RADICL™

DIB CYBERSECURITY MATURITY REPORT

2025 EDITION

A Word from Our CEO

Small to medium-sized businesses (SMBs) are creating the innovation and technology that fuels America's Defense Industrial Base (DIB) and the nation's critical infrastructure (CI). Yet because of that, they're prime targets for attacks from nation-state actors, ransomware gangs, and other cyber criminals on the hunt for sensitive data and looking to disrupt operations. The majority of SMBs are unprepared to deal with a motivated cyberthreat.

What these businesses need isn't just basic IT security controls, but a defense-in-depth strategy to reduce their cybersecurity incident risk. But how many are actually taking this approach?

This is the question we asked in last year's "DIB Cybersecurity Maturity Report 2024" and what we're asking in this year's report. This year's respondents provided insights into their current state of cybersecurity, their biggest security challenges, their experience working with outsourced service providers, and where they currently stand on their CMMC compliance.

We hope these findings, along with how they've changed from last year, help you benchmark your current security efforts and guide you towards strengthening your security posture in 2025.

Chris Petersen
Co-Founder & CEO, RADICL

Key Findings

77% say enhancing cybersecurity is a high priority. 66% have three or more people dedicating time to security, and 80% rate their security skill level as very high or high.

47% had four or more user accounts or emails compromised in the past year. 24% had more than ten user accounts or emails compromised, and 47% had four or more of their endpoints compromised in the past year.

54% say it would take two days or longer to respond to ransomware or a breach. Also, 38% would take a week or more to detect a threat in their environment. 44% would not be surprised to experience an operational disruption or data theft.

57% report low to medium effectiveness in threat hunting. Additionally, 56% report low to medium effectiveness in threat investigation and 55% report low to medium effectiveness

37% say cybersecurity-related incidents have cost their company $100,001. Of those, 4% report that cost to be more than $500,001.

The biggest security challenge is protecting sensitive data from breaches and leaks. They're also challenged with implementing and maintaining compliance with regulations and keeping up with evolving cyber threat landscapes.

The biggest challenge with outsourced providers is the inconsistent quality of service. Other challenges include being too expensive given the overall value delivered and Limited support for compliance management.

The top capability they're looking for in a new service provider is using the latest technologies to offer robust protection against evolving threats. They're also looking for providers with quality staff and swift, coordinated responses to security incidents.

While 71% have started CMMC, only 17% state they are Level 2 ready. 21% are compliant with Level 1, and 17% are compliant with Level 2.

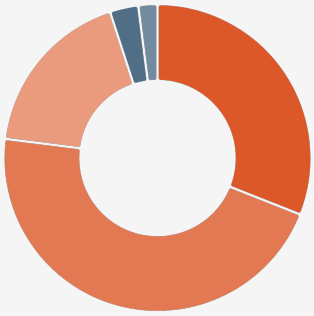
Table of Contents

Part 1: Current Program Effectiveness

SMBs in the DIB face relentless attacks from threat actors seeking to steal intellectual property and are high-value targets for motivated ransomware gangs and other cybercriminals. Yet they're the backbone of defending our nation, and in this section, they tell how well they're defending themselves from attack.

77% say enhancing cybersecurity is a very high or high priority

31% of respondents say enhancing their organization's cybersecurity measures over the next year is a very high priority and 46% say it's a high priority. 18% say it's a medium priority. 3% say it's low and 2% say it's very low.

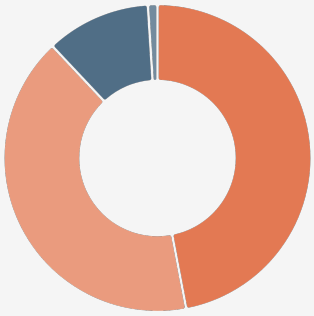


Q. How would you rank the priority of enhancing your organization's cybersecurity measures over the next 12 months?

Very High	31%	Low	3%
High	46%	Very Low	2%
Medium	18%		

47% meet monthly to discuss cybersecurity

47% say their leadership team meets to discuss security monthly, while 41% convene quarterly to discuss cybersecurity. 11% meet annually, and 1% weren't sure about the frequency. One respondent (<1%) said their leadership team never meets.

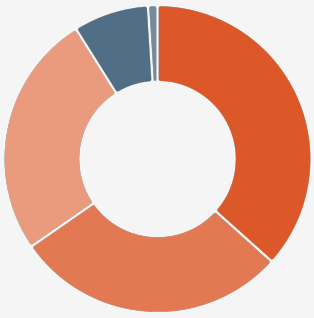


Q. How often does your executive leadership team meet to discuss security?

Never	0%	Annually	11%
Monthly	47%	I'm not sure	1%
Quarterly	41%		

66% have three or more people dedicating time to security

37% have four or more people who spend at least a quarter of their time on security, while 29% have three people who do. 26% have two people who spend at least a quarter of their time on security, 8% have one person, and 1% don't have anyone.

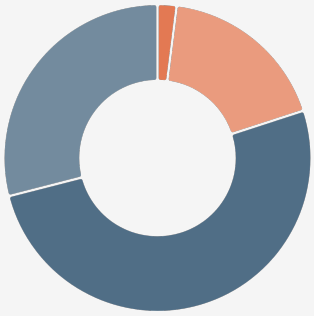


Q. How many people on your team spend more than 25% of their time on security?

4+	37%	1	8%
3	29%	0	1%
2	26%		

80% rate their security skill level as very high or high

29% rate the skill level of their in-house security team very high, while 51% rate their skill level as high. 18% rate their security team skill level as medium, 2% rated them low, and one respondent (<1%) rated them very low.



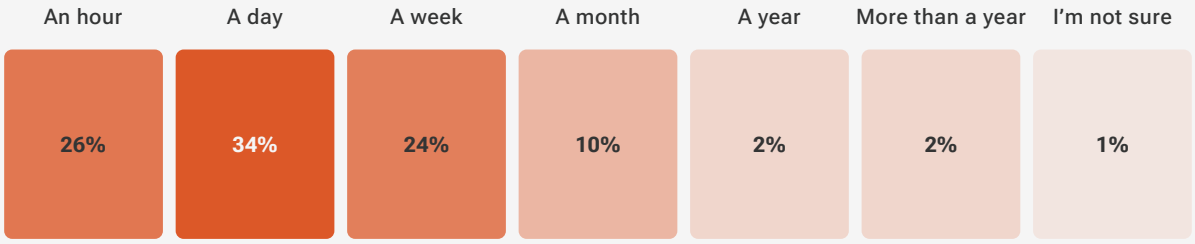
Q. How would you rate the skill level of your in-house security team on a scale from 1 to 5?

1 - Very Low	0%	4 - High	51%
2 - Low	2%	5 - Very High	29%
3 - Medium	18%		

38% would take a week or more to detect a threat in their environment

How quickly would respondents detect a threat that bypassed their defense and was operating from within their IT environment? 26% would detect it in an hour, and 34% would detect it within a day. For 24%, it would take a week, and for 10%, it would take a month. 2% would detect it in a year and 2% would detect it in more than a year. 1% wasn't sure how long it would take.

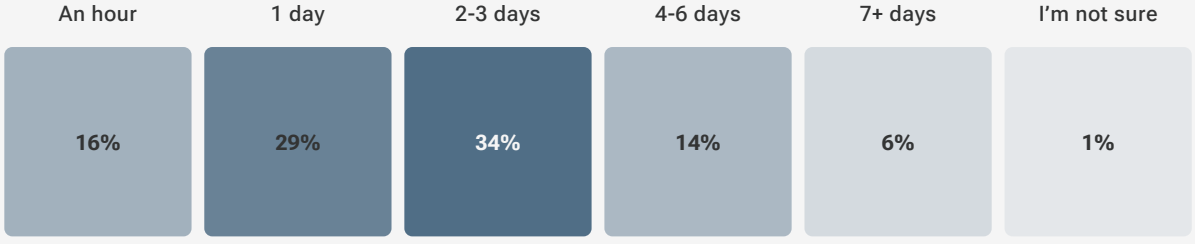
Q. If a threat bypassed your defense and was operating from within your IT environment, how quickly would you be able to detect its presence?



54% say it would take two days or longer to respond to ransomware or a breach

How quickly would respondents be able to conduct a full investigation and develop a comprehensive incident response plan if they had a ransomware or data breach incident? For 16%, it would take an hour, and for another 29%, it would take a day. 34% say it would take two to three days, and 14% say it would take four to six days. For 6%, it would take a week or more. 1% wasn't sure how long it would take.

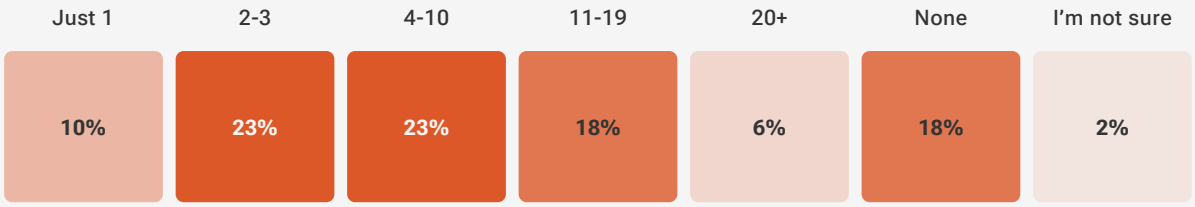
Q. If you had a ransomware or data breach incident, how quickly would you be able to conduct a full investigation and develop a comprehensive incident response plan?



47% had four or more of their endpoints compromised in the past year

18% say none of their endpoints have had a virus or malware compromise in the past 12 months. However, 10% have had one endpoint compromised, 23% have had two to three, and 23% have had four to ten. 18% say they've had eleven to nineteen, and 6% have had twenty or more. 2% weren't sure how long it would take.

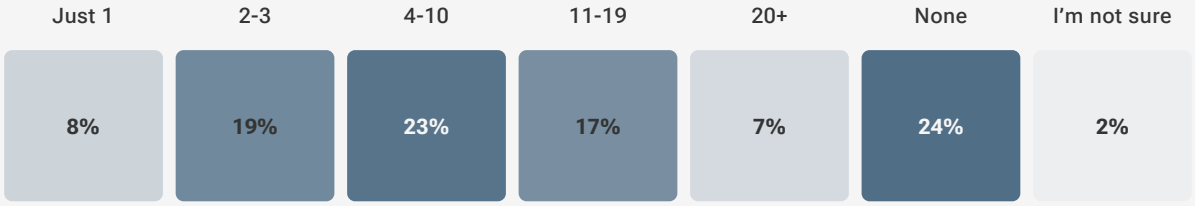
Q. How many of your organization's endpoints have had a virus or malware compromise in the past 12 months?



47% had four or more user accounts or emails compromised in the past year

24% say none of their user accounts or email addresses have been compromised in the past 12 months. However, 8% have had one account compromised, 19% have had two to three, and 23% have had four to ten. 17% say they've had eleven to nineteen, and 7% have had twenty or more. 2% weren't sure how long it would take.

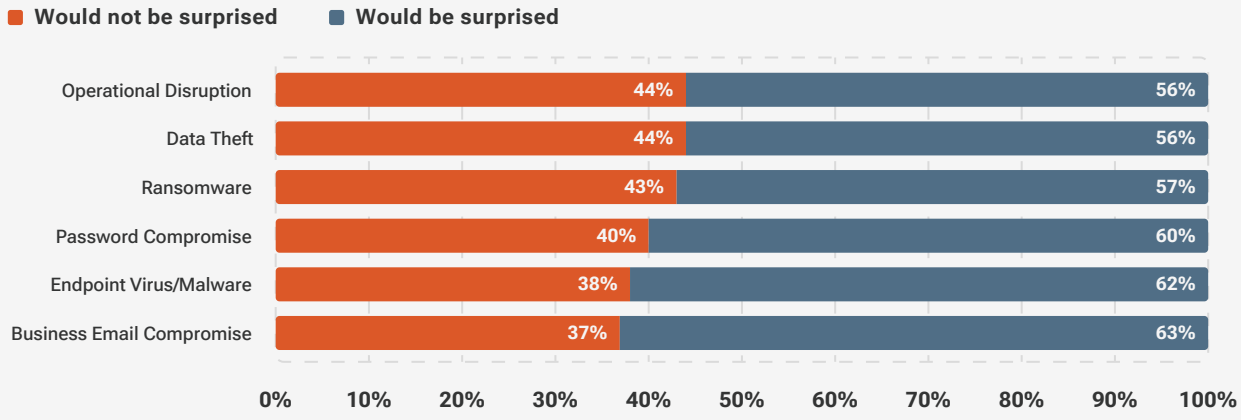
Q. How many of your organization's user accounts or email addresses have been compromised in the past 12 months?



44% would not be surprised to experience an operational disruption or data theft

Our respondents say they **would not be surprised** to experience the following — in other words, they know they may have vulnerabilities or gaps in security that would result in. Directly correlated, they **would be surprised** to experience the following — in other words, they believe their security capabilities are sufficient in these areas, so the likelihood of compromise is assumed to be low:

Q. Would you be surprised if you experienced any of the following security incidents in the next 12 months?

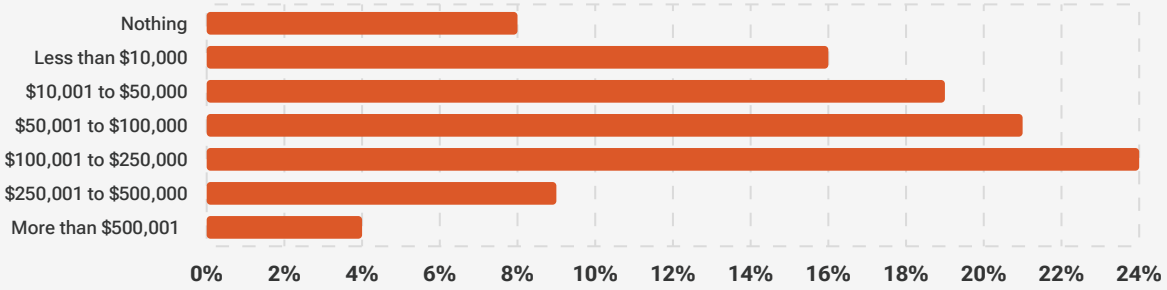


37% say cybersecurity-related incidents have cost their company $100,001 or more

How much money have cybersecurity-related incidents cost in lost time, productivity, or cash? For 8%, it was nothing. However, 16% say it was less than $10,000; 19% say $10,001 to $50,000; 21% say $50,001 to $100,000; 24% say $100,001 to $250,000; 9% say $250,001 to $500,000; and 4% say more than $500,001.

Overall, 37% have experienced costs of $100,001 or more in cybersecurity-related incidents.

Q. In economic terms, how much do you estimate cybersecurity-related incidents have cost your company in lost time, productivity, or cash?



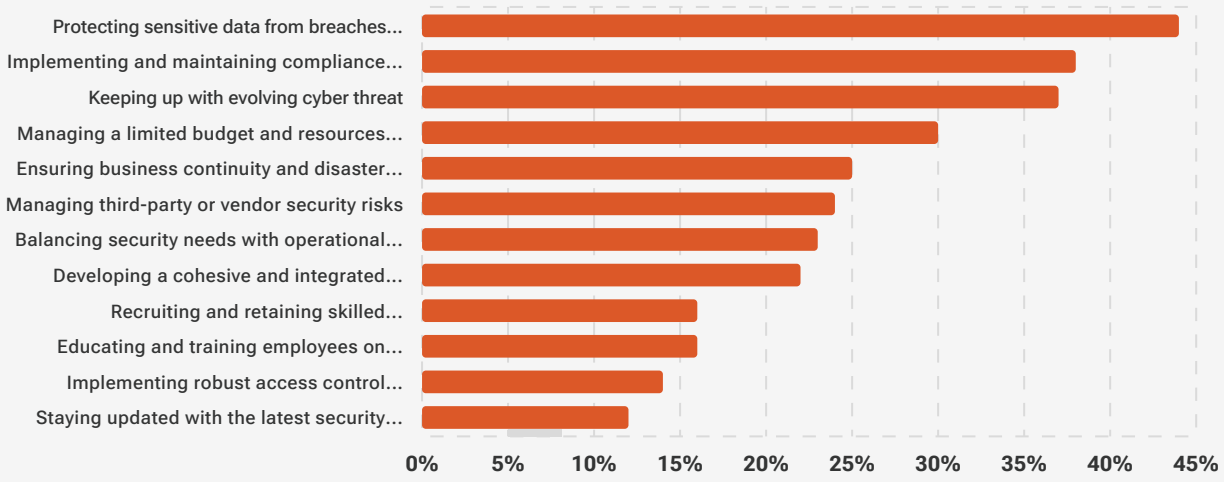
Top Five Challenges to Cybersecurity

When it comes to managing and executing an effective cybersecurity program, their greatest challenges today are (they chose all that applied):

1. Protecting sensitive data from breaches and leaks (44%)
2. Implementing and maintaining compliance with regulations, including Cybersecurity Maturity Model Certification (CMMC) (38%)
3. Keeping up with evolving cyber threat landscapes (37%)
4. Managing a limited budget and resources for comprehensive cybersecurity measures (29%)
5. Ensuring business continuity and disaster recovery planning (25%)

Other challenges include managing third-party or vendor security risks (24%), balancing security needs with operational efficiency (23%), developing a cohesive and integrated cybersecurity strategy (22%), recruiting and retaining skilled cybersecurity personnel (16% tie), educating and training employees on security best practices (16% tie), implementing robust access control and identity management systems (14%), and staying updated with the latest security technologies and tools (12%).

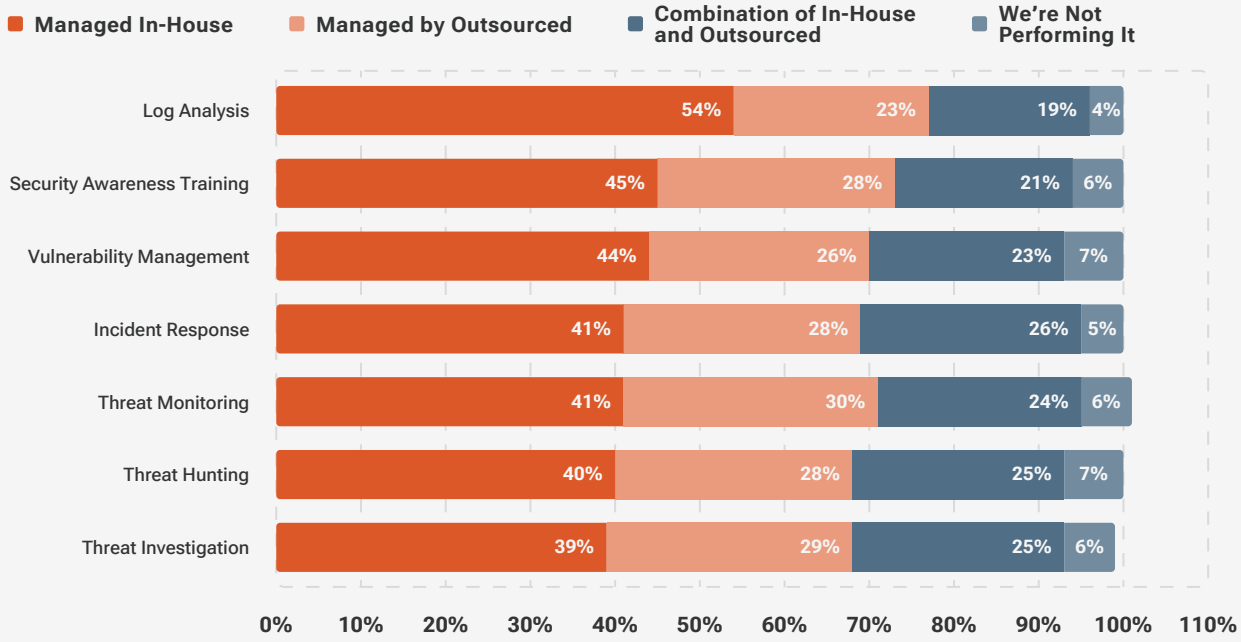
Q. Of the options listed below, what are your top three greatest challenges to cybersecurity today?



Top Functions They're Managing In-House, Outsourcing, or Combining

When it comes to managing security functions in-house, outsourcing, doing both, or doing neither, respondents are doing the following:

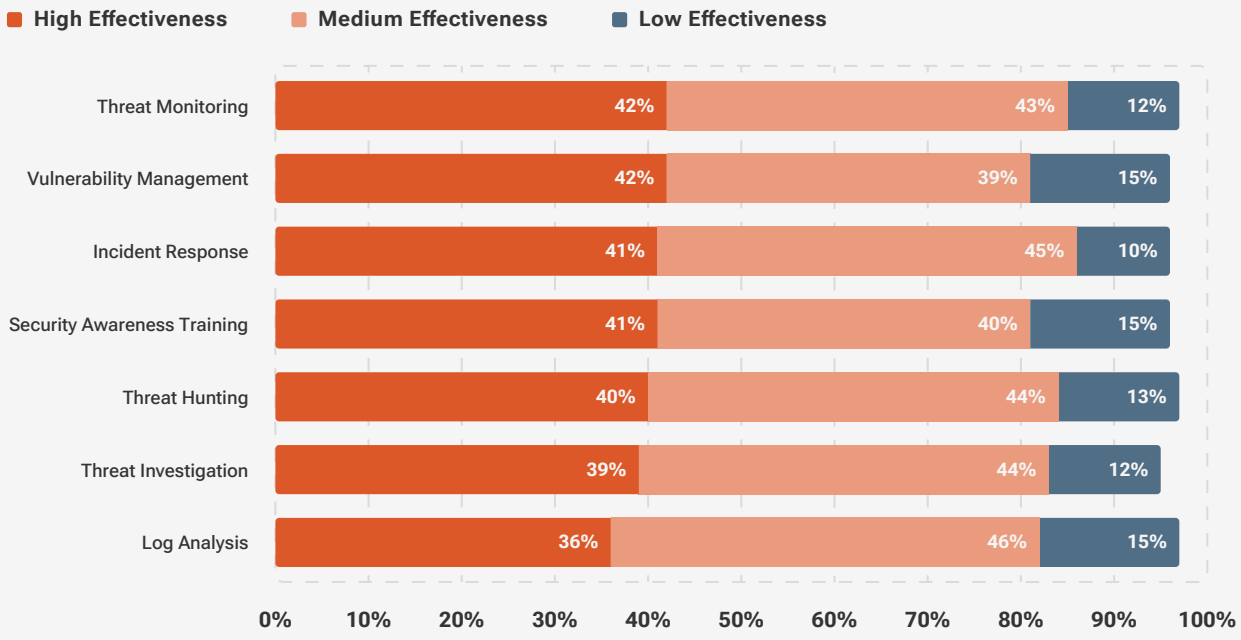
Q. Who is responsible for the following functions at your organization?



Security Program Function Effectiveness

When it comes to how effective they are at executing various security program functions, respondents say the following:

Q. Please rate how effective you are at executing the following functions of your security program:



Summary

The majority of respondents say that their companies are focusing time, energy, and resources on cybersecurity:

- 77% say cybersecurity is a very high or high priority
- 66% have three or more people dedicating time to security
- 80% rate their security skill level as very high or high
- 47% meet monthly to discuss cybersecurity

When compared to last year's report, we see a noticeable jump in attention paid to cybersecurity. This year:

- 16% more say enhancing cybersecurity is a very high or high priority
- 13% more rate their security skill level as very high or high

However, there are still areas of improvement, as 38% would take a week or more to detect a threat in their environment and 54% would take two days or longer to respond to ransomware or a breach. 47% had four or more of their endpoints compromised in the past year and 47% had four or more user accounts or emails compromised in the past year.

The good news is that these percentages are down from last year's report, reflecting ongoing improvements to security and threat detection. Additionally, 37% say cybersecurity-related incidents have cost their company $100,001 or more — down from 46% last year.

Despite the improving numbers, respondents still have areas to address, including "medium effectiveness" in log analysis and incident response, and "low effectiveness" in log analysis, vulnerability management, security awareness training.

Ultimately, their top challenges to effective cybersecurity today are protecting sensitive data from breaches and leaks and implementing and maintaining compliance with regulations, including CMMC.

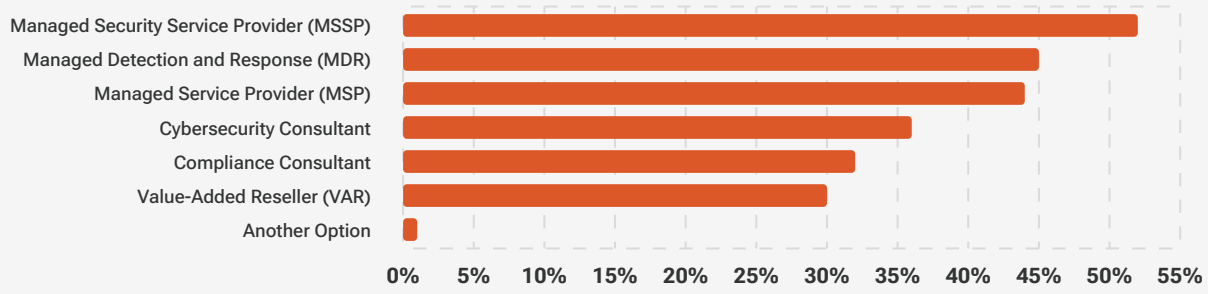
Part 2: Outsourced Cybersecurity

Small and medium sized businesses often leverage outsourced cybersecurity providers to augment and extend their capabilities. In this section we explore how companies are leveraging outsource providers, along with trends and challenges.

Top Three Outsourced IT or Security Partners

The top outsourced IT or security partners they use are (they chose all that applied):

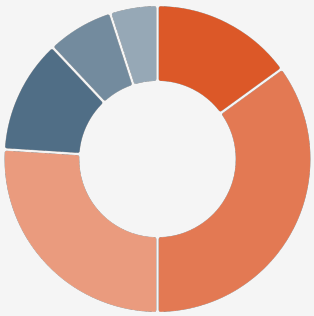
Q. Select all the types of outsourced IT/security partners you use:



76% spend $50,001 or more annually on outsourced security

7% spend less than $20,000 annually on outsourced security; 12% spend $20,001 to $50,000; 26% spend $50,001 to $100,000; 35% spend $100,001 to $250,000; and 15% spend more than $250,001. Finally, 5% don't spend any, as they don't outsource security.

Overall, 76% spend $50,001 or more annually on outsourced security.



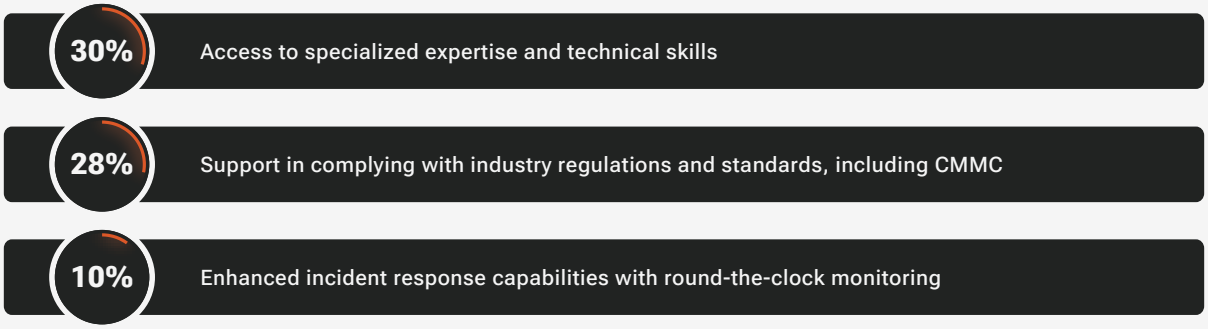
Q. How much do you spend annually on outsourced security?

More than $250,001	15%	$20,001 to $50,000	12%
$100,001 to $250,000	35%	Less than $20,000	7%
$50,001 to $100,000	26%	None - We don't outsource security	5%

Top Reasons to Outsource

The primary factors that influenced the decision to outsource security operations functions to a provider are:

Q. From the options listed below, what were the primary factors that influenced your decision to outsource security operations functions to an outsourced security provider?



Top Outsourced Provider Challenges

While many are outsourcing, they're not necessarily finding the results they expected. The greatest challenges they have experienced with their outsourced provider are:

Q. From the options listed below, what are the greatest challenges you have experienced with your outsourced provider?

52% will change their outsourced security provider

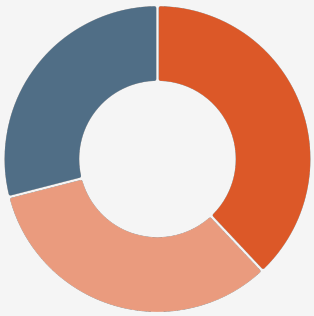
52% plan to make changes to their outsourced security provider in the next year. 48% will not.

Q. Do you plan to make changes to your outsourced security provider in the next 12 months?

Yes	52%
No	48%

38% plan to bring security in-house

For those who will make changes, 38% plan to bring security in-house, 33% will find a new outsourced provider, and 29% will do a combination of both.



Q. What best describes what you will do to replace them?

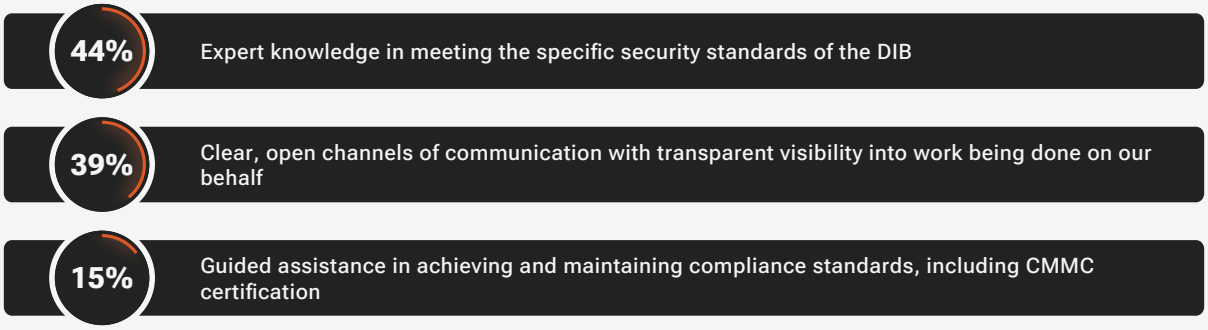
Bring security in-house	38%
Find a new outsourced provider	33%
Both of the above	29%

Top Service Provider Capabilities for Those Looking to Switch

Those wanting to find a new service provider say the following qualities and capabilities are most important (they chose all that applied):

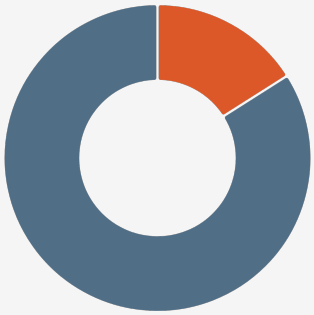
Q. When evaluating a new outsourced security provider, what qualities and capabilities are most important to you?

59%	Utilization of the latest technologies to offer robust protection against evolving threats
50%	Quality of the providers in terms of cybersecurity expertise and overall customer experience
47%	Swift, coordinated responses to security incidents to minimize potential damage
46%	Offering comprehensive cybersecurity coverage and capabilities from a single provider



16% of those who do not outsource now plan to in the next year

For those who replied above that they don't outsource security, 16% do plan to outsource security in the next 12 months, while 84% will not.



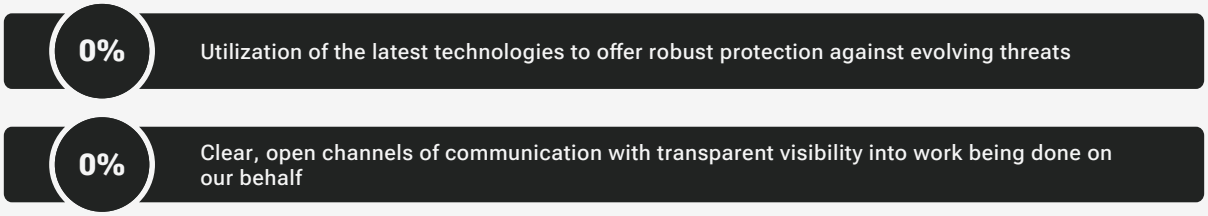
Q. Do you plan to outsource security in the next 12 months?

Yes	16%
No	84%

Top Service Provider Capabilities for First-Time Users

Of those who plan to outsource in the next year who aren't currently, the qualities and capabilities most important when evaluating a new outsourced security provider include (they chose all that applied):

Q. When evaluating a new outsourced security provider, what qualities and capabilities are most important to you?



Summary

Respondents are managing their cybersecurity programs through both in-house capabilities and outsourcing to MSSPs (52%), MDRs (45%), and MSPs (44%). Overall, 76% spend $50,001 or more annually on outsourced security.

Why are they outsourcing? The top reason is the opportunity to improve their security posture with access to advanced security tools and technologies — a reason that jumped from fourth last year to first this year. They're also outsourcing for the cost-effectiveness compared to building and maintaining an in-house team and the need for scalability and flexibility to adapt to changing business needs — both in their top reasons last year.

Those who outsource do encounter challenges, the primary being inconsistent quality of service, which jumped from fifth last year to first this year. Another challenge is that it feels too expensive given the overall value delivered, which jumped from third last year to second this year.

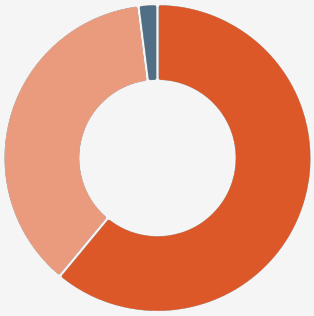
Because of this (or other reasons), 52% will change their outsourced security provider in the next year and 38% plan to bring security in-house. Those looking to switch service providers are prioritizing someone who uses the latest technologies to offer robust protection against evolving threats.

Part 3: CMMC Preparedness

All Department of Defense suppliers (prime contractors and subcontractors) that handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) are bound to the Cybersecurity Maturity Model Certification (CMMC). In this section, respondents share their familiarity and progress with CMMC readiness and compliance.

61% are very familiar with CMMC requirements

61% are very familiar with and have an in-depth understanding of the CMMC requirements. 37% are somewhat familiar and have a general understanding of the CMMC requirements. 2% are not familiar with and have limited or no understanding of the CMMC requirements.

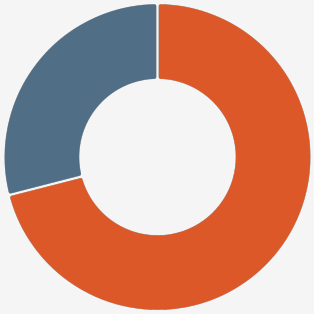


Q. How familiar are you with the requirements of the Cybersecurity Maturity Model Certification (CMMC)?

Very familiar - I have an in-depth understanding of the CMMC requirements	61%
Somewhat familiar - I have a general understanding of the CMMC requirements	37%
Not familiar - I have limited or no understanding of the CMMC requirements	2%

71% have started the CMMC compliance process

71% have started the process for CMMC compliance, while 29% have not.



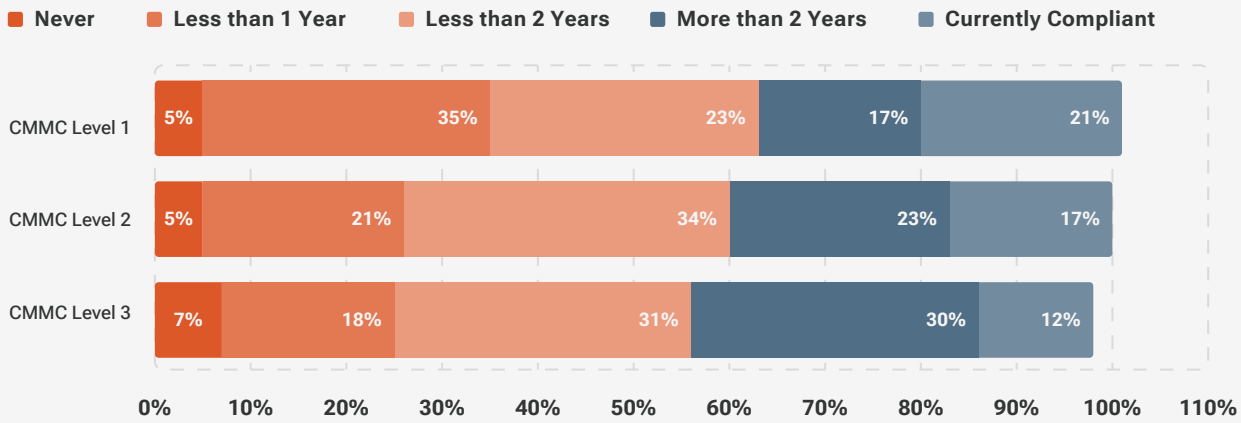
Q. Has your company begun the process for CMMC compliance?

Yes	71%
No	29%

How Much Time to CMMC Compliance

How soon do respondents plan to reach their CMMC compliance? Here's how long it will take our respondents to reach compliance:

Q. How soon do you plan to reach the following CMMC compliance levels?



Summary

This year, 98% of respondents are either familiar or very familiar with CMMC requirements, as compared to 90% last year. However, last year, 81% said they started the CMMC compliance process compared to 71% this year.

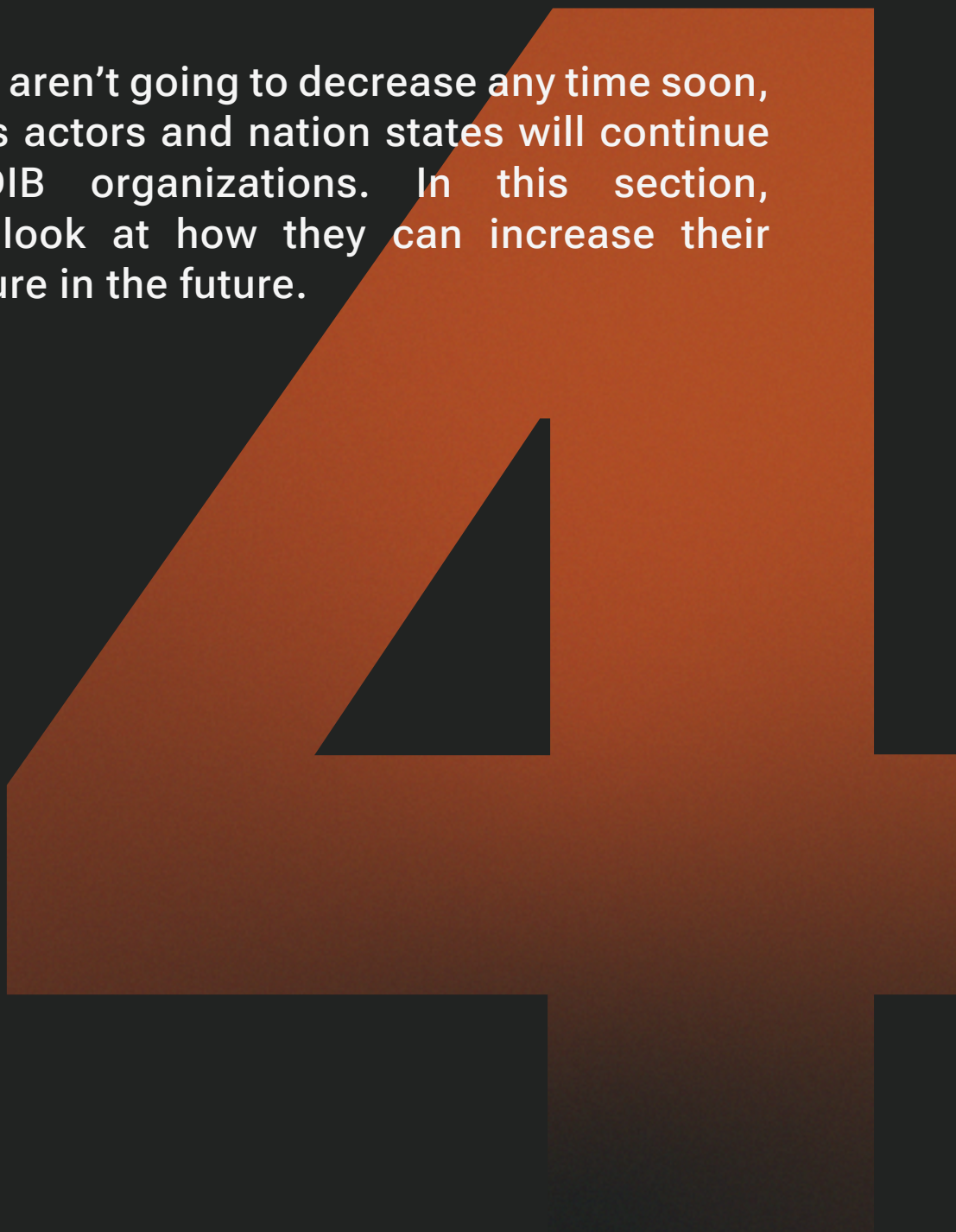
This year, there's more compliance than last year:

- 21% this year are currently compliant with Level 1, compared to 13% last year
- 17% this year are currently compliant with Level 2, compared to 11% last year
- 12% this year are currently compliant with Level 3, compared to 12% last year

There are fewer responses to "never" this year than there were to last year, too. This perhaps indicates that with more familiarity and guidance now, the process is less of a mystery than it was a year ago, and organizations feel more confident they can achieve their compliance.

Part 4: Future Strategies & Priorities

Cyber attacks aren't going to decrease any time soon, and malicious actors and nation states will continue to target DIB organizations. In this section, respondents look at how they can increase their security posture in the future.



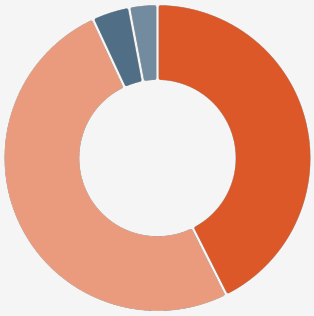
Top Cybersecurity Priorities

Top cybersecurity priorities for the next year include:

Q. From the options listed below, what are your top cybersecurity priorities for your company in the upcoming 12 months?

43% expect their general security budget to increase

Over the next fiscal year, 43% plan to increase budget allocation for cybersecurity, 51% plan to maintain the current budget allocation for cybersecurity, and 4% plan to decrease budget allocation for cybersecurity. 3% are not sure what the plan will be.

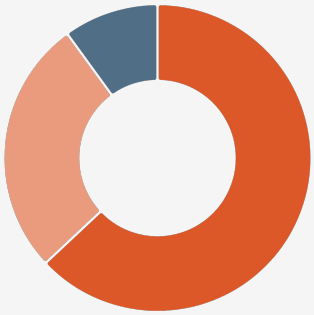


Q. How does your company plan to allocate its cybersecurity budget in the next fiscal year?

Increase budget allocation for cybersecurity	43%
Maintain the current budget allocation for cybersecurity	51%
Decrease budget allocation for cybersecurity	4%
I'm not sure	3%

63% expect their outsourced security budget to increase

63% expect their budget for outsourced security to increase, while 10% expect their budget for outsourced security to decrease. 27% expect no change to their budget.



Q. How do you expect your outsourced security budget to change in the next 12 months?

Increasing budget	63%
No change to budget	27%
Decreasing budget	10%

Summary

As security teams prepare for the next year, their biggest priority is deploying multi-factor authentication across most or all systems, enhancing network security, and strengthening access control policies. It seems that the biggest focus this coming year will be protecting employees and in-house users (MFA, access controls), while also engaging in proactive security against threats (enhancing network security).

This year, 43% that expect their general security budget to increase, which is lower than last year's 50%. However, the 63% who expect their outsourced security budget to increase is much higher than last year's 56% — perhaps signaling an increased awareness of the benefits of outsourcing rather than investing in-house.

Part 5: Executive Takeaways

It's clear that while respondents are actively working to improve their cybersecurity, there's still much to be done to find the right approach to robust security. These three takeaways can help SMB become more proactive and protected in their security stance.

1. Choose the right service provider

Entrusting your security to a third-party provider can be a great strategy, but only if that service provider can effectively protect your organization. There are a number of reasons to outsource security: access to advanced security tools and technologies, cost-effectiveness, and the need for scalability and flexibility to adapt to changing business needs.

As you begin to evaluate outsourced service providers, ask the following questions to be sure you're getting what you need when you need it:

- What third-party technologies are they using, and how up-to-date are their solutions?
- How do they attract, retain, and train top-tier talent?
- How do they utilize threat intelligence, and how reliable are their analytics and threat hunting capabilities?
- Will you have direct platform access and transparency into managed operations delivered on your behalf?
- How do they securely collaborate and communicate with you?

Outsourced security providers can also help guide you through the CMMC compliance process and ensure that your systems are prepared for the unique threats to those serving the DIB.

2. Start with CMMC — then keep going

Any organization contracting with the DoD must meet their robust cybersecurity standards, which is why CMMC compliance isn't just critical to protect an organization, it's necessary for future business. This year, 71% have started the CMMC compliance process, yet 21% are compliant with Level 1, 17% are compliant with Level 2, and 12% are compliant with Level 3.

MSP/MSSP familiarity and competence with CMMC varies. Ensure that if entrusting readiness or required capabilities to an outsource provider, they have the requisite expertise and appropriate certifications (e..g, RPO, CCA). Ideally work with providers who themselves plan to become CMMC compliant.

3. Incorporate threat hunting into your capabilities

Move from reactive to proactive by incorporating threat hunting into your security activities. Respondents reported low to medium effectiveness in threat hunting (57%), threat investigation (56%), and threat monitoring (55%). Yet by training your team on how to use threat intelligence and how to threat hunt, you can increase your awareness of potential attacks.

Instead of waiting for an alert to trigger, threat hunters can recognize the markers of malicious activity and root it out before considerable damage can be done. Threat intelligence provides security teams with the knowledge about tactics, techniques, and procedures (TTPs) of malicious actors intent on targeting their organization so they can take action before an attack.

Conclusion

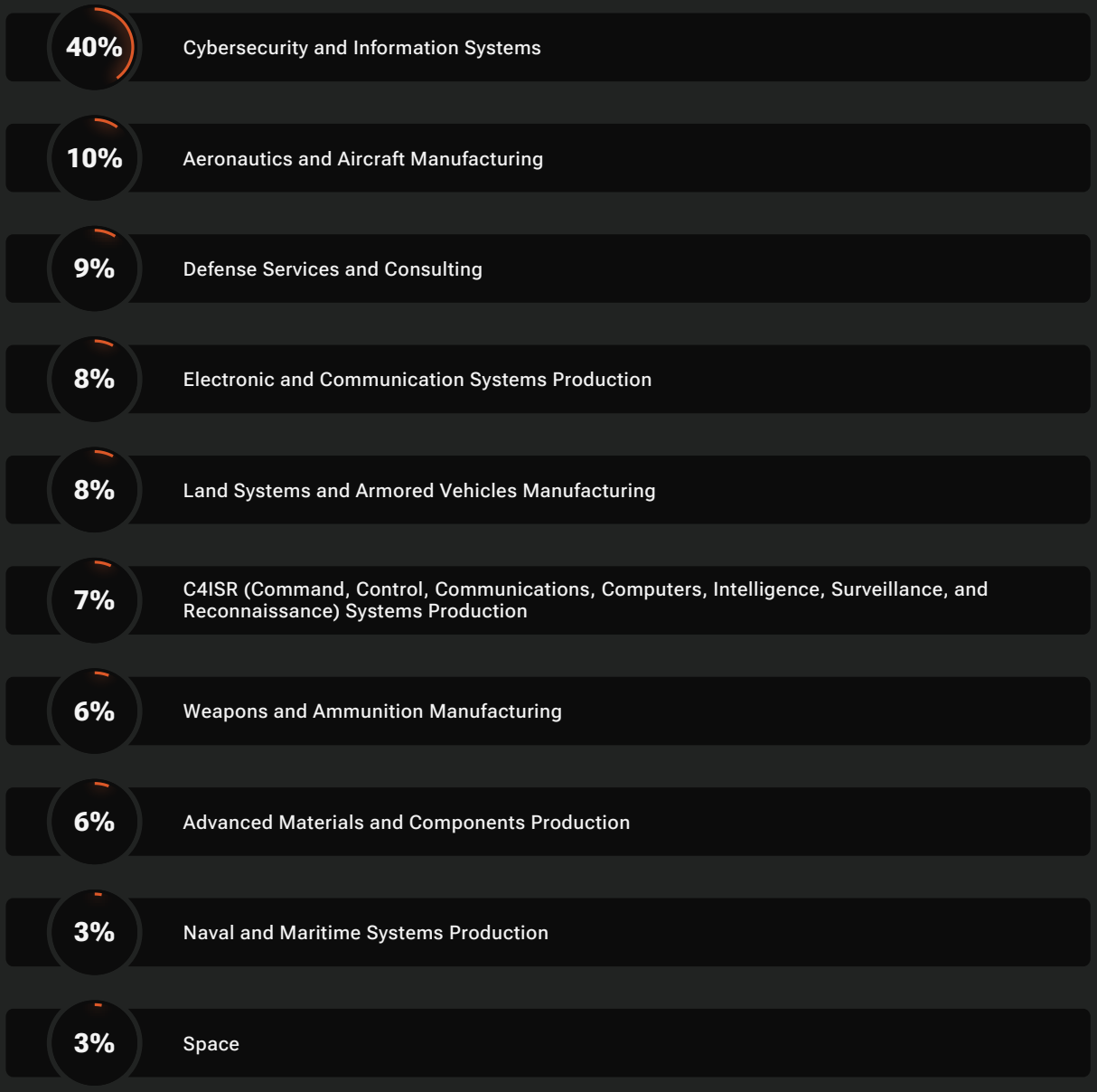
SMBs serving our Defense Industrial Base (DIB) contribute to America's safety and advancement around the globe. Yet as long as nation-states around the world continue to target them, SMBs must take steps to ensure that their security capabilities can protect against infiltration and attack. With the right tools and technologies, they can instead put up a great defense and protect the future of American innovation.

Profile of Who We Surveyed: Methodology and Participant Demographics

In order to provide greater context around these findings, here are more details on who we surveyed and the methodology used. Starting on Apr. 30, 2025, we surveyed 364 IT practitioners at companies where a significant portion of their business comes from defense contracts with government agencies. The survey was conducted online via Pollfish using organic sampling. Learn more about the Pollfish methodology here.

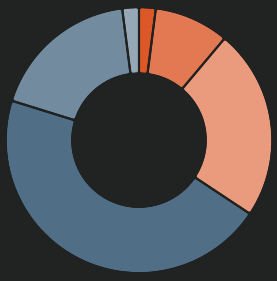
Question 1.

Which category best describes the nature of your business within the Defense Industrial Base?



Question 2.

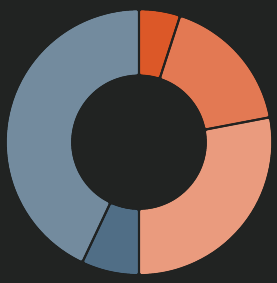
Approximately what percentage of your business is directly related to defense contracts?



Less than 10%	2%	51 - 75%	45%
10 - 25%	9%	76 - 99%	18%
26 - 50%	23%	100%	2%

Question 3.

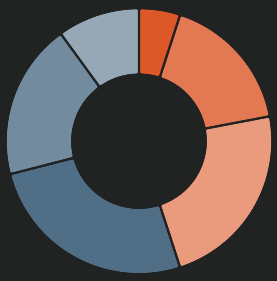
How much total venture funding have you taken?



Less than $10M	5%	More than $51M	7%
$10M - $25M	17%	None	43%
$26M - $50M	28%		

Question 4.

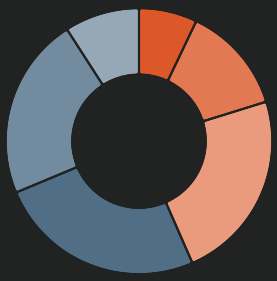
What's your estimated annual revenue for this fiscal year?



Less than $5M	5%	$26M - $50M	26%
$5M - $10M	17%	$51M - $100M	19%
$11M - $25M	23%	$101M+	10%

Question 5.

What's your estimated IT budget for this fiscal year?



Less than $100K	7%	$501K - $1M	25%
$101K - $250K	13%	$1.1M - $2M	22%
$251K - $500K	23%	More than $2.1M	9%

RADICL™

DIB CYBERSECURITY MATURITY REPORT

2025 EDITION