CyberBay

a survey report

CYBERBAY 2026

BUSINESS CYBERSECURITY REPORT

Bellini College of Artificial Intelligence, Cybersecurity, and Computing
Cyber Florida, The Florida Center for Cybersecurity
University of South Florida, Department of Criminology

Executive Summary

This report examines how small and mid-sized organizations implement cybersecurity practices and the factors that influence their implementation. Using survey data from 202 firms, it measures perceived cybersecurity risk, organizational priorities, cyber insurance, industry influences, and the extent of cybersecurity implementation.

The results show that organizations emphasizing cybersecurity and those influenced by professional networks, industry guidance, and regulatory expectations report stronger cybersecurity implementation. Regulatory and insurance requirements are also associated with greater adoption, while organizations perceiving higher cyber risk often report lower implementation, likely reflecting recognized gaps. Notably, firm size does not predict implementation, whereas leadership prioritization and program maturity are more strongly associated with implementation.

The report recommends coordinated efforts: regulators, industry groups, and professional associations should reinforce clear expectations, while internal leadership translates these into action. In short, institutional pressures and internal commitment appear to work together to improve cybersecurity outcomes.

Methodology

Sample and Recruitment

This survey captures the perspectives of organizations across a range of industries, rather than those of cybersecurity vendors or service providers alone. MarkITelligence collected data from 202 information technology and cybersecurity professionals using a convenience sample. They drew contacts from small and medium-sized businesses (SMB), managed service providers (MSP), and public sector organizations. Initial outreach focused on Florida and was later expanded to Georgia and Alabama.

Outreach targeted SMBs, MSPs, and public-sector organizations across Florida (63,153), Georgia (36,615), and Alabama (12,878). By organization type, the pool included 83,975 SMB contacts, 5,585 MSP contacts, and 23,086 public-sector contacts. Participants received a $30 incentive. A complete response was defined as a survey in which the respondent progressed through the entire instrument. All 202 cases included in this report are complete responses. No partial responses were retained in the analytic sample.

Key Findings from the Survey

- **Organizations that treat cybersecurity as a leadership priority implement stronger security practices.** Among firms that report high cybersecurity priority, about 69 percent report strong implementation of cybersecurity practices, compared with about 33 percent of firms that report only moderate priority. This pattern is not random; statistical tests confirm a strong association between leadership priority and implementation.
- **Professional networks and industry guidance play an important role.** Organizations that report stronger influence from professional peers, consultants, industry reports, and professional associations tend to report stronger cybersecurity implementation. Among organizations reporting high levels of

institutional influence, about 84 percent report high levels of cybersecurity implementation, compared with about 32 percent of organizations reporting low institutional influence. This pattern suggests that cybersecurity practices often spread through professional communities and shared industry guidance.

- **Regulatory and contractual pressures also encourage cybersecurity adoption.** Organizations that face stronger regulatory and external compliance pressures tend to implement stronger cybersecurity measures. Among organizations experiencing higher regulatory pressure, about 63 percent report strong implementation of cybersecurity practices, compared with about 41 percent of organizations reporting low regulatory pressure. Regulatory expectations and external compliance requirements can encourage organizations to strengthen cybersecurity practices.
- **Perceived cyber risk does not always translate into stronger security practices.** Organizations that perceive lower cyber risk often report stronger cybersecurity implementation. Among firms that believe cyber incidents are very *unlikely*, 75 percent report strong implementation of cybersecurity practices, compared with about 53 percent of firms that believe incidents are somewhat likely. This pattern suggests that organizations with stronger security practices may feel more confident in their defenses, while organizations that recognize gaps in their security posture may perceive greater exposure to cyber threats.
- **Phishing is recognized as the most likely cyber incident.** Across the different types of cybersecurity incidents included in the survey, phishing stands out as the one threat organizations consistently view as more likely than others. While most incident types show similar perceived likelihoods, phishing is rated as more likely to occur than ransomware, credential theft, or unauthorized access. This pattern suggests that phishing is widely recognized as the most common entry point for cyber incidents.
- **Firm size alone does not determine cybersecurity readiness.** Once leadership priority, institutional influences, and organizational maturity are considered, firm size does not independently predict the level of cybersecurity implementation.

Respondent Characteristics

Respondents came from a wide variety of industries. The main groups were private-sector "other" (33.7%), MSPs (13.9%), private-sector critical infrastructure (9.9%), and municipal or county government (9.4%). The remainder included academia, federal and state government, healthcare, finance, manufacturing, legal, utilities, transportation, and related sectors.

Most survey respondents held operational or managerial roles in information technology (IT) or cybersecurity. Nearly half (48.5%) identified as Directors or Managers of IT, and 11.9% as Directors or Managers of Cybersecurity. Analysts in IT (15.8%) and cybersecurity (5.9%) comprised another substantial portion of the sample. CISOs and other C-level executives together accounted for roughly 12%. Overall, the respondent pool primarily reflects individuals directly responsible for cybersecurity operations, implementation, or oversight. Each respondent was asked to answer the survey items on behalf of their firm.

Organizations varied in geographic scope. Approximately 31% operated locally within a single city or region, 30% nationally within the United States, 18% statewide, and 21% reported international operations. This

mix captures both geographically concentrated organizations and those with broader operational footprints.

Organizational size also varied. Seventeen percent reported fewer than 50 employees, 31% had 50 to 250 employees, 36% had 251 to 500 employees, and 15% had more than 500 employees. The highest concentration of respondents came from organizations with 50–500 employees, aligning with the study's focus on small and mid-sized entities.

Measurement Approach

The survey examined five domains: perceived cybersecurity risk, adoption of cybersecurity policies and practices, organizational cybersecurity priorities, cyber insurance, and external influences. Each item used a Likert-style response scale to measure respondents' assessments of their organization's cybersecurity environment.

We used multiple survey items to measure each major domain. Before combining those items, we examined whether respondents answered them similarly. When responses moved together, they indicated a common underlying concept, allowing us to group them into a single overall score for each domain. For example, we asked about the likelihood of nine types of cybersecurity incidents occurring in the next 12 months and then combined those responses into a single measure of overall risk. Think of this process as evaluating a car. A single question, "Do you like the car?" tells you something, but not much. If you also ask about the engine, safety, comfort, reliability, and fuel use, you learn much more. If those answers point in the same direction across respondents, they reflect an overall judgment of the car, from undesirable to desirable. Our survey items behaved similarly, so we combined them into single scores for risk, implementation, priority, and institutional influence.

Cybersecurity Incidents

One aspect of cybersecurity studied here was firms' perceptions of the threat landscape. To minimize potential social desirability bias that can occur when respondents evaluate their own organization directly, we asked them to consider organizations similar to theirs. We examined perceived cyber risks across nine incident categories using a five-point likelihood scale from (1) "very unlikely" to (5) "very likely," for each incident over the next 12 months. Figure 1 summarizes these evaluations.

The perceived likelihood of a cybersecurity incident is consistent across most incident types. In nearly every category, about one-fifth to one-third of respondents say such an incident is likely within the next 12 months, while a slightly larger portion believes it is unlikely. Extreme ratings are rare. Overall, respondents view most cyber incidents as possible but not urgent, indicating moderate vigilance rather than a sense of immediate danger.

Phishing is the exception. It is the only category in which the share rating of an incident as likely (77%) exceeds that of an incident as unlikely (13%). Phishing remains the primary entry point for downstream cyber-attacks, including ransomware, credential theft, and unauthorized access. In an otherwise flat risk profile, phishing occupies a distinct position at the top of the perceived threat hierarchy.

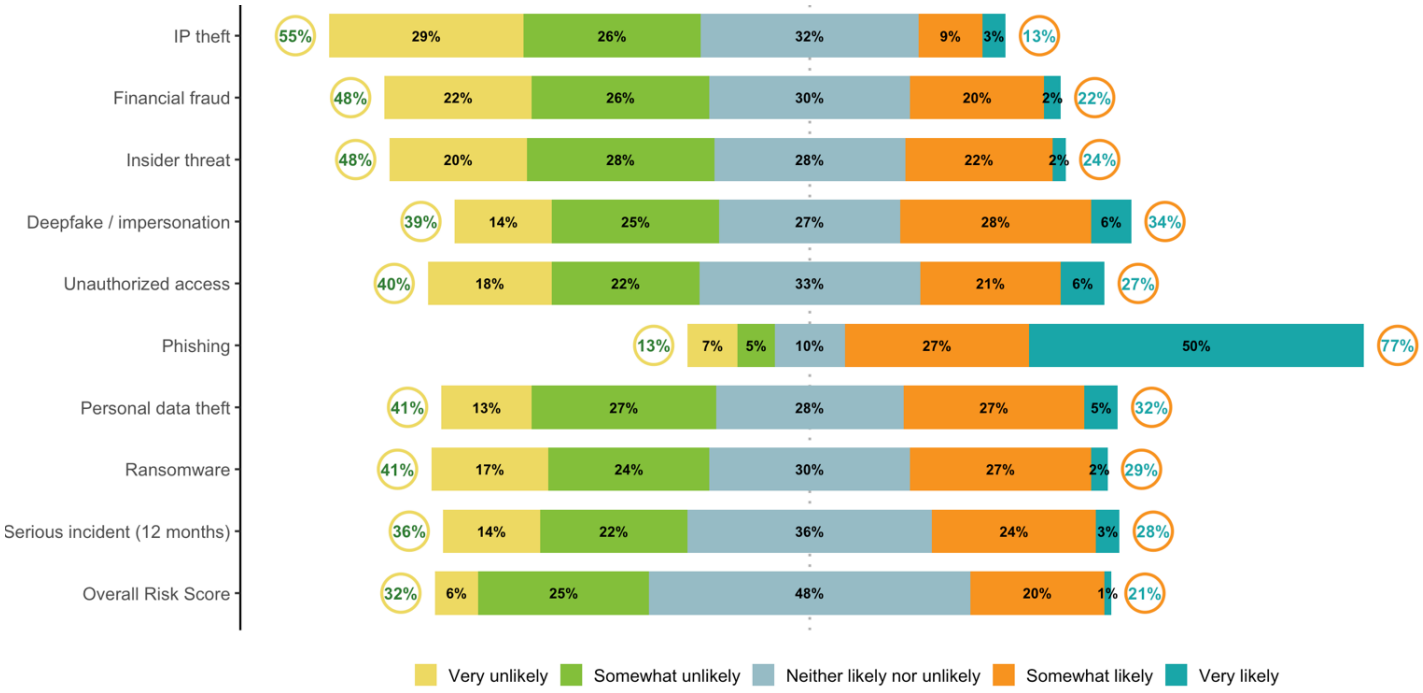

Figure 1. Perceived Likelihood of Cyber Attack in the Next 12 Months (n=202).

Notes: *Bar end percentages in circles show the rounded totals for the unlikely and likely categories. The "overall risk score" is computed by averaging each respondent's scores on all nine risk measures, then rounding the result up. The sample size for all measures was 202 respondents.*

The Overall Risk Score, the last item shown in Figure 1, represents the mean of the nine incident ratings on the five-point scale. The items are strongly related, with high inter-item correlations and a Cronbach's alpha of .88, indicating that respondents are evaluating a common dimension of cyber risk. We therefore combined the items into a single index used in subsequent analyses.

When the Overall Risk Score is grouped into unlikely, neutral, and likely categories, perceived risk tends to increase with firm size. Smaller firms are more likely to report that incidents are unlikely, while larger firms more often view them as likely. Organizations with 251 to 500 employees show the highest share of likely responses. Smaller firms may feel less exposed because they see themselves as less visible targets or perceive fewer attempted attacks. Larger firms operate more complex systems and face greater scrutiny, which may heighten awareness of potential threats.

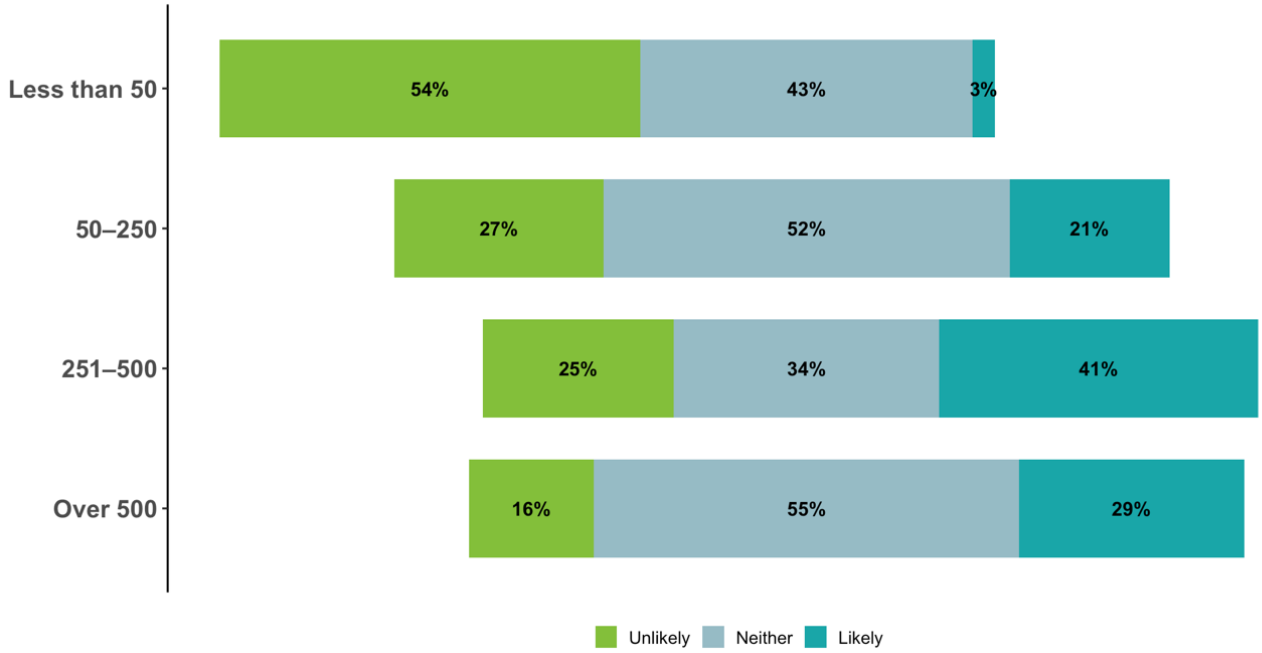

Figure 2. Overall Perceived Risk of Cyber Attack by Firm Size (n=202).

Notes: *The sample size was 202 respondents.*

Cybersecurity Policies and Practices Implementation

We also examined how fully organizations have implemented core cybersecurity practices across key operational domains, including governance, risk assessment, access control, monitoring, incident response, and recovery planning. These indicators capture cybersecurity in practice rather than as stated priority or intent.

Implementation varies across domains. Administrative and governance-related practices, such as defining roles, documenting information flows, conducting risk assessments, and providing user training, tend to be more widely adopted. Core control measures, such as managing access permissions and protecting data, are also broadly implemented. Conversely, more operationally demanding capabilities, such as network monitoring, incident detection, response actions, and incident containment, are less consistently implemented and regularly reviewed. The pattern indicates that many organizations have established basic governance and control structures, while monitoring and response capabilities are less fully developed.

The implementation items form a coherent measure of operational cybersecurity capacity. Because the items are strongly related, we combine them into a single composite index, the Overall Implementation Score, which is used in subsequent analyses.

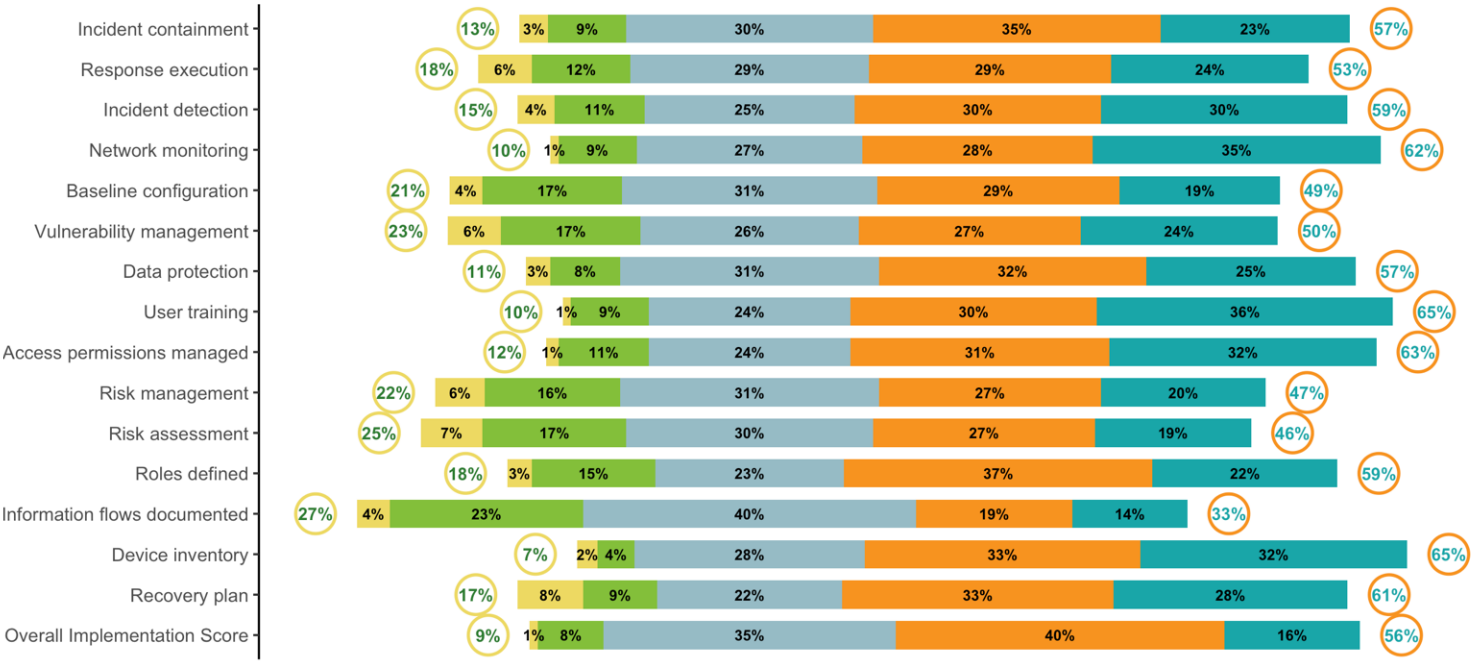

Figure 3. Level of Cybersecurity Implementation for policies and Practices (n=202).

Notes: *Bar end percentages in circles show the rounded totals for the* not implemented *and* likely implemented *categories for "Overall Implementation Score." This is computed by averaging each respondent's scores on all implementation measures, then rounding the result up. The sample size was 202 respondents.*

Implementation by Firm Size

When classified into low, moderate, and high levels, implementation is broadly similar across firm sizes. The distributions overlap heavily, with no clear trend by organizational size. Differences are modest and inconsistent rather than systematic. In this dataset, firm size alone does not appear to distinguish among implementation levels. This contrasts with the earlier finding that perceived risk increases with firm size.

Respondent Priorities Across a Range of Cybersecurity Practices

Cybersecurity priority reflects how organizations allocate attention and resources across policy areas. Unlike implementation, which captures completed actions, priority signals strategic intent and leadership emphasis. Across domains, responses cluster toward the upper end of the five-point scale. "High priority" is the most common response in most areas, and very few organizations report that a domain is not currently prioritized. Overall, cybersecurity is widely treated as an important organizational priority.

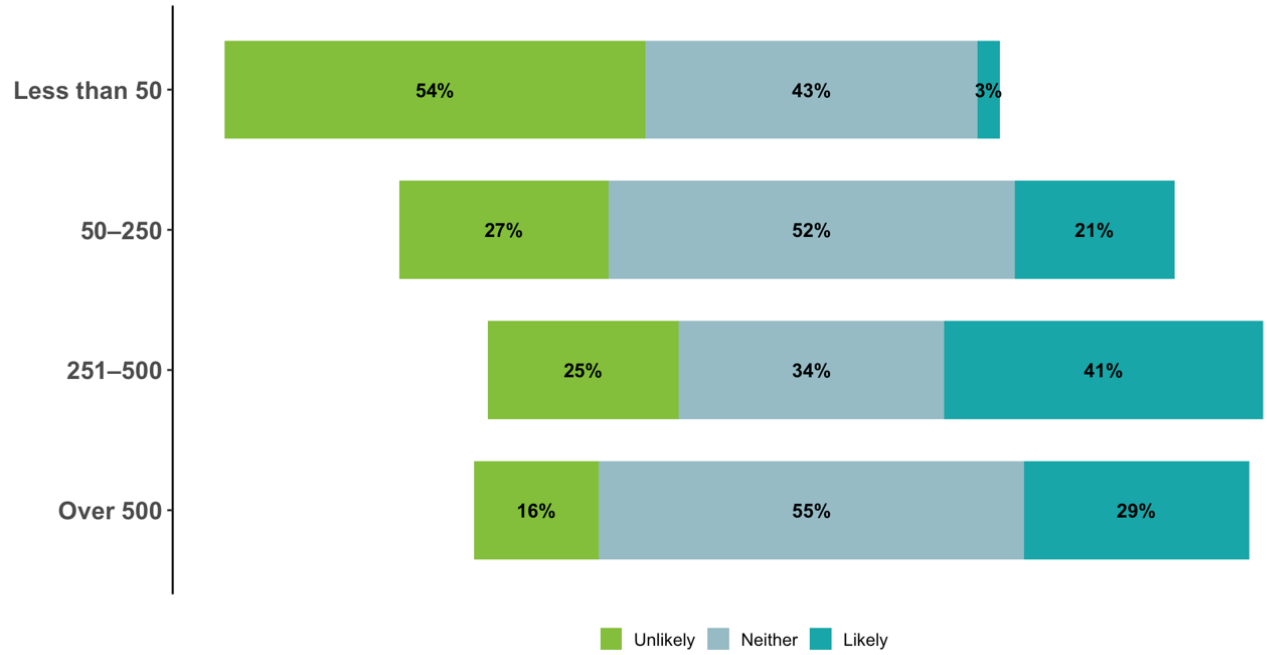

Figure 4. Overall Implementation of Cybersecurity Policies and Practices (n=202).

Notes: *The sample size was 202 respondents.*

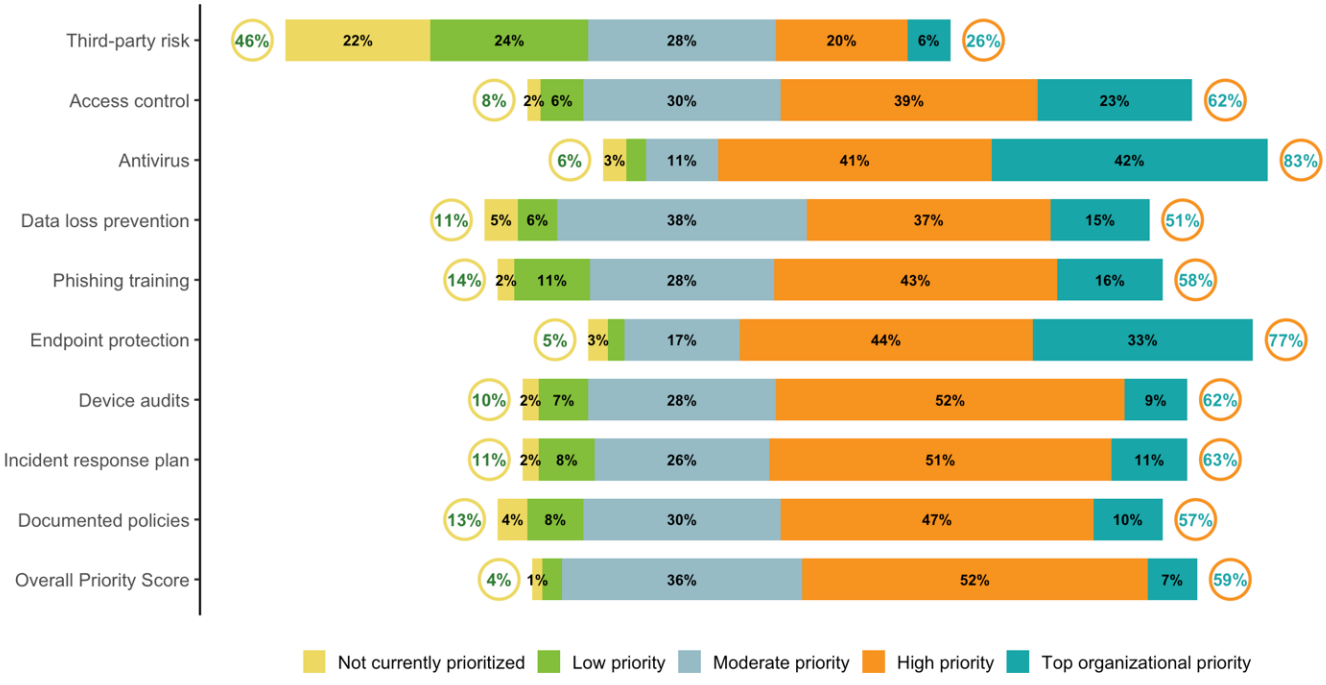

Figure 5. Level of Cybersecurity Priority for Policies and Practices (n=202).

At the same time, priorities are not uniform. Governance functions, such as documented policies and incident response planning, appear most frequently at the top of the scale. Core technical controls, including endpoint protection and access control, are also rated highly but show a wider spread across moderate and high categories. Third-party risk appears less frequently at the highest-priority levels, suggesting that vendor oversight may be less consistently integrated than internal controls.

The nine priority items are strongly related ($\alpha = .85$), indicating that organizations that emphasize one domain tend to emphasize others. Priority thus reflects a general organizational stance rather than a series of isolated decisions. We therefore aggregated the items into an Overall Priority Score that summarizes typical levels of cybersecurity emphasis across policy areas.

Cybersecurity priority is high across organizations of all sizes (see Figure 6). In every firm-size category, most respondents classify cybersecurity as a high priority. The share reporting high priority ranges from just over half of organizations with fewer than 50 employees (51%) to roughly two-thirds of firms with 251–500 employees (66%).

Neutral responses account for most of the remaining responses in each category, ranging from 32% to 45%. Low-priority classifications are uncommon across all firm sizes, never exceeding single-digit percentages. While mid-sized firms (251–500 employees) report the highest concentration of high priority, the differences among size categories are modest. Overall, cybersecurity priority appears broadly high across organizations, with little variation by firm size.

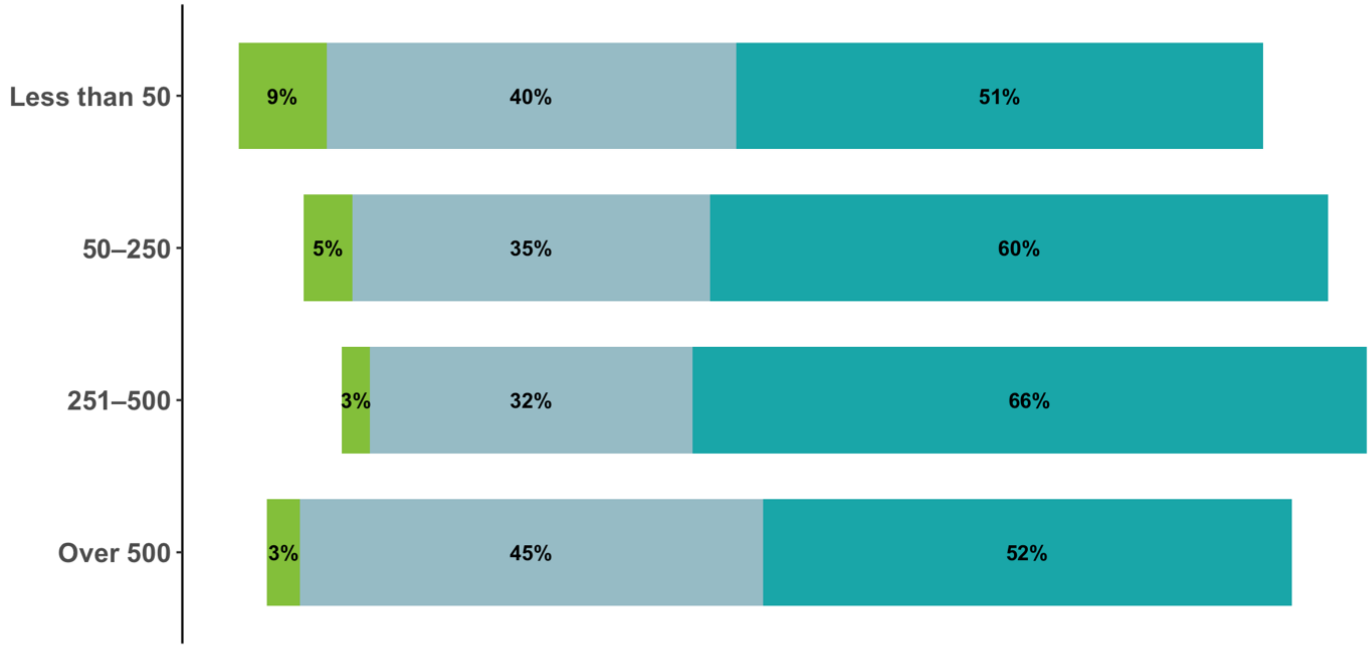

Figure 6. Overall Priorities of Cybersecurity Policies and Practices by firm size (n=202).

Notes: *The sample size was 202 respondents.*

Cyber Maturity

Respondents were asked to assess their organization's cybersecurity maturity. Most organizations place themselves in the middle or upper stages. About 42 percent describe their programs as moderate, and another 36 percent report advanced maturity. Smaller shares report lower levels, with about 18 percent describing their cybersecurity as developing and roughly 4 percent indicating minimal maturity. Overall, the distribution suggests that most organizations view their cybersecurity programs as reasonably established, with relatively few reporting very early-stage capabilities.

Cyber maturity varies somewhat by organizational size, although the differences are modest. Smaller organizations are more likely to report lower levels of cybersecurity maturity, while larger organizations are more likely to report advanced maturity. For example, about 24 percent of organizations with more than 500 employees describe their cybersecurity as advanced, compared with roughly 10 percent of organizations with fewer than 50 employees. At the same time, moderate maturity is common across organizations of all sizes.

Cyber Insurance

Most organizations report having cyber insurance. About 69 percent say their organization carries cyber insurance, while roughly 10 percent report not having it. Another 20 percent are unsure whether their organization has coverage, indicating that insurance decisions often occur at levels not directly visible to technical staff.

Respondents also report significant uncertainty regarding the cost of coverage. Almost two-thirds say they are unsure about their organization's annual premium. Among those who do report a cost, the largest share report premiums of $50,000 or more, while smaller proportions report premiums in lower ranges. Most respondents also indicate that their organization must meet cybersecurity requirements tied to their cyber insurance. About 69 percent report that such requirements exist, while roughly 28 percent are unsure, and only a small share report that no requirements apply.

Cyber insurance adoption varies somewhat across levels of cyber maturity. Organizations with more mature cybersecurity programs are more likely to report having cyber insurance. For example, about 78 percent of firms with moderate maturity report having cyber insurance, compared to about 57 percent of developing organizations. Firms with minimal maturity exhibit the greatest uncertainty about whether they have insurance. Overall, organizations with more mature cybersecurity programs tend to report higher rates of cyber insurance, although the differences between groups are relatively small.

Cybersecurity Influences

One aspect of cybersecurity preparedness we examined was which factors influence firms' cybersecurity policies and practices. Figure 7 shows these sources of influence and their percentage breakdown. Respondents rarely dismiss any source outright; most rate them as "somewhat influential," and a smaller but notable share rate them as "very influential."

Peer networks and professional forums, such as peers inside and outside the industry, cybersecurity consultants, professional conferences, and professional associations, consistently influence firms. Respondents generally rate these sources as "somewhat influential," with steady "very influential" responses, suggesting that these networks shape cybersecurity practices gradually rather than driving immediate changes. Formal authority stands apart. Respondents give state and federal regulations the strongest "very influential" ratings, with insurance policy requirements close behind. Unlike peer or informational sources, regulatory and contractual mandates are more likely to prompt concrete cybersecurity actions.

Informational inputs exert a weaker influence. Respondents most often rate academic papers and industry reports as "somewhat influential," while they usually rate social media as "Not at all influential." In short, professional networks provide information, while regulations more strongly shape cybersecurity practices.

Rather than combining all influence sources into a single index, we grouped them into three areas emphasized in the organizational literature on the diffusion of innovation: mimesis (peer copying), publications (industry and government reports), and associations (professional groups and conferences). This approach aligns the measure with established organizational theory rather than treating all sources as equivalent. We then combined the items within these areas to form an overall influence score ($\alpha = .80$), which showed strong internal consistency and is used in the implementation analysis that follows.

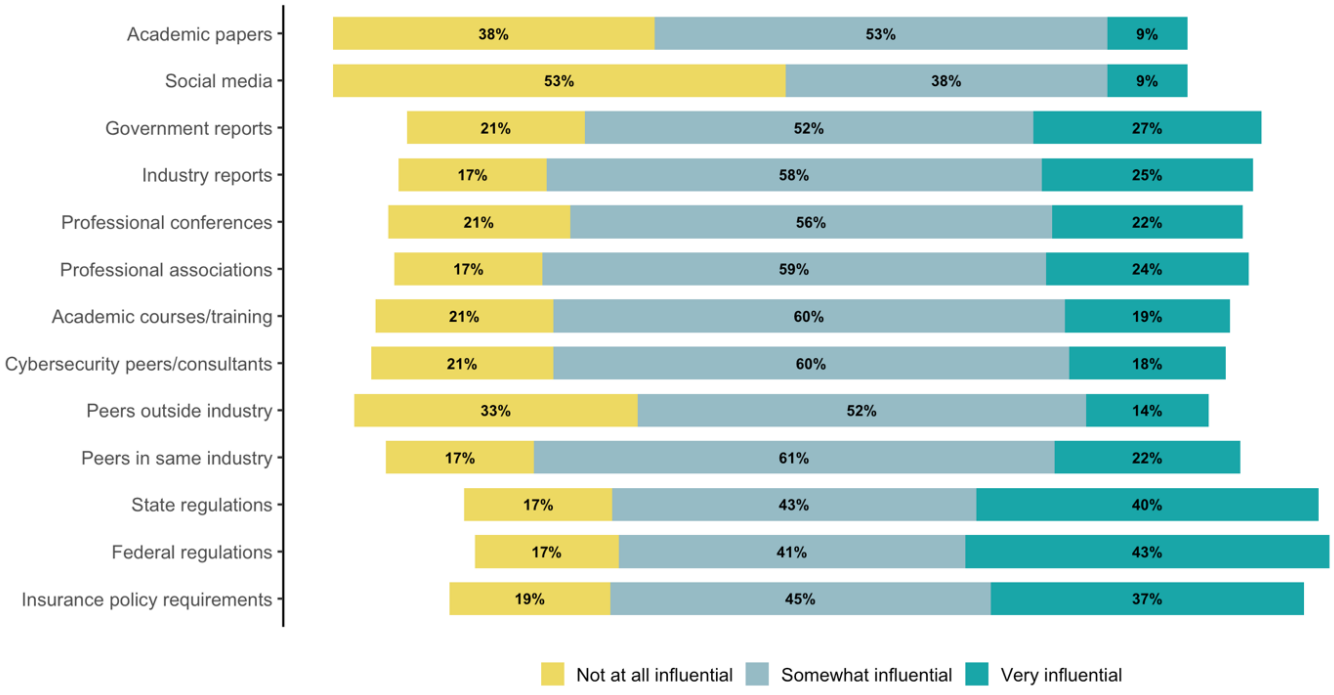

Figure 7. Influences on Cybersecurity Practices (n=202).

Predicting Implementation

We examined which factors are associated with stronger implementation of cybersecurity practices. Implementation is measured using a composite index of cybersecurity policies and operational practices scaled from 0 to 100. The analysis considers several influences simultaneously, including organizational cybersecurity priority, perceived cyber risk, institutional influences such as professional networks and industry guidance, regulatory pressures, firm size, and overall cyber maturity.

Figure 8 illustrates how these factors relate to implementation. Each point represents the estimated change in the implementation score associated with a one-unit increase in the factor. The horizontal lines indicate the statistical uncertainty around those estimates (95 percent confidence intervals). Values to the right of zero suggest factors linked to higher implementation, while those to the left indicate factors associated with lower implementation after accounting for the other variables in the model. When a confidence interval crosses the dashed vertical line at zero, the estimate is not statistically distinguishable from zero.

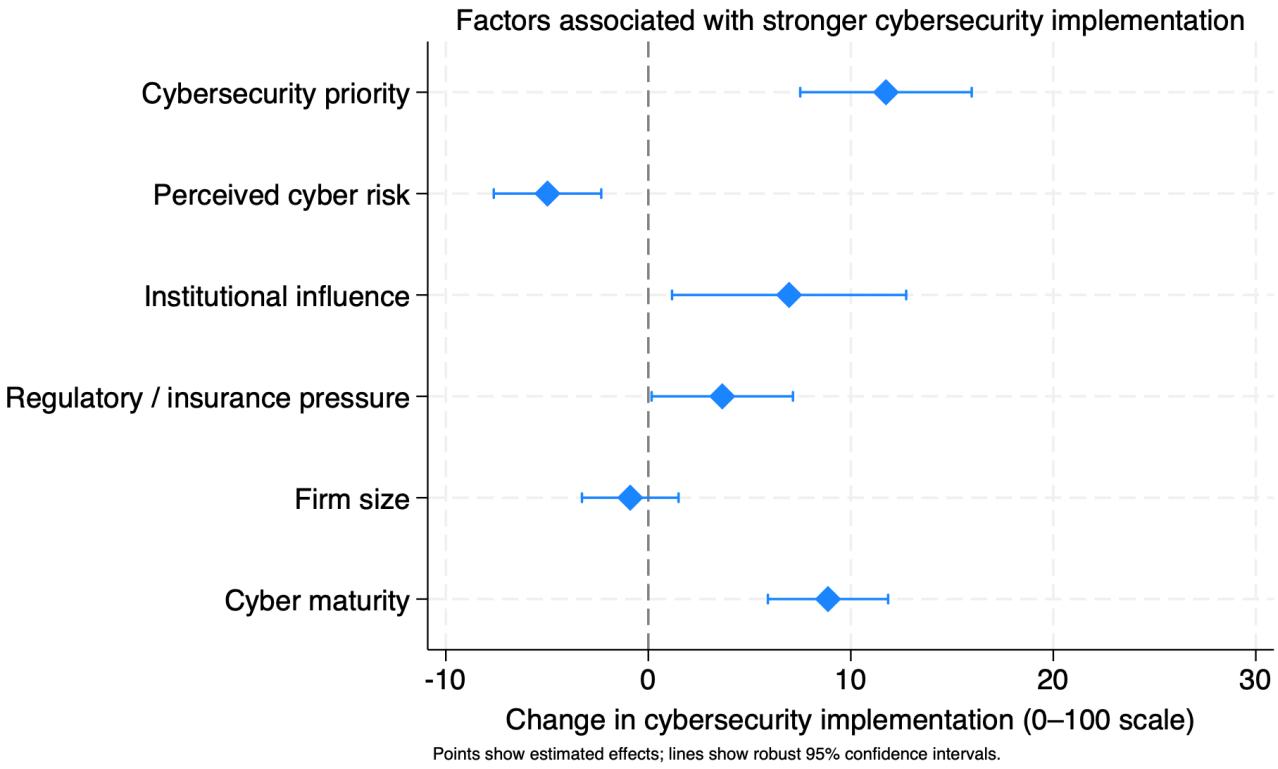

Figure 8. Prediction of Influences on Cybersecurity Implementation (n=202).

Notes: *The dependent variable is the Overall Implementation Score, a composite index from survey items aggregated into a 0–100 index where higher values indicate more complete practices. Independent variables are composite scales from related survey items within each domain, like risk, priority, and institutional influence, measured on the same Likert scales, with higher scores indicating greater levels of the underlying construct. The estimates are from an ordinary least squares regression model, which explains much of the variation in implementation.*

Several patterns emerge. Organizations that place a higher priority on cybersecurity tend to show stronger implementation of cybersecurity practices. Institutional influence, which includes the roles of professional networks, industry reports, and professional associations, is also positively associated with implementation. These results suggest that the organizational environment plays an important role in promoting cybersecurity alongside other organizational factors.

Regulatory and insurance pressures display a similar but somewhat smaller effect. Together, these results suggest that cybersecurity practices are shaped by professional and regulatory environments, where organizations respond to shared expectations, guidance, and external requirements. By contrast, organizations that perceive higher cyber risk tend to report lower implementation, likely reflecting the fact that organizations recognizing weaknesses in their defenses also perceive greater exposure to cyber threats. Firm size shows little independent relationship with implementation once these other factors are taken into account.

Taken together, the results suggest that cybersecurity implementation is shaped by a combination of external institutional pressures and internal organizational commitment. Professional networks, industry guidance, and regulatory signals appear to encourage organizations to adopt cybersecurity practices, while leadership priority and organizational maturity help translate those pressures into concrete operational practices.

The results suggest that efforts to strengthen cybersecurity should focus on reinforcing the institutional environments that influence organizational behavior. Professional networks, industry guidance, and regulatory expectations appear to play a meaningful role in encouraging organizations to adopt cybersecurity practices. Policies that support clear guidance, shared standards, and regular communication through professional associations and industry groups may therefore be especially effective in promoting stronger cybersecurity implementation. At the same time, initiatives that elevate cybersecurity as a strategic priority within organizations and support the development of more mature cybersecurity programs can help translate these external expectations into operational practices. In practice, coordinated efforts among regulators, industry groups, insurers, and professional organizations may be more effective than relying on any single policy lever alone.

CyberBay

UNIVERSITY OF SOUTH FLORIDA / CYBER FLORIDA / BELLINI CAPITAL

CYBERFLORIDA.ORG | 4202 E. FOWLER AVE., TAMPA, FL 33620