Developing Mandatory Reporting for Cyber-Attacks on U.S. Businesses

Baylor Franck and Mark Reith
Department of Electrical & Computer Engineering, Air Force Institute of Technology, WPAFB, USA
baylor.franck@us.af.mil
mark.reith@afit.edu

Abstract: The goal of this paper is to argue for the mandatory reporting of cyber-attacks on critical U.S. infrastructure, industries, and companies to the Department of Defense (DoD) for the DoD to improve national security through a clearer understanding of the threats and how to position the U.S. for better defense. The paper will first discuss who will be subject to mandatory reporting and propose a template for the requirements of reporting such as the turnaround time to report and the details needed from the attack. The paper will provide an argument showing the benefit to the DoD requiring reporting and why it should be concerned about external cyber-attacks on non-DoD systems. The paper will then look on the private sector viewpoints to discuss the benefits of mandatory reporting such as the bottom line and brand awareness. Additionally, the paper will also discuss how the consumer will benefit from mandatory reporting with a focus on both financial and privacy issues. Lastly, the paper will address some key points of dissent on the topic of mandatory reporting as well some evidence to push back or show how the negatives of not reporting outweighs the negative of reporting. After reading the paper, the reader will have a better picture of the current status of cyber-attacks on the private sector, how these attacks effect the DoD's mission, and why mandatory reporting can help enhance private sector cybersecurity. More research is needed to better understand the legal argument for requiring reporting on cyber-attacks as well as economic incentives for compliance, however this paper is not intending to answer that argument given the authors do not come from the legal or economic disciplines.

Keywords: cyber, DoD policy, business

1. Introduction

As the modern world continues to evolve, the DoD must also evolve itself in response to better fulfil its mission of defending the U.S. from internal and external threats. One key area of focus by the DoD is in the cyber domain as the rise of the Internet, accessible hacking techniques, and lucrative ransoms have allowed for a widespread increase in cyber-attacks both on the public and private sectors. Due to the large presence of contractors in infrastructure support and new technologies, the DoD needs to take critical steps to improve the cybersecurity of U.S. businesses and infrastructure to maintain the high performance of the U.S. military, not just its own systems. Therefore, the U.S. government needs to develop and enforce cybersecurity reporting standards for the DoD to preserve national security and its competitive technological advantages. The DoD needs to first assist companies and private entities in improving their cybersecurity by assisting companies when attacked as well as taking initiative to strengthen existing cybersecurity in other companies by evaluating systems and sharing information across the landscape to help companies better understand threats. Next, the U.S. government needs to push businesses to improve their cybersecurity by adding financial rewards for overachievers and sanctions for companies who do not meet minimum standards for cybersecurity. Lastly, the DoD needs to push the economic incentives such as better brand positivity, less ransom payments, and loss of intellectual property (IP) to help companies better realize the value of cybersecurity in terms of how it pertains to the bottom line. With the numerous benefits that exist for the DoD and private businesses themselves, key U.S. corporations and other key U.S. non-governmental organizations should report all cyber-attacks including the resolution of the attack to the DoD due to the interests of national security, interests of the attacked entity, and protecting individuals affected in these cyber-attacks. This paper will be split into four main parts; proposing the reporting requirements for U.S. entities, outlining the benefits of mandatory reporting, discussing the main counterarguments to mandatory reporting, and providing some concluding remarks that may temper counterarguments

2. Explanation of new reporting requirements

Before debating the importance of mandatory reporting, this section will be used to clearly layout who is required to report what information within certain time frames of the attack. Without clear rules and obligatory participation via the U.S. government, a combination of entities either deciding that they do not need to report when they do or giving information that is not helpful to determine how to stop the attack as well as what was

stolen will lead to an ineffective cybersecurity response to the growing problem. However, the current number of attacks pared with U.S. entities where money is exchanging hands will be too much for the DoD to keep up with. This means that a huge backlog of incidents will develop leading to companies not receiving help during the attack to critical attacks not being analyzed in detail many months later. As such, U.S. entities that are required to report on cyber-attacks must be limited to key areas and are as follows (NIAC-2017);

- a) Critical Infrastructure Companies - Power, Water, Sewage, etc.
- b) DoD Contractors/Sub-Contractors - Those who work on military contracts regardless of what part of the contract they belong to
- c) Medium to Large-Scale Companies - U.S. businesses who have a market cap/size over a certain amount

The desired result is that the number of companies who will have to report would be manageable for the DoD to monitor and respond while covering the most critical entities that support the DoD and its interests. Now that this has been determined who must report cyber-attacks, clear rules and guidelines must be implemented to effectively stay on top of cyber incidents that are ongoing. The timeline of reporting what information is provided below (NIAC-2017);

- 1. Initial Notification (Within 24 hours)
- a. Explains the status of the attack, type of attack used, and target of the attack
- b. Ask for assistance of federal authorities if needed or required if DoD mandates it.
- 2. Midterm Notification (Within 72 hours)
- a. Status of Attack - Has it been completed and contained or is attack still occurring?
- b. Was a financial payment required to stop attack, how is it occurring if so.
- c. Critical DoD risks - Was any software or hardware affected directly used by the DoD. Simply understanding what systems may be at risk.
- 3. Full Comprehensive Report (Within 14 Days)
- a. Clear understanding of attack, how bad actor got in and steps taken to resolve this issue
- b. Clear list of everything that was affected, including stolen data/IP, financial payment, etc.
- c. Bad actors behind attack - specific country or individual hacker?
- d. Full impact on DoD such as were any systems/IP used by the DoD affected and if so, what is your analysis on the potential impacts that could be seen by the DoD.
- e. Impact on consumers - need to change passwords, personal data stolen, etc.

In terms of sanctions, there needs to be strict penalties to generate compliance of the rules as meager fines and reprimands by Congress have showed little to no change in previous scenarios. There also needs to be incentives for the companies as well as top executives to further push compliance whether it is in terms of adding tax credits, adjusting bonuses for executives based on cybersecurity/reporting, and requiring minimum cybersecurity standards to receive government contracts. Combined with the limited power of the DoD to lawfully impose certain rules on privates businesses, additional research on both the legal and economic routes must be examined to both force and encourage compliance. Finally, the DoD should also look at the European Union (EU) NIS directive and other practices as a template for their policies and reporting.

3. Comparison to EU Standards

The DoD should look to other large governmental organizations to better guide their mandatory reporting policy. One organization is the EU as they have developed their NIS Directive below (ENISA).

- *1. National capabilities:* EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.
- *2. Cross-border collaboration:* Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.
- *3. National supervision of critical sectors:* EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health,

digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online market places, cloud and online search engines)

There are a few key takeaways that can be used by the DoD to effectively implement a mandatory reporting system. First, the DoD needs to ensure that it works with other U.S governmental agencies such as the FBI, CIA, and DHS to ensure that all agencies are on board with the policies, willing to help out, and able to effectively contribute to the problem at hand. Communication and collaboration is important in solving all sorts of problems and given the complexity of cyber-attacks, it is needed now. The other main idea to take from the EU is to determine which sectors are of importance to the health of the U.S. and this includes economically, medically, and defensively among others. Given the complexity of just the needs of the DoD, it is imperative that all critical sectors are determined and analyzed for their cybersecurity. The recent pandemic how shown how relatively few component shortages across several industries can affect the U.S. as it has led to production delays and re-designs. Given that cyber-attacks can also disrupt with the supply chains of these same industries more severely and rapidly, the DoD needs to be aware of where its resources should be dictated to combat cyber-attacks thus preventing the most critical production setbacks. With the large amount of possible rules and regulations that can be enacted, the DoD needs to use the success/failures of the EU NIS Directive to better implement their own policies. The proposed rules along thoughts on increasing participation, the benefits of mandatory reporting for both the DoD and business will now be discussed.

4. Discussion of National Security

U.S. contractors pride themselves on their ability to work and support the DoD. Cyber-attacks that expose key secrets and cyber security flaws put the DoD's advantages and intelligence at risk, therefore jeopardizing the national security of the U.S. U.S. businesses often develop key technologies to advance DoD operations both in the cyber domain and with physical assets; allowing foreign adversaries to steal critical information on these targets both improves their defensive response to our attacks as well as accelerating their own development of similar capabilities. An estimated 18% of attacks were performed by state actors, leading to the point that valuable IP and data are of importance instead of money (Council of Economic Advisers-2018). With this study being done 3 years ago and cyber-attacks continuing to grow from state-backed entities, more and more secret information and IP will keep being stolen from U.S. companies. One example of such an attack can be seen in the loss of valuable contractor IP through F-35 hack. Lockheed Martin was hacked by Chinese nationals, aiding in the quick development of a similar plane, the J-31 using F-35 data as evidenced in the similar design and intelligence gathered by the DoD. This is a considerable cost in national security as the advantage of the F-35 is mitigated by the abilities of J-31 as well as better understanding to counter F-35 through other ground/air to air attacks (Council of Economic Advisers 2018).

U.S. businesses also often serve as software contractors to the DoD and other government entities, resulting in lots of interactions and sharing of information between the two. Foreign actors can target weaker private cyber security systems first before then targeting DoD systems, making their chance of success much higher than a direct attack on DoD internal systems. This is since cybersecurity is like a chain; it is only as strong as its weakest link. Considering the DoD relies heavily on contractor work in terms of personnel and software, the DoD needs to ensure that these companies not only meet the high standards of the DoD cybersecurity but also report these incidents quickly. One area where the DoD is vulnerable due to the work its contractors do are through supply chain attacks where software and firmware that are used from private businesses are attacked and used against the DoD. The recent SolarWinds attack was a key example of enemy state actors using vulnerabilities in contractors such as SolarWinds, Microsoft, and VMWare to get into DoD systems as well as the U.S. Treasury and allied organizations such as NATO (Financial Stability Board-2021). While the current damage is still not fully known, it is believed that key policy and financial information was stolen in the attack which could affect the ability of the DoD to communicate and develop new technologies without risk of state actors knowing about their development. If not for the cybersecurity firm FireEye voluntarily releasing the information to the U.S. government, the lack of mandatory reporting could have cost the U.S. months to realize the issue and resolve it, leading to more information being stolen and used by our enemies.

Another aspect of the risk that the DoD faces is how the U.S. government sets standards for key contractors including those in cybersecurity which often propagates throughout other U.S. businesses. With these contactors often relying on other large U.S. cyber-focused companies to provide software, firmware, and other technology that is used, these large businesses tend to set the guidelines and rules for most cybersecurity. Poor cyber security business standards for large businesses will propagate through the entire U.S. business sectors as

smaller to medium size companies look to market leaders to ensure their products are similar in security. Currently, few standards exist at which cyber-attacks are reported, what must be reported, how long after the attack it must be reported with different jurisdictions having different requirements. Additionally, no standard for cyber terminology along with these previous factors makes cyber incident reports from companies widely vary (Cisco-2021). As per recent history, most companies will most likely meet the minimum standards of both cybersecurity and reporting which more than often have proven not to be enough. Until larger businesses get on board with better reporting standards and cybersecurity, both they and smaller companies will not make the change to be able to better block and mitigate cyber-attacks. This is especially true with small businesses as when they see larger businesses struggling with cyber issues and receiving no or minimal government sanctions, what is the incentive to upgrade their security. They also use the fact that they are a small business meaning that they may be able to fly under the radar as they cannot provide a large monetary ransom to bad actors meaning they are less likely to be attacked. This shows in the IT spending data from the Small Business Administration is less than $120 million for FY21. (Bluestein-2021) This number is a miniscule amount compared to the large spending done by bigger companies, only exacerbating the issue of cybersecurity. While many companies pride themselves on being supportive of the U.S. military and DoD, most companies will struggle to make serious changes in their reporting if it does not positively impact their bottom line.

5. Discussion on business aspects for corporations

Businesses often initiate change if the bottom line is affected, so the DoD needs to highlight the incentives to improve cyber collaboration between the U.S. government and private entities. This collaboration will allow for such as more efficient purchasing and deployment of cyber resources in addition to limiting costly attacks. Corporations must spend large amounts of financial and human resources to develop highly secure cyber systems and protocols with estimates believing around 3.8 billion was spent on IT in the 2020 fiscal year (Ziff Davis-2022). Even if one considers that year to be an aberration with transitions to working from home and heightened expenses for COVID, better understanding of current attacks on the industry and sharing of the cost of cyber security advances could cut down on those costs. The first example would be in purchasing and setting up internal systems that are more secure and less likely to be exposed to ransomware. Not only would this lead to more efficient purchasing of IT equipment instead of each company going at it alone but the savings in limiting ransomware would be significant as well. It is estimated that between $57 to $109 billion dollars was lost in the U.S. economy alone due to cyber-attacks in 2018 (Council of Economic Advisers 2018). Combined with the fact that this number is only from reported incidents to the DoD where the ransom could be confirmed, it is widely believed that the actual cost is much higher (Council of Economic Advisers 2018). Additionally, most firms believe cybersecurity and IT spending in general will continue to increase at a rate higher than that of their revenue (Ziff Davis-2022). Companies are already planning and having to spend large amounts on new cybersecurity, so efficient spending is a must to limit malware attacks while maintaining profit margins. By working with the DoD and other U.S. entities, companies can alleviate spending in addition to creating a more effective defense through mandatory reporting by determining current malware in existence, ensuring up-to-date patches from other software providers, and best security practices from the DoD to setup internal systems. By limiting the amount of money wasted on IT hardware and software that does not actually help against malware threats, companies will be able to see higher profit margins through lower costs.

In addition to the high costs of setting up cybersecurity or paying ransomwares, Corporations spend large amounts on research and development (R&D) to develop new technologies to gain advantages on competitors and increase profits. Poor cybersecurity can leave IP, communications, and other private company data vulnerable to bad actors of whom may be willing to sell to the highest bidders. Given the importance of, they can easily take the files they have stolen and sell them to rival companies with certain countries viewing corporate espionage as acceptable and even encouraging it. Company secrets can often be worth much more to competitors and a single breach could affect years of research and other built-up advantages, allowing competitors to catch up and reduce possible revenue from highly secretive projects. Looking at Apple and their development of the iPhone, one can realize how crucial secrecy really is due to how game changing the device really was. The iPhone became so dominant in part by how advanced it was compared to competitors at the time with features such as multi-touch and the compression of apps into such a small device. If a competitor had gotten iPhone IP sooner, one only must think how less dominant Apple would be today as instead of taking years for others to develop a phone of similar or better quality, it took years in which Apple carved out a large chunk of the smartphone industry. Another example can be seen in the recent SolarWorld (not to be confused with SolarWinds) attack in terms of theft of both key IP and long-term strategy planning. In the SolarWorld attack,

critical IP and trade secrets were stolen by Chinese hackers that enabled Chinese companies to duplicate their technologies at a cheaper price leading to a loss in market cap and future business loss that exceeded $150 million. To add further damage, financial documents were stolen allowing competitors to determine their future strategy to attack SolarWorld on costs through pricing where SolarWorld cannot make a profit or determine suppliers/customers they rely on (Council of Economic Advisers 2018). This simple cyber-attack has not only cost the company millions in lost profit, but to gain an advantage they will have to go a new direction in the industry to stand out in the market or hope that their R&D can generate another product that is better than their competitors which could take several more years.

Another area where corporations often spend large amounts of money is on their public relations (PR) to reflect key company values and the importance of hot-button issues such as privacy and secured data. A breach could hurt consumer confidence in the brand and expose internal documents that they may not want the public to see. Corporations value their positive brand awareness and a simple hack has the potential to tarnish the image the company has worked so hard to build up. One example is Facebook as several privacy scandals such as the Cambridge Analytica scandal have caused irreversible damage to the company. Despite their large status, many people have no confidence in Facebook when it comes to key issues such as privacy, honesty, and transparency. The lack of privacy has severely hurt the brand and one can wonder if the name change reflects the desire to shed the Facebook name and replace it with Meta (Jun,Kostyuk-2021). All the previous work, time, and money spent on PR is now down the drain due to a simple cybersecurity incident.

Finally, many U.S. companies have contracts with the U.S. to provide all sorts of advanced goods and services with many of them being secret in nature due to the heightened importance of the work being done. Repeated issues with cyber-attacks and reporting them to the DoD could hurt future chances at contracts as the U.S. government may be concerned in the ability of the company to execute the contract or safely protect DoD assets when they are entrusted to them. The DoD values the cutting edge technology provided by key U.S. businesses, but if they cannot secure it then the advantage will be short-lived. If the pattern repeats, the DoD is unable to rely on the company to deliver the advantages as they need as they will constantly worry if our adversaries already have seen this asset and are able to successfully defend against it. This will cost the company key revenue and profit as most government contracts are highly profitable for the companies who receive them. While certainly many positives to the arguments can be made for businesses to report cyber-attacks to the DoD, significant drawbacks exist that might adversely result from this practice.

6. Counterarguments to mandatory reporting

While U.S. businesses want to prevent cyber-attacks, mandatory reporting to the DoD would lead to adverse effects that would do more harm than good for most U.S. businesses. Often as a group grows larger, it is hard to maintain secrecy and not divulge sensitive information. Since many businesses would be required to partake in mandatory reporting and thus would see all shared data, bad actors could leak information to hackers to better target attacks, determine which attacks are not useful to limit wasting resources on them, and report on which companies are the worst at preventing cyber-attacks. Even if we could determine these bad actors, as they could create new businesses with the sole intention of observing information passed in the group. It would also be nearly impossible to restrict or block businesses from joining the group where cybersecurity is shared upon due to U.S. belief in equality of competition, meaning it would be impossible to prevent bad actors from seeing information in this database such as attacks that have succeeded and patches that have guarded against other attacks. Additionally, current SEC reporting standards require public companies to disclose IT spending, successful/failed attacks, and description of insurance coverage. (Division of Corporation Finance - SEC 2013) This information can allow for hackers to better target companies with minimal resources for maximum success as they can gauge what attacks work best and what companies can pay the most for it. The DoD would also need to regulate how information would be better shared to ensure that businesses stay secure without giving better financial information to certain investors or foreign entities.

Another pressing issue is the cost of upgrading cybersecurity as customers don't want to have to pay extra for something that they don't pay for already and businesses don't want to want to cut their profit margins while having to compete with limited resources and other firms overseas. This can be better realized in smaller U.S. businesses as they may not be able to afford and scale up cyber defenses at a rate of bigger companies, making them for vulnerable to attacks as well as identifying these businesses to a wider group of bad actors. The biggest issue is that small businesses tend to have even thinner margins and working capital than larger operations,

meaning that they often lack the funds to divert to cybersecurity as well as the inability to reduce profits through higher prices. They also may require a dedicated employee or hire a contractor/consultant to design/install their system as they may not have the cybersecurity knowledge necessary to implement an effective system given many businesses have a low amount of personnel. Another issue for smaller companies to join mandatory reporting is they may be stuck following federal rules on how to deal with a cyber-attack given their lack of political influence. Smaller businesses have less leverage and influence with the federal government meaning that if they do experience a cyberattack, they may be at the guidance of the federal agency instructions. This can be seen through the Kaseya investigation as the federal government as the FBI held the victim decryption key longer after paying the ransom to reverse engineer it to stop future attacks causing harm to the businesses affected by the attack but possibility benefitting their rivals (Jun,Kostyuk-2021). In addition, many of the businesses still did not invest in cybersecurity measures after the attack while other hackers could shift their resources away towards new attacks (Jun,Kostyuk-2021). With small companies at the mercy of federal agencies and their instructions on solving the cyber-attack then it might cause more trouble than simply going at it alone.

The last key argument against collaboration through mandatory reporting is that U.S. companies pride themselves for their innovations and technological advances, so obligatory sharing data or IP on cyber-attacks make companies more hesitant to invest and even share cyber incidents so that competitors cannot glean any insight into them (NIAC-2017). Many companies already take their cybersecurity more seriously and have spent the money and effort to develop tough systems that have been able to stand up to attacks, making them weary of sharing this info with competitors who can build the same system for cheap nullifying any competitive advantage. This will end up with some companies just doing the bare minimum and relying on the government and other companies to make improvements or spend their resources to implement effective cybersecurity before they make an effort to improve their own cybersecurity since now they can just copy. Competitors often try to glean any information about their competitors as evidenced by how outside company personnel read reports where the SEC requires all companies to disclose information what cybersecurity measures they have implemented and how they are working. (Division of Corporation Finance - SEC 2013) Competitors can easily look up the public information and the success to better determine where to invest in. This will allow them to catch-up to any cybersecurity advantages their competitors may have leading to a race to the bottom where a simple few companies or government efforts are used to build the cyber infrastructure for every other company. While some important points were brought up regrading cost and future risk to U.S. businesses which will need to be evaluated to develop mitigating solutions, many solutions can be found to solve or at least mitigate these problems as well as more benefits that outweigh the possible downsides.

7. Refuting counterarguments

The DoD will have challenges with getting U.S. companies on board with mandatory reporting but taking key steps and providing safeguards to companies will allow for an effective tool to maintain high national security and improving cybersecurity of private sector. The first key will be ensuring that outside actors cannot distinguish which companies are being discussed in mandatory reporting so as to not alert which companies may have weaker security measures. To maintain secrecy, companies will only be identifiable to the DoD and not to other companies. In addition, cyber-attacks will be brief to limit understand of how to produce these attacks with most of the shared information reporting being solutions to defend against similar versions of the attack. Secrecy requirements and rules already exist for cybersecurity attack reporting. In addition, current mandatory reporting of cybersecurity risks already occurs meaning that the infrastructure for companies to interact with the SEC and other agencies already exists. It would not be a burden on the companies and only strengthen both federal help and future systems (SEC-2013). In order to ensure that the reporting data is secure, the DoD can take note of other anonymous reporting systems exist such as HIPAA as they protect patient confidently through secure systems and compartmentalization of data to limit human access. Similar systems with DoD grade security can be used to secure the data properly and limit access both within and outside of the DoD. In addition, the companies will have to disclose cyber-attacks in SEC filings to investors, so the attack will be must public in-time, diminishing how important it is for companies to remain anonymous in these attacks.

Another issue is how to ensure small businesses build up their cyber capabilities and also deal with issues such as limited operating capital and small margins. Therefore, more effort needs to be put into the Small Business Administration (SBA) to assist these companies with some funding earmarked specifically for cybersecurity as well as technical support to get the system up and running. This shows in the IT spending data from the SBA as it is less than $120 million for FY22 (Bluestein-2021). They cannot afford to spend lavishly on this area so

targeted spending will yield better outcomes in preventing key attacks such as ransomware. Additionally, small U.S. businesses will be able to see solutions proposed to defend against attacks based on their industry and their operations so they can better focus their limited resources on certain attacks through data gathered by mandatory reporting. Through data collected by mandatory reporting, U.S. officials can help companies of this size on the most common attacks being conducted against them and how to build up their systems at an affordable rate to stop or better mitigate these attacks. At a minimum, this will establish a solid baseline to make bad actors put in some serious effort to get around their defenses while also ensuring that other small business can learn from the attack and not suffer the same fate.

Lastly, cybersecurity is such a rapidly changing field where constant innovations are required, meaning constant investment is needed. The reward is that companies who invest and have tougher cybersecurity not only experience less successful attacks but are also able to reduce the amount/importance of information stolen as well. This will also push bad actors to target other entities driving down the total number of attacks as they will want to go after easier targets as the effort required to obtain the reward is not worth it compared to other companies. Based upon the key points refuting the opposing viewpoints of mandatory reporting of cyber-attacks along with the advantages discussed earlier, mandatory reporting of cyber-attacks and sharing key details is a win-win for the public-private sector alliance the U.S. employs today for the DoD.

8. Conclusion

U.S. corporations and other non-governmental organizations that fit within the criteria listed in the second paragraph should be mandated to report all cyber-attacks up to and including the resolution of the attack to the DoD due to the interests of national security, efficiently building cyber security to minimize costs, and protecting individuals affected in these cyber-attacks. With U.S. businesses often developing key technologies to advance DoD operations both in the cyber and physical domain, poor cybersecurity will allow foreign adversaries to steal critical information or compromise communications on these targets resulting in improved enemy defensive responses to our attacks as well as accelerating their own development of similar capabilities. Another issue is that since U.S. business often serve as contractors to the DoD and other government entities, large volumes of interactions and sharing of information and cyber assets between the two occur. Therefore, foreign actors can target weaker private cyber security systems first before targeting DoD systems, making their chance of success much higher than a direct attack on DoD systems. Finally, most U.S. businesses often rely on other U.S. cyber-focused companies to provide software, firmware, and other technology that is used. Poor cyber security business standards for large businesses will propagate through the entire U.S. business sector putting DoD and U.S. businesses at risk of being attacked. The DoD needs to continue to get more serious about the possibility of cyber-attacks and realize that internal DoD systems are not the only target for our many adversaries. If the DoD is exposed on the cyber domain, our ability to produce advanced technologies at an industrial scale, which has been in a key factor in winning previous global conflicts, will be easily surpassed by our adversaries threatening the ability to defend ourselves in future conflicts.

Disclaimer: The views expressed are those of the authors and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

References

Bluestein, Keith - U.S. Small Business Administration. Information Technology Agency Summary. (2021, Sept. 30) Extracted from U.S. Small Business Administration Website: https://itdashboard.gov/drupal/summary/028

Cisco. Data Privacy Benchmark Study. (2021) Extracted from Cisco Website: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf

Council of Economic Advisers. The Cost of Malicious Cyber Activity to the U.S. Economy. (2018, Feb.) Extracted from the Department of Homeland Security Website through PDF download.

Davis, Ziff. 2022 State of IT. (2021, July) Extracted from Spiceworks Website: https://swzd.com/resources/state-of-it/#soit-2022

Division of Corporation Finance - SEC. CF Disclosure Guidance Topic No. 2. (2013, Oct. 11) Extracted from the SEC website: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

ENISA. NIS Directive. (14 Oct 2016). Extracted from EU Website: https://www.enisa.europa.eu/topics/nis-directive

Financial Stability Board. Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence. (2021, October 19) Extracted from the FSB Website: https://www.fsb.org/wp-content/uploads/P191021.pdf

Foret, Will – Forbes. Using Cybersecurity as a Competitive Advantage. (2019, Oct. 9) Extracted from Forbes Website: https://www.forbes.com/sites/forbesbusinesscouncil/2019/10/09/using-cyber-security-as-a-competitive-advantage/?sh=35d3ee1c7ff7

Jun, Jenny and Kostyuk, Nadiya - Lawfare. The Pros and Cons of Mandating Reporting From Ransomware Victims. (2021, Nov. 1) Extracted from the Lawfare Website: https://www.lawfareblog.com/pros-and-cons-mandating-reporting-ransomware-victims

NIAC. Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure. (2017 August) Extracted from NIAC (National Infrastructure Advisory Council) Website: https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

SEC. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. (2018, Feb. 26) Extracted from the SEC website: https://www.sec.gov/rules/interp/2018/33-10459.pdf