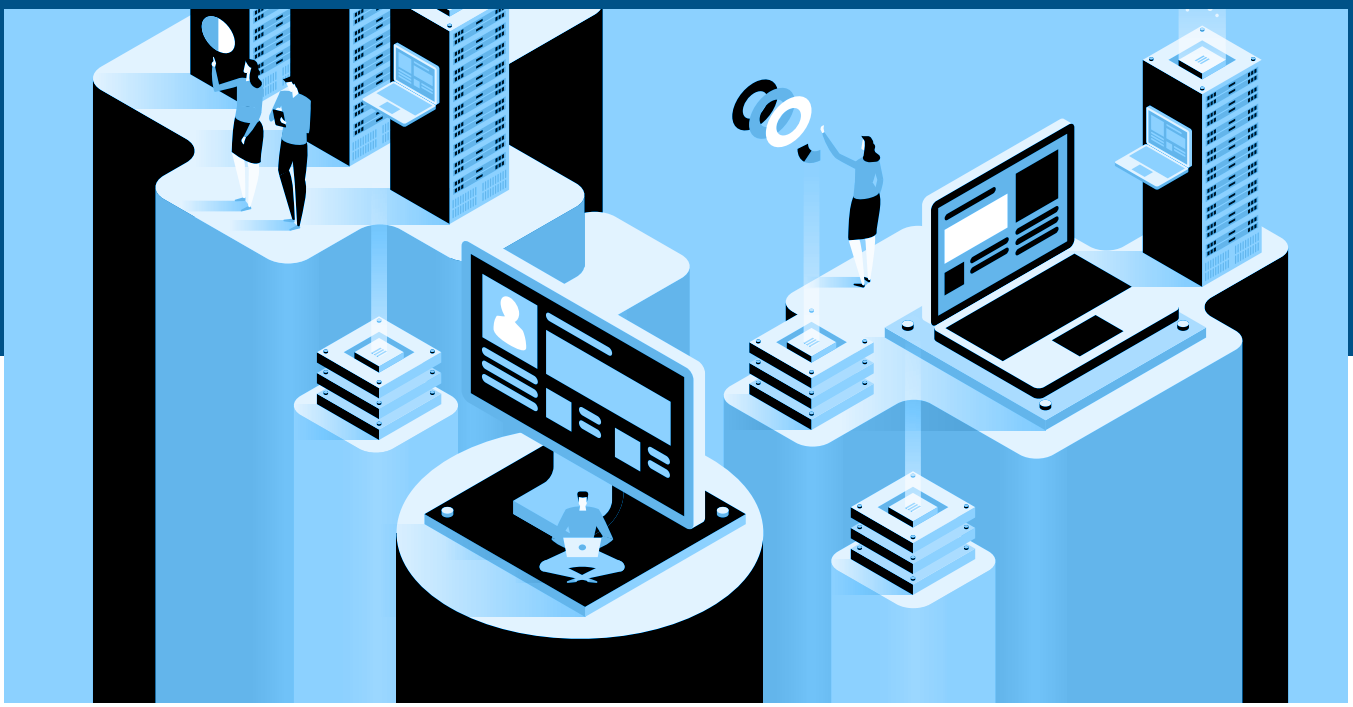
Small & Medium-Sized Business

Cybersecurity Survey

Findings Report
12/2020

Introduction

Cybersecurity is a major priority for all organizations and businesses today. However, small and medium-sized businesses (SMB) often lack the resources and capabilities to adequately protect themselves against a cyber attack. Through a joint effort between industry and government, a survey was administered from October – December 2019 to capture insights from the SMB community on cybersecurity practices, including their use of the NIST Cybersecurity Framework (CSF).



Approximately 100 SMBs responded to the survey, with 50 percent representing IT-related companies with revenues for most of the respondents ranging between from $500K to $30M. The survey findings illustrate their cyber risk perception, familiarity with the CSF, potential barriers to implementing it, their general concerns related to cybersecurity, and how those concerns rank relative to other business priorities. While the initial intent of the survey was to also capture cost effectiveness of using the CSF, data obtained related to cost-specific questions was insufficient.

Results Summary:

1

SMBs identified the top three barriers to implementing the CSF as 1) lack of technical expertise to support implementation, 2) insufficient budget, and 3) lack of specific technical information sources.

2

Thirty-eight percent of the SMB respondents believe it is UNLIKELY that their organization would experience a cyber incident in the next 2-3 years.

— The risk perception translates into lack of attention to cybersecurity and the resulting lack of action.

— This roughly coincides with the share of SMBs that a) use other standards and are not familiar with the CSF or b) does not use any cybersecurity standards or framework.

3

SMB respondents identified the top three cybersecurity focus areas that their organizations could improve upon as 1) training and awareness, 2) incident management and data breach response, and 3) vulnerability management.

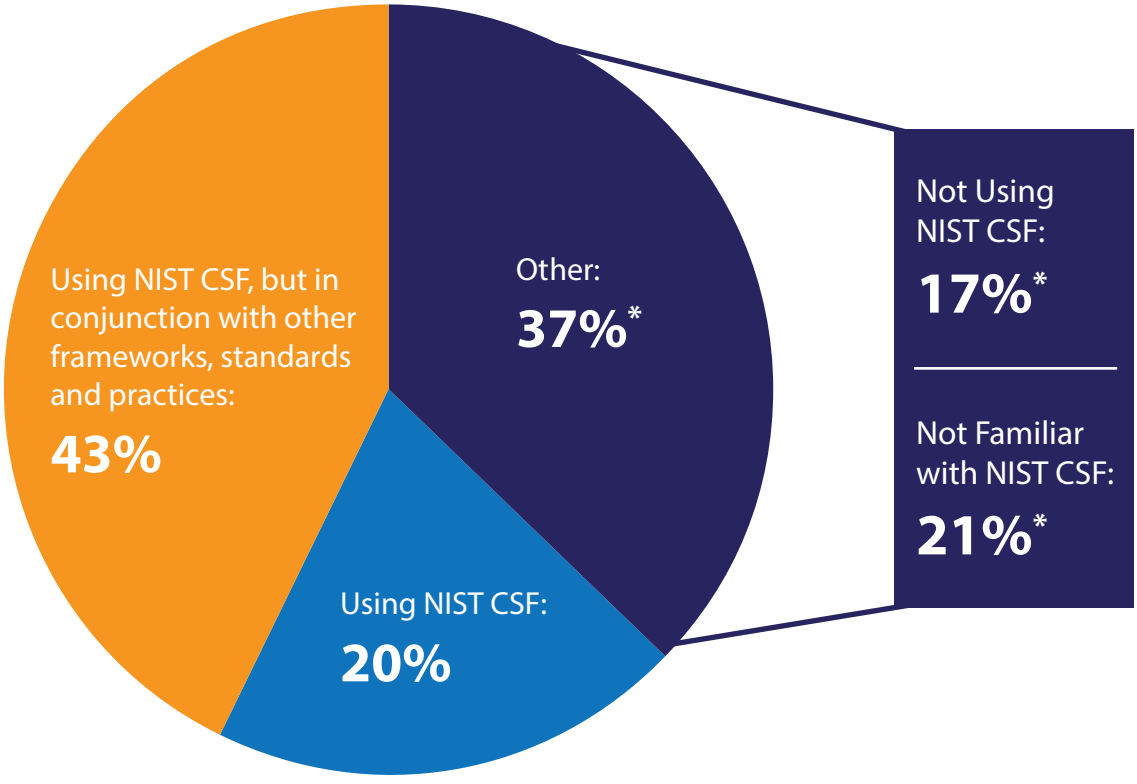


**Chart percentages are represented after rounding up to the nearest tenth.*

Findings Overview:

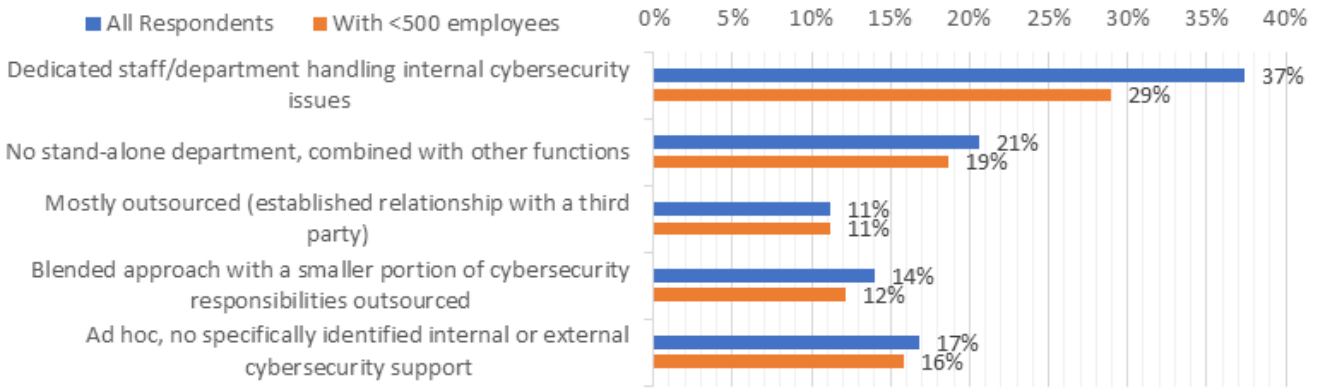
Cybersecurity Maturity

The findings illustrated very little difference in how SMBs with fewer than 500 employees and those with more than 500 employees approach their cybersecurity function. For example, 11% of both groups indicated their company's cybersecurity capabilities are mostly outsourced through an established relationship with a third party.

Thirty-seven percent of SMBs with more than 500 employees indicated they have dedicated staff to address internal cybersecurity issues whereas 29% of SMBs with fewer than 500 employees reported they have those capabilities on their staff.

11%

Outsource Cybersecurity Capabilities



In all categories, SMBs with 500+ employees or less than 500 employees, indicated they had very similar cybersecurity capabilities.

In a related question, when asked if a cyber incident were to occur, how would it be handled, 31% indicated it would be addressed by an ad hoc response underscoring those SMBs do not have the appropriate level of preparedness to respond to a cyber incident.

Not having dedicated cybersecurity resources on their staff is a potential area where CISA can support SMBs, through the existing government and industry partnership. Similar to other efforts, like the development of the Internet of Things (IoT) Acquisition Guidance Document, the SMB Working Group can lead the development of a guidance document and awareness materials that pull together existing resources SMBs can leverage to bolster their current cybersecurity capabilities.

Findings Overview:

Cybersecurity Priorities

When asked to rank their organization's cybersecurity and information security priorities relative to other core business objectives, SMBs indicated that:

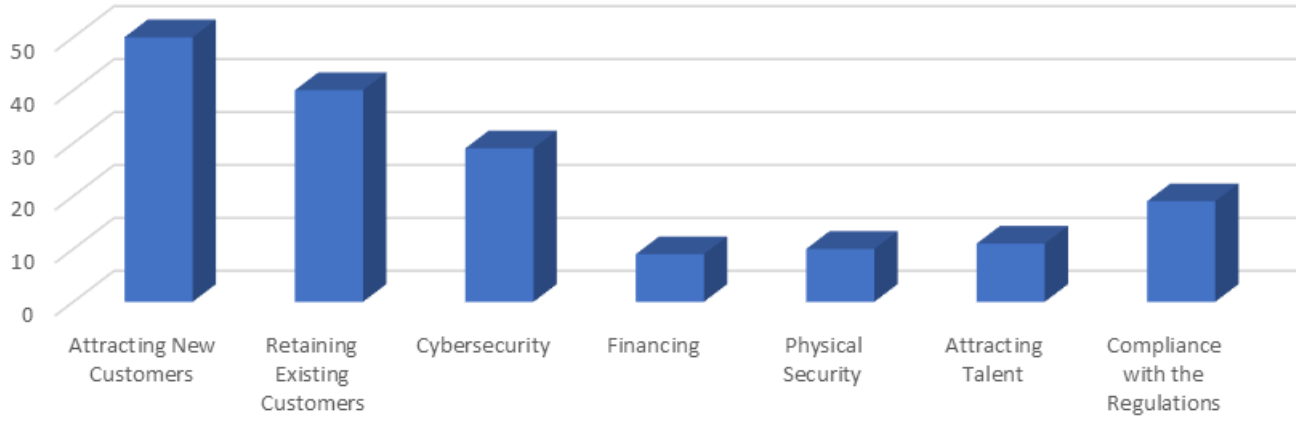
Their top three priorities were:

1) Attracting new customers
2) Retaining existing customers
3) Cybersecurity

Other priorities were listed in the following order:

4) Compliance with regulations
5) Attracting talent
6) Physical security
7) Financing

Business Priorities



Findings Overview:

The breakdown of SMBs not using the CSF reported the following:

13% not familiar with the CSF and do not use any framework or standard

7% not familiar with the CSF and use other frameworks or standards

9% familiar with the CSF and do not use any framework or standard

9% familiar with the CSF and use other frameworks or standards

When asked if they are implementing the CSF, 20% of SMBs indicated they were using it; 43% replied yes, but in conjunction with other frameworks and standards; and 37% indicated they were not using the CSF. As mentioned in the results summary, SMBs identified the top three barriers to implementing the CSF as 1) lack of technical expertise to support implementation, 2) insufficient budget, and 3) lack of specific technical information sources.

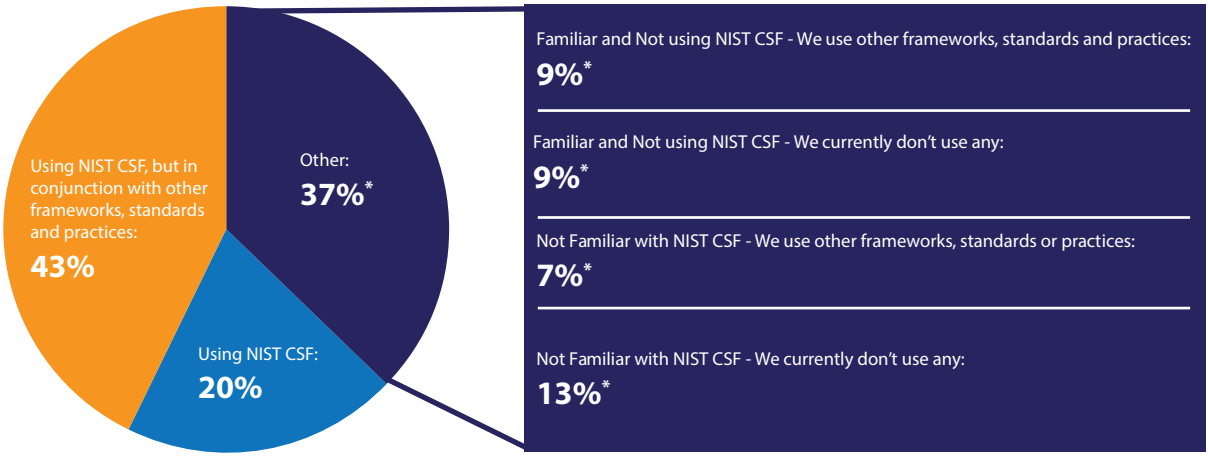


**Chart percentages are represented after rounding up to the nearest tenth.*

Areas for Improvement

SMBs identified the top three cybersecurity focus areas that their organizations could improve upon as 1) training and awareness, 2) incident management and data breach response, and 3) vulnerability management. This also informs potential areas where CISA can provide the most meaningful support to SMBs in addressing the identified gaps.

Conclusion:

Lack of technical expertise and insufficient budget to protect themselves against a cyber attack make small businesses a prime target for cyber criminals. Taking steps to improve their cyber hygiene and understanding where they are vulnerable can be a huge hurdle for SMBs who have limited personnel, ad-hoc approach to incident handling and typically outsource their cybersecurity capabilities to third parties. Feedback from the survey provides insight into the primary challenges faced by the SMB community. This information can serve as the basis for the identification of effective low-cost trainings, tools, accurate information and other resources available from CISA and/or its external partnerships. Sharing this type of information with SMBs, and providing effective tools and resources strengthens CISA's role in supporting the SMB community.

The questionnaire was administered as a voluntary survey where respondent selection procedure is a non-probability sampling method resulting in a convenience sample. The results of the survey should only be interpreted within the context of the number and characteristics of those who responded. No statistical representativeness can be claimed with respect to the survey results. Therefore, statistical inference of the survey results on the rest of the population (beyond the actual survey respondents) is not appropriate.