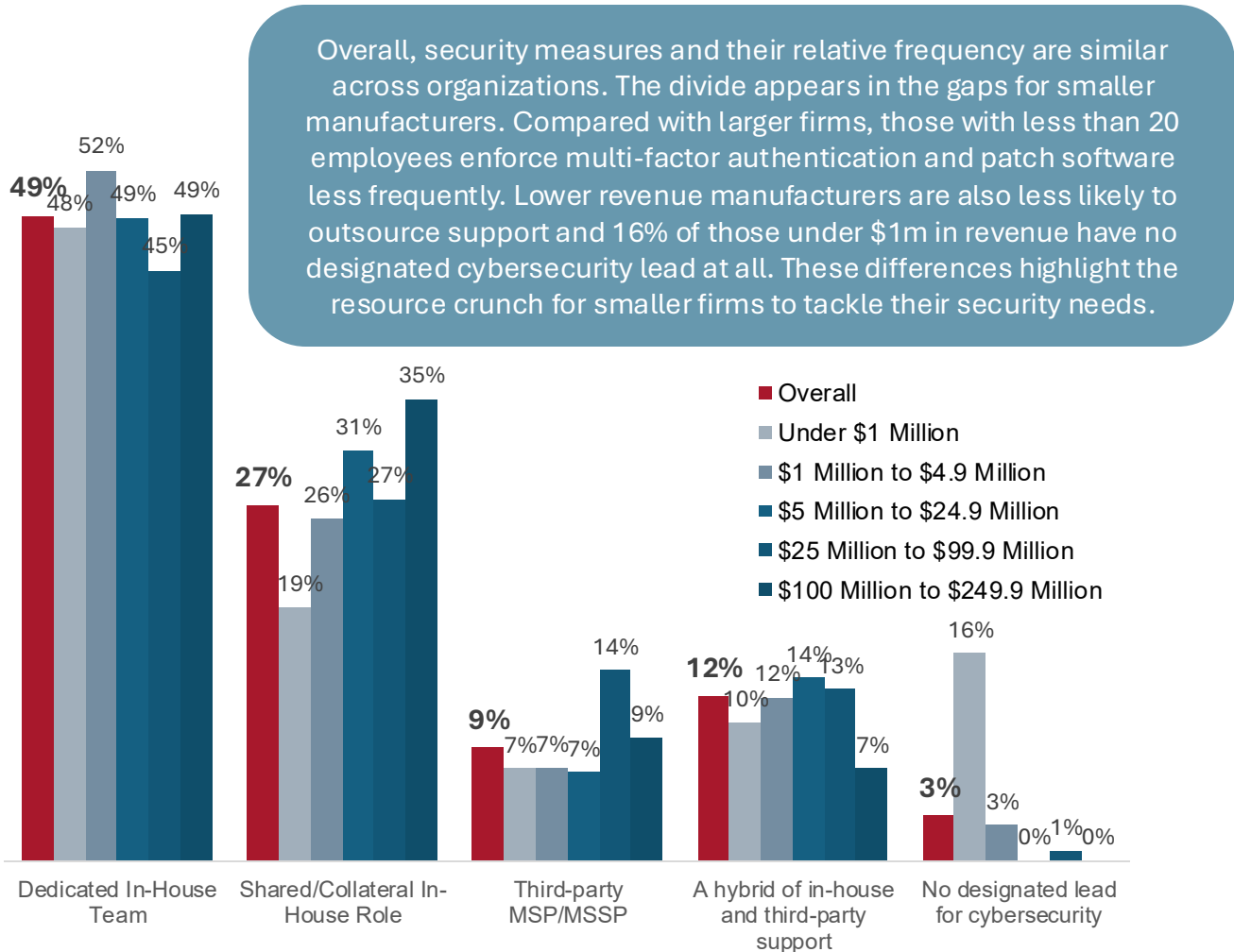
# Cybersecurity Procedures

## Security Measure Frequency



How frequently does your organization perform the following security measures? (Daily & Monthly)  
Base: n = 700 (all respondents)

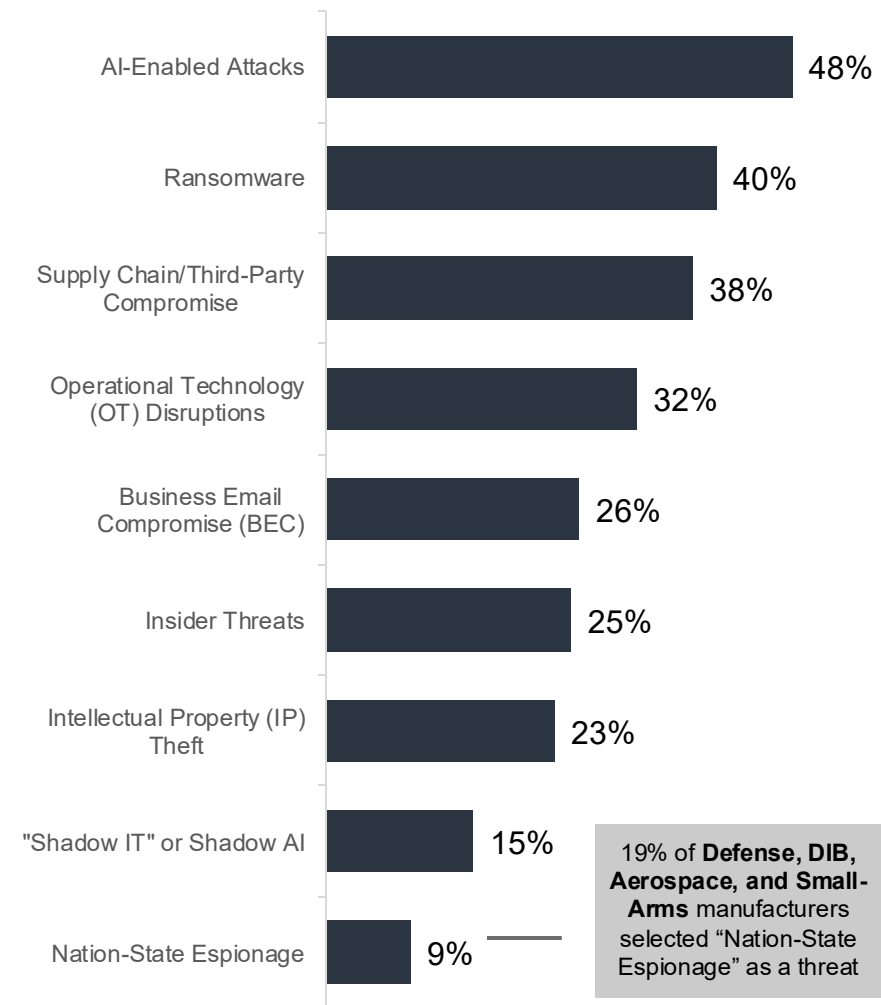
## Cybersecurity Responsibility



Who is primarily responsible for managing your company's cybersecurity?

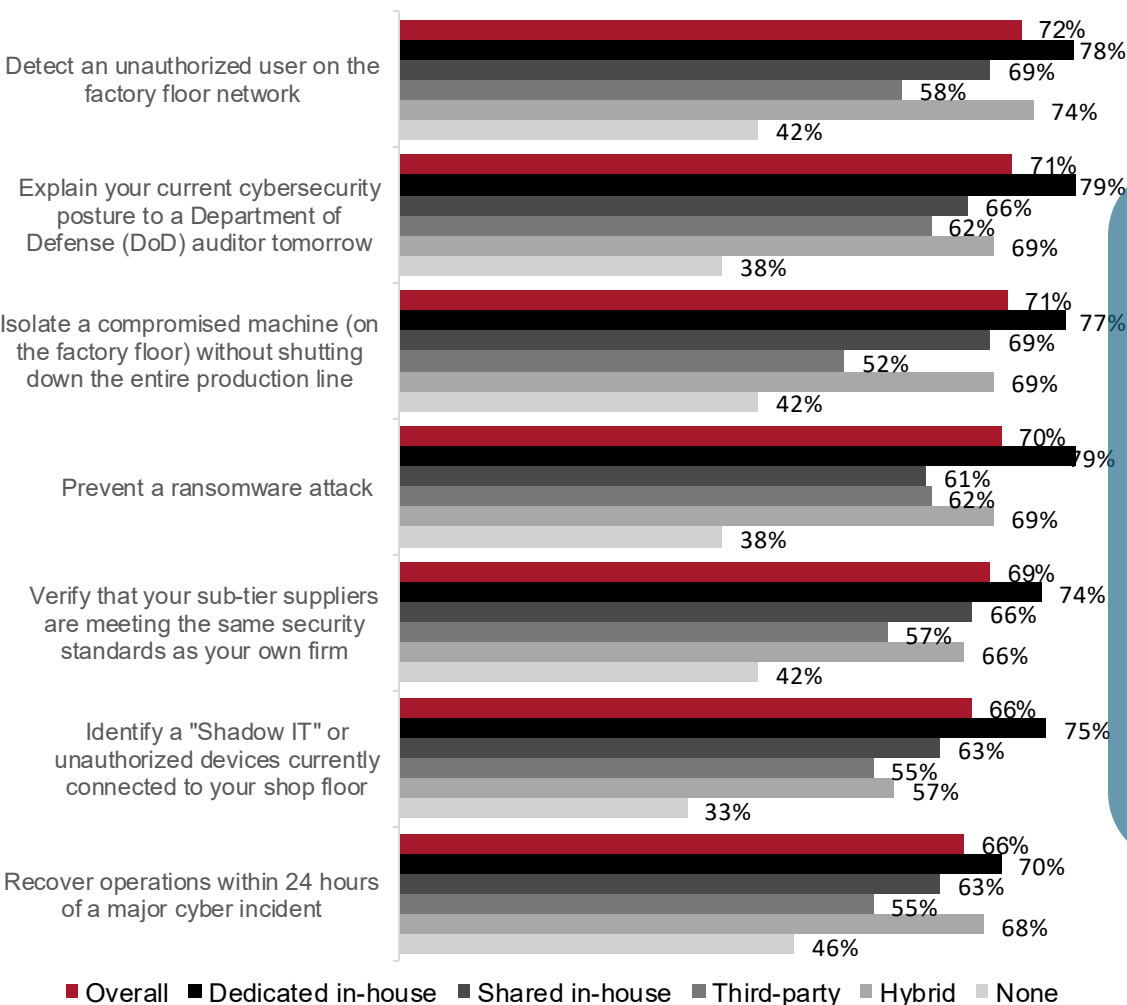
# Cybersecurity Threats & Preparedness

## Greatest Threat



Which of the following cybersecurity threats currently represent the greatest concern for your organization's leadership?  
Base: n = 700 (all respondents)

## Response Capability



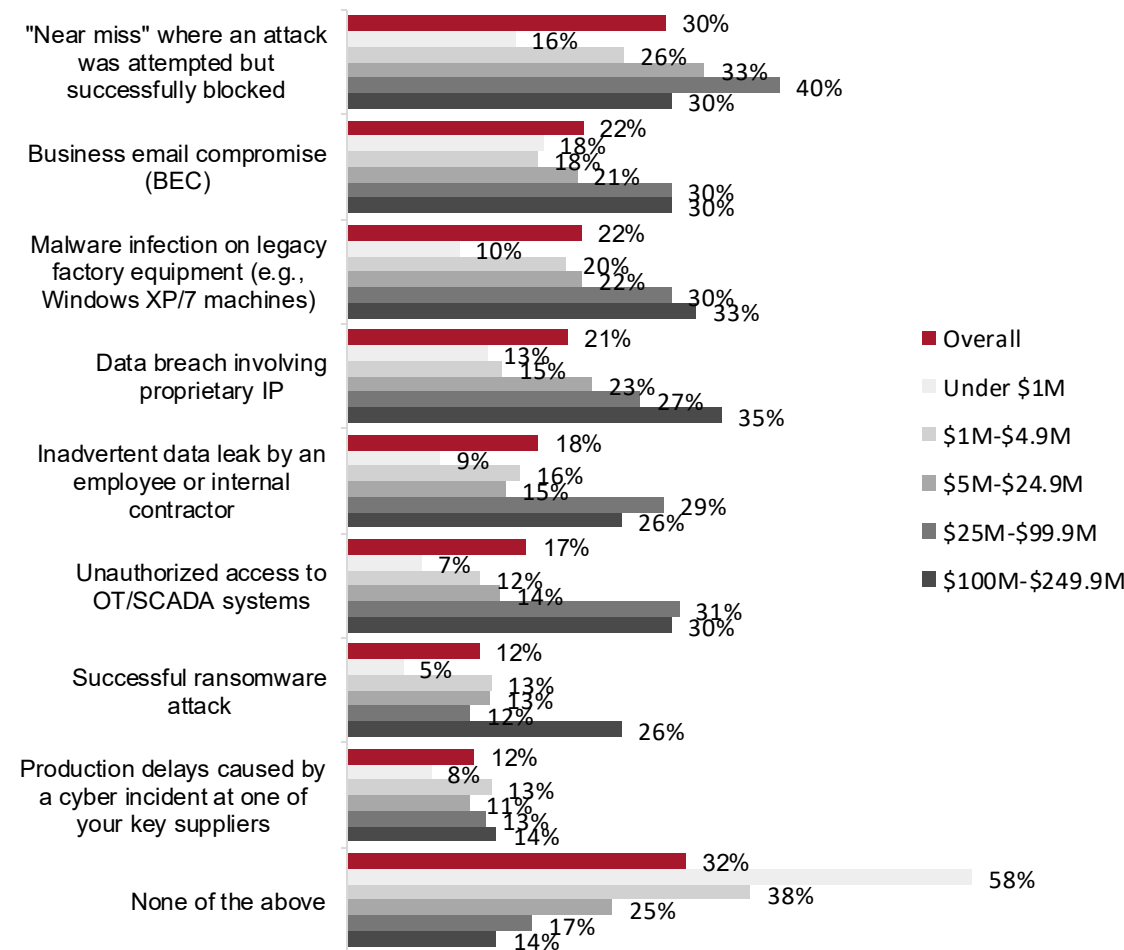
How would you rate your organization's ability to: (Extremely + Very Confident)

Firms with dedicated in-house teams are most confident in their capabilities, while firms that primarily outsource security to MSPs are least confident.

Unsurprisingly, less than half the firms with no cybersecurity lead, mostly those with under \$5m in revenue, are confident in their security responses.

# Cybersecurity Incidents

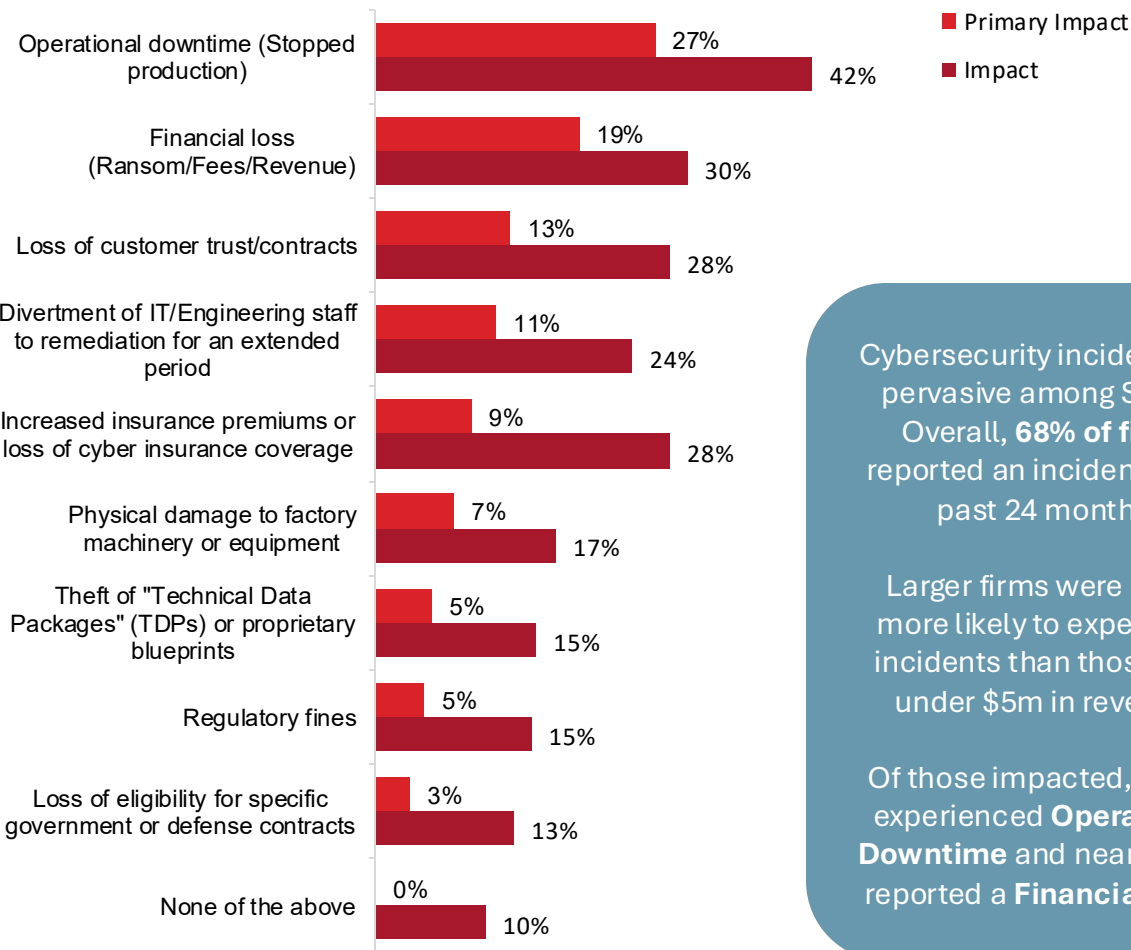
## Recent Experiences



Has your organization experienced any of the following in the past 24 months?

Base: n = 700 (all respondents)

## Incident Impacts



Base: n= 479

If you experienced an incident, what were the impacts?/  
If you experienced an incident, what was the primary impact?

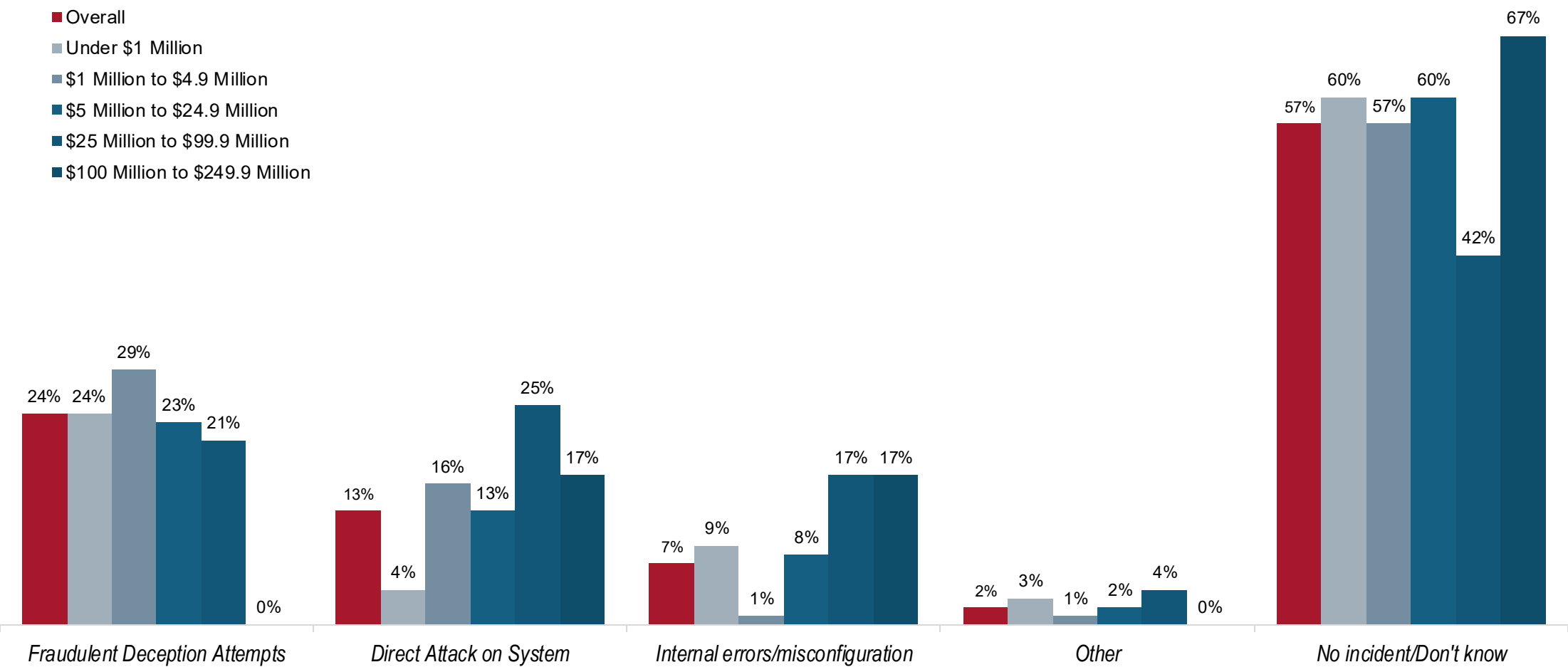
Cybersecurity incidents are pervasive among SMMs. Overall, **68% of firms** reported an incident in the past 24 months.

Larger firms were much more likely to experience incidents than those with under \$5m in revenue.

Of those impacted, over 1/4 experienced **Operational Downtime** and nearly 1 in 5 reported a **Financial Loss**.

# Qualitative Summary - Narrowly Avoided Incidents

Can you describe any incidents where a potential cyber threat or critical issue was narrowly avoided? What was the specific incident and how was it avoided?



# Narrowly Avoided Incidents Summary

The survey responses reveal a critical dichotomy in cybersecurity awareness among small and medium-sized manufacturers: while 57% (127 respondents) reported no incidents or were unsure, the remaining 43% described concrete near-miss scenarios that highlight real and present threats.

Among manufacturers who did experience close calls, credential-based attacks—particularly phishing and unauthorized access attempts—emerged as the dominant threat vector, affecting 24% of all respondents.

This data is particularly valuable for MxD's program design, as it not only identifies the most common attack patterns facing manufacturers but also reveals potential gaps in threat detection and awareness, with over half of respondents either experiencing no incidents or lacking visibility into potential threats. The responses also demonstrate varying levels of security maturity, from organizations relying on automated detection systems to those depending primarily on employee vigilance.

*"I received multiple emails from a supplier demanding payment. I checked the website and it was fake."*

*- Under \$1 Million*

*"An attack on our operation systems from an outside entity. Our firewalls prevented them from getting in."*

*- \$25 Million to \$99.9 Million*

*"It was an unauthorized user trying to gain access to classified information, but our MFA process caught it."*

*- \$1 Million to \$4.9 Million*

*"Not so much of a threat but an employee used software that was not authorized by IT."*

*- \$5 Million to \$24.9 Million*

*"We have had none recently although we were warned about a ransomware attack."*

*- \$5 Million to \$24.9 Million*

Can you describe any incidents where a potential cyber threat or critical issue was narrowly avoided? What was the specific incident and how was it avoided?

# Narrowly Avoided Incidents Top Themes

## Fraudulent Deception Attempts

When manufacturers did report near-misses, attacks from fraudulent actors dominated the threat landscape. Email-based attacks including phishing and spam were the most prevalent (13%, 29 responses), followed by suspicious login attempts and unauthorized access efforts (9%, 19 responses), and financial fraud or payment scams (3%, 7 responses). This pattern reveals that human-targeted social engineering remains the primary attack vector against manufacturers, suggesting that MxD's programs should prioritize security awareness training and email security controls as foundational elements for improving resilience across the manufacturing base.

*"Received a phishing file attachment containing a malicious macro file, detected by our endpoint security."*  
- \$5 Million to \$24.9 Million

*"An employee opened an email containing dangerous virus. The IT team was able to stop and remove it."*  
- \$1 Million to \$4.9 Million

*"A shadow threat was discovered, and the technical team attacked the threat successfully."*  
- \$25 Million to \$99.9 Million

## Direct Attack on System

A significant portion of manufacturers faced serious technical threats, with ransomware and malware near-misses representing 9% (19 responses) of all responses—a particularly concerning finding given the operational disruption these attacks can cause in manufacturing environments. Network attacks including DDoS and brute-force attempts accounted for 4% (8 responses). These incidents represent the most severe category of threats and underscore the importance of MxD's focus on the Defense Industrial Base, where such attacks could have national security implications beyond individual company impact.

*"We had malware downloaded onto 4 company laptops. We caught it before any damage could be done."*  
- \$1 Million to \$4.9 Million

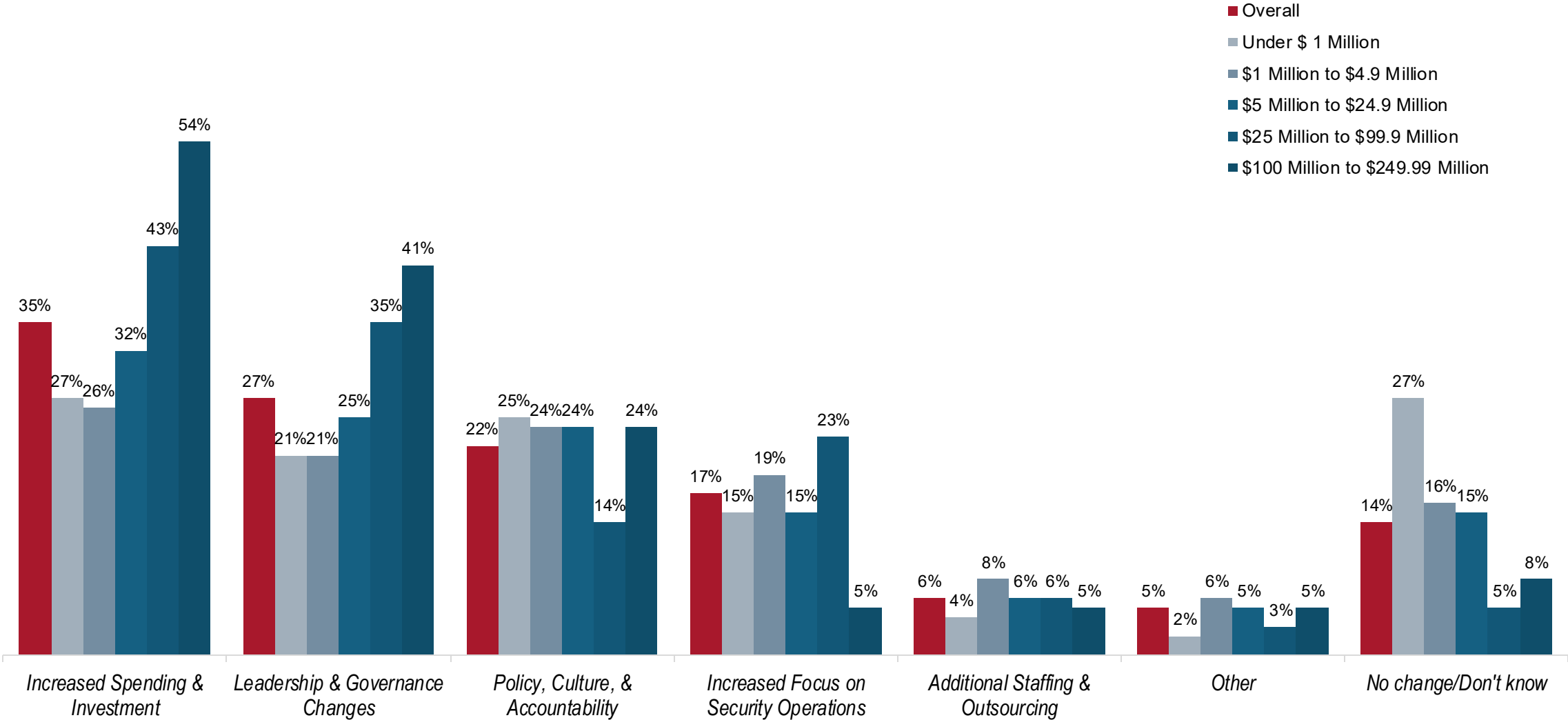
*"We had a potential ransomware attack but was able to catch in time before any damage was done."*  
- \$1 Million to \$4.9 Million

*"We once had our website come under a DOS attack and it was detoured really quick by our systems to a fake url."*  
- \$25 Million to \$99.9 Million

Can you describe any incidents where a potential cyber threat or critical issue was narrowly avoided? What was the specific incident and how was it avoided?

# Qualitative Summary - Incident Response

If your company has experienced an incident, how did it change the way leadership views cybersecurity spending?



# Incident Response Summary

The survey data reveals that cybersecurity incidents serve as powerful catalysts for organizational change among manufacturers, with 86% of respondents reporting some form of shift in how leadership views cybersecurity spending following an incident. This finding is particularly significant for MxD's goal of designing targeted interventions for small and medium-sized manufacturers, as it demonstrates that incidents create critical windows of opportunity for adopting stronger cybersecurity practices.

The responses show a multifaceted transformation that extends well beyond budget increases alone, encompassing leadership engagement, cultural shifts, and operational improvements. Understanding these post-incident changes can help MxD develop timely support programs that capitalize on heightened organizational readiness to invest in cybersecurity resilience.

*“Leadership saw the need to increase investment in cybersecurity and take it more seriously.”*

*- \$25 Million to \$99.9 Million*

*“Enhanced security management for cloud computing environments, with increased budget allocation.”*

*- \$1 Million to \$4.9 Million*

*“Starting to hire a third party to conduct penetration testing.”*

*\$100 Million to \$249.9 Million*

*“Use more advanced firewalls to protect against hacker attacks.”*

*- \$25 Million to \$99.9 Million*

*“We are always on alert and do more security checks.”*

*- \$5 Million to \$24.9 Million*

If your company has experienced an incident, how did it change the way leadership views cybersecurity spending?

# Incident Response Top Themes

## Increased Spending & Investment

Respondents primarily cited increased cybersecurity budgets (30%), demonstrating that incidents directly translate to financial commitment.

Additionally, 3% reported faster budget approvals and procurement processes, suggesting that incidents remove bureaucratic barriers that previously slowed security investments. Smaller but notable segments reported procurement shifts toward capability-focused buying (2%) and investment in advanced technologies like cloud, AI, and cryptography (2%), indicating that some organizations are not just spending more, but spending more strategically on cutting-edge solutions.

*“Budgets increased for proactive threat hunting and detection tools.”*

*- \$25 Million to \$99.9 Million*

*“The three-year security architecture upgrade plan has been approved, with an 40% increase in expenditure.”*

*- \$25 Million to \$99.9 Million*

*“Suddenly unlocked the budget for 24/7 monitoring.”*

*- \$5 Million to \$24.9 Million*

## Leadership & Governance Changes

Respondents reported shifts from reactive to proactive security posture (10%) and increased boardroom attention with leadership buy-in (10%), signalling that incidents elevate cybersecurity from an IT concern to an executive priority. Importantly, 8% of responses indicated that cybersecurity was reframed as a business risk rather than purely a technical issue—a fundamental change in perspective that aligns with MxD's goal of helping manufacturers understand cybersecurity's role in competitiveness and resilience. An additional 2% specifically mentioned experiencing business impact through downtime or financial loss, which likely drove these governance changes.

*“Moved from reactive fixes to proactive prevention spending.”*

*- \$25 Million to \$99.9 Million*

*“Shift from passive defense to proactive defense, and allocate more resources to employee training.”*

*- \$5 Million to \$24.9 Million*

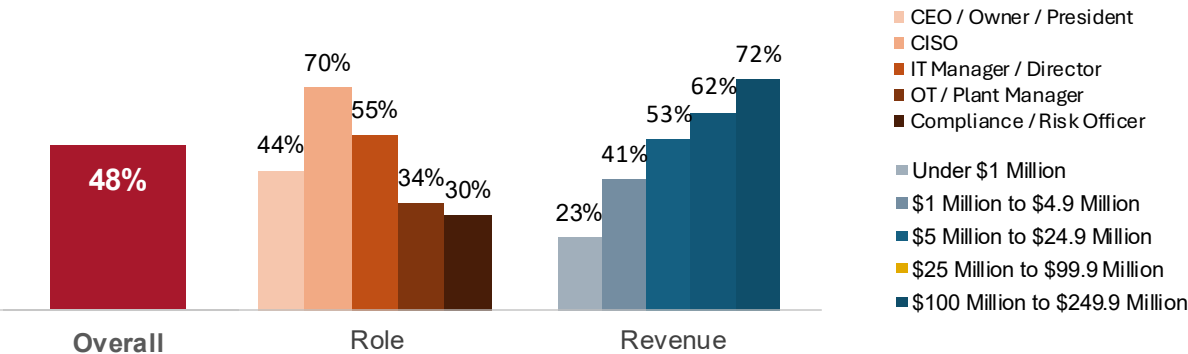
*“Leadership saw the need to increase investment in cybersecurity and take it more seriously.”*

*- \$5 Million to \$24.9 Million*

If your company has experienced an incident, how did it change the way leadership views cybersecurity spending?

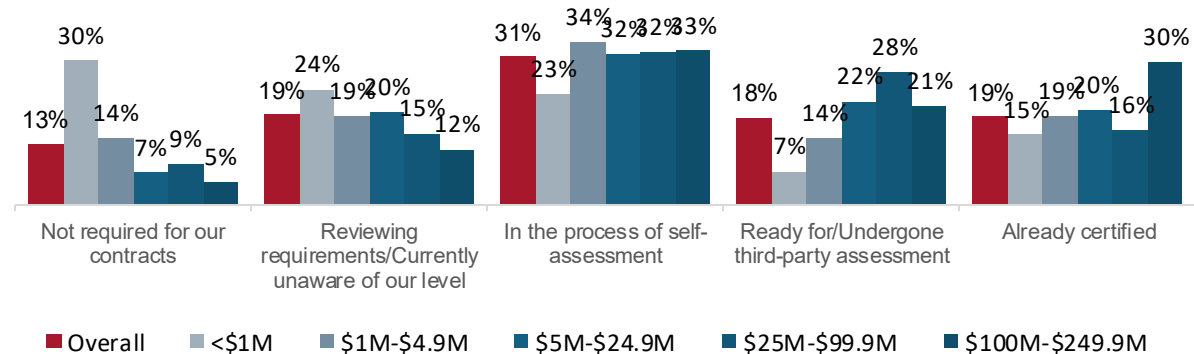
# CMMC Alignment

## CMMC Familiarity (T2B)



How familiar is your organization with CMMC? (Very familiar + Expert knowledge)

## CMMC Certification Status



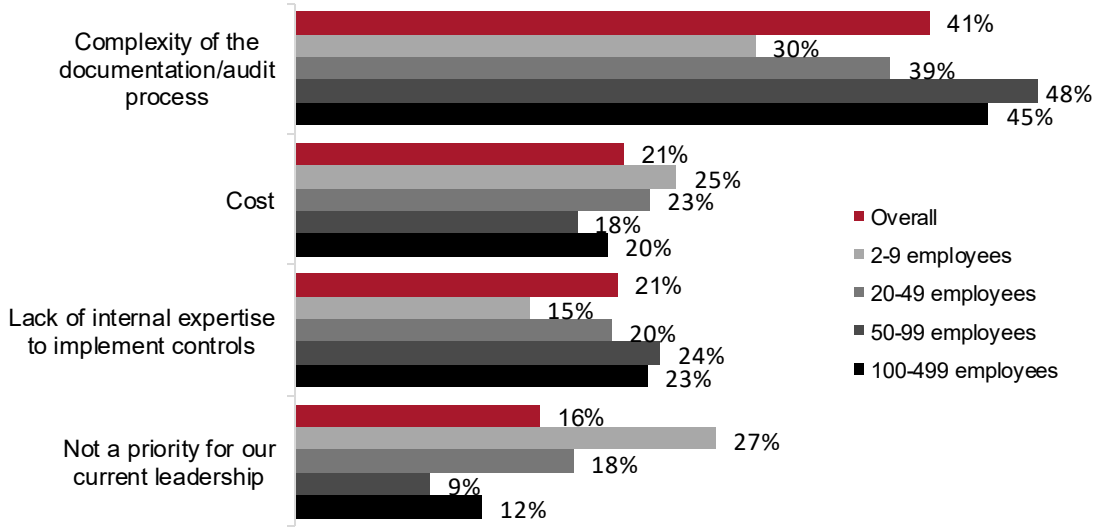
What is your current status regarding CMMC certification?

Base: n = 700 (all respondents)

CMMC compliance and expertise vary widely depending on the firm and who is answering. 70% of CISOs say they are Very Familiar or Experts, while only 30% of Compliance Officers do. Meanwhile, only 23% of respondents at firms with under \$1M in revenue are familiar with CMMC compared to over 70% at firms with revenue over \$100M.

Across the board, nearly 1/3<sup>rd</sup> of firms are in the self-assessment phase, with higher revenue firms more likely to ready or already certified. Nonetheless, cost is not the primary barrier but rather the complexity of the process – regardless of firm size. For the smallest shops, a secondary hurdle is simply making it a priority, as 27% of firms with under 10 employees admit that leadership hasn't yet put cybersecurity at the top of the to-do list.

## Main Barrier to Compliance



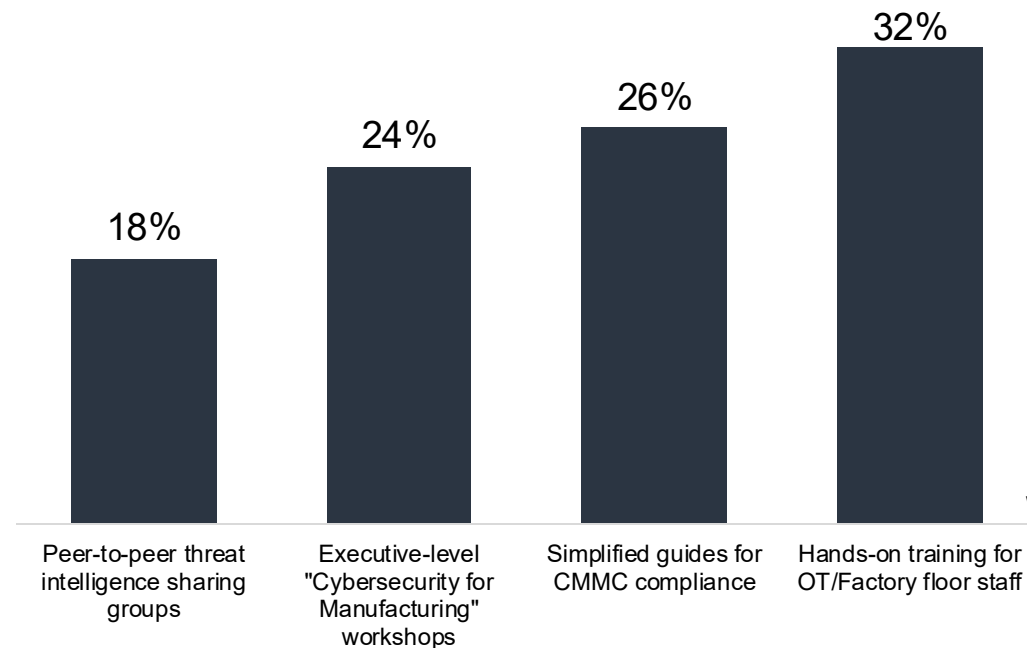
What is the biggest barrier to achieving full CMMC/NIST compliance?

# Supply Chain & Workforce

## Greatest Upskill Benefit

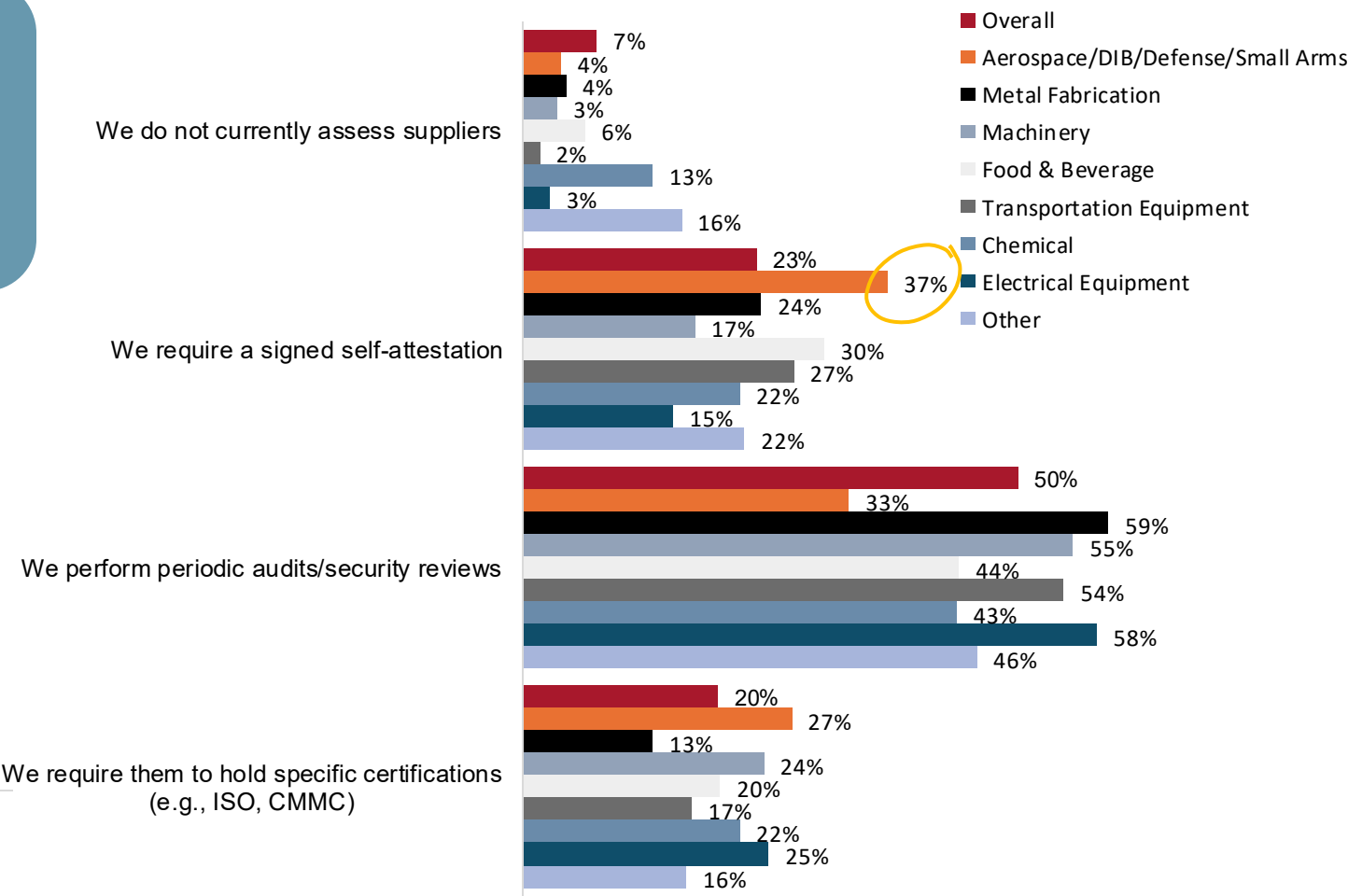
Firms selected staff training and simplified compliance guides as the most helpful for upskilling their workforce. This reflects both the challenge and importance of driving cybersecurity improvements from the bottom-up rather than through executive training or information sharing.

Interestingly, Defense / DIB/ Aerospace / Small Arms are less likely to perform audits and security of their reviews than other industries.



Which of the following would be most helpful for upskilling your workforce in digital/cyber transformation?  
Base: n = 700 (all respondents)

## Cybersecurity Assessment



How do you assess the cybersecurity posture of your own suppliers?

# Moving Forward – The Path to Resilience

While U.S. SMMs are increasingly aware of the escalating threat landscape, their ability to defend against these threats is being hampered by a trifecta of cultural, administrative, and economic barriers.

Currently, a significant portion of SMMs is trapped in a reactive cycle. Smaller firms, in particular, lack dedicated personnel to drive security initiatives, leading to a "complexity trap" where the administrative burden of compliance outweighs their capacities – either technical or administrative. This is compounded by a market where specialized cybersecurity guidance is both scarce and prohibitively expensive. Consequently, security is often treated as a cost rather than a foundational element of operational uptime and business stability.

## The Path Forward: Strategic Next Steps

To bridge this gap, the transition from "inaction to action" must focus on making cybersecurity accessible, affordable, and culturally urgent.

**Institutionalizing Urgency:** MxD should pivot from technical training to **Leadership Engagement**. By utilizing tools like the "Downtime Calculator," MxD can help IT champions translate cyber risk into the language of the C-suite: lost production hours and missed revenue.

**Simplifying the "Complexity Wall":** The creation of **Modular Compliance Toolkits** - "plain-English" policy templates and automated logging guides will allow small shops to meet NIST and CMMC requirements without needing a dedicated compliance department. AI can be leveraged here to help navigate these compliance guidelines.

**Democratizing Expert Access:** To combat the consultant shortage, MxD can facilitate a **Vetted Expert Marketplace** and **Peer-to-Peer Cohorts**. By pooling resources, smaller firms can access top-tier specialized guidance at a fraction of the cost of traditional individual retainers.

By addressing these human and market-driven hurdles, MxD will not only improve the cybersecurity posture of individual firms but will fundamentally strengthen the resilience and competitiveness of the entire U.S. manufacturing industrial base.

# Thank You!

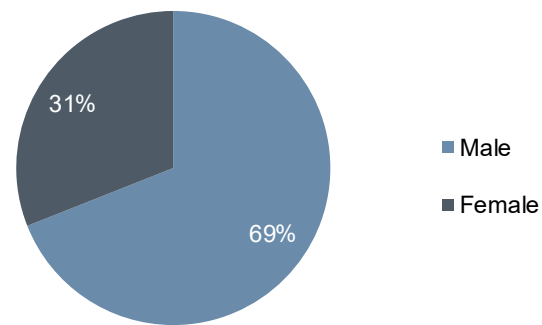
**Prepared By:**  
Questionpro

For any questions or to discuss the results further.  
Please contact [Patrick.Jones@questionpro.com](mailto:Patrick.Jones@questionpro.com)



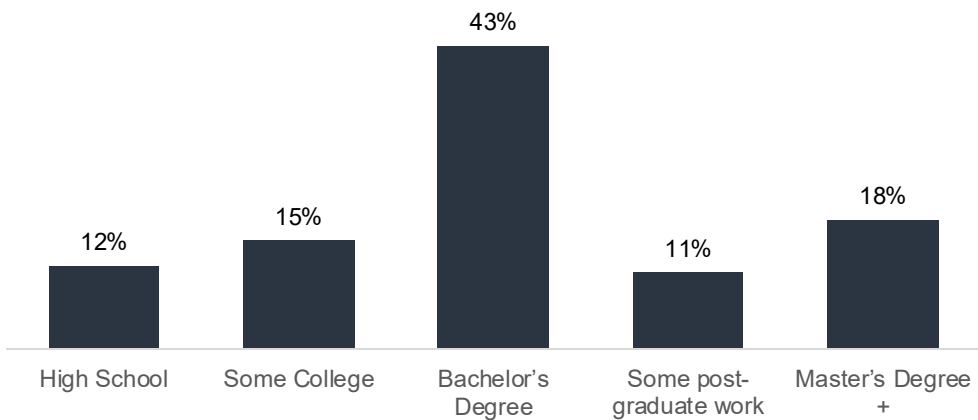
# Respondent Demographics

## Gender



Please indicate your gender:

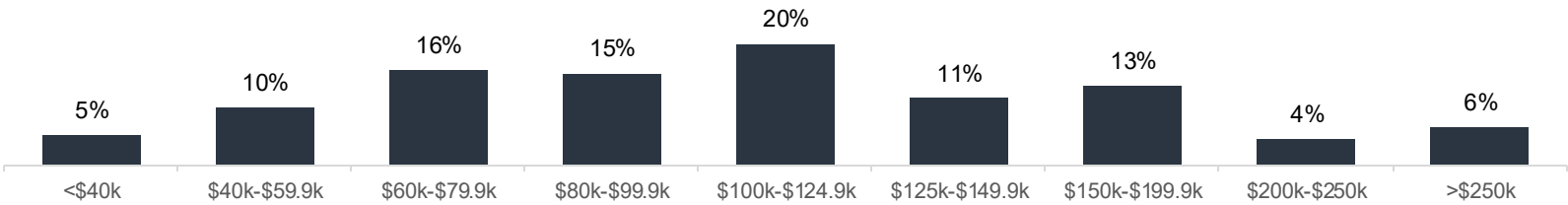
## Education Level



What is the highest level of education you have completed?

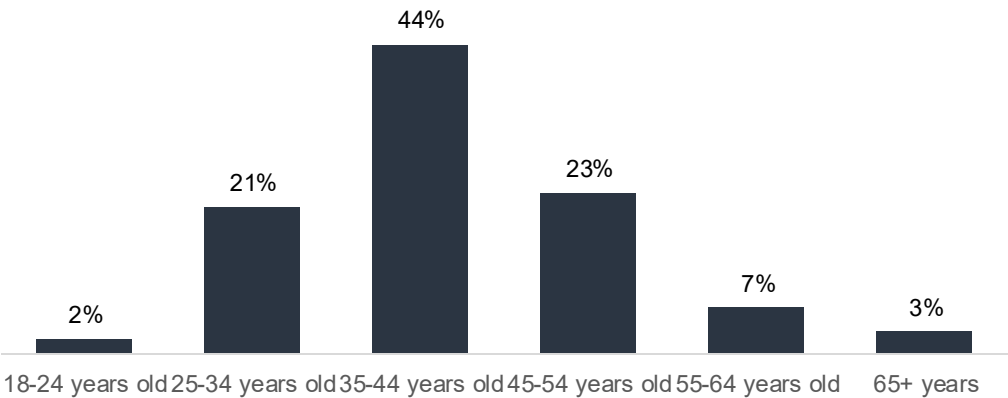
Base: n = 700 (all respondents)

## Income



What is your approximate yearly household income?

## Age Group



What age group do you fall under?