Scientific Research Publishing

Journal of Information Security, 2024, 15, 196-217
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Effective Utilization of Government-Provided CTI by Small Businesses within the Defense Industrial Base

Josiah Dykstra[1], Lawrence A. Gordon[2], Martin P. Loeb[2], Benjamin Wall[1], Lei Zhou[2]

[1]National Security Agency, Fort Meade, MD, USA
[2]Robert H. Smith School of Business, University of Maryland, College Park, MD, USA
Email: josiahdykstra@acm.org, lagordon@umd.edu, mploeb@umd.edu, bmwall@uwe.nsa.gov, lzhou@umd.edu

How to cite this paper: Dykstra, J., Gordon, L.A., Loeb, M.P., Wall, B. and Zhou, L. (2024) Effective Utilization of Government-Provided CTI by Small Businesses within the Defense Industrial Base. *Journal of Information Security*, **15**, 196-217.
https://doi.org/10.4236/jis.2024.152012

Received: February 15, 2024
Accepted: April 20, 2024
Published: April 23, 2024

Abstract

There are two broad objectives of the research reported in this paper. First, we assess whether government-provided cyber threat intelligence (CTI) is helpful in preventing, or responding to, cyber-attacks among small businesses within the U.S. Defense Industrial Base (DIB). Second, we identify ways of improving the effectiveness of government-provided CTI to small businesses within the DIB. Based on a questionnaire-based survey, our findings suggest that government-provided CTI helps businesses within the DIB in preventing, or responding to, cyber-attacks providing a firm is familiar with the CTI. Unfortunately, a large percentage of small firms are not familiar with the government-provided CTI feeds and consequently are not utilizing the CTI. This latter situation is largely due to financial constraints confronting small businesses that prevent firms from having the wherewithal necessary to effectively utilize the government-provided CTI. However, we found a significant positive association between a firm's familiarity with the government-provided CTI and whether a firm is being periodically reviewed by the Defense Counterintelligence and Security Agency (DCSA) or is compliant with the Cybersecurity Maturity Model Certification (CMMC) program. The findings from our study also show that the participating firms believe that external cyber threats are more likely to be the cause of a future cybersecurity breach than internal cybersecurity threats. Finally, our study found that the portion of the IT budget that small businesses within the DIB spend on cybersecurity-related activities is dependent on the perception that a firm would be the target of an external cyber-attack.

Keywords

Government-Provided CTI, Small Businesses, Defense Industrial Base

1. Introduction

According to the United States (U.S.) Chamber of Commerce ([1]), there are over 33 million small businesses in the U.S., making up over 99% of the businesses in America.[1] These businesses account for roughly 44% of the GDP and are responsible for creating close to two-thirds of the net new jobs in the U.S. Furthermore, it is generally acknowledged that small businesses are a fundamental driver of economic growth and innovation in the U.S.[2]

Despite the economic impact of small businesses in the U.S., it is well known that most small businesses do not have the resources required to establish a sophisticated cybersecurity program (e.g., see [2]). Indeed, resource constraints prevent many small businesses from hiring skilled cybersecurity personnel, or from hiring expensive cybersecurity consultants, required to establish a robust and mature cybersecurity risk management program.

Small businesses within the defense industrial base (DIB) are in the unique position of having interconnected information systems and sensitive data sharing with the U.S. Department of Defense (DoD). Although these interconnections are of a limited nature, the fact that they exist raises important national security concerns. Thus, unlike the typical small business, the government has strong incentives to facilitate the effective utilization of government-provided CTI by small businesses within the DIB.[3]

The U.S. Department of Defense takes a multi-pronged approach toward improving the cybersecurity risks of companies within the DIB. For instance, the Defense Counterintelligence and Security Agency (DCSA) periodically reviews the security of defense contractors who handle classified information. In 2021, DoD began piloting the Cybersecurity Maturity Model Certification (CMMC) program, a multi-level compliance program to improve the security posture and reduce risks to DoD contractors and subcontractors.[4] In addition, the government provides a variety of public and non-public cyber threat intelligence at no cost to both the public and to vetted partners. One such example is the Automated Indicator Sharing service from the Cybersecurity and Infrastructure Security Agency (CISA). The National Security Agency also provides several free cy-

[1]The U.S. Small Business Administration (SBA) "… defines a 'small business' either in terms of the average number of employees over the past 12 months, or average annual receipts over time" (see: https://www.state.gov/what-is-a-small-business/). What qualifies as a small business, for purposes of government contracting, varies by industry. The SBA has established size standards for different industries, using the North American Industry Classification System (NAICS). For detailed information on SBA's size standards, see https://www.ecfr.gov/current/title-13/chapter-I/part-121#121.201.

[2]The above statistics, as well as other related statistics, can be found at: https://www.uschamber.com/small-business/state-of-small-business-now.

[3]According to the Cybersecurity & Infrastructure Security Agency (CISA), "The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements" (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector). The precise number of defense contractors and subcontractors is difficult to quantify, but the government estimates there are more than 100,000.

[4]Originally, CMMC's Model 1.0 consisted of a five-level framework, but in 2020 it was changed to a three-level framework in Model 2.0 (see: https://dodcio.defense.gov/CMMC/about/).

bersecurity services to DIB companies.[5]

As a result of the above noted resource constraints, we hypothesized that most small businesses within the DIB cannot effectively utilize the large volume of complex cyber threat intelligence (CTI) data (*i.e.*, streams of data describing existing or potential cyber threats) provided free by government agencies and departments. If confirmed, this situation is troublesome because cyber-attacks on small businesses have been growing at a rapid rate and these firms have become common prey (*i.e.*, low hanging fruit) for cyber hackers ([3])[6].

There are two main objectives of the research reported in this paper. The first is to empirically assess whether CTI data provided free by government agencies and departments is helpful in preventing, or responding to, cyber-attacks on small businesses within the DIB. The second objective is to offer recommendations for improved strategies for providing CTI to small businesses within the DIB. To accomplish these objectives, we conducted a questionnaire-based survey of private sector firms within the DIB.

The key findings from the current research study are as follows. First, government-provided CTI is helpful to small businesses within the DIB in preventing, or responding to, cyber-attacks provided a firm is familiar with the government-provided CTI feeds. Unfortunately, a large percentage of firms are not familiar with the government-provided CTI feeds and consequently are not utilizing the information. Second, this latter situation is largely due to financial constraints confronting small businesses that prevent the firms from having the wherewithal necessary to effectively utilize the government-provided CTI. The third key finding concerns whether being periodically reviewed by the DCSA or whether a firm is compliant with the CMMC program had any impact on the utilization of government-provided CTI by small businesses within the DIB. We found there is a significant positive association between a firm's familiarity with the government-provided CTI and whether a firm is being periodically reviewed by the DCSA or is compliant with CMMC.

The fourth key finding from the current study is that small businesses within the DIB are significantly more concerned about external cyber threats (*i.e.*, hackers external to the firm) than they are about internal (*i.e.*, insider) cyber threats. The fifth finding is that the portion of the IT budget that small businesses within the DIB spend on cybersecurity-related activities is dependent on the perception that a firm would be the target of an external cyber-attack. In other words, the higher a firm perceives its probability of being the target of an external attack, the more it is willing to spend on cybersecurity activities. This finding regarding spending on cybersecurity-related activities notwithstanding, over 55% of the respondents do not believe their firm has a high probability of being

[5]https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/.

[6]See:
https://www.cnbc.com/2021/07/03/ransomware-attack-may-have-impacted-thousands-of-small-businesses.html;
https://www.forbes.com/sites/tedknutson/2021/07/27/small-businesses-bearing-brunt-of-ransomware-attacks-senate-told/?sh=1cf7320f9556.

a target for a cyber-attack.

The contributions of the current research study are as follows. First, to our knowledge, this is the first study to focus on the use of government-provided CTI to improve cybersecurity in small businesses within the DIB. Given that small businesses within the DIB have interconnected information systems with the U.S. DoD, combined with the fact that an integrated information system is only as strong as its weakest link, these businesses represent an important component of U.S. national security. Accordingly, efforts to improve the cybersecurity of these firms should be a national security priority. Second, the findings from our study have implications that could lead to improvements in the cybersecurity-related activities of small businesses within the DIB. In fact, based on the findings from our study, we make specific recommendations for increasing the effective utilization of government-provided CTI by small businesses within the DIB.

The remainder of this paper proceeds as follows. In the next section, we provide a review of the relevant literature. In the third section, we present the basic hypotheses that will be empirically tested. The design of our empirical study and the sample of firms included in the study are discussed in the fourth section. The fifth section presents the results of the empirical study. The sixth section provides a discussion of the overall implications and recommendations based on the research findings. The seventh, and final, section of this paper provides some concluding comments.

2. Literature Review

Most of the previous literature related to CTI provided by government agencies and departments implicitly assumes that organizations have the requisite resources to effectively utilize CTI (e.g., [4] [5] [6]). Although this assumption seems valid for large firms, most small businesses are unlikely to have the resources necessary to establish an internal cybersecurity group. Fanelli, Pessanha, Gwiazdowski, Chng-Castor, and Auger [2] (p12) note in summarizing some of their study's empirical findings regarding the state of cybersecurity in small businesses in North America, "…cost and the organization's lack of resources is the number one challenge these businesses face in adopting cybersecurity practices."[7] Lack of expertise, lack of information, and lack of training were other factors noted by [2] as hindering a small business's ability to advance cybersecurity efforts.

Other studies have pointed out that small businesses face resource constraints that impede their ability to develop sufficient cybersecurity risk management programs (e.g., [7] [8]). Thus, it is well established that resource constraints pose a serious barrier to cybersecurity activities within small businesses. These resource constraints clearly impede a small business' in-house ability to utilize CTI feeds that are provided free-of-charge by government agencies and departments.

[7]Most small businesses responding to the survey conducted by [2] were part of organizations with 10 or fewer employees and had revenues that do not exceed $1M.

As [9] note, most "…small and medium sized enterprises (SMEs), do not have the knowledge, time or resources to analyze the CTI themselves and either rely on the built-in analysis of the security tools they purchase, or outsource to third party providers that specialize in securing systems and identifying threats." Resource constraints also impede a small business' ability to hire high-priced outside security consultants or purchase expensive CTI from third-party private sector vendors.

The U.S. Small Business Administration (SBA) recognizes that cybersecurity is a critical concern for small businesses. As noted by the head of SBA, Isabella Guzman, "Cyber threats can be devasting to small businesses…" SBA's Cybersecurity for Small Business Pilot Program is a small, but important, step in the direction of addressing the impact of resource constraints on the ability of small businesses to implement effective cybersecurity procedures ([10]).

3. Research Hypotheses

As noted in the introduction to this paper, there are two main objectives of the current study. The first is to empirically assess whether government-provided CTI is helpful in preventing, or responding to, cyber-attacks among small businesses within the DIB. The second objective is to assist government agencies and departments to develop an improved strategy for providing valuable CTI to small businesses within the DIB. Although stated as two separate objectives, these objectives obviously overlap with each other.

Investigating the first objective is essentially concerned with answering the following general research question: Do small businesses within the DIB utilize government-provided CTI?[8] Given the volume and complexity of government-provided CTI, and the cost of hiring cybersecurity experts (either as internal staff members or as external consultants), there is a priori reason to assume that small businesses within the DIB are not able to effectively utilize government-provided CTI to either prevent, or respond to, cyber-breaches. In other words, there is reason to believe that small businesses within the DIB are like most small businesses when it comes to utilizing government-provided CTI.

Since DoD's information systems are interconnected with the information systems of firms within the DIB, weak cybersecurity by any firm within the DIB could result in cybersecurity-related problems for DoD and, in turn, national security. Thus, as noted in the introduction of this paper, DoD has a multi-prong approach towards improving the cybersecurity of businesses within the DIB. Consequently, there is also a priori reason to assume (or at least hope) that small businesses within the DIB are unique in terms of their ability to utilize government-provided CTI. Of course, whether small businesses within the DIB are unique in their ability to utilize government-provided CTI is an empirical

[8]Government agencies (e.g., NSA) and departments (e.g., DHS) provide a substantial amount of free CTI to companies and the public. The fundamental reason for providing such information is to help organizations and individuals prevent, and respond to, cyber-attacks.

issue.

The issue raised by the above discussion was initially empirically tested in the current study based on our two-part first hypothesis ($H_{1.1a}$ and $H_{1.1b}$). The hypothesis, in the one-sided null form, is stated below. However, it is possible that whether government-provided CTI is helpful to firms is dependent on the firms' familiarity with the CTI. This concern was tested based on the revised first hypothesis as shown below ($H_{1.2a}$ and $H_{1.2b}$).

$H_{1.1a}$: Government-provided CTI helps small businesses within the DIB prevent cyber-attacks.

$H_{1.1b}$: Government-provided CTI helps small businesses within the DIB respond to cyber-attacks.

$H_{1.2a}$: Government-provided CTI helps small businesses within the DIB prevent cyber-attacks, conditional on the firm being familiar with the government-provided CTI.

$H_{1.2b}$: Government-provided CTI helps small businesses within the DIB respond to cyber-attacks, conditional on the firm being familiar with the government-provided CTI.

Regardless of the findings concerning the above hypothesis, it is well known that most small businesses face serious resource constraints that impede their ability to develop a robust and mature cybersecurity risk management program (e.g., see [2]). Ultimately, resource constraints come down to financial constraints (*i.e.*, money can purchase any required resource). Whether financial constraints represent a major barrier to using government-provided CTI for the subset of small businesses within the DIB has not, however, been empirically investigated in previous studies. Thus, the current study empirically assesses whether financial constraints represent a major barrier to effectively utilizing government-provided CTI by firms within the DIB. The empirical findings related to this concern were tested based on our second hypothesis, stated in the one-sided null form below.

H_2: Financial constraints are not a major barrier for small businesses within the DIB to the effective utilization of government-provided CTI.

The findings related to whether financial constraints are a barrier to effectively utilizing government-provided CTI should be helpful in addressing both the first and second objectives of the current study. However, to assist government agencies and departments develop an improved strategy for providing valuable CTI to small businesses within the DIB (*i.e.*, the second key objective), our empirical study also addressed several other basic research questions. One of these questions has to do with the role of DoD programs in facilitating the use of government-provided CTI by small businesses within the DIB. Two such programs that are particularly relevant are DCSA and CMMC. The DCSA "provides industrial security engagement and counter-intelligence support to secure the trustworthiness of the U.S. government's workforce, contract support, technologies, servic-

es, and supply chains".[9] However, not all firms within the DIB are required to be reviewed by DCSA. Firms that have access to classified information are among the ones that need to be reviewed. As noted by the DCSA, "We protect America's trusted workforce, trusted workspaces, and classified information."[10]

The CMMC is a certification program that provides a cybersecurity framework for DoD contractors and sub-contractors within the DIB.[11] The purpose of the certification program is to improve the security of controlled unclassified information (CUI) in non-federal information systems. The framework is based on the security requirements found in the NIST (National Institute of Standards and Technology) Special Publication 800-171.[12]

We are interested in answering the following question considering the DCSA and the CMMC: What, if any, is the association between a firm's familiarity with government-provided CTI and the fact that the firm is periodically reviewed by DCSA or whether the firm is compliant with the CMMC? The concern raised by this question was addressed based on a two-sided teste of our two-part third hypothesis, stated in the null form below.

H_{3a}: The familiarity with government-provided CTI by a small business within the DIB is not associated with the fact that the firm is periodically reviewed by DCSA.

H_{3b}: The familiarity with government-provided CTI by a small business within the DIB is not associated with the fact that the firm is CMMC compliant.

It is often pointed out that internal (or insider) threats from employees represent a bigger cybersecurity concern than threats from external hackers. ID Watchdog, for example, reported that "Insider threats are reportedly the primary cause for 60 percent of data breaches."[13] Along similar lines, [8] (p18) notes that "Insiders-employees or others who work for a business—are a main source of security incidents." Etchie [12] also points out that "…insider threats are a bigger danger to enterprise security than external forces are."[14]

There are several reasons that could account for insider cyber threats being a

[9]See: https://www.usa.gov/agencies/defense-counterintelligence-and-security-agency#:~:text=The%20Defense%20Counterintelligence%20and%20Security,%2C%20services%2C%20and%20supply%20chains.

[10]See: https://www.dcsa.mil/About/.

[11]See: https://dodcio.defense.gov/CMMC/Model/.

[12]See: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf. For an excellent discussion of the CMMC see [11]. On December 26, 2023, DoD proposed new rules for CMMC (CMMC 2.0) that would require all firms within the DIB to comply with the CMMC program (see: https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program). CMMC 2.0 has three progressively higher levels of compliance (*i.e.*, Level 1, 2, and 3), where the compliance level corresponds to the degree of sensitivity of DoD information shared with the DIB contractor.

[13]See: https://www.idwatchdog.com/insider-threats-and-data-breaches#:~:text=60%25%20of%20Data%20Breaches%20Are%20Caused%20By%20Insider%20Threats&text=The%20current%20average%20annual%20cost,business%E2%80%94whether%20intentionally%20or%20unintentionally.

[14]See: https://www.infosecurity-magazine.com/next-gen-infosec/cyber-threats-hackers-insider/.

bigger concern to many firms than external threats, including the following three. First, insiders have access to the firm's information systems and may know how to bypass the firm's cybersecurity. Second, disgruntled employees may target their employers as a way of getting revenge. Third, inadequate employee training often leads to cyber breaches, especially in small firms that have limited funds to spend on cybersecurity training.

For small businesses, however, there are several reasons why one may anticipate that internal threats pose a less serious problem than external threats. The first among these reasons is the fact that small businesses (especially those with less than 20 employees) are more apt to have a close relationship between employees, including between the senior executives (or owners) of the firm and its non-executive employees. This relationship can foster comradery among those working for the business in such a way that it would mitigate some aspects of an insider threat. Second, the number of people who have access to a small business' sensitive information systems is usually limited to a handful, at most. Thus, these insiders are likely to realize that anyone causing a cyber breach in a small firm has a high probability of being identified. For small businesses within the DIB, there is a third factor that might lead to the expectation that internal threats pose less of a problem than external threats. That is since the information systems of small businesses within the DIB are interconnected with the DoD's information systems, employees within these firms that have access to the firm's information systems will likely realize that the potential penalties for intentionally creating a cyber breach (e.g., committing some sort of cyber fraud) could be more severe than might otherwise be the case (e.g., there is the potential for being prosecuted by the federal government).

Determining whether internal or external threats are perceived to be more important to small businesses with the DIB should be helpful to government agencies and departments in developing an improved strategy for providing CTI (*i.e.*, the second main objective of our study). Consequently, the current study collected data to address this issue. The concern raised by this issue was addressed based on a two-sided test of our fourth hypothesis, stated in the null form below.

> H_4: Small businesses within the DIB perceive internal threats and external threats to be equally likely to cause future cyber breaches.

Cybersecurity investments (*i.e.*, spending on cybersecurity-related activities) reduce an organization's vulnerability to cyber-attacks and increase its ability to respond to cyber-attacks that do occur. As a result, a body of literature has emerged that points out that organizations should determine the amount to spend on cybersecurity based on cost-benefit analysis (e.g., see [13]-[18]). The above notwithstanding, there is evidence that firms in the private sector tend to underinvest in cybersecurity (e.g., see [19] [20]). In fact, many firms take a "wait and see" approach (*i.e.*, waiting for a cyber-breach to occur) before making major cybersecurity investments (see [21] [20]). As noted by [20] (p510), "As a re-

sult of the difficulties associated with estimating the benefits from cybersecurity investments, there is a widespread belief that private sector firms tend to underinvest in cybersecurity activities. Furthermore, firms tend to defer much of their cybersecurity investments unless reacting to a major cybersecurity breach." Accordingly, a fundamental concern to the U.S. government over the past two decades is understanding ways of encouraging firms to increase their spending on cybersecurity related activities (e.g., see [19] [22]).

Studies have shown that it is common for firms to spend less than 5% of their IT budget on cybersecurity related activities, although in some firms the percentage is much higher (e.g., see [23]). It seems reasonable to anticipate that a factor driving the amount a firm spends on cybersecurity related activities is the perception that the firm will be a target of a future cyber-attack from an external threat. However, many small firms apparently do not perceive their firms as being a prime target of a future external cyber-attack due to their limited resources (more will be said about this point later in the paper). Thus, the current study collected data to address the following question: Is the portion of the IT budget that a firm within the DIB devotes to cybersecurity-related activities dependent on the perceived probability that the firm would be the victim of a cyber-attack from an external threat? The concern raised by this question was tested based on our fifth hypothesis, stated in the null form below.

> H_5: The portion of the IT budget devoted to cybersecurity related activities by small firms within the DIB is not dependent on the perceived probability that the firm would be the victim of a cyber-attack from an external threat.

4. Research Design and Sample

To test the hypotheses stated above, we developed a questionnaire-based survey instrument. The development of the survey instrument considered the issues described in our hypotheses, as well as the other issues noted above. We also had discussions with individuals familiar with the DIB during the initial development of the survey instrument. After completing a draft of the survey instrument, a pilot study was administered to six experts with knowledge of the DIB for comments. Based on the comments received from these experts, a revised version of the survey instrument was developed.[15]

The survey instrument included two sections. The first section consisted of questions that asked the respondents to place a checkmark in the box with the most correct answer. These questions related to various characteristics of a respondent's firm, such as the size of the firm, whether the firm was reviewed by DCSA, and whether the firm was compliant with the CMMC. The second section of the questionnaire-based survey consisted of a list of questions where the respondents were asked to indicate their level of disagreement/agreement based on a 7-point Likert scale. The scale ranged from Strongly Disagree (1) to Strongly Agree (7). The questions in the second section of the questionnaire were

[15]A copy of the survey instrument is available upon request.

aimed at gathering information related to the two main objectives of our research study, with a focus on being able to test the hypotheses discussed in the last section of this paper.

A paper copy of the final questionnaire was initially sent to a sample of 1711 firms, along with a cover letter and self-addressed postage return envelope. The sample of firms was drawn from the public database of US government contracts at USASpending.gov.[16] However, NSA deleted several firms from this list because a firm was considered an NSA client (*i.e.*, NSA did not want these firms to feel undue pressure on their need to respond to the survey). The mailing was addressed to the individual noted on the list as the contract contact person. In our survey cover letter, respondents were assured that their responses would be completely anonymous (*i.e.*, no attempt was made to identify respondents with responses).

From our mailing of the paper copy of the questionnaire, 91 were returned as not deliverable (*i.e.*, indicating that the person to whom the questionnaire was addressed was either no longer employed at the firm, the address for the firm had changed, or the firm went out of business). Thus, our initial sample size was reduced to 1620 firms. Follow-up mailings of the questionnaire were done via an electronic mailing. Since we had no way of identifying which firms were included in the returned paper copy of the survey (*i.e.*, due to our promise of complete anonymity), the electronic version of the survey was sent to the entire sample of 1711 firms, with a note indicating that, if the firm had already responded to the survey, it should ignore the follow-up mailing. In total, we received 71 responses to our survey, a response rate of 4.4%.[17] Of the 71 responses, 9 were only partially completed and were not used in much of the analysis. Accordingly, most of the analysis was based on 62 responses.

In analyzing the survey results from the second section of the questionnaire, we considered responses of 1 - 3 as Strongly Disagree, and responses of 5 - 7 as Strongly Agree. Responses of 4 were considered to represent a neutral response. Thus, our analyses of the data gathered based on the Likert scale was focused on determining if the responses were statistically greater than, or less than, 4.

5. Empirical Results

5.1. Demographic Data

The results of our survey are summarized below. We begin with some basic demographic statistics. As illustrated in **Figure 1**, most of the respondents (*i.e.*, more than 61%) come from firms with 20 or less employees.[18] Furthermore, firms with 40 or less employees account for more than 77% of the respondents to our survey. In addition, most of the respondents (*i.e.*, over 72%) come from

[16]See: https://www.usaspending.gov/.

[17]The difficulties associated with getting firms to respond to surveys concerning cybersecurity related activities is well known. For example, the Ponemon [24] study had a response rate of 3.8%.

[18]The actual question in the survey instrument that generated the results shown **in Figure 1** is at the top of the figure. The same approach is used for the remaining figures in this section of the paper (*i.e.*, the question in the survey instrument that generated each figure is at the top of the figure).

firms where annual gross revenues do not exceed $5 million and more than 86% of the respondents come from firms where annual gross revenues do not exceed $20 million. As illustrated in Figure 2, most of the respondents (*i.e.*, over 56%) were the CEO of their respective firms. Furthermore, note that less than 5% of the respondents were either a CIO or a CISO.

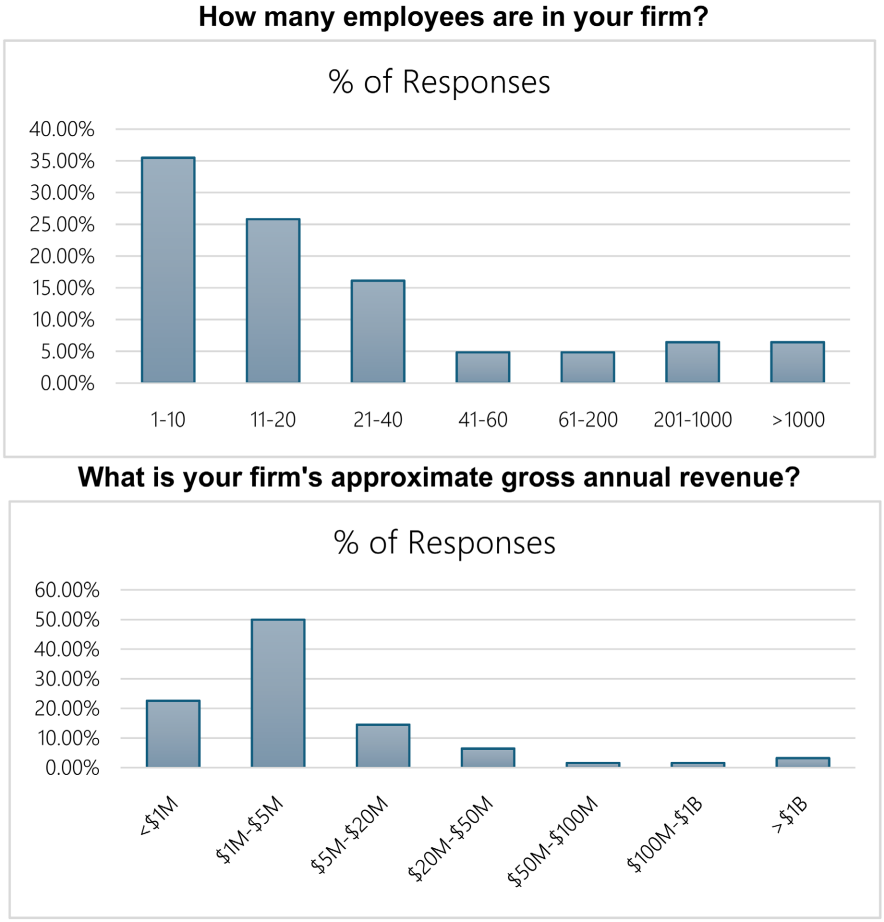

Figure 1. Firm size.

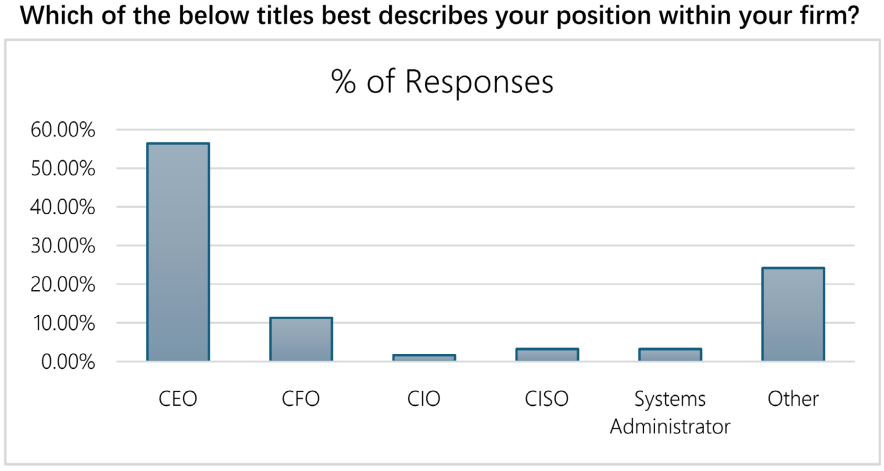

Figure 2. Title of respondents.

5.2. Tests of Hypothesis

At the most fundamental level, we were interested in assessing whether the CTI provided by government departments and agencies is being utilized by the small businesses with the DIB to prevent or respond to cyber breaches. We initially assessed this concern based on the survey responses to the following statement: Overall, government-provided CTI has helped my firm - a) prevent cyber-attacks, and n) respond to cyber-attacks. We conducted a one-sided test of our two-part first null hypothesis (*i.e.*, $H_{1.1a}$ and $H_{1.1b}$), by considering if the results were statistically different greater than a response of 4. Our statistical tests were based on parametric t-tests and nonparametric Wilcoxon Rank Sign tests. The results of the above tests are provided in Table 1.

As shown in Table 1, both parts of the first hypothesis are rejected at the 0.01 level of statistical significance. In other words, when treated as a stand-alone question, the respondents to our survey indicated that they do not consider the government-provided CTI to be helpful in preventing, or responding to, cyber-attacks. More than 68% of the respondents indicated that the government-provided CTI is not helpful to their firms in preventing cyber breaches and more than 71% indicated that the government-provided CTI is not helpful in responding to cyber breaches.

The issue being considered in the first hypothesis is, however, more complicated than the above analysis suggests. That is, given that we are dealing with small firms within the DIB, it is quite possible that the real problem is that these firms are not familiar with the available government-provided CTI rather than not finding the information helpful. To address this latter issue, we took into consideration the data collected via our survey related to the following statement: My firm is familiar with the vast amount of government-provided CTI feeds. We conducted a multivariate analysis based on the below regression equations (*i.e.*, Equations (1a) and (1b)) to examine the association between the responses to the two statements: 1) Overall, government-provided CTI has helped my firm - a) prevent cyber-attacks, and b) respond to cyber-attacks. 2) My firm is familiar with the vast amount of government-provided CTI feeds.

$$\begin{aligned}&\text{Gov CTI helps to prevent cyber attack}\\&= \alpha + \beta_1 \text{ Familiarity of Gov CTI} + \beta_2 \text{ Revenue} + \beta_3 \text{ Otherpublic CTI sources} \\&\quad + \beta_4 \text{ Using cost benefit analysis} + \varepsilon\end{aligned} \tag{1a}$$

Table 1. T-tests and Wilcoxon Sign Tests on Hypotheses $H_{1.1a}$ and $H_{1.1b}$.

	$H_{1.1a}$ Government CTI helps to prevent cyber attack		$H_{1.1b}$ Government CTI helps to respond to cyber attack	
	t-test: Mean of Reponses > 4	Wilcoxon Sign test: Median of Responses > 4	t-test: Mean of Reponses > 4	Wilcoxon Sign test: Median of Responses > 4
P-value	0.0000	0.0000	0.0000	0.0000

$$\text{Gov CTI helps to respond to cyber attack} = \alpha + \beta_1 \text{ Familiarity of Gov CTI} + \beta_2 \text{ Revenue} + \beta_3 \text{ Otherpublic CTI sources} + \beta_4 \text{ Using cost benefit analysis} + \varepsilon \quad (1b)$$

The results from the regressions are shown in Table 2. As shown in Table 2, we find a significant statistically positive association (at the 0.01 level) between a firm's familiarity with the government-provided CTI and whether the CTI helps the firm prevent, or respond to, cyber-attacks. In other words, our findings indicate that government-provided CTI is helpful to small businesses within the DIB in preventing, or responding to, cyber-attacks providing a firm is familiar with the government-provided CTI feeds. Thus, we cannot reject either part of our revised first hypothesis based on a multivariate analysis. Unfortunately, a large percentage of firms responding to our survey are not familiar with the government-provided CTI feeds and consequently are not utilizing the CTI.

The second basic issue addressed based on the survey data collected was whether financial constraints represent a major barrier for small businesses within the DIB to effectively utilize government-provided CTI. We assessed this concern based on a test of our second null hypothesis (*i.e.*, H_2), by considering if the results were statistically greater than a response of 4, based on parametric t-tests and nonparametric Wilcoxon Rank Sign tests. The results of the above tests are provided in Table 3.

As shown in Table 3, the second null hypothesis is rejected at the 0.05 level of statistical significance for the t-test and 0.01 level for the nonparametric test. In other words, the respondents to our survey clearly consider financial constraints to be a barrier to effectively utilize government-provided CTI.

A visual illustration of the results regarding the second hypothesis is provided in Figure 3. As illustrated in Figure 3, 55% of the respondents indicated that financial constraints represent a major barrier to their firm's effective utilization

Table 2. Regression results on hypotheses $H_{1.2a}$ and $H_{1.2b}$.

$H_{1.2a}$ Government CTI helps to prevent cyber attack conditional on firm's familiarity with CTI.			$H_{1.2b}$ Government CTI helps to respond to cyber attack conditional on firm's familiarity with CTI.		
	Coefficient	P-value		Coefficient	P-value
Intercept	0.3116	0.626	Intercept	0.6005	0.290
Familiarity of Gov CTI	0.4668	0.000	Familiarity of Gov CTI	0.3465	0.000
Revenue	0.3718	0.009	Revenue	0.2669	0.032
Other public CTI Access	−0.2141	0.079	Other public CTI Access	−0.1092	0.307
Cost-benefit analysis	0.1770	0.073	Cost-benefit analysis	0.0988	0.259
R-Squared	0.3589		R-Squared	0.2613	

Table 3. T-test and Wilcoxon sign test on hypothesis H_2.

H_2 Financial constraints are not a serious impediment to the cyber risk management program.		
	t test: Mean of Reponses < 4	Wilcoxon Sign test: Median of Responses < 4
P-value	0.0137	0.0066

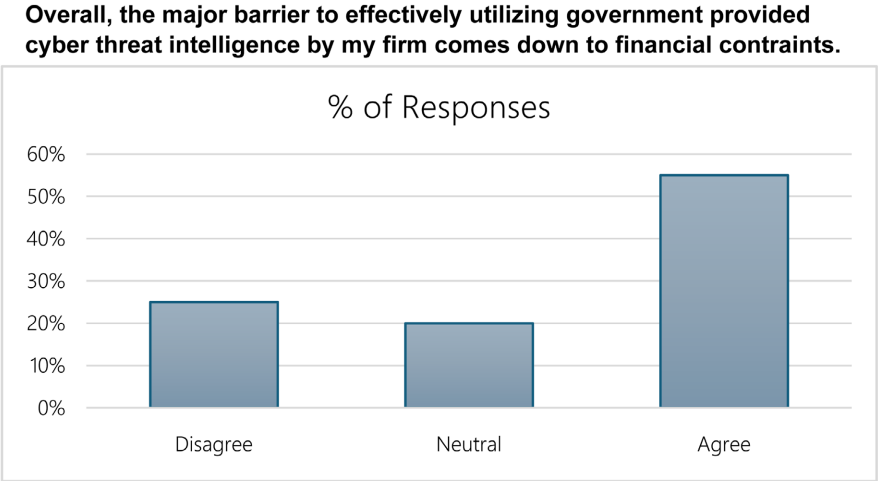

Figure 3. Financial constraint.

Table 4. Regression results on hypotheses H_{3a} and H_{3b}.

H_{3a} Familiarity of government CTI and DCSA review			H_{3b} Familiarity of government CTI and CMMC compliance		
	Coefficient	P-value		Coefficient	P-value
Intercept	7.288	0.000	Intercept	4.728	0.000
Revenue	0.188	0.248	Revenue	0.191	0.280
Reviewed by DCSA	−2.425	0.001	CMMC Compliant	−1.179	0.022
R-Squared	0.1563		R-Squared	0.0745	

of government-provided CTI. Although these findings are not surprising, they do raise a serious problem from a national security perspective that needs to be addressed.

Our third hypothesis is concerned with assessing whether there is an association between the familiarity with government-provided CTI by small businesses within the DIB and the fact that the firm is periodically reviewed by DCSA or whether the firm is compliant with CMMC. We assessed this concern based on a test of our two-part third null hypothesis (*i.e.*, H_{3a} and H_{3b}), using the regression equations shown below (*i.e.*, Equation (2a) and Equation (2b)). The results of the tests for this hypothesis are provided in **Table 4**.

$$\text{Familiarity of Gov CTI} = \alpha + \beta_1 \text{ Revenue} + \beta_2 \text{ Reviewed by DCSA} + \varepsilon \quad (2a)$$

$$\text{Familiarity of Gov CTI} = \alpha + \beta_1 \text{ Revenue} + \beta_2 \text{ CMMC Compliant} + \varepsilon \quad (2b)$$

As shown in Table 4, we find a statistically significant positive association between the familiarity of government-provided CTI by a small business within the DIB and the fact that the firm is periodically reviewed by DCSA at the 0.01 level. We also find a statistically significant positive association between the familiarity of government-provided CTI by small businesses within the DIB and the fact that the firm is CMMC compliant at the 0.05 level. Thus, we reject both parts of the third null hypothesis.

Despite the positive association between the familiarity of government-provided CTI by small businesses within the DIB and the periodic review of these firms by DCSA, over 90% of the respondents indicated that their firm is not being periodically reviewed by DCSA. In addition, more than 68% indicated that their firm is not compliant with CMMC. These findings raise important issues in terms of expanding government-required DCSA periodic reviews and CMMC compliance for DoD contractors. More will be said about this point in the next section of the paper.

The fourth hypothesis concerns whether small businesses within the DIB perceive internal or external threats as equally likely to cause a future cybersecurity breach. We assessed this concern based on a test of our fourth null hypothesis (*i.e.*, H_4).

As shown in Table 5, we find a significant difference (at the 0.01 level of statistical significance) in how the respondents to our survey perceive the threats that may cause future cyber breaches. More specifically, the respondents clearly perceive external threats as more likely to cause a future cybersecurity breach for their firms than internal threats. Thus, we reject the fourth null hypothesis. This finding is interesting because, as pointed out in the third section of the paper, it is often argued that internal threats are more serious than external threats.

The fifth hypothesis is concerned with the issue of whether the portion of the IT budget devoted to cybersecurity-related activities by small businesses within the DIB is dependent on the perceived probability that the firm would be the victim of a cyber-attack from an external threat. We assessed this concern based on the participants' responses to the following question and statement: 1) Approximately what portion of your firm's IT budget is devoted to cybersecurity related activities? 2) The probability that my firm will be the target of a cyber-attack

Table 5. T-test and Wilcoxon Sign Test on Hypothesis H_4.

H_4 Internal threats are equally likely to cause future cyber breaches to external threats.		
	T-test: Mean of Reponses to internal threats = Mean of Reponses to external threats	Wilcoxon Sign test: Median of Reponses to internal threats = Median of Reponses to external threats
t-value or Z-value	−3.9092	−3.326
P-value	0.0002	0.0009

from an external threat is quite low. A test of our fifth null hypothesis (*i.e.*, H_5) was based on the regression equation shown below (*i.e.*, Equation (3)). The results of the tests for this hypothesis are provided in Table 6.

$$\text{Portion of IT budget devoted to Cybersecurity} = \alpha + \beta_1 \text{ Perceived probability of future attack to be low} + \beta_2 \text{ Revenue} + \varepsilon \quad (3)$$

Figure 4 illustrates the percentage of the IT budget devoted to cybersecurity-related activities by the firms responding to our survey. As shown in that figure, over 56% of the firms indicated that they spend 5% or less of their IT budget on cybersecurity-related activities.

As shown in Table 6, we find a statistically significant association (at the 0.05 level) between the portion of the IT budget devoted to cybersecurity related activities by small businesses within the DIB and the perceived probability that the firm would be the victim of a future cyber-attack from an external threat. Thus, we reject the fifth null hypothesis. It is common to see firms increase their spending on cybersecurity activities as a result of a cyber breach (e.g., see Target Inc.'s Congressional Testimony in 2014).[19] The ultimate amount of the increased spending could be determined via an economic model, such as the Gordon-Loeb

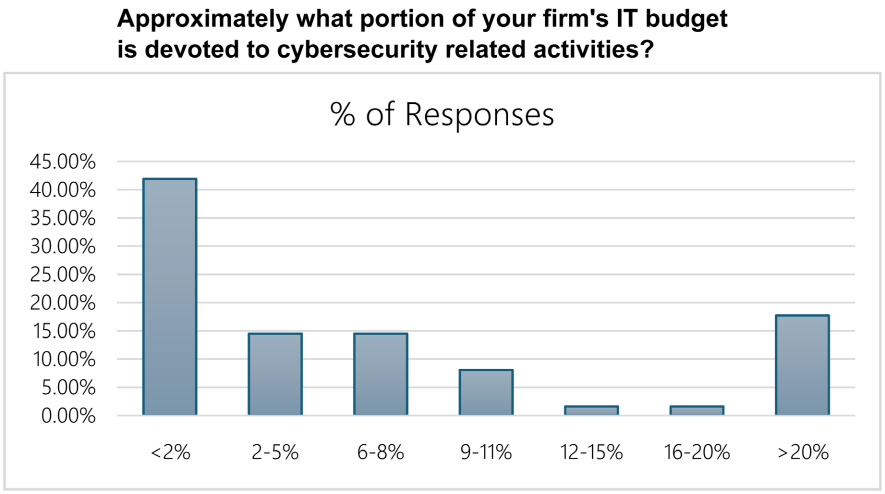

Figure 4. Cybersecurity expenditures

Table 6. Regression results on hypothesis H_5.

H_5 The portion of the IT budget devoted to cybersecurity related activities by small firms within the DIB is not associated with the perceived probability that the firm would be the victim of a cyber-attack from an external threat.		
	Coefficient	P-value
Intercept	4.280	0.000
Perceived probability of future attack to be low	−0.407	0.018
revenue	0.048	0.830
R-Squared	0.0798	

[19]See: https://www.c-span.org/video/?317553-1/cybercrime-privacy.

Table 7. Summary of results

- Government-provided CTI is helpful to small businesses within the DIB in preventing and responding to cyber-attacks, providing a firm is familiar with the government-provided CTI feeds. (H1.2a, H1.2b)
  - A large percentage of firms are not familiar with the government-provided CTI feeds and consequently are not utilizing the information in preventing and responding to cyber-attacks. (H1.1a, H1.1b)
- Financial constraints are a major barrier for small businesses within the DIB to the effective utilization of government-provided CTI. (H2)
- Familiarity with government-provided CTI by a small business within the DIB is associated with the firm being periodically reviewed by DCSA or being CMMC compliant. (H3a, H3b)
- Small businesses within the DIB perceive external threats as more likely to cause a future cybersecurity breach for their firms than internal threats. (H4)
- The portion of the IT budget devoted to cybersecurity related activities by small firms within the DIB depends on the perceived probability that the firm would be the victim of a cyber-attack from an external threat. (H5)

Model for investing in cybersecurity ([13] [16]).

Table 7 provides a summary of the results of the tests of the hypotheses.

6. Implications

In this section of the paper, we discuss some of the important implications of the empirical findings from our study. In discussing these implications, we draw upon the findings related to the hypotheses tested in the last section of the paper, as well as additional data collected from our survey. The additional data includes responses to structured questions and responses to open-ended questions on the survey instrument.

The first, and most fundamental, implication of the findings from our empirical study is that government-provided CTI is helpful to small businesses within the DIB in preventing or responding to, cyber-attacks providing a firm is familiar with the government-provided CTI feeds. Unfortunately, over 61% of the firms responding to our survey are not familiar with the government-provided CTI. This latter situation seems to be largely due to financial constraints confronting small businesses that prevent the firms from having the wherewithal necessary to effectively utilize the government-provided CTI.

The findings concerning the use of government-provided CTI strongly suggest that the problem is not with the CTI being provided by government agencies and departments. Instead, the inability to effectively utilize the government-provided CTI apparently stems from the fact that a large percentage of firms within the DIB lack the wherewithal to utilize the information. As indicated by the respondents to our survey, most firms don't have the financial means to hire technical experts, or high-priced consultants, who are aware of and can properly interpret, the government-provided CTI. The fact that over

56% of the respondents to our survey are the CEOs of the respective firms emphasizes the fact that these firms do not have staff to address their cybersecurity needs. As one of the respondents noted, "Most small businesses can't afford to hire a C.S. expert like a large business; yet we realize how important it is." Another respondent noted, "As a small business with no dedicated in-house expert, we need to have access to clear directives and assistance with identifying and handling threats."

Given the importance and magnitude of the work being done by small businesses within the DIB, combined with the fact that the information systems of these businesses are interconnected (at least to some extent) with the information systems of DoD, the above implication raises a national security concern. Accordingly, we believe it is important for DoD to address the resource constraint issue head-on. One way to address this issue is to consider providing incentives to small businesses within the DIB to utilize government-provided CTI more effectively. For example, most of the respondents (*i.e.*, over 82%) to our survey indicated that grants and cost-sharing would be helpful in facilitating their firms' ability to better utilize government-provided CTI. As one respondent clearly stated, "We need funding from Government to increase security of our IT system." A significant problem with direct financial incentives, such as grants and cost-sharing, is that it is difficult to prevent firms from substituting government funding for their own spending.

Most of the respondents (*i.e.*, over 67%) also indicated that technical assistance from the government would be beneficial in helping them effectively utilize government-provided CTI. In this regard, several of the respondents indicated that their firms would welcome the opportunity to attend training sessions that provide technical assistance in utilizing government-provided CTI. In the words of one respondent, "Our employees are aware of cybersecurity issues through university resources, but government-based training could be useful especially if free." Addressing the technical needs of small businesses within the DIB is, of course, a complicated issue. However, a combination of government-funded online tutorials and regional short training workshops would most likely be welcomed by the firms and go a long way toward helping them more effectively utilize the available government-provided CTI.

Another incentive that most of the respondents (*i.e.*, over 67%) ranked high. in terms of helping to improve their firms' ability to effectively utilize government-provided CTI, is priority government contracting contracting. Of course, this raises the question of how the government agencies and departments would determine which firms get such priority (*i.e.*, would it be based on some sort of measure of a firm's security, cybersecurity expertise, etc.). Nevertheless, the fact that small businesses within the DIB see priority government contracting as an important incentive for improving their cybersecurity is certainly worthy of further consideration.

An important issue concerns the need to effectively communicate the CTI to small firms within the DIB. DoD could help to establish some type of specialized

information sharing organization for small businesses. For example, DoD could establish an ISAO (Information Sharing and Analysis Organization) for small businesses within the DIB, where part of its focus is the goal of assisting firms in understanding and using government provided CTI. DoD could also develop short videos and webinars as tutorials that focus on helping small businesses with the DIB better utilize government-provided CTI.

The second implication of the findings from our study relates to the fact that existing government programs that are designed to improve the cybersecurity of firms within the DIB appear to be working. In fact, there is a significant positive relationship between those firms that are being periodically reviewed by DCSA or are compliant with CMMC and the firms' familiarity with the government-provided CTI. The above raises the following question: Should the DCSA and CMMC programs be expanded to include more firms? There is clearly no single answer to this question. More to the point, there are cost-benefit considerations if the DCSA and CMMC programs were to be expanded. However, it is worth noting that there is a proposed rule by DoD that would make CMMC mandatory for firms in the DIB.[20]

The third implication of the findings from our study relates to the findings that the portion of the IT budget devoted to cybersecurity related activities by small businesses within the DIB is dependent on the perceived probability that a firm would be the victim of a cyber-attack from an external threat. This finding suggests that firms would spend more on cybersecurity related activities if they believed that external cyber threats were a serious concern even for small businesses. Unfortunately, over 55% of the respondents seem to believe their firm has a low probability of being a target of a cyber-attack from an external threat. However, although small businesses do not have the assets of large firms, they also don't have the resources to invest in a sufficient cybersecurity program. Consequently, as pointed out by NIST (2016, p.4) "…many cyber criminals view them as soft targets." Along a similar vein, StrongDM notes, "Despite the attitude among many small business owners that hackers only go after behemoths, smaller companies make increasingly attractive prey."[21] In fact, from a cost-benefit perspective, many cybercriminals have realized that there are larger net benefits associated with targeting small businesses rather than large firms that have funds to invest in sophisticated cybersecurity procedures.

The third implication suggests that one way to increase the spending on cybersecurity by small businesses within the DIB is to provide these firms with data on the number and magnitude of external cyber threats confronting small businesses, including those small businesses with very limited resources. It would also be helpful to explain to the firms within the DIB that hackers look at potential targets from a cost-benefit basis perspective, and due to their limited ability to commit resources to cybersecurity activities many hackers view small

[20]See https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program.

[21]See https://www.strongdm.com/blog/small-business-cyber-security-statistics

businesses as very attractive preys.

7. Concluding Comments

The research reported in this paper was focused on two broad objectives. The first objective was to assess whether government-provided CTI is helpful in preventing or responding to, cyber-attacks among small businesses within the Defense Industrial Base (DIB). The second objective was to identify ways of improving the effective utilization of government-provided CTI to small businesses within the DIB. To accomplish these objectives, we conducted a questionnaire-based survey of private-sector firms within the DIB.

The findings from our study indicate that that government-provided CTI is helpful to small businesses within the DIB in preventing or responding to, cyber-attacks providing a firm is familiar with the government-provided CTI feeds. Unfortunately, a large percentage of firms responding are not familiar with the government-provided CTI feeds and consequently are not utilizing the CTI. This latter situation is largely due to financial constraints confronting small businesses. These financial constraints prevent the firms from having the wherewithal necessary to effectively utilize the government-provided CTI.

Although beyond the scope of the current study, future research could conduct case studies to gain a more detailed assessment of the effectiveness of government-provided CTI. In addition, as with all studies, the study described in this paper has limitations. The following four limitations are among the most obvious in connection with the study described in this paper. First, as with nearly all studies related to the cybersecurity activities of firms, only a small percentage of firms responded to our survey.[22] The second limitation relates to whether the most appropriate person within the firm completed the survey. Although respondents were asked to identify their position within the firm, there is never a guarantee as to who completed the survey. The third limitation concerns the limited richness of data gathered via a survey.[23] The fourth limitation of the study discussed in this paper is that, although financial constraints pose a serious impediment to the effective utilization of government-provided CTI, specific details on financial constraints related to cyber activities are rarely available (*i.e.*, firms are reluctant to share confidential financial information on cybersecurity expenditures). The above limitations notwithstanding, we believe our study makes important contributions to the existing literature concerning the effective utilization of government-provided CTI by small businesses with the DIB.

Acknowledgements

The authors thank Melissa Vice and an anonymous reviewer for insightful comments. Drs. Gordon, Loeb, and Zhou thank UMD's Smith School of Busi-

[22]Response rates to surveys directed at gathering information related to the cybersecurity activities of firms are known to be low, and our survey suffered from the same problem.

[23]It is for this reason that many argue for case studies when examining complicated issues like the cybersecurity activities of firms.

ness and the National Security Agency for financial support associated with this research. The views and conclusions expressed in this paper are those of the authors, and do not necessarily represent those of the Department of Defense or U.S. Federal Government.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] U.S. Chamber of Commerce (2023) The State of Small Business Now. https://www.uschamber.com/small-business/state-of-small-business-now

[2] Fanelli, B., Pessanha, R., Gwiazdowski, A., Chng-Castor, A. and Auger, G. (2017) State of Cybersecurity among Small Businesses in North America. *Council of Better Bureaus*. https://saginllc.com/wp-content/uploads/2017/10/Cybersecurity_FINAL_LoRes_Embargoed.pdf

[3] Hayes, J. and Bodhani, A. (2013) Cyber Security: Small Firms under Fire. *Engineering & Technology*, **8**, 80-83. https://doi.org/10.1049/et.2013.0614

[4] Onwubiko, C. and Lenaghan, A.P. (2007) Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. 2007 *IEEE Intelligence and Security Informatics*, New Brunswick, 23-24 May 2007, 244-249. https://doi.org/10.1109/ISI.2007.379479

[5] Dykstra, J., Gordon, L.A., Loeb, M.P. and Zhou, L. (2022) The Economics of Sharing Unclassified Cyber Threat Intelligence by Government Agencies and Departments. *Journal of Information Security*, **13**, 85-100. https://doi.org/10.4236/jis.2022.133006

[6] Dykstra, J., Gordon, L.A., Loeb, M.P. and Zhou, L. (2023) Maximizing the Benefits from Sharing Cyber Threat Intelligence by Government Agencies and Departments. *Journal of Cybersecurity*, **9**, tyad003. https://doi.org/10.1093/cybsec/tyad003

[7] Alahmari, A. and Duncan, B. (2020) Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (*CyberSA*), Dublin, 15-19 June 2020, 1-5. https://doi.org/10.1109/CyberSA49311.2020.9139638

[8] Paulsen, C. and Toth, P. (2016) Small Business Information Security: The Fundamentals. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

[9] Chadwick, D.W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A. and Wang, X.S. (2020) A Cloud-Edge Based Data Security Architecture for Sharing and Analysing Cyber Threat Information. *Future Generation Computer Systems*, **102**, 710-722. https://doi.org/10.1016/j.future.2019.06.026

[10] U.S. Small Business Administration Press Release 23-52, U.S. Small Business Administration Announces New Cybersecurity Grant Recipients for 2023. https://www.sba.gov/article/2023/08/14/us-small-business-administration-announces-new-cybersecurity-grant-recipients-2023.

[11] Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J. and Mod-

aresnezhad, M. (2022) Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base. *Journal of Information Systems Applied Research*, **15**, 17-29.

[12] Etchie, M. (2021) The Biggest Cyber Threat Isn't Hackers, It's Insider Threats. Infosecurity Magazine. https://www.infosecurity-magazine.com/next-gen-infosec/cyber-threats-hackers-insider/

[13] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security* (*TISSEC*), **5**, 438-457. https://doi.org/10.1145/581271.581274

[14] Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) A Model for Evaluating IT Security Investments. *Communications of the ACM*, **47**, 87-92. https://doi.org/10.1145/1005817.1005828

[15] Hausken, K. (2006) Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers*, **8**, 338-349. https://doi.org/10.1007/s10796-006-9011-6

[16] Gordon, L.A., Loeb, M.P. and Zhou, L. (2016) Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, **7**, 49-59. https://doi.org/10.4236/jis.2016.72004

[17] Wang, S.S. (2019) Integrated Framework for Information Security Investment and Cyber Insurance. *Pacific-Basin Finance Journal*, **57**, Article 101173. https://doi.org/10.1016/j.pacfin.2019.101173

[18] Fedele, A. and Roner, C. (2022) Dangerous Games: A Literature Review on Cybersecurity Investments. *Journal of Economic Surveys*, **36**, 157-187. https://doi.org/10.1111/joes.12456

[19] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015a) Increasing Cybersecurity Investments in Private Sector Firms. *Journal of Cybersecurity*, **1**, 3-17. https://doi.org/10.1093/cybsec/tyv011

[20] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015b) The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective. *Journal of Accounting and Public Policy*, **34**, 509-519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

[21] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, **22**, 461-485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

[22] Gordon, L.A. (2007) Incentives for Improving Cybersecurity in the Private Sector: A Cost-Benefit Perspective, Congressional Testimony before Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, and published in Congressional Record. https://docplayer.net/2498875-Incentives-for-improving-cybersecurity-in-the-private-sector-a-cost-benefit-perspective.html

[23] Gordon, L.A., Loeb, M.P. Lucyshyn, W. and Zhou, L. (2018) Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security*, **9**, 133-153. https://doi.org/10.4236/jis.2018.92010

[24] Ponemon Institute (2021) The State of Threat Feed Effectiveness in the United States and United Kingdom.