Summer 7-24-2023

Practical Approaches and Guidance to Small Business Organization Cyber Risk and Threat Assessments

Stanley Mierzwa
Kean University, smierzwa@kean.edu

Aneta Klepacka
ISC(2), anetaxk@hotmail.com

Practical Approaches and Guidance to Small Business Organization Cyber Risk and Threat Assessments

Stanley J. Mierzwa
Kean University Center for Cybersecurity
Cloud Security Alliance NJ Chapter

Aneta Klepacka
ISC(2) New Jersey Chapter

Cyber-attacks and breaches can occur in any organization type, and the areas of small businesses are not exempt from this nefarious activity. This research note and rapid review provide various cybersecurity tools, guidelines, and frameworks that a small business can consider when embarking on the action to assess its cybersecurity hygiene and defensive stance. The content was pulled together in response to the need for an easy-to-digest approach that a small business utilizes to gain valuable confidence to undertake a self-assessment or third-party review of an organization's cybersecurity plans. Regarding cybersecurity concerns, doing nothing is not an option, and taking an initial step to review computing, information technology, and data systems practices will only be beneficial in attempting to sustain a business and organization.

Keywords: cybersecurity risk, cybersecurity, risk management, small business, frameworks

INTRODUCTION

When approaching an organization's cybersecurity risk or threat assessment, an entry-level or initial question may arise is what framework or strategy should be approached? With so many industry and sector-specific frameworks to utilize, which is the best to method? In this short review, background, options, and rapid literature review, content related to the variety and available cyber frameworks and cyber checklists one can utilize to cyber assess and determine the threat assessment to an organization may be. For many and any organization, particularly the small to medium business sector, understanding and being aware of the potential threats and risks are valuable to preventing the deterrence of a sustaining operation. The goals of this research report include a combination that provides useful content that consists of a review of frameworks, when and where to approach them, and a background into the available toolsets that can aid a small to medium-sized business with approaching cyber risk assessments.

SMALL BUSINESS BACKGROUND GLOBALLY

Globally, over 90 percent of the worldwide business economy resides within the Small to Medium-sized business community (Chidukwani et al., 2022). Within the United States, an estimated 28.2 million

businesses exist, according to the Small Business Administration, and remain an important aspect of our nation's economic infrastructure (Paulsen & Toth, 2016). Small and Medium-sized enterprises/businesses (SMEs/SMBs) experience constraints in tackling cybersecurity best practices because of a lack of awareness, resources, and general expertise (Paulsen, 2016; Bada & Nurse, 2019). In essence, these businesses contend with many of the same types of cybercrime and cybersecurity threats as larger organizations but cannot tackle the challenges with the same vigor. SMEs may lack the funding for approaching the most basic of preparedness tasks, such as awareness training, and this proposal emphasizes making available very affordable but effective security tasks.

Since the emergence of the COVID-19 pandemic, focused attention on the business end-to-end supply chain has been raised, especially with increased data breaches. Small business plays a pivotal role in the supply chain and are now being more scrutinized for their security practices, especially in light of corporate social responsibility related to customer data security and privacy (Chidukwani et al., 2022).

BACKGROUND ON THE EFFORT OF ORGANIZATION EXTERNAL INFORMATION TECHNOLOGY SECURITY AUDITS

Organizations of every type, whether for-profit, non-profit, non-governmental, or public agency, for example, may require or benefit from the effort of an information technology security or cybersecurity risk assessment activity. Many times these organizations will entertain the activity of a self-assessment prior to having an external entity perform the action. An initial thought may be to follow what other organizations have done in this task when approaching such an evaluation. For this activity, the idea of what framework, checklist, or audit tool to utilize will emerge. In addition, as these small to medium-sized businesses grow, they may enter the realm of external auditing activities, which will most likely include the effort to perform a cyber-risk assessment.

VARIETY OF AUDIT OR CYBER RISK ASSESSMENT STRATEGY GUIDELINES AND FRAMEWORKS

In the United States, there are several cyber risk assessment strategy guidelines and frameworks that organizations of all sizes can utilize to protect themselves against cyber threats. The United States government agency National Institutes of Standards and Technology (NIST), housed under the Department of Commerce, provides many industry-specific and focused guidelines and frameworks that can be adopted by small to medium-sized businesses, including those with an international presence. The materials provided by NIST are freely and publicly available for review and adoption. These frameworks are instrumental when partaking in the effort to create or apply a customized cybersecurity framework within the genres of global public health or in the case of helping to contend or prepare for malware incidents, such as ransomware (Mierzwa et al., 2020 & Mierzwa et al., 2022).

In 2014 the National Institute of Standards and Technology published the NIST Cybersecurity Framework (NIST 1.0) as a voluntary guideline to help organizations access and mitigate cybersecurity risk. The framework was revised in 2018 (NIST 1.1). Currently, NIST is working towards updating the current Cybersecurity Framework (CSF 2.0). The framework references five areas: identification, protection, detection, response, and recovery of the organization's assets. Using this framework helps organizations to select the operational areas which require investment in cybersecurity protection and spending (NIST, 2023).

Other cyber risk assessment guidelines and frameworks include those produced and available through the Center for Internet Security as well as several others. This variety of strategy guidelines is outlined below.

CIS Risk Assessment

The Center for Internet Security (CIS) is a non-profit organization. The organization offers business entities of all sizes various security measures such as resources, guidelines, controls, benchmarks, and tools

to assist them with assessing and implementing security controls to safeguard the business environment and provide better defense related to existing security threats. CIS controls, and benchmarks cover products from over 25 vendors, such as Microsoft, Cisco, Linux, VMware, and many others (Center for Internet Security, 2023). Organizations can implement CIS Risk Assessment Methodology to evaluate their current position against the best practices and critical security measures (Center for Internet Security, 2023). Furthermore, CIS offers a prioritized approach for implementing best practices and controls, which helps decrease the attack trajectories of affected systems (Echeverria et al., 2021).

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) issued a Cybersecurity Resource Guide for Financial Institutions. The guide, revised in November of 2022 from the earlier 2018 resource, provides financial institutions with the resources to access and evaluate their current security and cybersecurity posture (FFIEC.GOV, 2023). In addition, FFIEC established the Cybersecurity Assessment Tool, which aims to recognize the institution's risk and allows it to appraise its resilience over time (Federal Financial Institutions Examination Council, 2022). The Cybersecurity Assessment Tool contains two main or pertinent sections for organizations to perform, an inherent risk profile and leveling of the cybersecurity maturity level (FFIEC, 2017).

ISO

Another tool that companies can voluntarily utilize is an International Standard ISO/IEC 27001, published by the International Organization for Standardization and the International Electrotechnical Commission (2022). This standard guides the secure implementation and preservation of the company asset and, as a result, improves the company's cybersecurity posture. Organizations that meet the requirements can be further certified by an independent audit (ISO, 2023).

COBIT

The Information Systems Audit and Control Association (ISACA) developed Control Objectives for Information and Related Technologies (COBIT) framework to help the organization with information technology asset management and protection. This framework aims to connect the business and information technology objectives while addressing the overall business risk (COBIT, 2019). A common theme of the framework is implementing effective governance to implement technology with success and innovation in mind. A version of the COBIT 2019 guidance and framework has been developed for small to medium-enterprise organizations. This focused version of COBIT can be beneficial to business owners and managers that have limited in-house IT skills or capacity, may outsource their more complex IT activities, aim towards buying solutions rather than building, may include a more high-risk tolerance, and are very conscious of costs (ISACA, 2019).

Sector Specific

The Department of Homeland Security (DHS) established Cybersecurity and Infrastructure Security Agency (CISA) to focus on cybersecurity and protection of government agencies. CISA provides guidance and resources for organizations to strengthen their security postures. The agency focuses on cybersecurity best practices, and risk management and provides information regarding current cyber hazards. It also provides services to the Government and public sectors. On January 10, 2023, CISA published a resource guide: Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks developed by the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force. This valuable resource guide provides advice for businesses with limited resources on how to evaluate and prioritize their purchasing decisions to minimize and better manage business risks (CISA, 2023).

PCI-DSS

The credit card industry needs to comply with Payment Card Industry Data Security Standard (PCI DSS). This standard, developed by the PCI Security Standard Council (PCI SSC), established requirements for credit card processors to protect the information of cardholders' data (PCI Security Standards Council, 2022).

HIPAA

The Health Insurance Portability and Accountability Act (HIPPA), established in 1996, is a federal law that regulates how healthcare providers must collect, process, and store sensitive patient health information and prohibits the disclosure of this information without the patient's consent (HIPPA, 1996). Healthcare providers can be categorized in many different areas with work roles. In one set of definitions, the California Department of Consumer Affairs provides licensing and regulations to over 19 healthcare work roles, including nurses, doctors, psychology experts, occupational therapists, and many others (California Department of Consumer Affairs, 2023).

GLBA

The Gramm-Leach-Bliley Act (GLBA), the Financial Services Modernization Act of 1999, regulates how financial institutions are obligated to collect, process, and store financial information. The act also mandates that financial institutions provide customers with written privacy policy notices regarding how the institutions will handle customer information .

CONSIDERATIONS FOR INTERNATIONAL GUIDELINES AND REGULATIONS REGADING INFORMATION SECURITY

In August 2016 European Union established a Directive on Security of Network and Information Systems (EU 2016/1148), NIS Directive (Lex - 32016L1148 - EN - EUR-Lex), the first European statute addressing evolving cybersecurity matters among its members. This Directive aimed to improve the cybersecurity resilience of the member countries and mandate reporting of cybersecurity incidents. As a result, the members of the EU were obligated to implement domestic regulations based on the above directives. To strengthen the cyber resilience of its members and address evolving cybersecurity threats in the present geopolitical climate, in December of 2022, the European Parliament published NIS 2 Directive (EU) 2022/2555 (Lex - 32022L2555 - EN - EUR-Lex). This amended Directive established measures to identify critical infrastructure entities based on their societal, economic, or functional roles in the community or sector and further mandated their requirements related to cybersecurity resilience.

To provide guidelines and enhancements to the cybersecurity framework, assist the member countries with providing best practices, and unify the effort to address cyber threats European Union instituted European Union Agency for Cybersecurity, which currently operates under the Regulation No 526/2013 (EUR-Lex - 32013R0526 - EN - EUR-Lex (europa.eu)). Further, the Regulation (EU) 2019/881 of the European Parliament and of the Council published on April 17 of 2019 the Cybersecurity Act, which provided ENISA with the authority to establish and maintain a cybersecurity certification framework for digital products, processes, and services.

The General Data Protection Regulation (GDPR), effective in May of 2018, is the most comprehensive and standardized in the European Union. It regulates the data privacy of EU citizens and promotes the implementation and controls of thorough data protection measures.

REVIEW OF SMALL TO MEDIUM-SIZED BUSINESS-REPORTED BREACHES OR ATTACKS

Implementing CIS controls helps strengthen the existing information technology infrastructure, ensure the closure of unused ports, and manage available services and user access. An example study performed at a large, unnamed multinational corporation aimed to evaluate its existing information technology

infrastructure against CIS Benchmarks showed that the company scored 28.87% against the established benchmarks. After implementing all CIS Security controls, the company score improved to 98.26% (Sasidharan, 2022).

It is important that organizations implement NIST Framework while continuing to evaluate their current infrastructure using cost-benefit analysis (Gordon et al., 2020). The implementation of specific frameworks should be appraised and utilized by organizations based on their risk maturity level and cost-benefit analysis (Alshar'e, 2023).

AVAILABLE AND FREE TOOLS TO AID SMALL BUSINESSES WITH RAPID CYBER RISK AND THREAT ASSESSMENTS

Cyberplanner Online Tool

The Federal Communications Commission (FCC), recognizing the need to enable and assist small businesses, created both Cybersecurity Tip Sheets but also a guide site to help create a custom plan to assist these organizations (Federal Communications Commission, 2023). The planner is an excellent way to include relevant topics such as privacy and data security, mobile devices, and payment cards to help provide a starting block for small businesses as a plan of both self-assessments and answering questions that detail their needs. A resulting customized report is provided to the business that can be utilized.

The Cyber Security Evaluation Tool (CSET)

Through the Department of Homeland Security, a freely available tool that can be downloaded and installed on a local computer can be used for various self-assessment activities; the tool is called the Cyber Security Evaluation Tool (CSET). This tool has gone through a variety of upgrades, and most recently, the welcomed addition of a ransomware readiness assessment is added. The utility and tool are non-intrusive, meaning that once installed it can walk an end-user through the variety of questions to be addressed when self-assessing or externally assessing a small business for cybersecurity threats and vulnerabilities. The tool can be used in large organizations and those from particular sectors but can certainly be approached by any small to medium-sized business. Upon running the utility prompts, select requirements that align with many government and industry standards are provided. These prompts allow one to zero in on a particular framework such as the NIST Special Publications 800-53, the NIST Cybersecurity Framework, the NERC Critical Infrastructure Protection Standard 002-009, and the NIST Special Publication 800-82 Guide to Industrial Control Systems Security.

NIST 7621. Small Business Information Security: The Fundamentals

The National Institutes of Standards and Technology maintain many frameworks and cybersecurity guidelines for government entities, but the available materials can be utilized by private organizations globally. The NIST 7621 reference guide is intended for small businesses that use information technology and are approachable with a non-technical language delivery (Paulsen & Toth, 2016). Background and content are provided surrounding the understanding of risks, identifying and prioritizing information types, creation of an inventory of both hardware and software utilized, identifying threats to Confidentiality, Integrity, and Availability, safeguarding information via the Cybersecurity Framework categories, and many other important elements.

Center for Internet Security CIS Critical Security Controls

Previously known as the SANS Critical Security Controls – with a top 20 set of controls for organizations to consider, review and implement, these now are in the current form of 18 CIS Critical Security Controls (Center for Internet Security, 2023). The controls range from item categories of specifically inventorying hardware and software assets to content related to account and access management, as well as email and web protection controls and network monitoring and defense. These controls can be seen as an excellent way to begin to work towards compliance in areas required for healthcare (HIPAA), and the payment card regulations (PCI-DSS). These controls can be an approachable

mechanism for small to medium-sized businesses to create a priority and self-awareness of their current cyber hygiene.

UNMET OR EXISTING GAPS

Small to medium-sized businesses that are not focused on information security or cybersecurity will experience challenges by default if utilizing technology in their organizational operations. Consider a business that provides office cleaning services or supplies to businesses and organizations; their main goal may not include the security of the technology they utilize but rather the core business they provide. The recently released White House National Cybersecurity Strategy includes content relevant to helping small to medium-sized businesses by recognizing that these outlets will have limited capability to defend against cyber threats and carry way too much of a burden (Whitehouse.gov – National Cybersecurity Strategy, 2023). One approach outlined is to rebalance the responsibility of defending against cyber threats putting more responsibility on those organizations in the best position to apply resources. In essence, this can be the Managed Service Providers or hardware and software solution product providers. To meet the gap of protecting small businesses with their cyber risk management, this strategy is valuable and would help meet the unmet needs of this sector of businesses. Over time, ensuring higher quality and attention to cyber and security defenses in products delivered will help all businesses. The next and successive further step in this research effort is to create a self-report survey questionnaire to distribute to the small business community. Such an activity would provide valuable insights into such valuable qualities as to what strategies and frameworks are employed, the level of concern, the rate of attacks witnessed, and similar by these organizations. Such a questionnaire could initially be completed by organizations in a single state in the United States and then further follow up with more organizations nationally. There is the possibility of working with the Small Business Development Centers of each state in coordination of such a self-report electronic survey activity.

FUTURE DIRECTIONS

Most small businesses need more resources and expertise to use existing guidelines and tools to protect themselves against rising security threats. Despite this, existing threats cannot be overlooked or ignored because of the harm the cyber threats can do to the business, such as loss of revenue or reputational loss. Notwithstanding the many available resources, small businesses must rely on Managed Service Providers (MSPs) or cybersecurity experts and their technical and consulting support. Minimum protection efforts fail to provide a standard adequate to protect businesses from the creativity and uncompromising efforts of Cyber Security threats and attacks. Many MSPs do not offer “security by design” approaches while implementing new hardware or software. One major shortcoming of this type of practice is applying default settings to convey system vulnerabilities, which exposes companies to cyber threats. It will be beneficial if there is a requirement for service providers to ensure that all products they are offering will be implemented with the best practices and recommendations from the industry standards, for example, the one offered by CIS Benchmarks. Several limitations exist with this research report; first a study was not approached to survey or benchmark what frameworks and resources small businesses are implementing or utilizing to address cyber risks in their organizations. A future activity involving a small business survey would add to the available literature on this topic. Additionally, partnering with the state and federal small business programs was not initiated or advanced, and a future effort should include such collaboration for a more formidable and comprehensive research product.

CONCLUSION

As the number of technology solutions increase in organizations and businesses, regardless of size or sector, the potential for cyber or information security risks will also increase. For small to medium-sized organizations and businesses, there may often be the priority to maintain and grow a business from a profit

and innovation standpoint, but not necessarily to assess cyber defenses and cyber hygiene. In the current technological climate, with the rapid implementation of cloud and mobile solutions, these smaller outfits may need to quickly find methods to perform cyber risk assessments, especially during times of change, growth, or rapid integrations. This brief research report can provide these organizations with a method to review approachable frameworks and a toolbox small to medium businesses can consider or reach inspiration for creating their approaches with a mix of solutions. As outlined previously, the recent National Cybersecurity Strategy provides hope that going forward into the decade, the need for small to medium-sized businesses to place energy into cyber risk assessment may decrease. This is yet to be seen, but until that time arrives, such organizations need to take the appropriate and proactive steps to secure and sustain their operations.

ACKNOWLEDGEMENTS

Formidable acknowledgment to the New Jersey Chapters of ISC(2) and the Cloud Security Alliance (CSA) New Jersey chapter for providing excellent opportunities for subject matter experts to collaborate. This write-up is the result of a professional and sector relationship created during the time of professional networking at ISC(2) and CSA events hosted at Kean University and presentations and situational awareness outreach activities. The Kean Center for Cybersecurity is a conduit for research-based collaboration opportunities, and this effort is grateful to this focus.

REFERENCES

Alshar'e, M. (2023). Cyber Security Framework Selection: COMPARISION of NIST and ISO27001. *Applied Computing Journal*, pp. 245–255. https://doi.org/10.52098/acj.202364

ASPE. (n.d.). *Health Insurance Portability and Accountability Act of 1996*. Retrieved March 25, 2023, from https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

Bada, M., & Nurse, J.R.C. (2019). Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs). *Information & Computer Security*, *27*(3).

California Department of Consumer Affairs. (2023). *Consumer's Guide to Healthcare Providers*. Retrieved March 27, 2023, from https://www.dca.ca.gov/publications/healthcare_providers.pdf

Center for Internet Security. (2023). About us. Retrieved March 6, 2023, from https://www.cisecurity.org/

Center for Internet Security. (2023). *Controls*. Retrieved March 12, 2023, from https://www.cisecurity.org/controls

Chidukwani, A., Zander, S. & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, *10*.

CISA.GOV. (n.d.). *Securing Small and medium-sized business supply chains.* Retrieved March 11, 2023, from https://www.cisa.gov/sites/default/files/publications/Securing-SMB-Supply-Chains_Resource-Handbook_508.pdf

Cybersecurity and Infrastructure Security Agency. (2023). *The Cyber Security Evaluation Tool (CSET)*. Retrieved March 6, 2023, from https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

Cybersecurity and Infrastructure Security Agency. (n.d.). About us. Retrieved March 11, 2023, from https://www.cisa.gov/

Echeverría, A., Cevallos, C., Ortiz-Garces, I., & Andrade, R.O. (2021). Cybersecurity model based on hardening for secure internet of things implementation. *Applied Sciences*, *11*(7), 3260. https://doi.org/10.3390/app11073260

EUR. (2013, May 21). *Lex - 32013R0526 - en - EUR-lex*. Retrieved January 10, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0526

EUR. (2016, July 6). *Lex - 32016L1148 - en - EUR-lex*. Retrieved January 10, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A194%3ATOC
EUR. (2022, December 14). *Lex - 32022L2555 - en - EUR-Lex*. Retrieved January 10, 2023, from https://eur-lex.europa.eu/eli/dir/2022/2555
EUR. (n.d.). *Lex - 32019R0881 - en - EUR-Lex*. Retrieved January 10, 2023, from https://eur-lex.europa.eu/eli/reg/2019/881/oj
Federal Communications Commission. (2023). *Cyberplanner 2.0*. Retrieved March 6, 2023, from https://www.fcc.gov/cyberplanner
Federal Trade Commission. (2023). *Gramm-Leach-Bliley Act*. Retrieved from https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
FFIEC Home Page. (2023). About us. Retrieved March 6, 2023, from https://www.ffiec.gov/
FFIEC.GOV. (2017). *FFIEC Cybersecurity Assessment Tool.* Retrieved March 27, 2023, from https://www.ffiec.gov/pdf/cybersecurity/ffiec_cat_may_2017.pdf
FFIEC.GOV. (2022). Cybersecurity Resource Guide for Financial Institutions. Retrieved on March 27, 2023, from https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf
Gordon, L.A., Loeb, M.P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa005
Henry, S., & Brantly, A.F. (2018). Countering the Cyber Threat. *The Cyber Defense Review*, *3*(1).
ISACA. (2019). *COBIT for Small and Medium Enterprises Using COBIT 2019.* Retrieved March 27, 2023, from https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004L2noEAC
ISACA. (2023). C*OBIT: Control objectives for Information Technologies*. Retrieved March 11, 2023, from https://www.isaca.org/resources/cobit
ISO. (2023, February 3). *ISO/IEC 27001 and related standards - information security management*. Retrieved March 11, 2023, from https://www.iso.org/isoiec-27001-information-security.html
Masombuka, M., Grobler, M., & Duvenage, P. (2021). *Cybersecurity and Local Government: Imperative, Challenges and Priorities*. DOI: 1034190/EWS.21.501
Mierzwa, S., RamaRao, S., Jung Ah, Y., & Gyo, B. (2020). Proposal for the Development and Addition of a Cybersecurity Assessment Section into Technology Involving Global Public Health. *International Journal of Cybersecurity Intelligence & Cybercrime*, *3*(2). https://www.doi.org/10.52306/03020420BABW2272
Mierzwa, S.J., Drylie, J.J., Ho, C., Bogdan, D., & Watson, K. (2022). Ransomware Incident Preparations with Ethical Considerations and Command System Framework Proposal. *Journal of Leadership, Accountability and Ethics*, *19*(2). https://doi.org/10.33423/jlae.v19i2.5112
NIST. (2023, March 21). *Cybersecurity framework*. Retrieved March 25, 2023, from https://www.nist.gov/cyberframework
Paulsen, C. (2016). Cybersecuring Small Businesses. *Computer*, *49*(8).
Paulsen, C., & Toth, P. (2016). N*ational Institutes of Standards and Technology: Small Business Information Security: The Fundamentals*. NISTIR 7621. Revision 1.
PCI Security Standards Council. (2022, September 26). About Us. Retrieved March 11, 2023, from https://www.pcisecuritystandards.org/about_us/
PCI Security Standards Council. (2023). Official PCI Security Standards Council Site. Retrieved March 11, 2023, from https://www.pcisecuritystandards.org/
Sasidharan, R. (2022). A case study to implement windows system hardening using CIS controls. *International Journal of Computer Trends and Technology*, *70*(7), 1–7. https://doi.org/10.14445/22312803/ijctt-v70i7p101

Whitehouse.Gov. (2023). *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*. Retrieved March 12, 2023, from https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

Whitehouse.Gov. (2023). *National Cybersecurity Strategy*. Retrieved March 12, 2023, from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf