ISSN: 2473-4901
v11 n6411

Alarming Revelations in Organizational Cyber Security

Kevin J. Slonka
kslonka@francis.edu
Computer Science & Cyber Security Department
Saint Francis University
Loretto, PA 15940 USA

Neelima Bhatnagar
bhatnagr@pitt.edu
Information Sciences Department
University of Pittsburgh
Greensburg, PA 15601 USA

Abstract

This exploratory research surveyed organizations about their cyber security posture in the latter three domains (Functions) of the NIST Cybersecurity Framework (CSF). The data showed alarming insights into critical issues facing organizations of all sizes, such as lack of dedicated cyber security personnel, inability to respond to malicious activity, and inability to recover from malicious activity. With nearly every business sector mandating minimum cyber security requirements as of 2025, the issues reported in this study are not only unacceptable, they are also outright dangerous.

Keywords: cyber, security, organization, uncertainty, vulnerable, dangerous

Alarming Revelations in Organizational Cyber Security

Kevin J. Slonka and Neelima Bhatnagar

1. INTRODUCTION

Cyber threats are of immense concern for all business sectors: from aviation to shipping to healthcare to academia (Badea et al., 2025; Eleimat & Őszi, 2025; Lallie et al., 2025; Żurawski et al., 2025). This concern has been codified by legally binding cyber security regulations being enacted in many sectors, the most recent of which being the Cybersecurity Maturity Model Certification (CMMC) for Department of Defense contractors (the Defense Industrial Base (DIB)) that is estimated to be fully codified in Q4 2025 (Defense Acquisition Regulations System, 2024). Despite the various requirements to implement a basic cyber security program, many organizations choose negligence, opting to direct their dollars to any part of the business except cyber security, even though these regulations most often reflect only the bare minimum cyber security controls required to protect sensitive information (U.S. Department of Defense Inspector General, 2019).

Although business sectors often have their own required cyber security framework/regulation, the NIST Cybersecurity Framework "is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks" (National Institute of Standards and Technology, 2024, p. 1). The NIST CSF serves as a common denominator among the various industry frameworks. Organizations can meet their existing regulations and also map their security control implementation to the CSF in order to improve the experience of cross-industry collaboration. It was for this reason that the NIST CSF is often chosen as the framework of choice for research studies, such as a recent study (Chidukwani et al., 2022) that suggested further investigation into organizational implementations in three of the six core Functions (Detect, Respond, and Recover) and examining the differences across varying business sizes.

Thus, the research questions for this study are as follows:

R1. What are the differences in the implementations of security controls in the Detect, Respond, and Recover Functions of the NIST CSF between organizations of different size?

R2. What are the differences in the implementations of security controls in the Detect, Respond, and Recover Functions of the NIST CSF between organizations of different business sectors?

2. REVIEW OF THE LITERATURE

Cyber security frameworks give organizations a structured approach to managing and mitigating cyber risk. Not only do frameworks provide guidelines and best practices, but they enable organizations to have consistent and repeatable processes. While some organizations must comply with certain frameworks to meet legal regulations, adhering to a cyber framework is essential for organizations to keep their data secure with the continuing evolution of cyber threats (Tolulope, 2024).

Common Frameworks

The NIST Cybersecurity Framework (CSF) is perhaps the most popular framework, assisting organizations to protect against both internal and external threats. Initially designed for critical infrastructure (e.g., power plants, dams, etc.), the CSF helps businesses of all sizes better understand, manage, and reduce their cyber risk (Kidd, 2024; National Institute of Standards and Technology, 2024). According to Tolulope (2024) this framework focuses on cybersecurity risk management and is a broad framework adaptable across industries for organizations of all sizes looking for flexibility. Its key features include six core functions: govern, identify, protect, detect, respond, and recover.

The ISO/IEC 27001 framework focuses on information security management and is best suited for organizations that need to be ISO 27001 certified. It is an internationally recognized framework that focuses on the CIA triad (confidentiality, integrity, and availability). In addition, this framework is applicable across varying business sectors and is widely adopted (International Organization for Standardization, 2022).

The Center for Internet Security (CIS) Controls framework is another option for organizations that are starting out with only basic cyber security in place. Created to help protect organizations that do not necessarily have to meet other, more robust, frameworks or regulations, CIS Controls

is effective on its own or when paired with other frameworks. The guidance is split into a basic and an advanced benchmark level and into three control groups: basic, foundational, and organizational (Center for Internet Security, 2025).

The Payment Card Industry Data Security Standard (PCI-DSS) framework focuses on payment card data protections and is ideal for payment processing and cardholder data. It is suitable for organizations handling payment card transactions, such as retail transactions, and has 12 core requirements (PCI Security Standards Council, 2024).

The Health Insurance Portability and Accountability Act (HIPAA) is the main regulation mandated for those working with Protected Healthcare Information (PHI). It focuses on the privacy of medical records and other healthcare data (U.S. Department of Health and Human Services, 2024). Building on HIPAA is the Health Information Trust Alliance Common Security Framework (HITRUST CSF). This framework combined HIPAA, HITECH (an addition to HIPAA), and other regulations making it a comprehensive solution for any healthcare organization (HITRUST, 2025).

The Control Objectives for Information and Related Technologies (COBIT) framework, initially released in 1996, was developed by ISACA "in response to the growing concerns of computer systems" (Taherdoost, 2022, p. 8). It should be used by organizations in need of strong IT governance, with its features including aligning with IT strategy and business goals (ISACA, 2025).

The Cybersecurity Maturity Model Certification (CMMC) program encompasses a three-tiered model based on the NIST SP 800-171 framework for setting the minimum baseline of security within the Defense Industrial Base (DIB). It is used for organizations that store, process, and transmit both Federal Contract Information (FCI) as well as Controlled Unclassified Information (CUI). The main feature of this program is the third-party assessment requirement, ensuring that organizations cannot be awarded Department of Defense (DoD) contracts unless their organization's security has been certified by a third-party, removing the allowance of self-assessment for the majority of contractors (Department of Defense Chief Information Officer, n.d.).

Cyber Attacks

Month after month, more companies fall victim to various cyber attacks. United Natural Foods, North Face, Cartier, Zoom Car, Episource, WestJet, and The Washington Post were just some of the organizations breached during the month of June 2025 (Cyber Management Alliance, 2025). Whether these organizations failed to have the right people, implement the right processes, or conduct the proper preparation, the end result was always a loss of revenue or the exposure of customer information.

Baker (2024) lists the most common cyber attacks as Malware, Denial-of-Service (DoS) Attacks, Phishing, Spoofing, Identity-Based Attacks, Code Injection Attacks, Supply Chain Attacks, Social Engineering Attacks, Insider Threats, DNS Tunneling, IoT-Based Attacks, and AI-Powered Attacks. Some of these have been on display over the years as some of the worst cyber attacks ever. The WannaCry ransomware affected more than 200,000 computers in over 150 countries in 2017. The NotPetya virus caused billions of dollars in damage during the same year. When Equifax was breached, the private information of 147.9 million Americans (plus countless millions from other countries) was stolen. A comprehensive cyber security strategy, such as one that includes any of the aforementioned frameworks, could have helped prevent many of these and is critical to remaining safe.

Small and Medium Businesses

Chidukwani et al. (2022) noted that large percentages of countries' economies are not large businesses, but small and medium businesses. They further noted that these businesses often do not have mature cyber security programs (or any at all), frequently barely complying with the first two Functions in the NIST CSF. With very little research presently conducted on small and medium businesses' ability to detect, respond to, and recover from cyber attacks, this study will attempt to contribute.

3. METHODOLOGY

An online survey was developed to elicit the cyber readiness of organizations in the last three Functions (domains) of the NIST CSF (Detect, Respond, & Recover) in an effort to fill the gap noted by Chidukwani et al. (2022). This was to answer the study's research questions:

R1. What are the differences in the

implementations of security controls in the Detect, Respond, and Recover Functions of the NIST CSF between organizations of different size?

R2. What are the differences in the implementations of security controls in the Detect, Respond, and Recover Functions of the NIST CSF between organizations of different business sectors?

The survey, presented in full in Appendix A, began with consent and was followed by four demographic questions:

- Do you fulfill one of the following roles within your organization (this may be a dual role and not necessarily your primary job)?
- Is the previously selected role one of multiple roles you fulfill in your organization (e.g., you are the Principal Architect but also act as IT Support)?
- Please select the best fit for the size of your organization.
- Please select the best fit for the business sector of your organization (based on NAICS code).

Following the demographics were three series of Yes/No/Not Sure questions. These survey items map to each of the Subcategories within each of the three Functions and ask the participant whether or not their organization implements the specific security control. Each survey item was a simple rewording of the item from the CSF in question form. The Detect Subcategory contained 18 survey items, the Respond Subcategory contained 16 survey items, and the Recover Subcategory contained six survey items.

The survey was distributed in a snowball fashion, starting with the local contacts of the researchers (e.g., chambers of commerce, cyber/IT industry groups, business contacts, etc.) followed by posts on social media cyber/IT groups. This led to a starting N=62.

Data Cleaning

The consent and the first demographic question acted as the first method of removing participation. After removing those responses that did not consent, did not work in an IT, Cyber, or Management role, or did not progress beyond this point in the survey, the remaining responses were N=52.

One last cleanse was performed to remove those participants who did not complete the entire survey. This led to a final N=29.

Data Recoding

10 additional variables were added to the dataset as recodes of the participant responses. The first three variables were the raw percentage of each Function's implementation based on the "Yes" answers to that Function's survey items. The fourth new variable was a Total Security variable, calculated as the average of the previous three Function implementation variables. The fifth numeric variable was the Uncertainty Index, calculated as the raw percentage of "Not Sure" answers across all Functions. Though not a data point included in the research questions, analyzing the number of "Not Sure" answers will add a helpful dimension to the explanation of the results.

The remaining five variables were all nominal (categorical) in nature. The three new Function implementation variables were recoded into four equal categories (0-25%, 26-50%, 51-75%, 76-100%). The Total Security variable was recoded into five categories (0-10%, 11-25%, 26-50%, 76-89%, 90-100%) to better showcase the data at the extremes. Lastly, the Uncertainty Index was recoded into four categories (No Uncertainty, 0-19%, 20-49%, 50-100%).

An important note is that though these variables contain the word "total" they do not represent the organizations' entire cyber posture since only three of the CSF Functions were studied. All data from this study can only represent the portion of an organization's cyber posture based on the three Functions.

Statistical Approach

Due to the low number of valid responses (N=29), relying on the typical quantitative statistical methods alone (e.g., T-Test, ANOVA, etc.) may not result in much. Significant results would only detect large effect sizes in such a sample. As such, the majority of this exploratory research's contribution is noting findings from the descriptive data (Isaac & Michael, 1995).

Statistical methods were utilized, however, to uncover any large effects. Chi Square, ANOVA, and Pearson Correlation tests were run against all appropriate variables (note the parametric tests due to the assumption of normality of the data because of the small sample size).

4. RESULTS & DISCUSSION

Demographics

The data set for this study (N=29) consisted of

responses from approximately 75% IT/Cyber staff and 25% senior management. Surprisingly, 65.5% of the respondents said that they wear multiple hats within their organization. This data is shown in Table 1.

Role	
IT/Cyber Security	22
Senior Management	7
Serve in Multiple Roles	
Yes	19
No	10

Table 1: Employee Roles & Multi-Roles

What is even more surprising is that of the 22 IT/Cyber Security participants, 14 (63%) acknowledged that IT/Cyber Security is not their only role. Five of the 7 (71%) senior managers acknowledged that they, too, have responsibilities beyond their management role. While this may not come as a shock in the year 2025, where companies are constantly trying to do more with less, the lack of employees focusing the entirety of their attention on their organization's cyber security posture is a stark foreshadowing of this study's remaining findings.

Table 2 displays the remaining demographics of the participant population, mapping the business sector in which the organization operates, based on U.S. Bureau of Labor Statistics (2022), to the size of the organization, based on Gartner (2022).

	Small	Medium	Large	**TOTAL**
Manufacturing	0	2	2	4
Trade, Transport, Utilities	2	0	3	5
Information	1	2	1	4
Financial Activities	0	0	2	2
Prof./Business Services	1	2	2	5
Education/Health Services	1	1	4	6
Leisure/Hospitality	0	1	1	2
Other Services (Charity)	1	0	0	1
TOTAL	6	8	15	29

Table 2: Business Sector by Size

Revisiting the dual-role employees based on the size of their organization, eight of the 15 (53%) employees of large businesses acknowledged that they have multiple roles, an alarming finding that should not occur given the massive revenue of such organizations. To make matters worse, all eight (100%) of those employees were IT/Cyber Security employees, suggesting that even large businesses may not place enough value on their cyber security posture to dedicate full-time employees.

Uncertainty

The 40 survey items covering the three Functions of the NIST CSF investigated in this study had three possible answers: Yes (i.e., my company implements this cyber security practice), No (i.e., my company does not implement this cyber security practice), and Not Sure. Participants were instructed that, if they were not absolutely certain of the Yes or No answer, they should select Not Sure. This allowed the researchers to not only have a more precise measure of an organization's security but also provide a metric for organizations that are unaware of their security posture.

Tables 3 and 4 depict the level of uncertainty (Total Uncertainty variable) split by role and by organization size.

	None	< 20%	20-49%	>=50%
IT/Cyb	7	10	4	1
Mgmt	1	4	1	1

Table 3: Uncertainty by Role

	None	< 20%	20-49%	>=50%
Small	2	2	1	1
Medium	3	2	2	1
Large	3	10	2	0

Table 4: Uncertainty by Org Size

While the majority of organizations have less than 20% uncertainty about their security posture, it is disheartening to see that four IT/Cyber personnel are 20-49% uncertain and one is above 50% uncertain. While it is misguided to say that senior management is less uncertain than IT/Cyber personnel (given that management often lacks the detailed awareness to justify such an opinion), the number of IT/Cyber personnel with uncertainty is cause for trepidation.

The last measure of uncertainty is comparing organizations' total security with their level of uncertainty. Table 5 presents some information that was expected as well as some information that was not expected. The majority of organizations that were fairly certain about their security (i.e., 20% or less uncertainty) exhibited the highest level of security. One could reasonably assume that would be the case. The same can be said for the opposite case; as uncertainty increases total security decreases. The unexpected data from Table 5 is there are seven organizations that are fairly certain (i.e.,

20% or less uncertainty) that list themselves as less than 50% secure. To state that another way, these organizations know they are insecure.

		Total Security					
		0-10%	11-25%	26-50%	51-75%	76-89%	90-100%
Uncertainty	None	1	0	2	0	0	5
	< 20%	1	2	1	3	3	4
	20-49%	0	2	1	2	0	0
	>=50%	0	1	1	0	0	0

Table 5: Uncertainty by Total Security

Security Implementation

Another interesting view of total security is by organization size. The data in Table 6 aligned with the researchers' preconceived notions, given their experience. Small organizations, those that typically do not have dedicated IT/Cyber personnel exhibited the least security while large organizations, those that typically do have dedicated IT/Cyber personnel exhibited the most security. Medium-sized businesses were evenly split across the total security spectrum.

		Total Security					
		0-10%	11-25%	26-50%	51-75%	76-89%	90-100%
Size	Small	1	3	2	0	0	0
	Medium	1	1	2	1	1	2
	Large	0	1	1	4	2	7

Table 6: Size by Total Security

While looking at an organization's total security score in summary is useful, it is also useful to look at the scoring per Function. Appendix B Table 1 shows organizational total security scores per Business Sector broken down by Function. 16 organizations rated themselves in the highest bracket for the Detect category, but only 11 rated themselves in the highest bracket for both the Respond and Recover categories. This suggests that the small majority (55%) of organizations are capable of detecting malicious activity on their network, but many are not able to do anything about it. 11 (38%) organizations rated themselves as 50% or below for the Respond category and 16 (55%) organizations rated themselves at 50% or below for the Recover category. The sharpest decline was the Education and Health Services sector, which had 4 of the 6 organizations in the top tier for Detect but only 2 in each of Respond and Recover. While there is not enough data to say that any particular business sector is better than any other, the finding suggests that organizations do not invest enough resources in being able to stop malicious activity once it starts and then being able to recover their business operations.

Appendix B Table 2 shows similar information, except broken down by organization size. This paints a much clearer picture, clearly showing that small organizations are worse off in all three Functions than their medium and large counterparts. Interestingly, large organizations seem to suffer the same fate as seen in the previous table: they are good at detecting malicious activity but not good at responding to or recovering from it.

Statistical Analysis

As originally described in the methodology section, statistical tests, such as Chi Square, ANOVA, and Correlations were run on all appropriate variables. Though significant findings will not imply generalizability, they will offer credence to some of the above descriptive data explanations.

The first significant finding came by comparing the raw Function percentages against organization size. Chi Square tests were initially run to see if any significant findings occurred with this low power test. One test had a significant result: comparing the implementation rate for the Detect Function against organization size, shown in Table 7. Detect implementation was used in two ways: the categorical variable for the Chi Square and the raw percentage for the ANOVA. The significant differences from the Chi Square test existed between the Small and Large organizations for the 0-25% implemented category and between both Small/Large and Medium/Large for the 76-100% category.

Test	Significance/Value
Chi Square	.002
Cramer's V	.593 (Large)
ANOVA	<.001
Eta squared	.583 (Large)

Table 7: Detect % by Organization Size

Although, as previously explained, all significant

results should be viewed as having a large effect size due to the population size, Cramer's V was also run to corroborate. The resulting Cramer's V value also showed the effect size as large, meaning that this finding is clearly visible to the naked eye.

Any time a Chi Square test finds a significant result it is always prudent to run a higher power test (if the data allows) to see if it also finds significance. An ANOVA test was run and also found a significant result. The test found that significant differences existed between all sizes of organizations. These differences are clearly seen in the data, with Large organizations reporting much higher implementations of items in the Detect Function than Small or Medium organizations.

Test	Significance/Value
Chi Square	.026
Cramer's V	.604 (Large)

Table 8: Total Security by Business Sector

The only other test to have significant results was comparing an organization's Total Security (the categorical variable) by Business Sector, shown in Table 8. This test also produced a Cramer's V value suggesting a Large effect size but was unable to determine between which groups the significant difference occurs. Comparing these variables (swapping the categorical Total Security variable with the raw percentage) with the ANOVA test, unfortunately, did not find significance, so this result may not be as meaningful.

No correlation tests returned significant results.

5. CONCLUSION

Limitations

As previously stated, the small sample size was the main limitation of this study. Given that this study only found two significant differences, the reader could draw one of two conclusions: either the study is correct (there are very few differences between the groups studied) or the study is erroneous and more significant differences exist that were not found (Singh & Masuku, 2014).

Study Significance

This study stands as the first study to analyze the Detect, Respond, and Recover Functions as they are implemented by organizations and offer insight into potential deficiencies that need addressed. The number of employees in both cyber and managerial positions who are unsure about their organization's cyber security posture and the number of unmet controls reported by organizations depicts an embarrassing truth about organizations in the United States: they are vulnerable to attack and will not be able to recover. The researchers hereby call on industry to revisit their priorities, realign their resources, and bring their cyber security posture up to a minimum level capable of withstanding the attacks of 2025.

Future Research

More studies need to be conducted in this critical area. A replication of this study with a much larger sample size should be the start; however, deeper research needs conducted into each of the CSF Functions to understand if organizations are actually failing to implement the security controls, understand why organizations are failing to do so, and offer suggestions for becoming more secure.

9. REFERENCES

Badea, M., Bucoveţchi, O., Gheorghe, A. V., & Raicu, G. (2025). Cyberattacks on port infrastructures: A decade of trends, incidents, and mitigation strategies (2011-2024). *Land Forces Academy Review, 30*(2), 175-189. ☐ https://doi.org/10.2478/raft-2025-0017

Center for Internet Security. (2025). *CIS Critical Security Controls*. https://www.cisecurity.org/controls

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access, 10*, 85701-85719.

Cyber Management Alliance. (2025, July 1). *Major cyber attacks, ransomware attacks and data breaches of June 2025*. https://www.cm-alliance.com/cybersecurity-blog/major-cyber-attacks-ransomware-attacks-and-data-breaches-of-june-2025

Defense Acquisition Regulations System. (2024, August 15). *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)*. Federal Register. https://www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

Department of Defense Chief Information Officer. (n.d.). *About CMMC*. https://dodcio.defense.gov/cmmc/About/

Eleimat, M. & Őszi, A. (2025). Cybersecurity in aviation: exploring the significance, applications, and challenges of cybersecurity in the aviation sector. *Periodica Polytechnica Transportation Engineering, 53*(2), 169-183. https://doi.org/10.3311/PPtr.37153

Gartner. (2022, December 28). *Small and midsize business (SMB)*. https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses

HITRUST. (2025, April). *HITRUST CSF: Our cybersecurity framework.* https://hitrustalliance.net/hitrust-framework

International Organization for Standardization. (2022). *ISO/IEC 27001:2022*. https://www.iso.org/standard/27001

Isaac, S. & Michael, W.B. (1995). *Handbook in Research and Evaluation*. San Diego: EdITS.

ISACA. (2025). *COBIT: An ISACA framework*. https://www.isaca.org/resources/cobit

Kidd, C. (2024, October 9). *Cybersecurity frameworks: What they are & how to use them*. https://www.splunk.com/en_us/blog/learn/cybersecurity-frameworks.html

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), 1-28. https://doi.org/10.3390/computers14020049

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf https://doi.org/10.6028/NIST.CSWP.29

PCI Security Standards Council. (2024, June). *Payment Card Industry Data Security Standard: Requirements and testing procedures version 4.0.1*. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Singh, A. S. & Masuku, M. B. (2014). Sampling techniques & determination of sample size in applied statistics research: An overview. *International Journal of Economics, Commerce & Management, 2*(11), 1-22.

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards: A review and comprehensive overview. *Electronics, 11*(14), 1-20. https://doi.org/10.3390/electronics11142181

Tolulope, M. (2024, August 13). *Cybersecurity frameworks comparison: 10 common frameworks*. https://tolumichael.com/cybersecurity-frameworks-comparison/

U.S. Bureau of Labor Statistics. (2022, December 28). *Industries by supersector and NAICS code*. https://www.bls.gov/iag/tgs/iag_index_naics.htm

U.S. Department of Defense Inspector General. (2019). *Audit of protection of DoD controlled unclassified information on contractor-owned networks and systems*. https://media.defense.gov/2019/Jul/25/2002162331/-1/-1/1/DODIG-2019-105.PDF

U.S. Department of Health and Human Services. (2024, July 19). *HIPAA for professionals*. https://www.hhs.gov/hipaa/for-professionals/index.html

Żurawski, S., Chodyka, M., Nowicka, J., Grudniewski, T. M., Dawidziuk, R., & Gralak, K. (2025). The impact of cyberthreats on the security of important sectors of the economy on the example of the healthcare sector. *European Research Studies Journal, 28*(2), 150-162.

APPENDIX A
Survey Instrument

Demographics
Do you fulfill one of the following roles within your organization (this may be a dual role and not necessarily your primary job)?

- IT/Cyber Security
- Senior management (C-Suite or equivalent for smaller organizations)
- Risk/Compliance/Public Relations
- I am not working in one of the above roles

Is the previously selected role one of multiple roles you fulfill in your organization (e.g., you are the Principal Architect but also act as IT support)?

- Yes
- No

Please select the best fit for the size of your organization.

- Small (less than 100 employees and/or less than $50m in revenue)
- Medium (less than 1000 employees and/or less than $100m in revenue)
- Large (greater than 1000 employees and/or greater than $100m in revenue)

Please select the best fit for the business sector of your organization (based on NAICS code).

- Natural Resources and Mining
- Construction
- Manufacturing
- Trade, Transportation, and Utilities
- Information
- Financial Activities
- Professional and Business Services
- Education and Health Services
- Leisure and Hospitality
- Other Services (except Public Administration) - please specify

Detect
Domain: Detect - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Please only select Yes or No if you are certain; otherwise, select Not Sure.

	Yes	No	Not Sure
My organization has a baseline of normal IT systems activity so they can easily detect anomalous activity.			
Once anomalous activity is detected, my organization will analyze the activity to determine if it is malicious.			
My organization pieces together anomalous activity detected by multiple systems throughout the organization to build a bigger picture.			
After anomalous activity has been analyzed, my organization determines the impact of the events causing the activity.			
My organization sets a proper level for activity alerts to lessen false positives while still being able to detect malicious activity.			
My organization's computer network is monitored by systems able to detect possible malicious activity.			
My organization's physical buildings are monitored (guards, video cameras, etc.) to detect possible malicious activity.			
My organization monitors the actions of its employees (physically and digitally) to detect intentional or unintentional sensitive information disclosure.			

My organization has technical means of detecting malicious software, such as viruses.			
My organization has technical means of detecting malicious mobile code, such as Adobe Flash, Powershell, or JavaScript (this is different from the previous question on viruses).			
When my organization receives technical support from external service providers (e.g., allowing an application company's technical support into your system) the activity of the external service provider is monitored to prevent malicious activity.			
My organization's computer systems monitor for users connecting unauthorized devices, installing unauthorized software, etc.			
My organization regularly runs vulnerability scans on its systems to ensure no new vulnerabilities have been introduced.			
My organization's cyber security staff have clearly defined roles and responsibilities for detection of malicious activity.			
My organization's malicious activity detection is at the appropriate level for all applicable laws and compliance frameworks by which we have to abide.			
My organization simulated malicious activity to test their detection processes.			
When my organization detects malicious activity, that information is properly communicated to the appropriate parties as well as the whole of the organization for awareness purposes.			
My organization constantly updates its malicious activity detection processes to ensure new threats are taken into account.			

Respond
Domain: Respond - Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Please only select Yes or No if you are certain; otherwise, select Not Sure.

	Yes	No	Not Sure
My organization has a written plan for responding to an active cyber incident and executes it accordingly.			
The employees at my organization with IT responsibilities understand their specific role(s) when a cyber incident is detected.			
Cyber incidents at my organization are reported to the appropriate authorities (whether internal IT staff or external entities due to legal obligations) in a timely manner after detection.			
Necessary information about cyber incidents is shared within my organization (e.g., informing IT staff for protection measures or informing the organization at-large for awareness/prevention measures).			
Activities about cyber incidents is coordinated with all necessary aspects of the organization (e.g., IT, management, Compliance, PR, etc.).			
My organization shares information and lessons learned from cyber incidents to external entities in order to help inform others about current cyber threats.			
My organization has trained cyber security staff that investigates each alert from the organizational threat detection system.			
Every cyber incident is analyzed not only for its impact on technical systems but also on business processes/goals.			

When a cyber incident occurs, my organization captures any malicious files/software used in the incident in order to analyze and determine the attacker's tactics, techniques, and procedures.			
Every cyber incident is correctly categorized by my organization's cyber staff so that an appropriate response can occur.			
My organization has trained cyber security staff that follows written, approved procedures for responding to cyber issues reported by both internal employees and external watchdog sources.			
My organization's cyber security staff is able to contain all cyber incidents that occur so that the organization is not affected.			
My organization's cyber security staff actively protects our network so that cyber incidents never occur.			
When new cyber threats are identified, my organization's cyber security staff quickly acts to implement protections if necessary.			
After every cyber incident my organization's cyber incident response plan is updated to include newly learned lessons and best practices.			
As new strategies develop in the global threat landscape my organization integrates those new strategies into its cyber incident response plan.			

Recover
Domain: Recover - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Please only select Yes or No if you are certain; otherwise, select Not Sure.

	Yes	No	Not Sure
My organization has a written plan for recovering after a cyber incident and executes it accordingly.			
My organization's recovery plan is constantly changing, incorporating lessons learned from past cyber incidents.			
As technologies change my organization updates its recovery plan to ensure the fastest recovery with the least amount of loss.			
When cyber incidents occur that affect sensitive data my organization's public relations officials properly handle our public narrative.			
My organizational officials quickly work to repair any reputational damage that may have occurred because of a cyber incident.			
When my organization's recovery plan is being executed all stakeholders, internal and external, are kept in the communication loop at all phases.			

APPENDIX B
Tables Referenced in the Body

D=Detect, R=Respond, V=RecoVer	0-25%			26-50%			51-75%			76-100%		
	D	R	V	D	R	V	D	R	V	D	R	V
Manufacturing	0	1	1	1	0	0	0	0	0	3	3	3
Trade, Transportation, and Utilities	1	3	3	1	0	0	1	0	0	2	2	2
Information	1	0	2	0	0	0	1	2	1	2	2	1
Financial Activities	0	0	0	0	0	0	0	1	0	2	1	2
Professional and Business Services	0	0	1	0	2	2	3	2	1	2	1	1
Education and Health Services	1	1	1	0	1	3	1	2	0	4	2	2
Leisure and Hospitality	1	2	2	0	0	0	0	0	0	1	0	0
Other Services (Charity)	0	1	0	1	0	1	0	0	0	0	0	0

Table 1: Business Sector by Security Percentage per Function

D=Detect, R=Respond, V=RecoVer	0-25%			26-50%			51-75%			76-100%		
	D	R	V	D	R	V	D	R	V	D	R	V
Small (<100 employees and/or <$50m)	3	4	4	2	1	2	1	1	0	0	0	0
Medium (<1000 employees and/or <$100m)	1	2	4	1	1	1	3	2	1	3	3	2
Large (>1000 employees and/or >$100m)	0	2	2	0	1	3	2	4	1	13	8	9

Table 2: Organization Size by Security Percentage per Function