CORVUS

Policyholder Cybersecurity Benchmarking Report

Executive Summary

We're excited that you, our Corvus Insurance policyholders, have taken an interest in learning more about industry and company benchmarks around cybersecurity and risk mitigation efforts. The information included in this report has been compiled based on a recent survey of Corvus Cyber and Technology Errors & Omissions (Tech E&O) policyholders, conducted in Q4 2021. We were thrilled to see your enthusiasm, which was evidenced by the strong response rate. The survey's results will help Corvus plan for new tools and services that are optimally matched to you and where you are on your path to a better security posture.

You'll find key takeaways and actionable insights you can use to not only better protect your company, but also learn about what other similarly sized organizations are focused on when it comes to cybersecurity.

Key findings include:

- The need for a Chief Information Security Officer (CISO) — on staff, when possible — to bridge the gap between technologists and business executives.
- Increased spending should be expected as new threats come to light.
- Smaller companies are more concerned with staying current on new threats, while larger companies worry more about vendor breaches.
- A majority of respondents have low confidence in their company's ability to manage third-party risk.
- Security is a continuum and always evolving, such that organizations should never consider themselves "done" with security implementation.

By reviewing this report in tandem with recommendations from our Virtual CISO (vCISO) tool, we hope you'll be able to confidently prioritize your investments in 2022 and beyond.

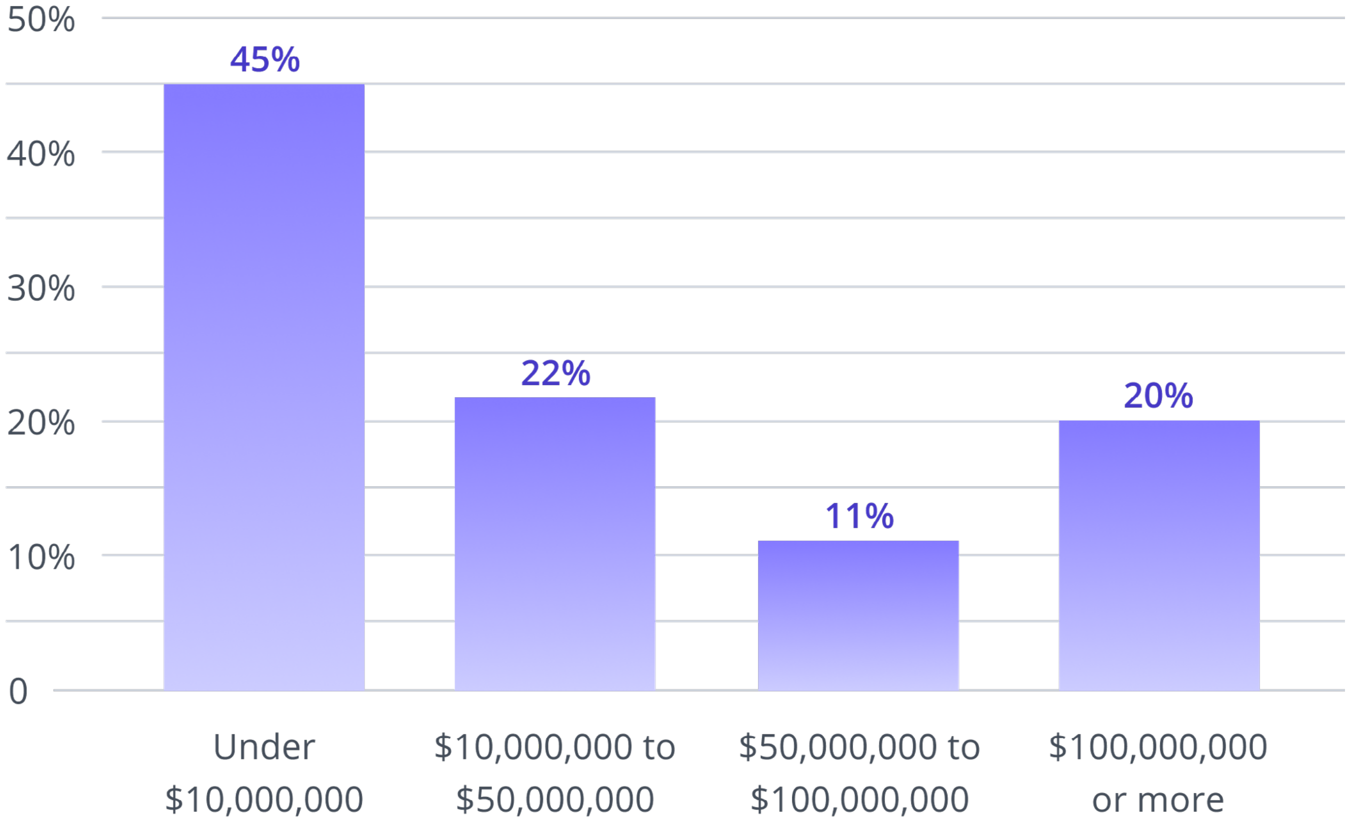
Table of Contents

Participants

A total of 289 Corvus policyholders participated in our inaugural benchmarking survey. These survey results and subsequent findings are intended to help our policyholders understand how similarly sized companies are currently addressing not only their cybersecurity needs, but their top concerns in today's cyber threat landscape. Throughout this report, results are broken down by size of company — defined by either number of employees or gross annual revenue. In certain cases, results are further segmented by staffing structure to allow additional insights.

Number of Participants	Participants' Company Size
133	<50 employees
85	50-249 employees
71	250+ employees
Total = 289	

Gross Annual Revenue

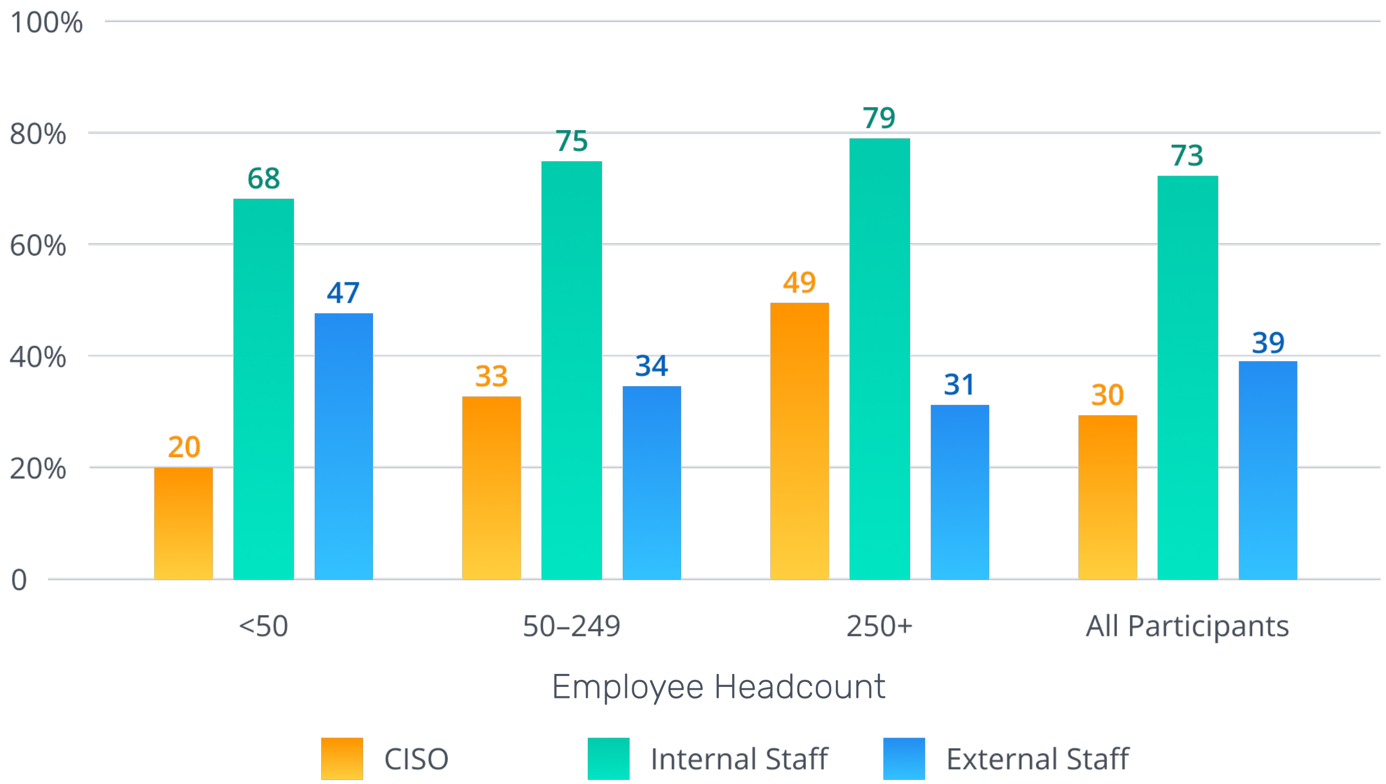


Organizational Structure and Support

Our survey results support the idea that the larger an organization, the more likely it is to have a Chief Information Security Officer on staff, leading the company's cybersecurity efforts. Only 20% of the smaller companies (<50 employees) reported having a CISO on staff, compared to 45% of the larger organizations.

To analyze the impact of having a CISO on staff, responses were categorized as follows: companies with a CISO on staff; those using internal staff only (with no CISO); and those using external support staff with no internal CISO. For survey participants who noted having internal staff only, they reported an average team size of 2-3 employees.

Party Responsible for Planning, Oversight, & Execution of Cybersecurity



Note: total does not equal 100%, as survey participants could select multiple answers

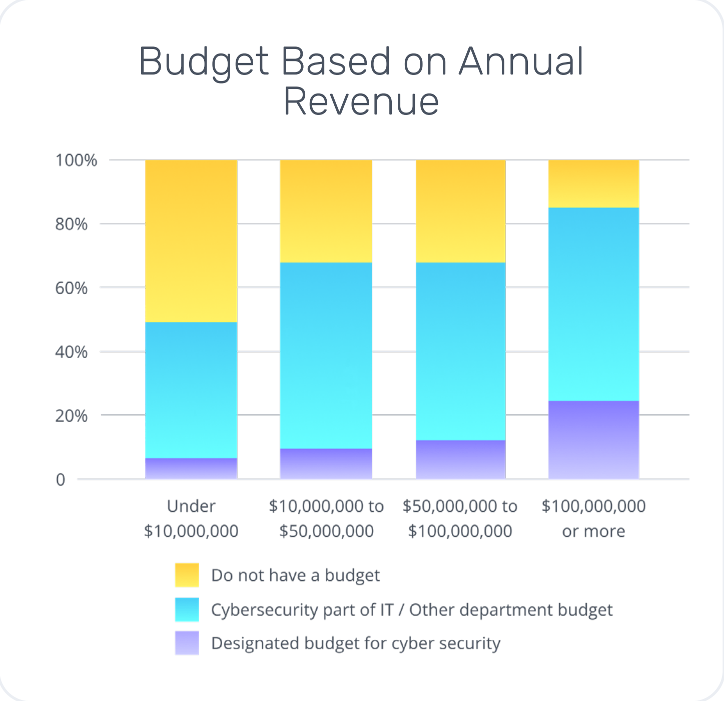
Findings show that while a majority of participants feel supported by their CEO and senior management, policyholders with an internal-only security team and no CISO on staff reported feeling slightly less supported. Respondents' comments throughout the survey indicated that staffing pressures could be a cause for the slightly lower management support rating. At the same time, when a CISO is brought on staff, they can help to bridge the gap between technologists and business leaders, resulting in decreased reliance on external security staff.

Cybersecurity Budget and Spend

Budget

Regardless of their company's size, few policyholders reported having a designated budget for cybersecurity. Instead, cybersecurity expenses are most likely to be accounted for under a general Information Technology (IT) budget or that of another department. However, companies with less than $10 million in annual revenue are least likely to track cybersecurity expenditures as a separate budgetary line item.

It's also noteworthy that based solely on survey responses, 18% of companies with 250+ employees do not have a cybersecurity budget, whether designated or rolled into another department's budget. As a company's security needs mature, many (63% of those with 250+ employees) allocate a percentage of overall technology spend and headcount to grow security efforts. Not having a dedicated budget can mean that investing in security becomes an ad hoc behavior. As companies increase security investments, they often need to create a dedicated budget to avoid these pitfalls.



Budget Based on Employee Count

Budget Status	Number of Employees		
	<50	50-249	250+
Designated budget for cybersecurity	8%	14%	18%
Cybersecurity part of IT / Other department budget	45%	51%	63%
Do not have a budget	47%	35%	18%

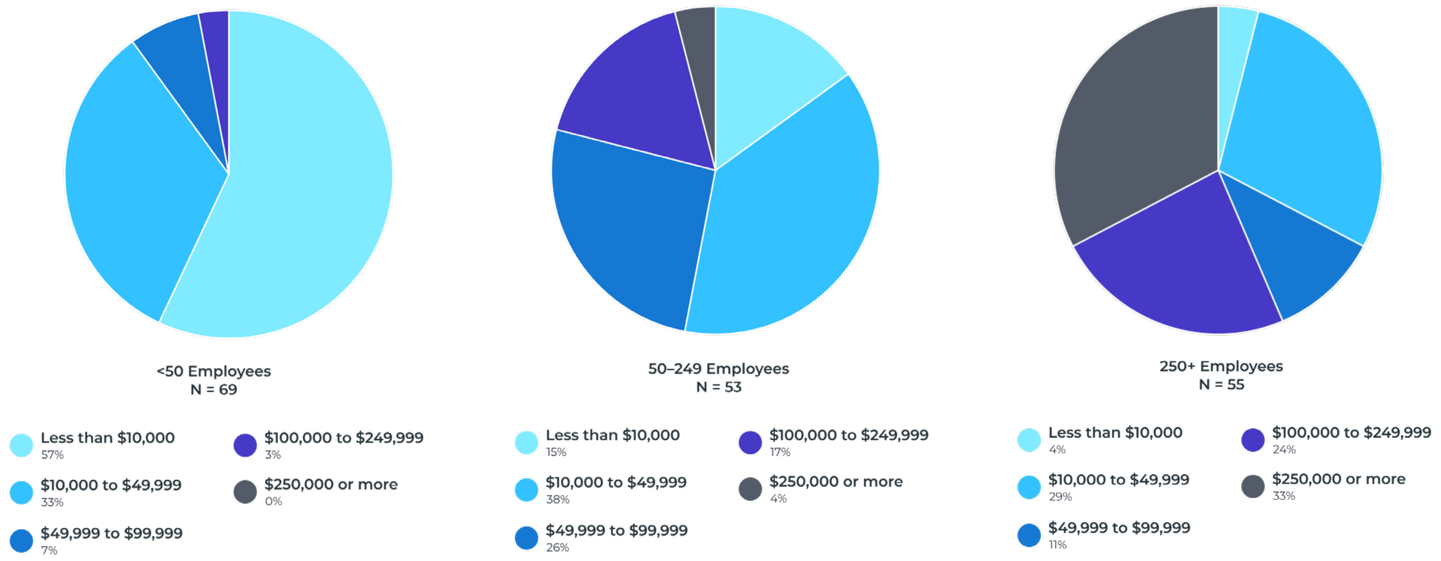
Spend

Smaller companies in both size and annual revenue spent less on cybersecurity in the past year, averaging just over $25,000. In fact, 57% of participants with less than 50 employees reported spending less than $10,000.

This finding may be due to the fact that smaller organizations are more likely to rely on built-in security features in IT technology — though these features often don't provide all of the security coverage needed.

Across all participants, the median spend was $25,000, while the average was $122,600 and the highest spend was approximately $4 million.

Spend on Cybersecurity in the Past Year, Excluding Insurance (By Employee Count):

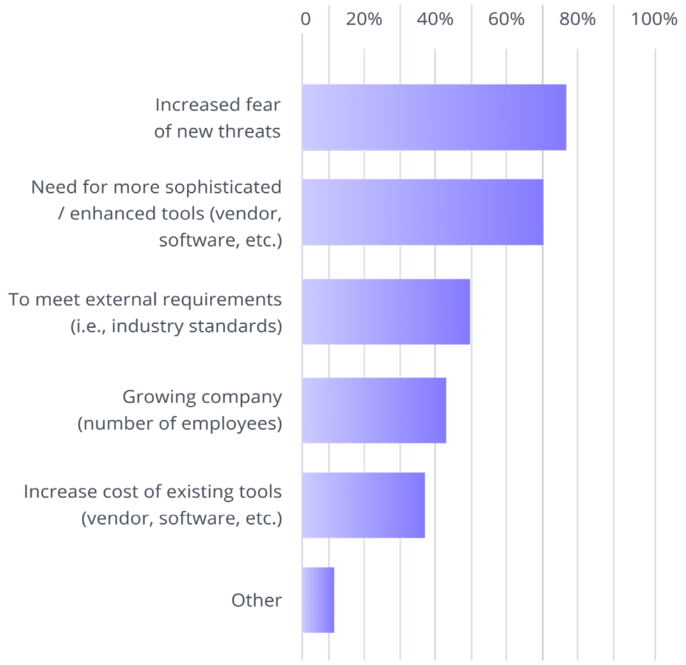


Increased Spending is Expected

Regardless of their company size, 60% of survey participants stated their security spending is expected to increase in the next year. Even the smallest companies — those with under 50 employees — expect to see a cybersecurity spend increase, as reported by 54%.

Participants acknowledged the need to increase spending to protect against new threats, as well as to enhance existing security tools. We see this as a recognition of today's evolving landscape, where security is no longer about simply purchasing a few products and calling it a day. Organizations still need to make investments in market-leading tools, but they now require more support to manage them — especially as attackers get better at bypassing traditional controls and causing greater damage.

Reasons Behind Increased Spending



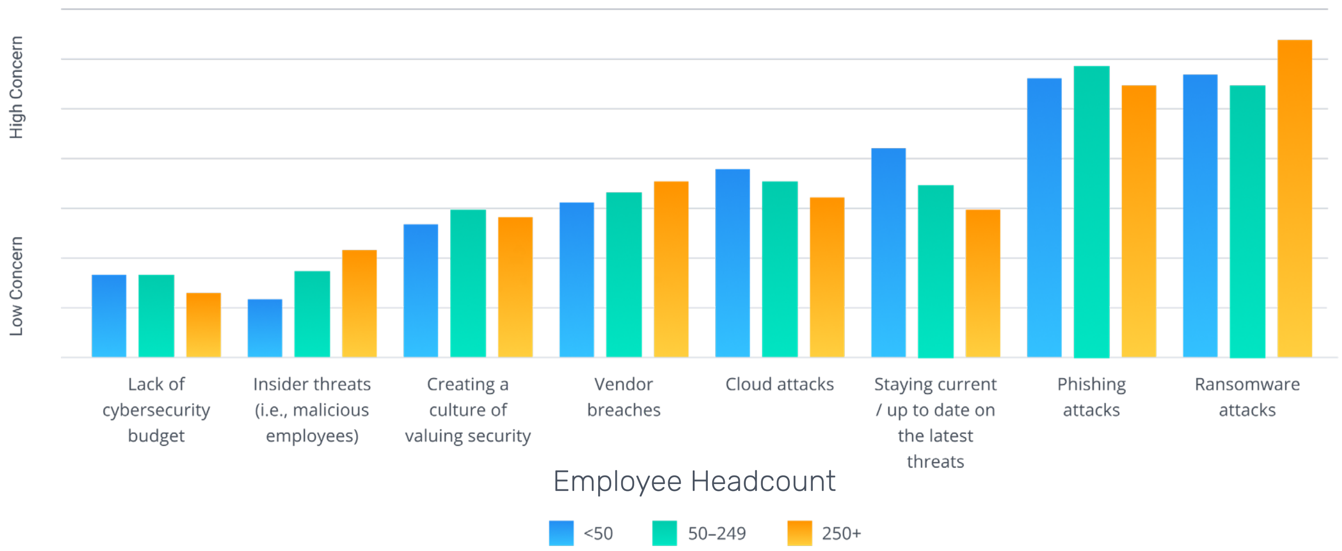
Cybersecurity Concerns

Greatest Concerns

Based on survey responses, ransomware and phishing attacks are the top cybersecurity concerns for Corvus policyholders — a point validated by internal metrics that show these attack vectors comprise the vast majority of cyber claims. Currently, lack of budget is a lower priority concern. These findings are consistent whether or not there is a CISO on staff.

Opinions begin to deviate by employer size when it comes to "staying current on the latest threats": smaller companies reported a higher degree of concern here, while larger companies worry more about vendor breaches. We see these varied concerns as highlighting how security sophistication grows as companies grow. It's an evolution of the security mindset: an organization's main concerns at the start are survival and getting foundational needs in place. As growing companies start to have a grip on those aspects that are fully in their control, they can then focus on other areas like vendor breaches, which are outside of their direct purview.

Ranking of Cybersecurity Concerns by Company Size

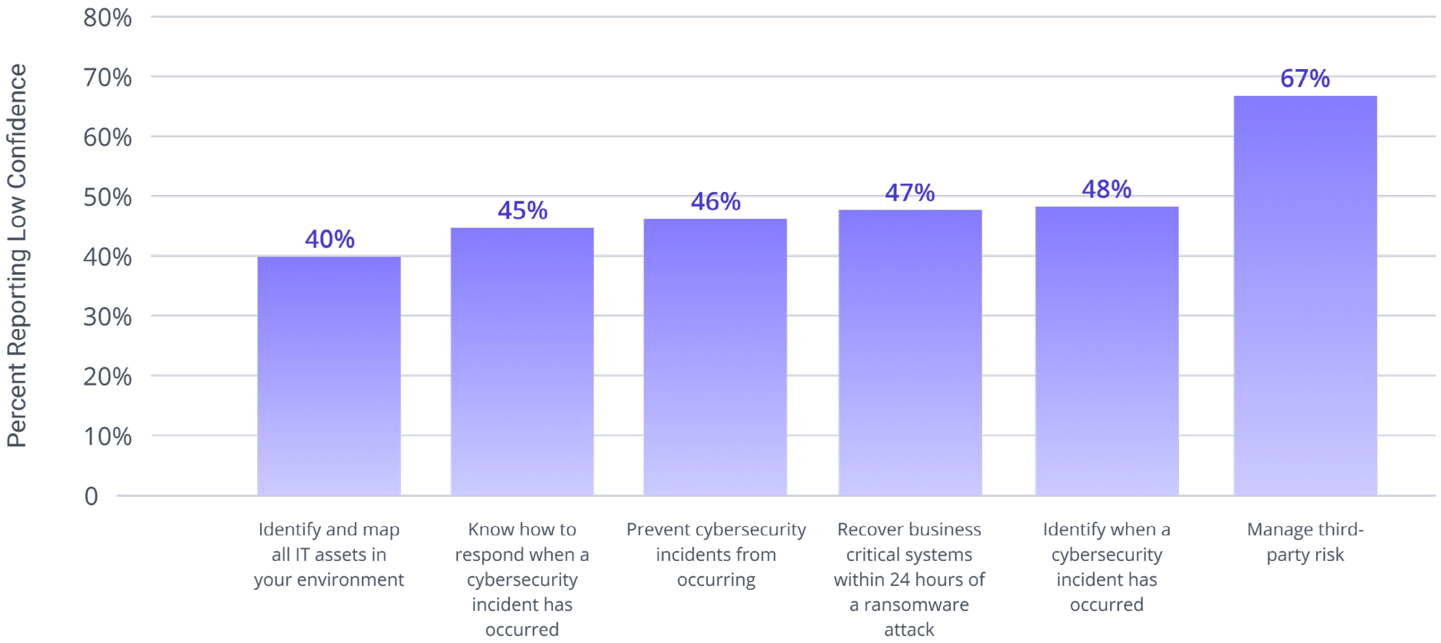


Level of Confidence

For all the categories outlined in the policyholder benchmarking survey, 40%+ of participants reported low confidence in their company's ability to understand and mitigate overall cybersecurity risk. This finding is most pronounced when considering third-party risk management — nearly 70% reported low confidence.

Survey participants employed at companies with an on-staff CISO reported greater confidence in their organization's ability to prevent or respond to incidents. Only 38% of respondents with a CISO reported low confidence for these areas.

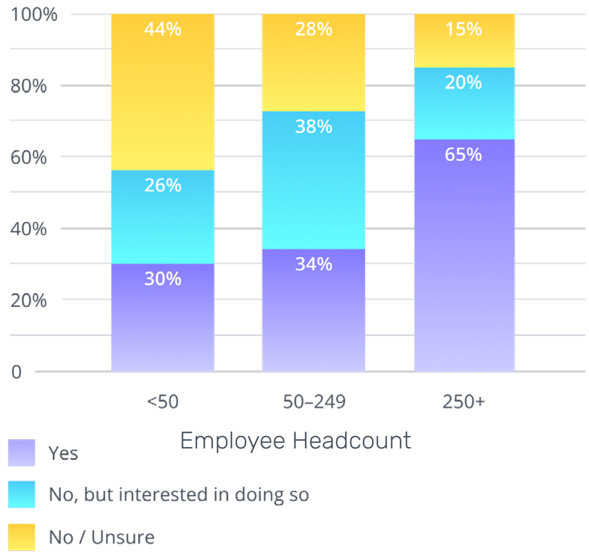
Low Confidence in Company's Ability To...



Comparing to an Industry Standard

Comparing security measures to an industry standard is one way organizations can build confidence and ensure security posture is up to date. Those participants from larger companies are more likely to conduct such a comparison than those from smaller companies. Standard frameworks vary depending on industry, however the most frequently mentioned include NIST and HIPAA.

Are Company's Security Measures Compared to an Industry Standard?



Most Frequently Mentioned Standards:

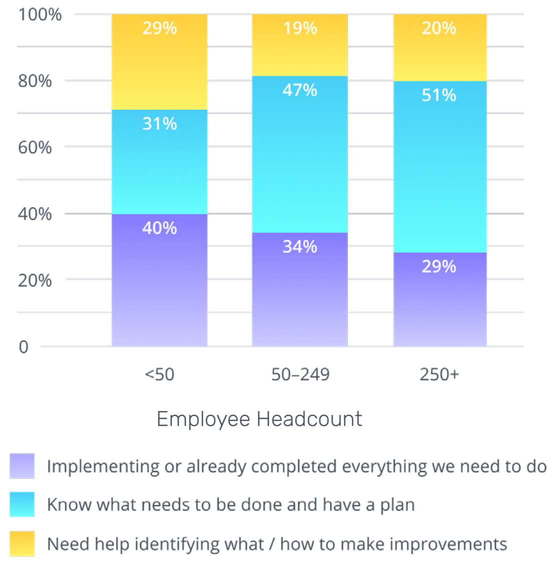
Rank	Security Framework	Reason for Implementation
1	NIST Cybersecurity Framework	Optional (represents more mature security posture)
2	HIPAA Security Rule	Industry requirement
3	CIS Controls	Optional (represents more mature security posture)
4	SOC2	Optional (represents more mature security posture)
5	ISO 27001 and ISO 27002	Optional (represents more mature security posture)
6	NY DFS	Industry requirement
7	HiTrust	Industry requirement
8	PCI/PCI DSS	Industry requirement

Preparedness

Interestingly, survey participants from the smallest companies had the highest level of confidence that they have implemented or are in the process of implementing all necessary steps from a cybersecurity risk standpoint. Of the participants who stated that they *do* need help with security improvements, 72% were companies that lacked a CISO.

From a CISO's perspective, if an organization believes it has implemented all the necessary steps for cybersecurity, it is almost certainly thinking too small — security is a never-ending journey.

Company Preparedness to Identify and Implement Cybersecurity Improvements



Of course, It is important to note the rating of preparedness is subjective and based on the individual's perspective. We know from comments that policyholders using external support may not have the clearest understanding of their security posture. As one policyholder put it, "We assume we are safe because we haven't had a problem yet."

Such comments might help explain the different results when comparing staffing structure. The policyholders relying on external staff to lead their company's cybersecurity and risk mitigation efforts were the least likely to state they need assistance creating and implementing a cybersecurity plan. Comments provided, however, seem to bring to light a potential false sense of security.

Factors Preventing Improvements

Of those participants who reported they would like to improve their security posture, lack of resources and complexity were the driving factors as to why more hasn't been done. Thankfully, lack of support from senior management was the least mentioned factor, which confirms our earlier finding that most policyholders feel senior management makes cybersecurity a priority.

Another factor in today's market that may further prevent improvements is the current shortage of qualified labor. Hiring managers in the cybersecurity space can **lean on the knowledge of those experienced in finding qualified cyber talent.**

The table below highlights key factors cited as preventing cybersecurity improvements and how they relate to company size. The benchmarking insights here can help answer the question: "How do similarly sized companies view today's challenges and what could our challenges look like in the future?"

Factors Preventing Improvements	Employee Count		
	<50	50-249	250+
Complexity of cybersecurity / lack of knowledge	77%	63%	63%
Internal resource constraints	58%	77%	86%
Budget constraints	35%	29%	29%
Inability to prioritize	27%	16%	18%
Support from senior management	3%	16%	4%
N =	79	56	49

Cybersecurity Services

Services Being Utilized

While this survey found that most policyholders currently use a mix of vendors and internal staff to address their company's cybersecurity needs, survey results also delved into other risk mitigation efforts, including: employee security training; penetration testing; security monitoring; and vulnerability management.

Survey responses illustrated:

- Participants at larger companies are more likely to be currently implementing the four tactics, whereas those at smaller companies are less likely.
- When segmenting by size, larger companies are more likely than smaller ones to use a vendor for employee security training and penetration testing.

- Nearly a quarter of the policyholders surveyed do not currently incorporate penetration testing, making it the least addressed of the four tactics.

Percent of Companies Currently Implementing Tactics:

Company Size (By Employee Count)	Employee Security Training	Penetration Testing	Security Monitoring	Vulnerability Management
<50	80%	54%	83%	72%
50-249	91%	71%	87%	79%
250+	92%	76%	87%	87%

Percent of Companies Using Third-Party Vendors for Security:

Company Size (By Employee Count)	Employee Security Training	Penetration Testing	Security Monitoring	Vulnerability Management
<50	44%	47%	67%	60%
50-249	66%	66%	62%	59%
250+	69%	72%	66%	65%

Closing Remarks

We hope you've found the insights gleaned from Corvus's Cybersecurity Policyholder Benchmarking Survey to be valuable. Using the data collected, we aim to better our policyholders' security posture in both the near and long terms. As we discussed, measures including hiring an on-staff CISO, keeping up to date on new and emerging threats, and viewing security as an ongoing journey are all highly advisable when looking to mitigate loss and secure your organization. As a next step, if you haven't already done so, be sure to log in to your Policyholder Dashboard and complete your vCISO Security Questionnaire to get additional recommendations. If you have any questions regarding cybersecurity risk mitigation tactics or implementation, please **reach out to Corvus's Risk + Response team**.

Legal Disclaimer: This report is intended for general guidance and information purposes only. This report is under no circumstances intended to be used or considered as specific insurance or information security advice. Please consult your broker with respect to the information presented herein.

CORVUS

About Corvus

Corvus Insurance is building a safer world through insurance products and digital tools that reduce risk, increase transparency, and improve resilience for policyholders and program partners.

Our market-leading specialty insurance products are enabled by advanced data science and include Smart Cyber Insurance®, Smart Tech E&O^{SM}, Smart Cargo®, and a suite of products for Financial Institutions. Our digital platforms and tools enable efficient quoting and binding and proactive risk mitigation.

Corvus Insurance offers insurance products in the US, Middle East, Europe, Canada, and Australia. Current insurance program partners include AXIS Capital, Crum & Forster, Hudson Insurance Group, certain underwriters at Lloyd's of London, R&Q's Accredited, SiriusPoint, and Skyward Specialty Insurance. Corvus Insurance and Corvus London Markets are the marketing names used to refer to Corvus Insurance Agency, LLC and Corvus Agency Limited. Both entities are subsidiaries of Corvus Insurance Holdings, Inc. Corvus Insurance was founded in 2017 and is headquartered in Boston, Massachusetts with offices across the US and in London, UK. For more information, visit corvusinsurance.com.