RADICL™

DIB CYBERSECURITY MATURITY REPORT

2024 EDITION

A WORD FROM OUR CEO

There's a lot of innovation to be found in the small and medium-sized businesses (SMBs) serving our Defense Industrial Base (DIB) and U.S. Critical Infrastructure (CI) today. Their inventions, ideas, and technologies support the advanced defense systems that are keeping our nation safe both domestically and around the world.

But who's keeping these vital SMBs safe? Nation states around the world eye these SMBs as easy targets through which to steal confidential data and national secrets. Companies who achieve their Cybersecurity Maturity Model Certification (CMMC) compliance will undoubtedly become a harder target — but that's only the beginning.

The way to protect against these cyber attacks is to establish a reasonable security baseline with CMMC, then go further with a harden-detect-respond mindset and tireless operations to shrink the attack surface, constantly monitor for threats, and be ready to investigate and respond around the clock.

But are SMBs today actively taking these steps? To better understand how SMBs protect themselves, we surveyed 581 IT practitioners at companies with 101 to 250 employees, and for whom a significant portion of their business comes from defense contracts with government agencies. They shared their 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. To help ensure actionable results, we omitted all data from respondents that expressed low confidence in their answers, leaving us with 423 total responses in our results.

We hope these findings will help you understand where the industry currently stands on security, and help benchmark your efforts against your peers.

CHRIS PETERSEN
Co-Founder & CEO, RADICL

KEY FINDINGS

HERE ARE NINE KEY FINDINGS ON THE STATE OF CYBERSECURITY IN SMBs.

1- **61% say cybersecurity is a very high or high priority.**

75% have three or more people dedicating time to security and 67% rate their security skill level as very high or high.

2- **61% report low to medium effectiveness in threat investigation.**

Additionally, 56% report low to medium effectiveness in threat monitoring, and 54% report low to medium effectiveness in threat hunting.

3- **59% would take a week or more to detect a threat in their environment.**

Also, 64% say it would take two days or longer to respond to ransomware or a breach, and 39% would not be surprised to experience a ransomware attack.

4- **46% say cybersecurity-related incidents have cost their company $100,001.**

Of those, 12% report that cost to be more than $500,001.

5- **60% had four or more user accounts or emails compromised in the past year.**

Additionally, 59% had four or more of their endpoints compromised in the past year.

6- **The biggest security challenge is implementing and maintaining compliance with regulations, including CMMC.**

They're also challenged with protecting sensitive data from breaches and leaks and managing a limited budget and resources for comprehensive cybersecurity measures.

7- **The biggest challenge with outsourced providers is inadequate response time to security issues and incidents.**

Other challenges include limited support for compliance management, especially CMMC, and the overall value delivered feels too expensive.

8- **The top capabilities they're looking for in a new service provider include someone with a deep understanding of DIB requirements.**

They're also looking for providers with quality staff and comprehensive services.

9- **81% have started the CMMC compliance process.**

However, only 13% are compliant with Level 1 and 11% are compliant with Level 2.

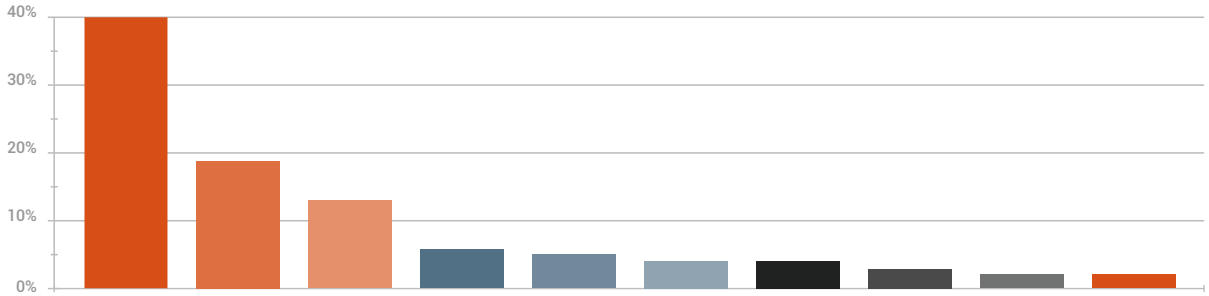
CONTENTS

PROFILE OF WHO WE SURVEYED:

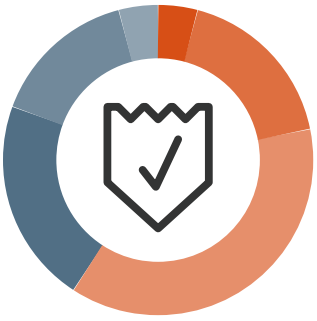
METHODOLOGY AND PARTICIPANT DEMOGRAPHICS

To provide greater context around these findings, here are more details on who we surveyed and the methodology used. Starting on Nov. 1, 2023, we surveyed 581 IT practitioners at companies where a significant portion of their business comes from defense contracts with government agencies. Of those, 158 said they were "uncertain" or "not confident" in their answers to the survey based on their knowledge of the IT environment and present-day security capabilities. Those respondents were removed, leaving 423 respondents.

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



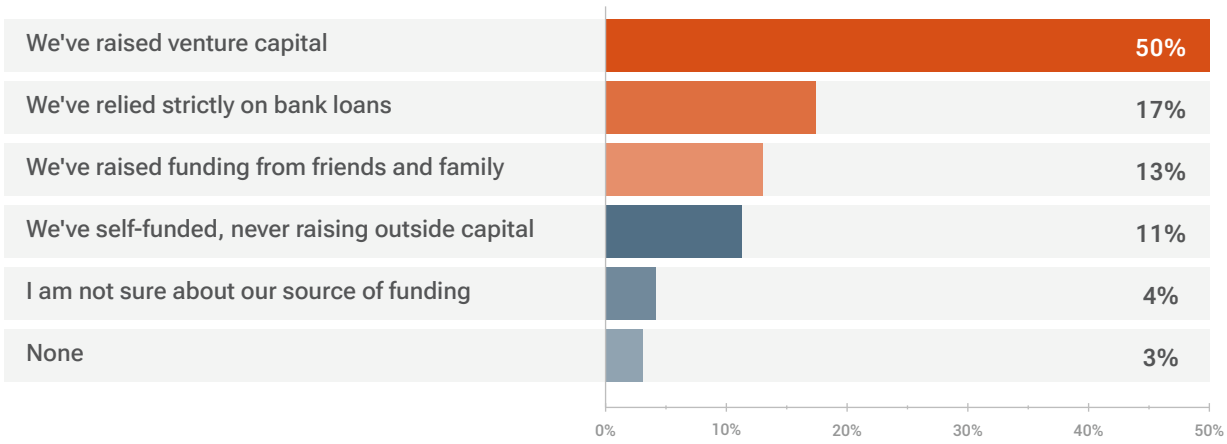
C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) Systems Production	40%
Cybersecurity and Information Systems	19%
Aeronautics and Aircraft Manufacturing	13%
Electronic and Communication Systems Production	6%
Defense Services and Consulting	5%
Naval and Maritime Systems Production	4%
Weapons and Ammunition Manufacturing	4%
Land Systems and Armored Vehicles Manufacturing	3%
Space	2%
Advanced Materials and Components Production	2%



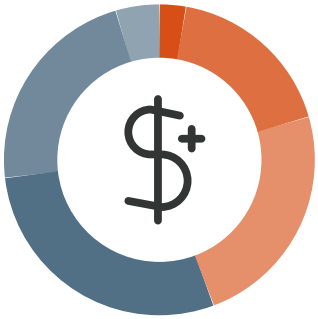
Approximately what percentage of your business is directly related to defense contracts?

Less than 10%	6%	51 to 75%	21%
10 to 25%	18%	76 to 99%	14%
26 to 50%	36%	100%	6%

Which of the following is most accurate when it comes to your source of funding?



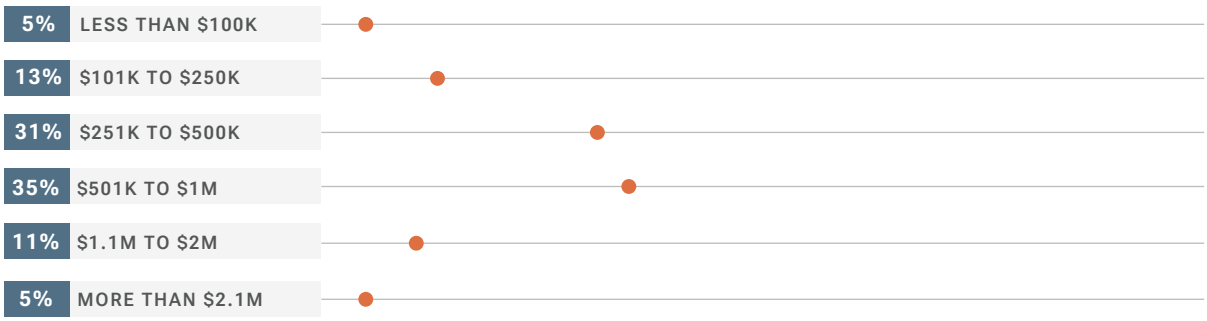
How much total venture funding have you taken?



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

Less than $5M	4%	$26M to $50M	27%
$5M to $10M	17%	$51M to $100M	20%
$11M to $25M	25%	More than $101M	6%

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



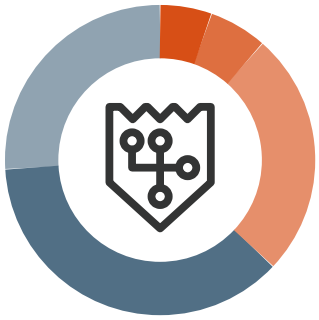
PART #1

CURRENT CYBERSECURITY PROGRAM

SMBs that are part of the DIB contribute crucial technology that helps defend our nation and empower defense programs around the world. Yet how are they doing at defending themselves? In this section, our respondents give us insights into the current state of their cybersecurity programs and their biggest challenges.

61% SAY CYBERSECURITY IS A VERY HIGH OR HIGH PRIORITY

Enhancing cybersecurity measures over the next year is a major priority, with 25% saying it's a very high priority and 36% saying it's a high priority. 23% say it's a medium priority, with only 9% saying it's low and 7% saying it's very low.



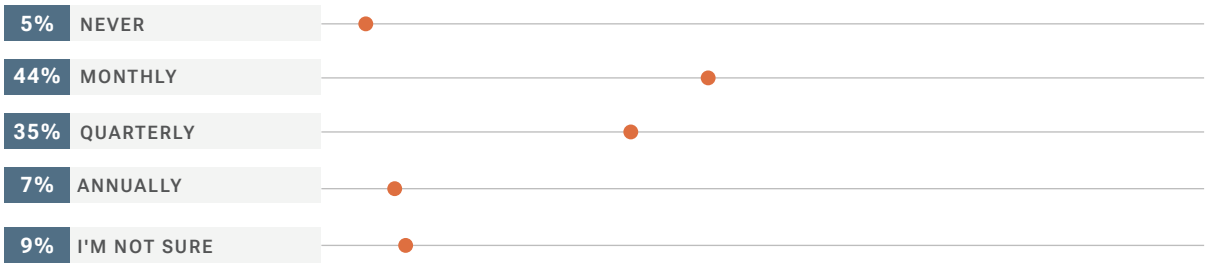
How would you rank the priority of enhancing your organization's cybersecurity measures over the next 12 months?

1 - Very Low	7%	4 - High	37%
2 - Low	9%	5 - Very High	25%
3 - Medium	23%		

44% MEET MONTHLY TO DISCUSS CYBERSECURITY

44% say their leadership team meets to discuss security monthly, while 35% convene quarterly to discuss cybersecurity. 7% meet annually, while 5% never meet. 9% weren't sure about the frequency.

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



75% HAVE THREE OR MORE PEOPLE DEDICATING TIME TO SECURITY

38% have four or more people who spend at least a quarter of their time on security, while 37% have three people who do. 12% have two people who spend at least a quarter of their time on security, 6% have one person, and only 7% don't have anyone.

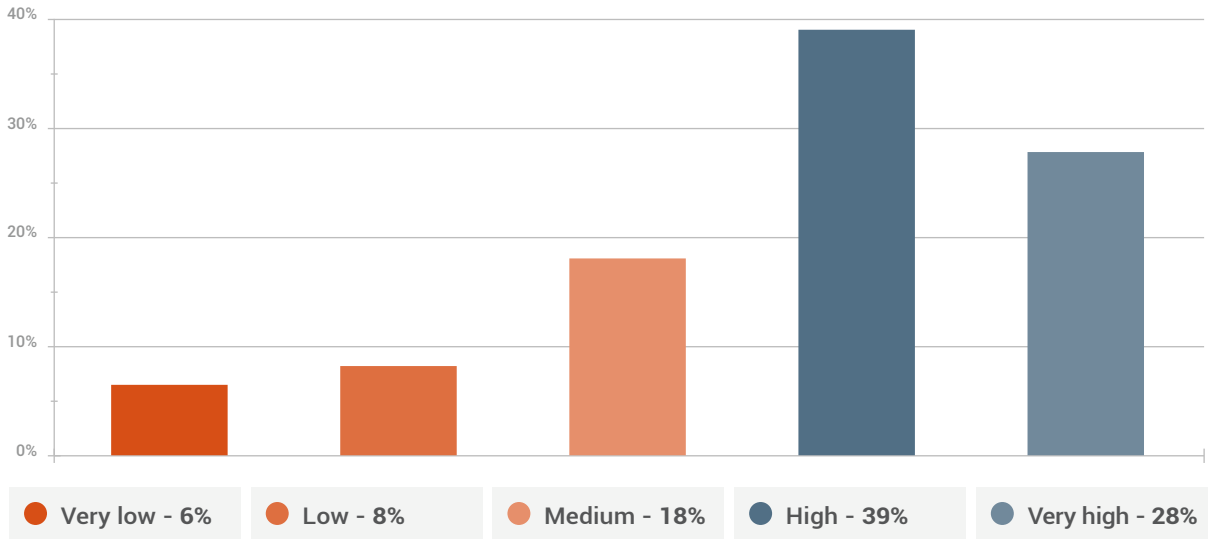
How many people on your team spend more than 25% of their time on security?

0	7%	3	37%
1	6%	4+	38%
2	12%		

67% RATE THEIR SECURITY SKILL LEVEL AS VERY HIGH OR HIGH

When rating the skill level of their in-house security team, 28% rate them very high, while 39% rate their skill level as high. 18% rate their security team skill level as medium, 8% rate them low, and only 6% rate them very low.

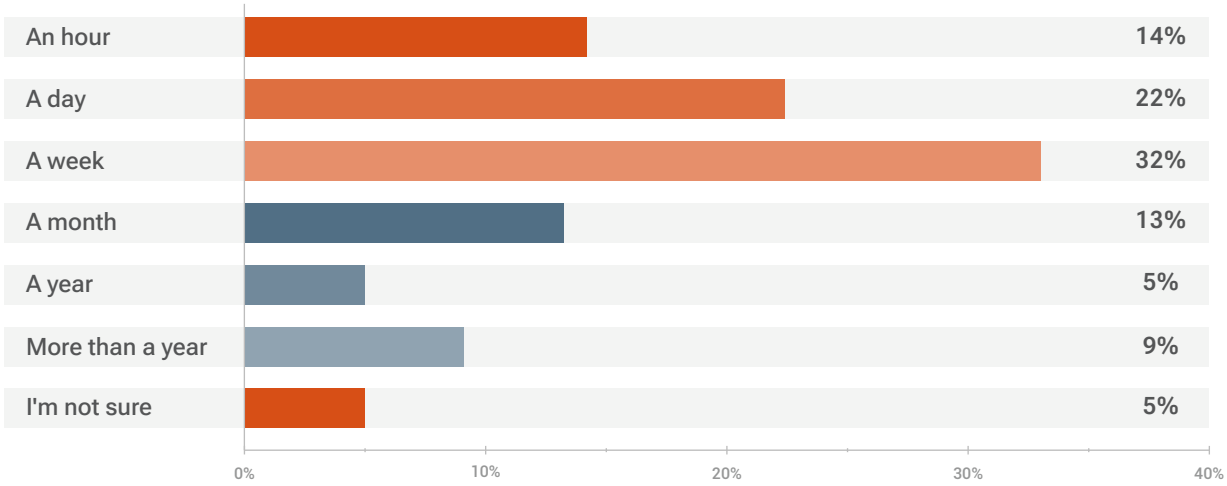
Which category best describes the nature of your business within the Defense Industrial Base?



59% WOULD TAKE A WEEK OR MORE TO DETECT A THREAT IN THEIR ENVIRONMENT

How quickly would respondents be able to detect a threat that bypassed their defenses and was operating from within their IT environment? 14% would detect it in an hour, and 22% would detect it within a day. For 32%, it would take a week, and for 13%, it would take a month. 5% would detect it in a year and 9% would detect it in more than a year. Finally, 5% aren't sure how much time it would take.

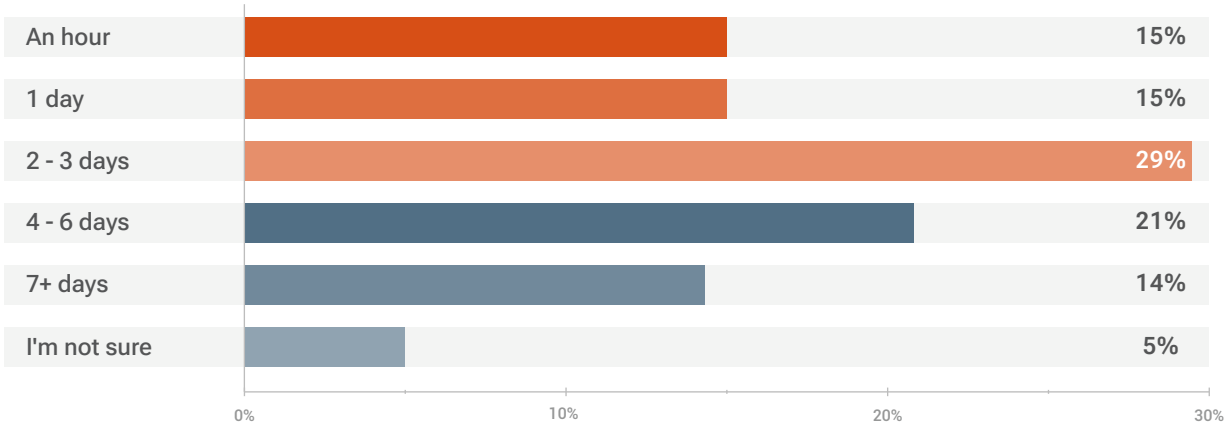
If a threat bypassed your defense and was operating from within your IT environment, how quickly would you be able to detect its presence?



64% 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 15%, it would take an hour, and for another 15%, it would take a day. 29% say it would take two to three days, and 21% say it would take four to six days. For 14%, it would take a week or more. Finally, 5% weren't sure how long it would take.

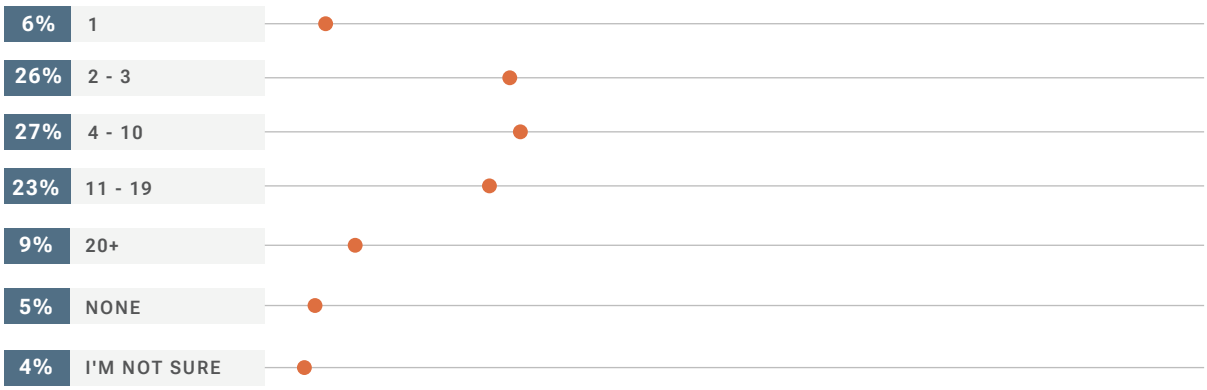
If you had a ransomware or data breach incident, how quickly would you be able to conduct a full investigation and develop a comprehensive incident response plan?



59% HAD FOUR OR MORE OF THEIR ENDPOINTS COMPROMISED IN THE PAST YEAR

Only 5% say none of their endpoints have had a virus or malware compromise in the past 12 months. 6% have had one endpoint compromised, 26% have had two to three, and 27% have had four to 10. 23% say they've had 11 to 19, and 9% have had 20 or more. Finally, 4% aren't sure how many compromises they've had.

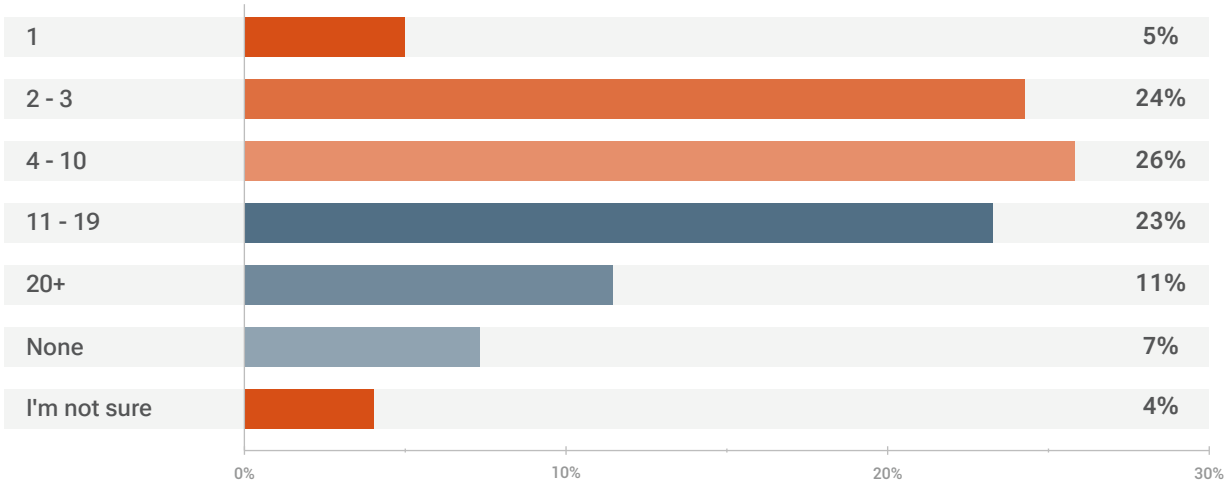
How many of your organization's endpoints have had a virus or malware compromise in the past 12 months?



60% HAD FOUR OR MORE USER ACCOUNTS OR EMAILS COMPROMISED IN THE PAST YEAR

Only 7% say none of their user accounts or email addresses have been compromised in the past 12 months. 5% have had one account compromised, 24% have had two to three, and 26% have had four to ten. 23% say they've had eleven to nineteen, and 11% have had twenty or more. Finally, 4% aren't sure how many compromises they've had.

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



39% WOULD NOT BE SURPRISED TO EXPERIENCE A RANSOMWARE ATTACK

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:

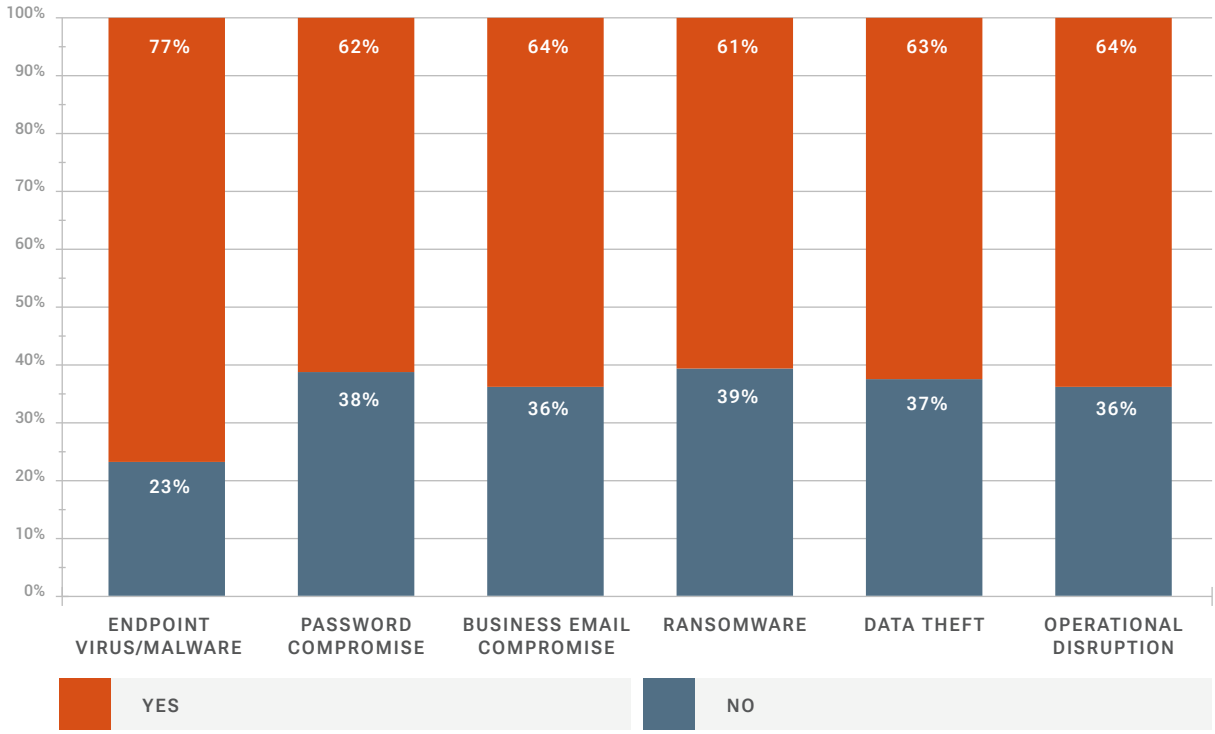
- RANSOMWARE (39%)
- PASSWORD COMPROMISE (38%)
- DATA THEFT (37%)
- OPERATIONAL DISRUPTION (36% TIE)
- BUSINESS EMAIL COMPROMISE (36% TIE)
- ENDPOINT VIRUS/MALWARE (23%)

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:

- ENDPOINT VIRUS/MALWARE (77%)
- OPERATIONAL DISRUPTION (64% TIE)
- BUSINESS EMAIL COMPROMISE (64% TIE)
- DATA THEFT (63%)
- PASSWORD COMPROMISE (62%)
- RANSOMWARE (61%)

Overall, respondents say they lack the capabilities to protect against ransomware, password compromise, and data theft, while they have the capabilities to protect against endpoint viruses or malware, operational disruption, and business email compromise.

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

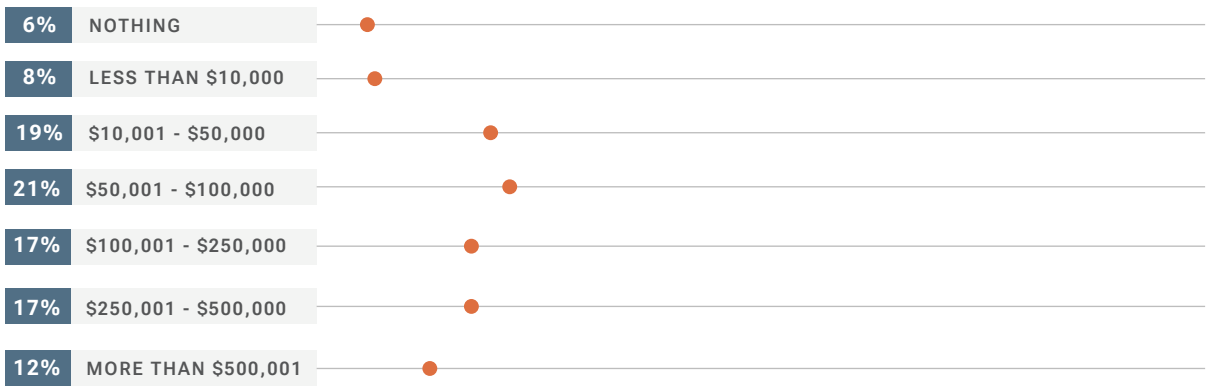


NEARLY HALF SAY CYBERSECURITY-RELATED INCIDENTS HAVE COST THEIR COMPANY $100K OR MORE

In economic terms, how much have cybersecurity-related incidents cost in lost time, productivity, or cash? For 6%, it was nothing. However, 8% say it was less than $10,000; 19% say $10,001 to $50,000; 21% say $50,001 to $100,000; 17% say $100,001 to $250,000; 17% say $250,001 to $500,000; and 12% say more than $500,001.

Overall, 46% have experienced costs of $100,001 or more in cybersecurity-related incidents.

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



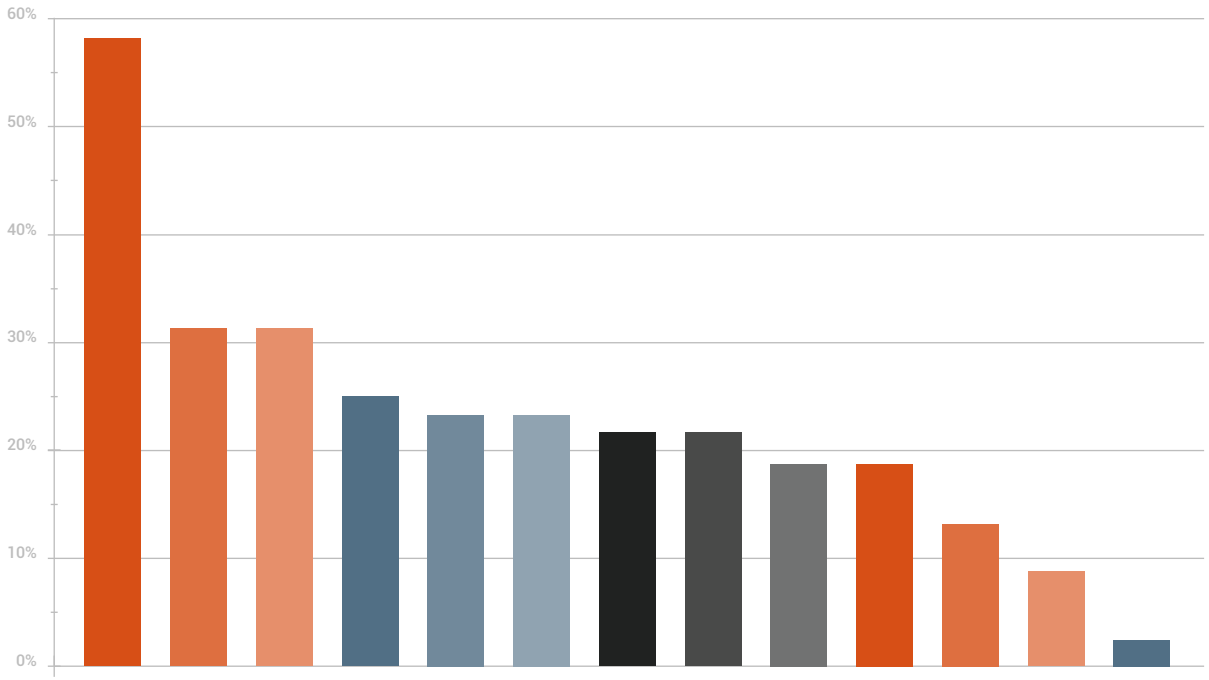
TOP SIX CHALLENGES TO CYBERSECURITY

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

58%	**IMPLEMENTING AND MAINTAINING COMPLIANCE WITH REGULATIONS, INCLUDING CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)** Over half are struggling with implementing their CMMC compliance to meet the requirements for government contractors.
31%	**PROTECTING SENSITIVE DATA FROM BREACHES AND LEAKS** They're challenged with creating efficient methods and taking action to protect against data breaches overall.
31%	**MANAGING A LIMITED BUDGET AND RESOURCES FOR COMPREHENSIVE CYBERSECURITY MEASURES** They also struggle to build a robust, effective cybersecurity program on limited budgets or resources.
25%	**KEEPING UP WITH EVOLVING CYBERTHREAT LANDSCAPES** Another challenge is staying one step ahead of malicious actors through proactive threat hunting and intelligence.
24%	**EDUCATING AND TRAINING EMPLOYEES ON SECURITY BEST PRACTICES** Increasing internal security knowledge and awareness so they have internal expertise is also a challenge.
24%	**MANAGING THIRD-PARTY OR VENDOR SECURITY RISKS** Not only do they need to manage their own risk, but they struggle to manage the risk of third parties or vendors as well.

Other challenges include recruiting and retaining skilled cybersecurity personnel (22% tie), developing a cohesive and integrated cybersecurity strategy (22% tie), ensuring business continuity and disaster recovery planning (19% tie), balancing security needs with operational efficiency (19% tie), implementing robust access control and identity management systems (13%), staying updated with the latest security technologies and tools (9%), or other challenges (2%).

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



Implementing and maintaining compliance with regulations, including Cybersecurity Maturity Model Certification (CMMC)	58%
Protecting sensitive data from breaches and leaks	31%
Managing a limited budget and resources for comprehensive cybersecurity measures	31%
Keeping up with evolving cyber threat landscapes	25%
Educating and training employees on security best practices	24%
Managing third-party/vendor security risks	24%
Recruiting and retaining skilled cybersecurity personnel	22%
Developing a cohesive and integrated cybersecurity strategy	22%
Ensuring business continuity and disaster recovery planning	19%
Balancing security needs with operational efficiency	19%
Implementing robust access control and identity management systems	13%
Staying updated with the latest security technologies and tools	9%
Other	2%

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, here are what respondents are doing today:

TOP 3 AREAS: MANAGED IN-HOUSE

1. LOG ANALYSIS (39%)
2. VULNERABILITY MANAGEMENT (29% TIE)
3. INCIDENT RESPONSE (29% TIE)

They also manage security awareness training (27% tie), threat investigation (27% tie), threat hunting (24%), and threat monitoring (23%).

TOP 3 AREAS: MANAGED BY OUTSOURCED SECURITY PROVIDER

1. THREAT MONITORING (39% TIE)
2. SECURITY AWARENESS TRAINING (39% TIE)
3. THREAT INVESTIGATION (36%)

They also outsource threat hunting (34%), incident response (33%), log analysis (31% tie), and vulnerability management (31% tie).

TOP 3 AREAS: COMBINATION OF IN-HOUSE AND OUTSOURCED

1. THREAT HUNTING (33%)
2. VULNERABILITY MANAGEMENT (32%)
3. THREAT MONITORING (29%)

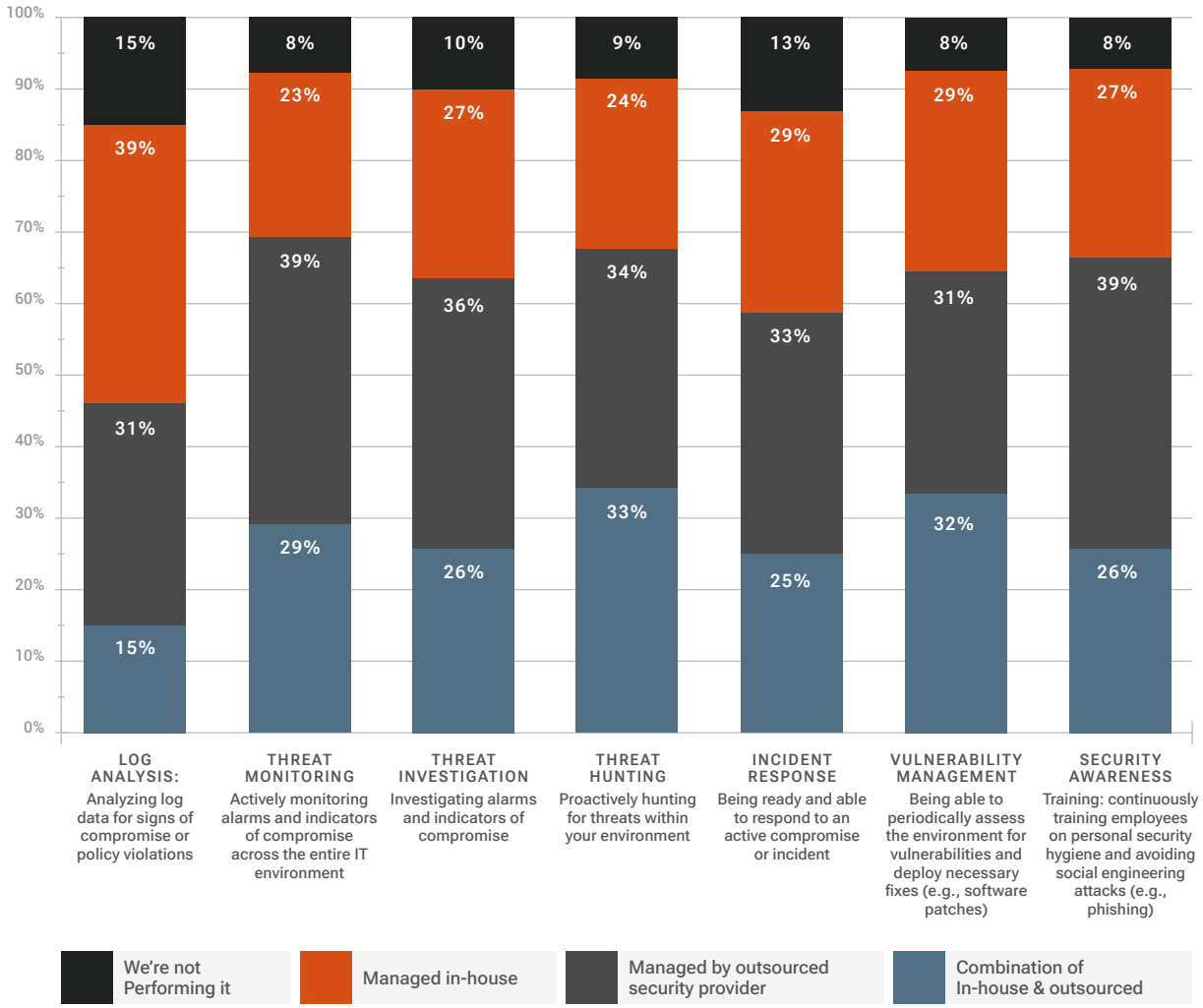
They also do a combination of threat investigation (26% tie), security awareness training (26% tie), incident response (25%), and log analysis (15%).

TOP 3 AREAS: WE'RE NOT PERFORMING IT

1. LOG ANALYSIS (15%)
2. INCIDENT RESPONSE (13%)
3. THREAT INVESTIGATION (10%)

They're also not performing threat hunting (9%), threat monitoring (8% tie), vulnerability management (8% tie), and security awareness training (8% tie).

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:

TOP 4 AREAS: HIGH EFFECTIVENESS

1. THREAT HUNTING (37%)
2. INCIDENT RESPONSE (35%)
3. VULNERABILITY MANAGEMENT (33% TIE)
4. THREAT MONITORING (33% TIE)

Other areas of high effectiveness include security awareness training (31% tie), threat investigation (31% tie), and log analysis (25%).

TOP 4 AREAS: MEDIUM EFFECTIVENESS

1. Threat Investigation (41%)
2. Security Awareness Training (40%)
3. Log Analysis (36% tie)
4. Threat Hunting (36% tie)

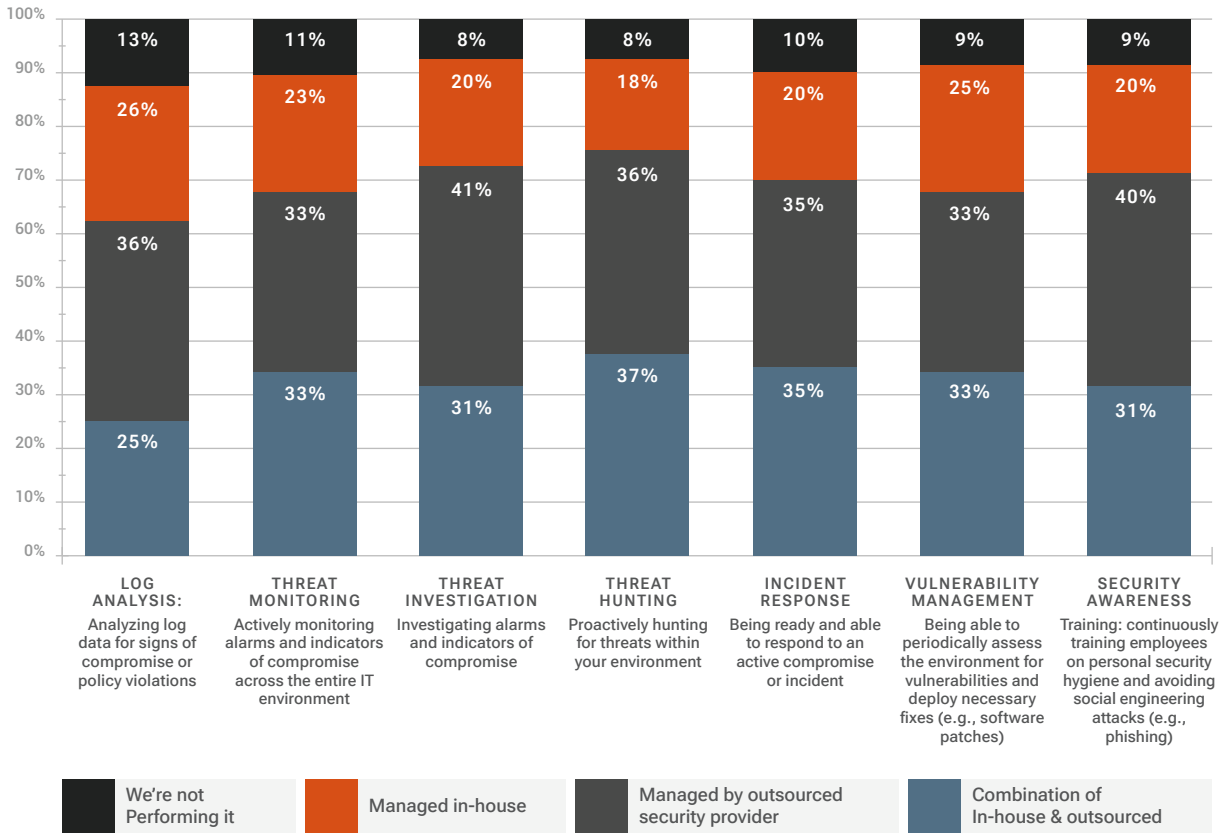
Other areas of medium effectiveness include incident response (35%), threat monitoring (33% tie), and vulnerability management (33% tie).

TOP 3 AREAS: LOW EFFECTIVENESS

1. Log Analysis (26%)
2. Vulnerability Management (25%)
3. Threat Monitoring (23%)

Other areas of low effectiveness include incident response (20% tie), threat investigation (20% tie), security awareness training (20% tie), and threat hunting (18%).

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. Many are managing security function in-house, outsourcing them, or doing a combination of both:

- 61% say cybersecurity is a very high or high priority.
- 75% have three or more people dedicating time to security.
- 67% rate their security skill level as very high or high.
- 44% say leadership meets monthly to discuss cybersecurity.

- **SPEED MATTERS IN MATTERS OF DETECTION, INCIDENT RESPONSE, AND COMPROMISES.**

  There's still progress to be made with speeding up detection and incident response, and reducing compromise. It would take 59% a week or more to detect a threat in their environment, and it would take 64% two days or longer to respond to ransomware or a breach. 59% have had a compromise in four or more of their endpoints in the past year, and 60% have had a compromise in four or more user accounts or emails in the past year.

- **CYBERSECURITY IS HARD. SMBs NEED HELP. THEY'RE STRUGGLING WHEN MANAGING CYBERSECURITY SOLELY IN HOUSE AND ONLY REPORT HIGH CONFIDENCE WHEN SHARING THE WORK WITH OUTSOURCED PARTNERS.**

  They're finding "high effectiveness" in managing threat hunting, incident response, vulnerability management, and threat monitoring. Respondents reporting high effectiveness also report mostly using a combination of in-house and outsourced functions, while respondents reporting low effectiveness report mostly managing functions in-house.

- **FACING DAUNTING CHALLENGES THAT INCLUDE CMMC, BREACHES, BUDGETS and LOSSES**

  The biggest challenges they face today include implementing and maintaining compliance with regulations, including CMMC; protecting sensitive data from breaches and leaks; and managing a limited budget and resources for comprehensive cybersecurity measures. Nearly half (46%) say cybersecurity-related incidents have cost their company $100,001 or more.

- **LITTLE TO NO CORRELATION BETWEEN CYBERSECURITY HYGIENE PRIORITIES AND CYBERSECURITY EFFECTIVENESS**

  In analyzing the four questions about response — time to detect, incident response to a data breach, endpoint compromise, and user account compromise — there's no direct correlation between organizations who "do or have X" and who see faster response and fewer compromises. For example:

IT BUDGET

- **$2.1M+ IT budget:** detect in a month; incident response in 1 day; 4-10 endpoints compromised; 20+ accounts compromised (largest segments counted)
- **<$100k IT budget:** detect in a week; incident response in 1 day; 2-3 endpoints compromised, tied with 0 endpoints compromised; 11-19 accounts compromised (largest segments counted)

PRIORITY OF CYBERSECURITY

- **Very high:** detect in a day; incident response in an hour; 2-3 endpoints compromised; 2-3 accounts compromised (largest segments counted)
- **Very low:** detect in an hour; incident response in an hour; 1 endpoint compromised; 11-19 accounts compromised (largest segments counted)

PEOPLE DEDICATING TIME TO SECURITY:

- **4 or more people:** detect in a day; incident response in 2-3 days; 11-19 endpoints compromised; 11-19 accounts compromised (largest segments counted)
- **None or one person:** detect in more than a year; incident response in 4-6 days; 2-3 endpoints compromised; 11-19 accounts compromised (largest segments counted)

SKILL OF IN-HOUSE TEAM:

- **Low skill:** detect in an hour; incident response in an hour; 4-10 endpoints compromised; no accounts compromised (largest segments counted)
- **High skill:** detect in a day; incident response in an hour; 2-3 endpoints compromised; 2-3 accounts compromised (largest segments counted)

WHEN LEADERSHIP MEETS:

- **Monthly:** detect in a day; incident response in 2-3 days; 2-3 endpoints compromised; 2-3 accounts compromised (largest segments counted)
- **Annually:** detect in a week; incident response in 4-6 days; 4-10 endpoints compromised; 4-10 accounts compromised (largest segments counted)

While there do seem to be benefits to having more people dedicating time to security (faster time to detect, faster incident response) and having leadership meet more frequently (faster time to detection, faster incident response, fewer compromises), there are no strong correlations to what leads to better security.

Ultimately, the answer to "what leads to better security" is likely the quality of tools and technology deployed, combined with the expertise to drive those tools and technology effectively. Regardless of budget, priority, people, skills, or meetings, if you have the right combination of security tools and technology and those with expertise to use them, you'll be secure. If you don't, you won't.

PART #2

OUTSOURCEED SERVICE PROVIDERS

For the majority of respondents, their approach to security includes outsourcing various functions to third-party service providers. But are those service providers meeting their security needs, or are SMBs left just as challenged and vulnerable as before? Here are some insights into their experiences and why many seek new providers in 2024.

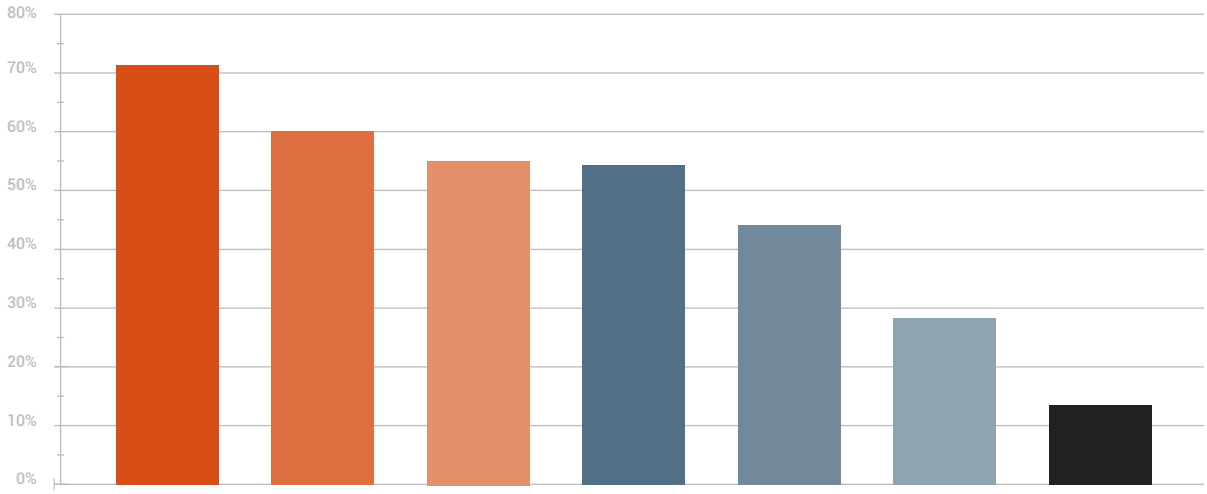
TOP THREE OUTSOURCED IT OR SECURITY PARTNERS

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

71%	MANAGED SECURITY SERVICE PROVIDER (MSSP) MSSPs provide network cybersecurity and monitoring.
60%	MANAGED DETECTION AND RESPONSE (MDR) MDRs perform threat hunting and incident response.
55%	MANAGED SERVICE PROVIDER (MSP) MSPs provide broader IT operational services.

They're also using a value-added reseller (VAR) (53%), a cybersecurity consultant (44%), a compliance consultant (28%), or another option (12%).

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

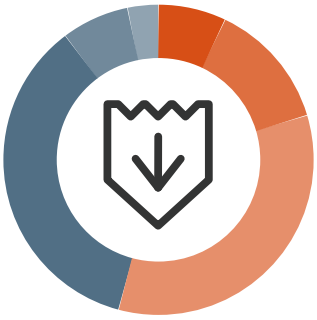


Managed Security Service Provider (MSSP)	71%
Managed Detection and Response (MDR)	60%
Managed Service Provider (MSP)	55%
Value Added Reseller (VAR)	53%
Cybersecurity Consultant	44%
Compliance Consultant	28%
Other	12%

77% SPEND $50,001 OR MORE ANNUALLY ON OUTSOURCED SECURITY

7% spend less than $20,000 annually on outsourced security; 13% spend $20,001 to $50,000; 34% spend $50,001 to $100,000; 34% spend $100,001 to $250,000; and 9% spend more than $250,001. Finally, 3% don't spend any, as they don't outsource security.

Overall, 77% spend $50,001 or more annually on outsourced security.



How much do you spend annually on outsourced security?

Less than $20,000	7%	$100,001 to $250,000	34%
$20,001 to $50,000	13%	More than $250,001	9%
$50,001 to $100,000	34%	Nothing	3%

TOP REASONS TO OUTSOURCE

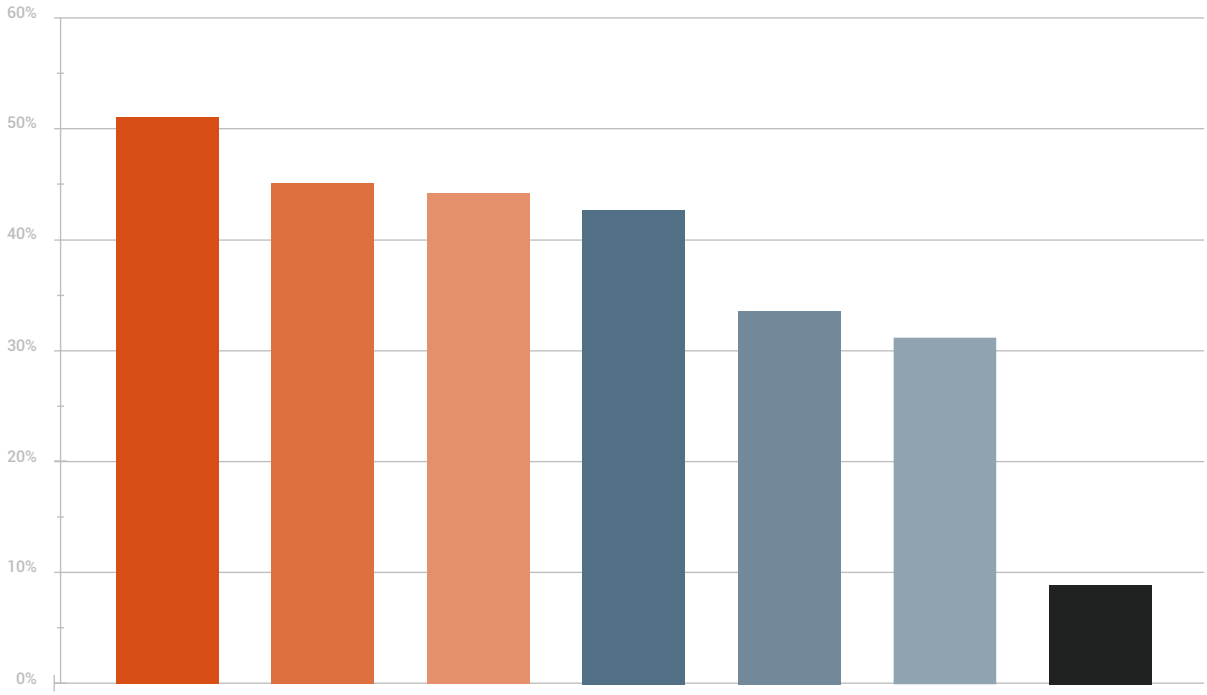
These were the primary factors that influenced the decision to outsource security operations functions to an outsourced provider:

51%	COST-EFFECTIVENESS COMPARED TO BUILDING AND MAINTAINING AN IN-HOUSE TEAM Considering one of the top challenges was limited budget and resources, respondents turn to outsourced providers to help save costs.
45%	SCALABILITY AND FLEXIBILITY TO ADAPT TO CHANGING BUSINESS NEEDS They see outsourced providers as being more scalable and flexible than an internal team, perhaps alleviating the resources needed to constantly "stay ahead" — another challenge listed above.
44%	ACCESS TO SPECIALIZED EXPERTISE AND TECHNICAL SKILLS If they don't have a robust internal cybersecurity team, they turn to outsourced providers as the experts.
42%	IMPROVED SECURITY POSTURE WITH ACCESS TO ADVANCED SECURITY TOOLS AND TECHNOLOGIES Another reason to outsource is because they see service providers as having state-of-the-art tools and technologies that they might not be able to purchase for in-house teams.

34%	**ABILITY TO FOCUS INTERNAL RESOURCES ON CORE BUSINESS FUNCTIONS** They also decide to outsource so they essentially "set it and forget it" and can focus resources on other business areas.

Other reasons include support in complying with industry regulations and standards, including CMMC (31%), and enhanced incident response capabilities with round-the-clock monitoring (9%).

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



Cost-effectiveness compared to building and maintaining an in-house team	51%
Scalability and flexibility to adapt to changing business needs	45%
Access to specialized expertise and technical skills	44%
Improved security posture with access to advanced security tools and technologies	42%
Ability to focus internal resources on core business functions	34%
Support in complying with industry regulations and standards, including CMMC	31%
Enhanced incident response capabilities with round-the-clock monitoring	9%

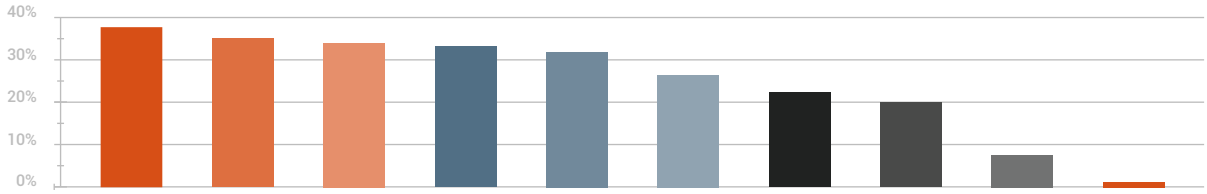
TOP OUTSOURCED PROVIDER CHALLENGES

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

37%	**INADEQUATE RESPONSE TIME TO SECURITY ISSUES AND INCIDENTS** When it comes to security, seconds make a difference — yet outsourced service providers aren't responding fast enough.
35%	**LIMITED SUPPORT FOR COMPLIANCE MANAGEMENT, ESPECIALLY CMMC** The biggest challenge above is implementing and maintaining compliance with CMMC, something they find their providers cannot do.
34%	**FEELS TOO EXPENSIVE GIVEN THE OVERALL VALUE DELIVERED** They turn to service providers to save costs, yet ultimately don't feel like they're getting value in return.
33%	**LACK OF TECHNICAL EXPERTISE OR SPECIALIZATION** They also turn to service providers for their expertise, yet find that they don't have the knowledge they say they do.
32%	**INCONSISTENT QUALITY OF SERVICE** They've experienced that service providers are inconsistent in the overall quality of their work.

Other challenges include ineffective workflow and collaboration between the provider and internal staff (26%), not using the latest and greatest cybersecurity technologies to protect them (22%), lack of transparency on the work they are performing on the respondent's behalf (20%), or none of the above (1%). Only 8% say they have no challenges with their current outsourced security provider.

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



Inadequate response time to security issues and incidents	37%
Limited support for compliance management, especially CMMC	35%
Feels too expensive given the overall value delivered	34%
Lack of technical expertise or specializatio	33%
Inconsistent quality of service	32%
Ineffective workflow and collaboration between the provider and internal staff	26%
Not using the latest and greatest cybersecurity technologies to protect us	22%
Lack of transparency on the work they are performing on the respondent's behalf	20%
I have no challenges with my current outsourced security provider	8%
None of the above	1%

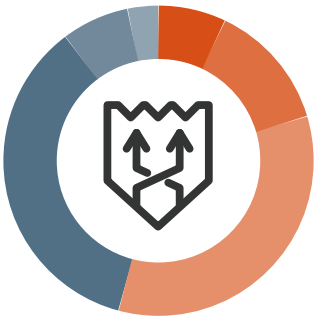
82% WILL CHANGE THEIR OUTSOURCED SECURITY PROVIDER

Eight out of ten (82%) plan to change their outsourced security provider in the next year. 18% will not.

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

46% PLAN TO COMBINE IN-HOUSE AND OUTSOURCED CAPABILITIES

For those who will make changes, 23% plan to bring security in-house, 31% will find a new outsourced provider, and 46% will do a combination of both.



What best describes what you will do to replace them?

Bring security in-house	23%
Find a new outsourced provider	31%
Both the above	41%

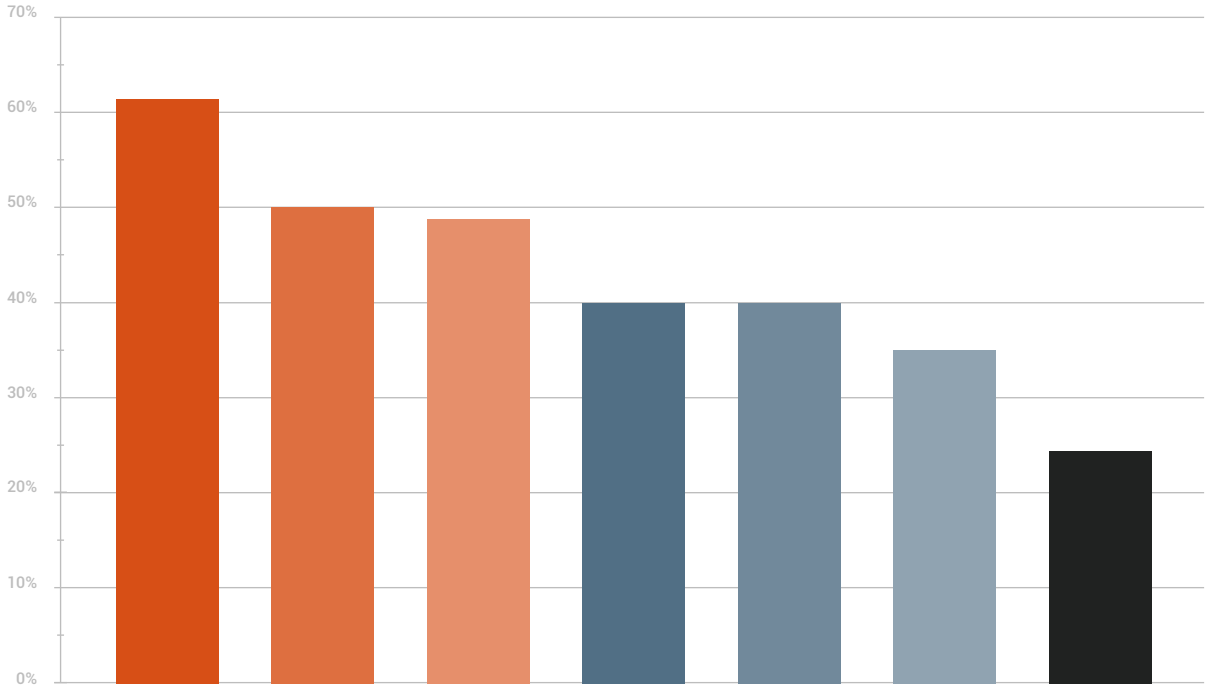
TOP SERVICE PROVIDER CAPABILITIES FOR THOSE LOOKING TO SWITCH

For those wanting to find a new service provider, the qualities and capabilities most important when evaluating a new outsourced security provider include (they chose all that applied):

61%	**DEEP UNDERSTANDING OF DIB REQUIREMENTS** They're looking for a service provider with expert knowledge in meeting the specific security standards of the Defense Industrial Base.
50%	**QUALITY STAFF** Quality of the provider's staff in terms of cybersecurity expertise and overall customer experience — especially when one of the challenges was lack of expertise.
49%	**COMPREHENSIVE SERVICES** They're also looking for comprehensive services, and to receive a lot of cybersecurity coverage and capabilities from a single provider.
40%	**RESPONSIVE INCIDENT MANAGEMENT** Considering the top challenge with providers was slow response time, they're looking for swift, coordinated responses to security incidents to minimize potential damage.
40%	**ADVANCED TECHNOLOGY** They want a provider to utilize the latest technologies to offer robust protection against evolving threats.
35%	**TRANSPARENT OPERATIONS** They want clear, open channels of communication with transparent visibility into work being done on their behalf.
24%	**COMPLIANCE AND CERTIFICATION SUPPORT** They're also looking for guided assistance in achieving and maintaining compliance standards, including CMMC certification.

Other challenges include recruiting and retaining skilled cybersecurity personnel (22% tie), developing a cohesive and integrated cybersecurity strategy (22% tie), ensuring business continuity and disaster recovery planning (19% tie), balancing security needs with operational efficiency (19% tie), implementing robust access control and identity management systems (13%), staying updated with the latest security technologies and tools (9%), or other challenges (2%).

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



Deep understanding of DIB requirements	61%
Quality staff	50%
Comprehensive services	49%
Responsive incident management	40%
Advanced technology	40%
Transparent Operations	35%
Compliance and Certification Support	24%

42% OF THOSE WHO DO NOT OUTSOURCE PLAN TO IN THE NEXT YEAR

For those who replied above that they don't outsource security, 42% do plan to outsource security in the next 12 months, while 58% will not.

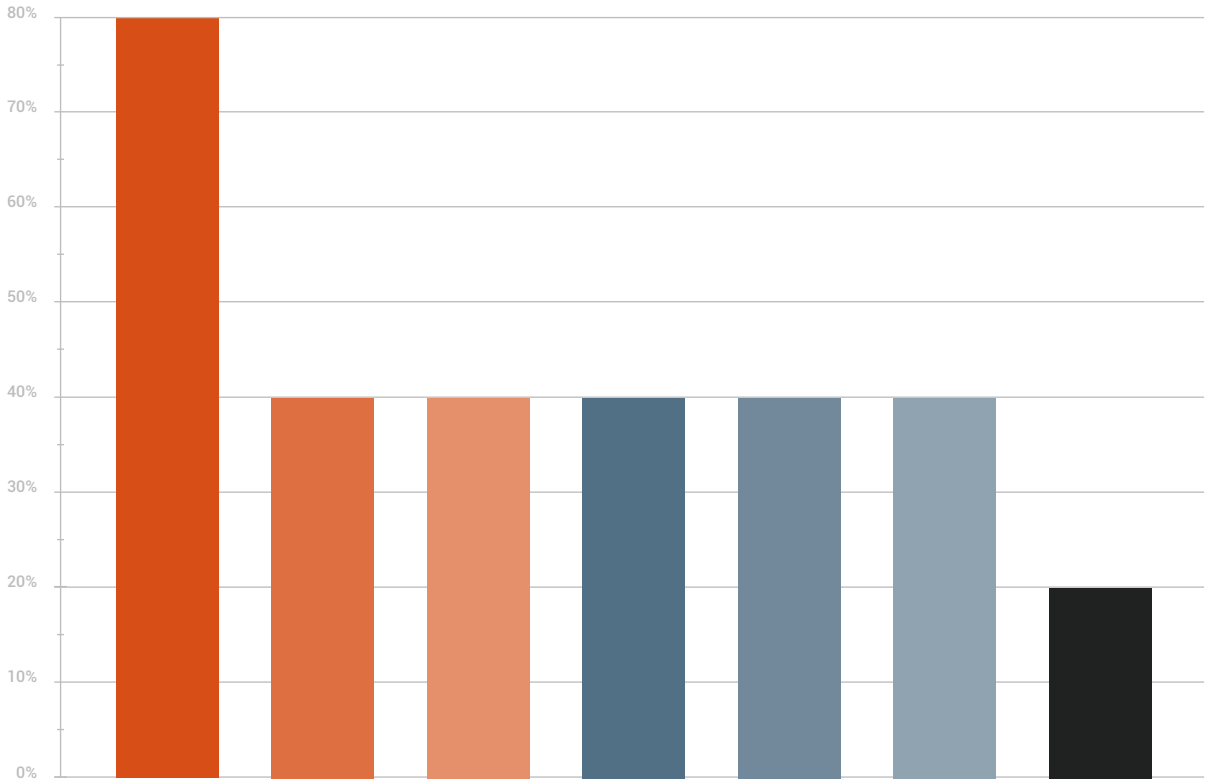
Do you plan to outsource security in the next 12 months?

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):

80%	**DEEP UNDERSTANDING OF DIB REQUIREMENTS** They're looking for a service provider with expert knowledge in meeting the specific security standards of the Defense Industrial Base.
40%	**QUALITY STAFF** Quality of the provider's staff in terms of cybersecurity expertise and overall customer experience — especially when one of the challenges was lack of expertise.
40%	**COMPREHENSIVE SERVICES** They're also looking for comprehensive services, and to receive a lot of cybersecurity coverage and capabilities from a single provider.
40%	**RESPONSIVE INCIDENT MANAGEMENT** Considering the top challenge with providers was slow response time, they're looking for swift, coordinated responses to security incidents to minimize potential damage.
40%	**TRANSPARENT OPERATIONS** They want clear, open channels of communication with transparent visibility into work being done on their behalf.
40%	**COMPLIANCE AND CERTIFICATION SUPPORT** They're also seeking guided assistance in achieving and maintaining compliance standards, including CMMC certification.
20%	**ADVANCED TECHNOLOGY** They want a provider to utilize the latest technologies to offer robust protection against evolving threats.

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



Deep Understanding of DIB Requirements: Expert knowledge in meeting the specific security standards of the Defense Industrial Base	80%
Quality of the providers staff in terms of cybersecurity expertise and overall customer experience	40%
Offering Comprehensiveness: receiving a lot of cybersecurity coverage and capabilities from a single provider	40%
Responsive Incident Management: Swift, coordinated responses to security incidents to minimize potential damage.	40%
Transparent Operations: Clear, open channels of communication with transparent visibility into work being done our behalf.	40%
Compliance and Certification Support: Guided assistance in achieving and maintaining compliance standards, including CMMC certification	40%
Advanced Technology: Utilization of the latest technologies to offer robust protection against evolving threats.	20%

SUMMARY

As we saw in Part 1, our respondents are managing their cybersecurity functions with both in-house staff as well as outsourcing to third-party providers. In this section, we learned the types of third-party service providers they use are Managed Security Service Providers (MSSP), Managed Detection and Response (MDR), and Managed Service Providers (MSP). 77% are spending $50,001 or more annually on outsourced security

- **REASONS FOR OUTSOURCING:**

  The top reasons they're outsourcing include cost-effectiveness compared to building and maintaining an in-house team; scalability and flexibility to adapt to changing business needs; and access to specialized expertise and technical skills.

- **OUTSOURCING CHALLENGES:**

  However, they're encountering many challenges with their outsourced providers, including inadequate response time to security issues and incidents; limited support for compliance management, especially CMMC; and the overall value delivered feels too expensive.

- **LOOKING FOR A NEW SERVICE PROVIDER:**

  Likely as a result of these challenges, 82% plan to change their outsourced security provider in the next year, with 46% of those combining in-house and outsourced capabilities. Those looking for a new service provider want someone with a deep understanding of DIB requirements, quality staff, and comprehensive services.

- **A LOWER PRIORITY ON CMMC?:**

  While their primary challenge in Part 1 is "implementing and maintaining compliance with regulations, including CMMC," they're not readily seeking service providers with CMMC compliance top-of-mind. Of their top reasons to outsource, "support for CMMC" came in sixth. Of the top capabilities they look for in a new service provider, "support for CMMC" came in seventh. This either shows a disconnect between the urgency of CMMC compliance, or their need for more immediate and basic security needs first.

PART #3 //R

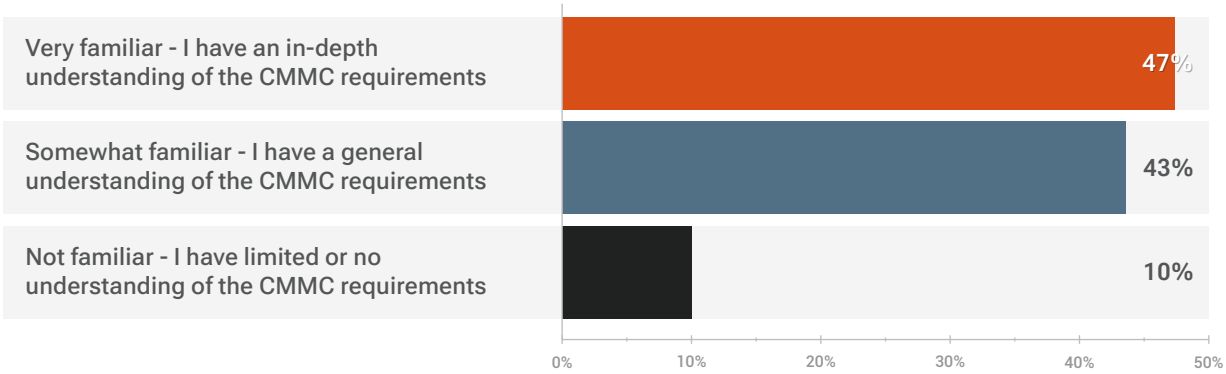
CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PREPAREDNESS

To protect the companies it does business with, the Department of Defense has rolled out the Cybersecurity Maturity Model Certification (CMMC), a set of cybersecurity certifications that defense contractors must abide by. How are respondents doing on their certification checklist?

47% ARE VERY FAMILIAR WITH CMMC REQUIREMENTS

47% are very familiar with and have an in-depth understanding of the CMMC requirements. 43% are somewhat familiar and have a general understanding of the CMMC requirements. 10% are unfamiliar with and have limited or no understanding of the CMMC requirements.

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



81% HAVE STARTED THE CMMC COMPLIANCE PROCESS

81% have started the process for CMMC compliance, while 19% have not.

Has your company begun the process for CMMC compliance?

HOW MUCH TIME TO COMPLIANCE

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

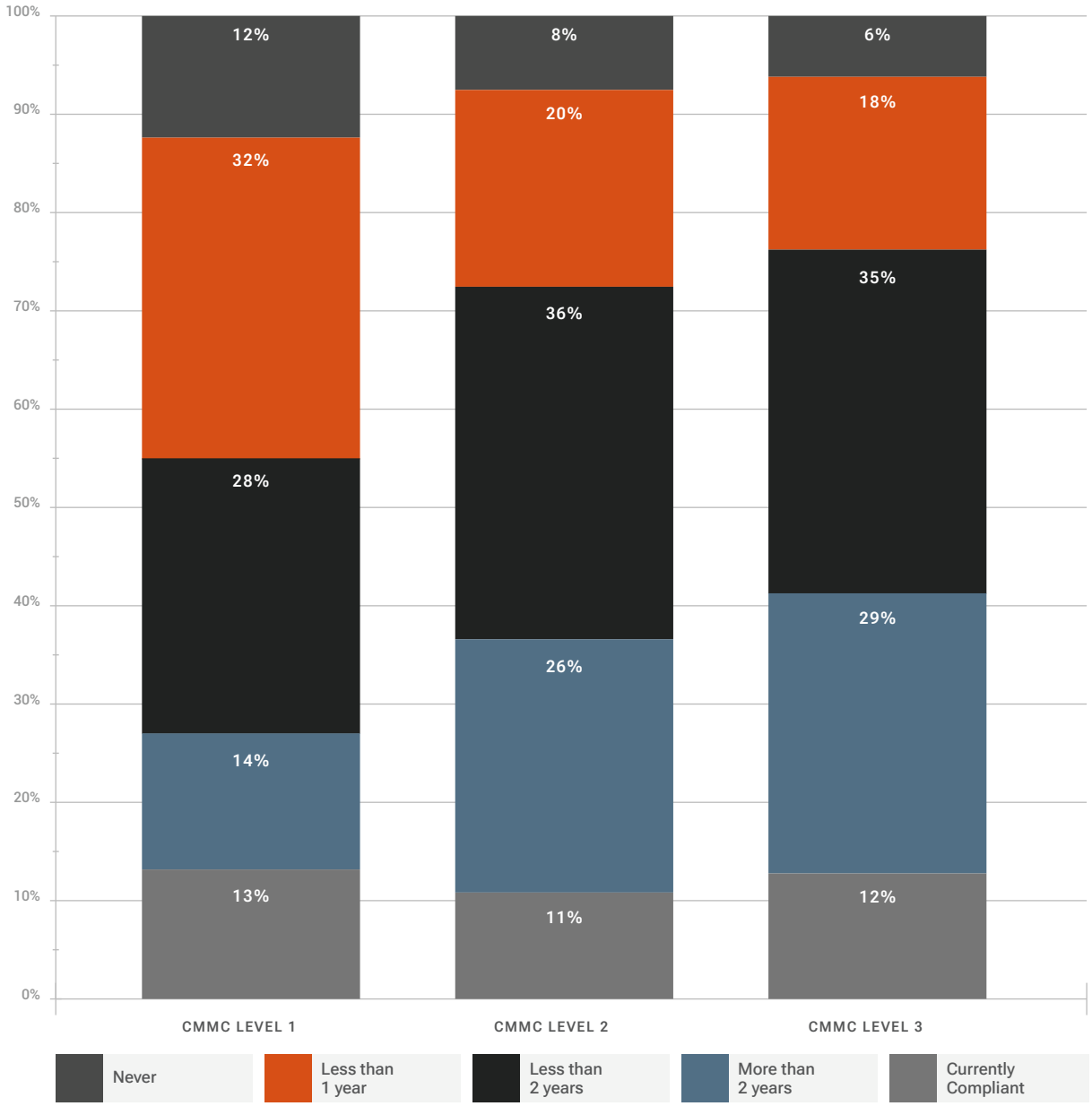
CMMC LEVEL 1

- CURRENTLY COMPLIANT (13%)
- LESS THAN 1 YEAR (32%)
- LESS THAN 2 YEARS (28%)
- MORE THAN 2 YEARS (14%)
- NEVER (12%)

CMMC LEVEL 2

- CURRENTLY COMPLIANT (11%)
- LESS THAN 1 YEAR (20%)
- LESS THAN 2 YEARS (36%)
- MORE THAN 2 YEARS (26%)
- NEVER (8%)

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



SUMMARY

When it comes to CMMC compliance, respondents are generally aware of what it is and what they need to do. 47% have an in-depth understanding of the CMMC requirements, while 43% have a general understanding of the CMMC requirements. 81% have already started the CMMC compliance process — but only 13% are compliant with Level 1 and 11% are compliant with Level 2. However, compliance will take another few years for many, and a handful say they'll never reach compliance.

In looking deeper at the "never" segment, it's unclear why they feel that way. For example, of those who replied they'd "never" get to Level 1, 78% have already begun the process. In fact, those who say "never" for Level 1 have higher revenue, the same IT budgets, and the same level of familiarity as those already compliant with Level 2, rank their cybersecurity priority as "high," and have four or more people ranked with "high" skill dedicating time to security. If it's not a budget, skills, or personnel issue, there may be another underlying technical issue that's keeping them from meeting CMMC. Or they may have replied "never" if they're pursuing Level 2 compliance and see Level 1 as irrelevant.

PART #4

FUTURE STRATEGIES AND PRIORITIES

In the last section, we found that respondents are already looking ahead to completing their CMMC requirements over the next year or two. Here's what else they prioritize in 2024 to increase their capabilities and improve their security posture.

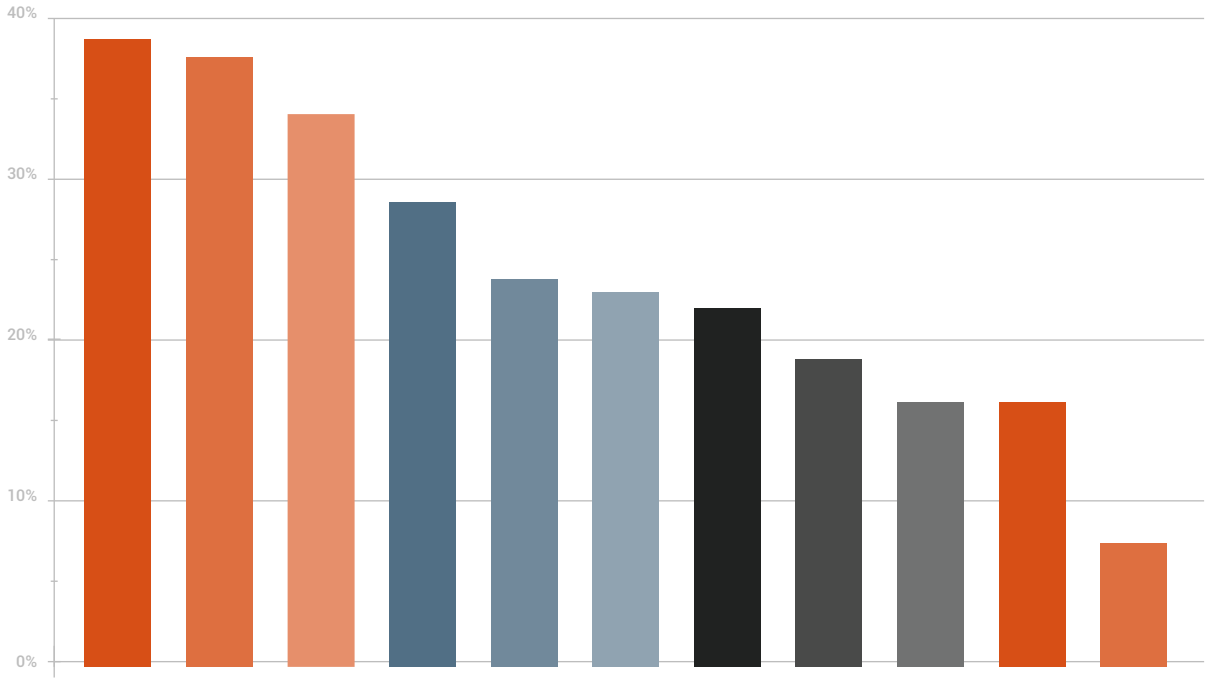
TOP CYBERSECURITY PRIORITIES

Top cybersecurity priorities for the next year include:

38%	STRENGTHENING ACCESS CONTROL POLICIES AND ENFORCEMENT AROUND SENSITIVE DATA Considering one of their biggest challenges was protecting from data breaches and leaks, they're focusing on shoring up their networks and systems in 2024.
37%	ACHIEVING OR ADVANCING COMPLIANCE (E.G., CMMC) REQUIREMENTS Their biggest challenge was ensuring compliance, especially with CMMC, so they're focused on achieving that compliance in the next year.
34%	DEPLOYING MULTI-FACTOR AUTHENTICATION ACROSS MOST OR ALL SYSTEMS Again, they prioritize taking action to protect sensitive data by adding extra steps to prove identity for access.
28%	ENHANCING NETWORK SECURITY TO SAFEGUARD AGAINST EXTERNAL THREATS In the next year, they also want to take steps to strengthen their network so they have a strong front against malicious actors.
24%	DEPLOYING ADVANCED ENDPOINT PROTECTION (E.G., EDR TECHNOLOGY) Considering that 59% have had a compromise in four or more of their endpoints in the past year, they're taking steps for more protection — especially in a more remote world.

Other priorities include improving cloud security monitoring and protection (23%), strengthening incident response planning and execution capabilities (22%), conducting regular vulnerability assessments or penetration testing (19%), improving log analysis and incident investigation capabilities (16% tie), enhancing security awareness and training programs for employees (16% tie), and finding an outsourced security provider (e.g., MSSP, MDR) (7%).

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

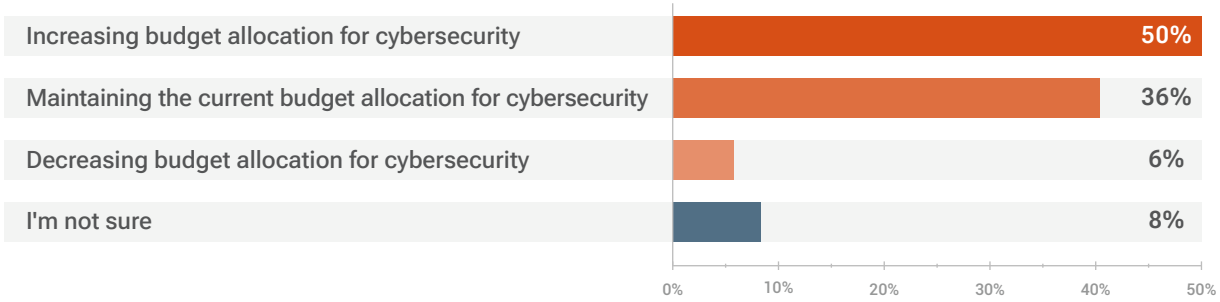


Strengthening access control policies and enforcement around sensitive data	38%
Achieving or advancing compliance (e.g., CMMC) requirements	37%
Deploying multi-factor authentication across most or all systems	34%
Enhancing network security to safeguard against external threats	28%
Deploying advanced endpoint protection (e.g., EDR technology)	24%
Improving cloud security monitoring and protection	23%
Strengthening incident response planning and execution capabilities	22%
Conducting regular vulnerability assessments or penetration testing	19%
Improving log analysis and incident investigation capabilities	16%
Enhancing security awareness and training programs for employees	16%
Finding an outsourced security provider (e.g., MSSP, MDR)	7%

50% EXPECT THEIR GENERAL SECURITY BUDGET TO INCREASE

Over the next fiscal year, 50% plan to increase budget allocation for cybersecurity, 36% plan to maintain the current budget allocation for cybersecurity, and 6% plan to decrease budget allocation for cybersecurity. 8% are not sure what the plan will be.

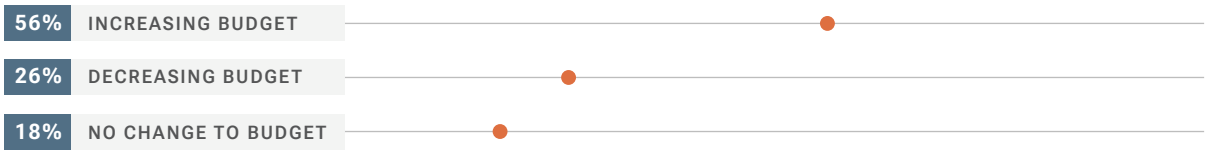
How does your company plan to allocate its cybersecurity budget in the next fiscal year?



56% EXPECT THEIR OUTSOURCED SECURITY BUDGET TO INCREASE

56% expect their budget for outsourced security to increase, while 26% expect their budget for outsourced security to decrease. 18% expect no change to their budget.

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



SUMMARY

Cybersecurity will continue to be a growing priority for SMBs in the DIB. Budgets will continue to increase, as 50% plan to increase their budget allocation for cybersecurity and 56% expect their budget for outsourced security to increase.

Top cybersecurity priorities for 2024 include strengthening access control policies and enforcement around sensitive data; achieving or advancing compliance (e.g., CMMC) requirements; and deploying multi-factor authentication across most or all systems.

Overall, the top five priorities focus on taking steps to expand and strengthen basic security capabilities. Their priorities also address their top challenges from Part 1: implementing and maintaining compliance with regulations like CMMC, and protecting sensitive data from breaches and leaks.

PART #5

ACTIONABLE TAKEAWAYS FOR SMB LEADERS IN THE DIB

Prioritizing cybersecurity is crucial for SMBs contributing to government contracts and American innovation. Yet they often aren't sure where to begin--especially with limited budgets and resources. And the idea of protecting against nation-state attacks can seem too overwhelming to approach. Based on the results of this research, following are three actions every SMB in the DIB can take to begin the journey toward improved cybersecurity posture.

01 IF YOU'RE OUTSOURCING CYBERSECURITY NEEDS, BE WISE ABOUT CHOOSING A SERVICE PROVIDER.

Respondents are strengthening and expanding their baseline security capabilities, yet many found that their outsourced service providers couldn't deliver those capabilities. They experienced inadequate incident response time, limited support for compliance, lack of expertise, inconsistent quality, and an overall lack of value for what they were paying.

Therefore, look for a new service provider who:

- ✓ Has a deep understanding of DIB requirements and can guide you in implementing CMMC Level 2 upon which you can build your security program.
- ✓ Helps you expand your basic IT security practices to include networks, systems, and data access management, firewall policies, multi-factor authentication, and more.
- ✓ Builds out your security approach with advanced, modern endpoint protection, holistic detection capabilities, and security operations capabilities that can quickly investigate intrusion and compromise indicators.
- ✓ Uses the latest technologies and is ideally building their proprietary tech stack, has expert staff who keeps you in-the-know on decision-making, and who provides quality services for their price.

02 IF YOU HAVEN'T STARTED YOUR CMMC COMPLIANCE JOURNEY, GIDDY UP!

81% of respondents have already started the CMMC compliance process. However, less than 15% are already in compliance, and less than half (47%) have an in-depth understanding of the CMMC requirements. Additionally, CMMC compliance is the biggest challenge today.

While you can get started on the list of CMMC requirements today, located on the *Department of Defense website*, you don't have to go it alone — and that may be where many organizations are getting stuck. Seek out service providers with knowledge of CMMC requirements and the DIB to help guide you in your compliance steps.

However, remember that CMMC compliance is only the start of building a robust security program, especially for companies that work in fields of interest to motivated cybercriminals and nation-state cyber espionage.

03 THE RIGHT TOOLS AND TECHNOLOGY, AS WELL AS THOSE WITH THE EXPERTISE TO USE THEM, ARE KEY TO BETTER SECURITY.

As we saw in Part 1, what likely matters most in lowering your risk and improving your security posture isn't necessarily a bigger IT budget, more staff dedicating time to security, more expertise and knowledge, or how often your leadership team meets about security. It's having the right enterprise-grade tools and technologies, and the right people with the right knowledge to use them.

Look for service providers with a deep understanding of DIB requirements creating best-in-class proprietary technology to help you develop a Harden-Detect-Respond mindset and operational capabilities. This includes hardening IT and cloud, endpoints, and people; increasing detection and visibility; and implementing 24/7 investigation and response. This approach will not only meet the minimum CMMC requirements but also go above and beyond to achieve strong resiliency.

CONCLUSION

The innovations and operations of SMBs serving America's Defense Industrial Base (DIB) and Critical Infrastructure (CI) are critical to our security and prosperity. Nation-state threats and cybercriminals will continue to target them. SMBs must take the necessary steps to improve their cybersecurity maturity. Fortunately, the majority of SMBs are making this a high priority.

Critical to their success will be investing in the necessary technology and operations to harden themselves from initial compromise and subsequent lateral movement. They must also increase investment and capability in threat detection, mitigation, and response.

CMMC Compliance alone will be insufficient. DIB/CI adversaries are highly motivated and will, over time, find an avenue of compromise.

Putting obstacles in the road will slow them down or deter them entirely. However, the prudent CEO should assume cybercriminals and adversaries will eventually break through or emerge from within. 24 x 7 monitoring and incident response backed by modern technologies with qualified incident investors and responders is a must.

SMBs that plan and invest appropriately can withstand the advances of highly motivated adversaries – better protecting themselves, better protecting America's national security.

RADICL™

DIB CYBERSECURITY MATURITY REPORT

2024 EDITION

RADICL provides SMBs in America's Defense Industrial Base Xtended Threat Protection (XTP). RADICL's purpose-built and proprietary XTP platform delivers SMBs full-spectrum threat protection and compliance management that is quick, easy, and affordable. The RADICL XTP Platform powers an AI-augmented virtual Security Operations Center (vSOC) delivering customers heavily automated and expert-driven threat monitoring, threat hunting, incident response, vulnerability management, security awareness training, and managed compliance adherence. RADICL enables SMBs in the DIB to spend more time running a profitable business to support our country and less time worrying about security and compliance.
To learn more about RADICL XTP visit *RADICL.com*