The Scholar: St. Mary's Law Review on Race and Social Justice

Volume 24 | Number 2 Article 5

5-13-2022

Small Business Cybersecurity: A Loophole to Consumer Data

Matthew R. Espinosa
St. Mary's University School of Law

SMALL BUSINESS CYBERSECURITY: A LOOPHOLE TO CONSUMER DATA

MATTHEW R. ESPINOSA*

* Juris Doctorate Candidate at St. Mary's University School of Law, May 2022. B.A., Our Lady of the Lake University, 2018. I write this piece out of my growing interest in cybersecurity and data privacy, and its intersection with the legal system. Furthermore, I believe small businesses and especially minority-owned small businesses are not only pivotal to our economy, but one of the greatest benefits in the communities they serve due to their outreach. Cyberattacks can have catastrophic impacts to the survival of the business as well as their patrons' data. Therefore, I hope my analysis of existing legislation, regulation, and programs along with my suggestions help bridge the cyber gap for small businesses.

I want to thank my family and specifically my parents, Lisa and Rene Espinosa, for their unwavering love and support; as well as instilling values that have helped me persevere and succeed through my law school journey. Additionally, I want to thank my fiancé Samantha Whisenhunt for staying up and supporting me through long days and nights as Staff Writer comment deadlines approached. I could not have accomplished this feat without her constant love, support, and encouragement. Furthermore, I want to thank Bob Butler for guiding me through a new subject matter I have no experience in and connecting me with other individuals who assisted in my research. In addition, I would like to thank Victor Malloy, a cybersecurity professional who has been a mentor for me throughout this whole process, pointing me to resources for my research, and connecting me with other professionals for guidance. Lastly, I want to thank Volume 23 of *The Scholar* for the support and encouragement throughout the writing process, as well as Volume 24 of *The Scholar* for their assistance in editing this piece.

INTRODUCTION

Most people do not think about cybersecurity and how it affects their lives on a daily basis.[1] A majority of people don't even consider cybersecurity matters, other than the password that protects their mobile devices.[2] However, when people do think of cybersecurity matters, the topic generally revolves around nation states—such as China, Russia, Iran, and the United States—hacking each other to retrieve intelligence secrets.[3] In a world where individuals and businesses utilize the latest technology to connect to the internet, continental barriers cease to exist to protect nation states.[4] Almost every industry in the global economy has been affected by cyberattacks in one shape or form.[5] Beyond that, cyberattacks have reached the world's largest corporations and governments at the federal, state, and local levels.[6] In 2020, the global average total cost of a data breach was $3.86 million; the United States outpaced the global cost of a data breach, averaging $8.64

1. *See generally* Frank Konkel, *Survey: Most Americans Don't Worry About Cybersecurity Despite Increased Attacks,* NEXTGOV (June 23, 2020), https://www.nextgov.com/cybersecurity/2020/06/survey-most-americans-dont-worry-about-cybersecurity-despite-increased-attacks/166373/ [https://perma.cc/LRM2-UCUP] ("More than two in three Americans are not concerned about internet security despite a massive spike in cyber activity targeting people working remotely due to the coronavirus . . . ").

2. *See generally* Aaron Smith, *Americans and Cybersecurity*, PEW RSCH. CTR., (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/ [https://perma.cc/Z4KK-YWNA] (highlighting that many Americans are failing to follow digital security best practices in their own personal lives even though a majority expect major cyberattacks will be a fact of life in the future).

3. *See* PONEMON INST., IBM SEC., COST OF A DATA BREACH REPORT 2020 39 (2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf [https://perma.cc/TW4U-EC2J] (understanding that the data breach conversation often revolves around nation states but introducing data breaches as root causes that affect businesses).

4. *See* Nelson N. Neto et al., *A Case Study of the Capital One Data Breach* 17 (MIT SLOAN SCH. OF MGMT., Working Paper CISL No. 2020-16, 2020), http://web.mit.edu/smadnick/www/wp/2020-16.pdf [https://perma.cc/W9P9-YYWS] (explaining how these broken continental barriers can result in a domino effect of compromised security in organizations).

5. *Cf. id.* (concluding from a statistical analysis of data leaks in a four-year span that cyberattacks can happen within any industry).

6. *See The Cybersecurity Program*, U.S. ATT'Y OFF. CENT. DIST. OF CAL., https://www.justice.gov/usao-cdca/cybersecurity-program [https://perma.cc/ZC2X-82X4] (last updated July 12, 2021) ("All types of businesses have been victimized, from banks to retailers, to mom-and-pop financial firms, to entertainment companies, to restaurant chains, to health care providers. Hacking can cost businesses millions of dollars each year.").

million.[7] Data breaches occur from different types of attacks ranging from malicious attacks, system glitches, or human error.[8] Although these cyberattacks have the largest impact on nation states or large corporations, there is also an impact on small businesses.[9] Here, in the United States, 61% of small businesses have experienced cyberattacks that can be detrimental to the business as well as to the individual consumers if their private data is compromised.[10]

Due to the financial strain cyberattacks place on the economy and the detrimental impact on corporations and consumers, there is substantial legislative and regulatory oversight on safe cybersecurity practices.[11] However, the legislation, regulations, and programs in place are all aimed at assisting specific industries, large corporations, and government entities.[12] It is important to ensure those industries, corporations, and entities have reliable cybersecurity standards and procedures in place to prevent a potential data breach which could cause more widespread harm to the public and consumers in general.[13] While most of the regulations

7. *See* PONEMON INST., *supra* note 3 (illustrating that although some may believe data breach costs have plateaued, there is a growing divide in costs between organizations with more advanced security processes and those with less advanced security postures).

8. *See id.* (reporting the varying percentages of breaches caused by malicious attacks, system glitches, and human error in countries located in the Middle East, Africa, South America, Europe, and North America).

9. *See generally id.* (illustrating the varying cost of cyberattacks on different sized organizations while also making reference to the impacts of cyberattacks on these businesses. Furthermore, IBM asserts that even with these risks, only a fraction of the businesses deploy full scale cyber defenses).

10. *See* FRANKLIN D. KRAMER & ROBERT J. BUTLER, ATL. COUNCIL 4 (2019), https://www.atlanticcouncil.org/in-depth-research-reports/report/cybersecurity-changing-the-model/ [https://perma.cc/K359-M8P2] (identifying how small businesses that fall victim to cyberattacks largely contribute to the overall expense of cyberattacks and prove fatal to the individual business).

11. *See State Data Security Laws*: *Overview*, THOMSON REUTERS PRACT. L, https://1.next.westlaw.com/Document/I48b98d81178f11e698dc8b09b4f043e0/View/FullText.html?transitionType=SearchItem&contextData=(sc.Search) [https://perma.cc/G5GT-TNN9] (comparing state data security laws and standards that are utilized to regulate corporations and industries).

12. *See* NAT'L ASS'N OF INS. COMM'R & THE CTR. FOR INS. POL'Y AND RSCH., THE NAIC INSURANCE DATA SECURITY MODEL LAW 1 (2020), https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf [https://perma.cc/KX9Y-UNY2] (suggesting industry regulation, specifically for licensed insurance companies, that states could adopt to create a cybersecurity standard and protect consumers data); *see also* Neto et al., *supra* note 4 (discussing different Federal Agency regulations regarding cybersecurity standards for different industries).

13. *See generally* PONEMON INST., *supra* note 3 (detailing a broad overview of the longtail costs cyberattacks and data breaches have on the global economy).

and policies in place are both expensive and a hassle to implement, government entities and corporations have the means to implement the policies and abide by them as well as the assistance from the regulating entities.[14] The legislation, regulations, and programs that assist in bolstering cybersecurity practices tend to exclude small businesses due to the minor impact that would occur from a cyberattack.[15]

The large variety of cyberattacks and unique ways cybercriminals are conducting them makes cybersecurity a constant challenge for smaller businesses.[16] Even with basic protection, small businesses and especially small, minority-owned businesses may not even attempt to address cybersecurity issues because it is too much of an economic detriment to do so.[17] Whether it is the fear of data sharing with other small businesses, industry regulations that are too expensive for them to implement, or lack of government assistance in securing quality cybersecurity, the cost of a data breach may force a small businesses into bankruptcy.[18] In San Antonio, Texas, there is a plethora of small minority-owned businesses.[19] Therefore, if cybersecurity standards are

14. *See Cybersecurity Insurance*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cybersecurity-insurance [https://perma.cc/T5CB-26VE] (providing information and resources for private sector and government entities on the best cybersecurity strategies).

15. *See generally* PONEMON INST., *supra* note 3 (focusing primarily on data breaches, known as mega breaches, impacting large industries and corporations).

16. *See generally* Courtney King, *Texas Cybersecurity: Protecting Data Systems,* COMPTROLLER.TEX.GOV (Mar. 2019), https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/cybersecurity.php [https://perma.cc/MG76-CPXP] (emphasizing basic cybersecurity protection such as anti-virus software or firewalls are not enough for small businesses or individuals to protect their data in the ever-evolving world of cyber threats).

17. *Cf.* Paul Flahive, *Texas Cities Struggle to Defend Against Cybercrime with Sparse Resources*, TEX. PUB. RADIO (May 1, 2019, 5:04 PM), https://www.tpr.org/post/texas-cities-struggle-defend-against-cybercrime-sparse-resources [https://perma.cc/HM8P-VDZM] (relating the woes of cyberattacks on small cities to the effect it would have on small businesses. Both struggle with the funding to adequately defend themselves from the continuing risk of data breaches).

18. *See generally* Samantha Ehlinger, *Small Businesses in Texas at Rising Risk of Cyberattacks*, SAN ANTONIO EXPRESS-NEWS (Jan. 19, 2018), https://www.expressnews.com/business/technology/article/Small-businesses-in-Texas-at-rising-risk-of-12510741.php [https://perma.cc/7HXW-RNYN] (detailing the impact and consequences if small businesses do not maintain good cybersecurity practices. For instance, Texas consumers and businesses reported losing approximately $77.1 million to internet criminals in 2016 alone).

19. *See* Caitlin Cowart, *San Antonio Small Businesses Face $8.3 Billion Capital Gap, with Less Capital Going to Black- and Hispanic-Owned Businesses,* SANANTONIO.GOV (Apr. 2, 2021), https://www.sanantonio.gov/gpa/News/ArtMID/24373/ArticleID/20331/San-Antonio-Small-Busi

subpar, unenforced, and no assistance is given to implement them, in effect the small business's minority consumers are negatively impacted.[20] If a consumer's personal data is stolen, it could lead to identity theft, loss of money, or additional data breaches affecting any entities they are associated with.[21] Federal, state, and local governments failing to assist small, minority-owned businesses inadvertently place minority consumers' personal data at risk as compared to their corporate consumer counterparts.[22] Thus, without more tailored support through legislation and regulation at the federal, state, and local levels, small businesses and their patrons are essentially being disenfranchised and left to suffer the consequences alone.[23]

A. Small, Minority-Owned Businesses Economic Impact

To qualify as a Small Minority and/or Woman Business Enterprise (S/M/WBE) in Bexar County, there must be, "a sole proprietorship or corporation owned, operated, and controlled by one or more minority group members or women that have at least 51% ownership."[24] As of 2017, at least one million of the United States eight million minority-

---

nesses-Face-83-Billion-Capital-Gap-With-Less-Capital-Going-To-Black-and-Hispanic-Owned-Businesses [https://perma.cc/CKC2-LLY8] ("San Antonio and Bexar County are home to approximately 34,000 small businesses and approximately 145,000 sole proprietorships. These small businesses and sole proprietors account for 34% of the local workforce.").

20. *Cf. Table of Experts: Cybersecurity Professionals on Handling a Data Breach*, SAN ANTONIO BUS. J. (Apr. 2, 2020, 12:01 AM), https://www.bizjournals.com/sanantonio/news/2020/04/02/table-of-experts-cybersecurity-professionals-on.html [https://perma.cc/4ACD-Y9R8] (stating that small businesses have limited IT resources and smaller budgets making them less likely to have reliable cybersecurity systems in place).

21. *See* Merritt Baer, *Cybersecurity is a Social Justice Issue*, FELS INST. OF GOV'T: UNIV. PENN. (Nov. 3, 2017), https://www.fels.upenn.edu/recap/posts/1404 [https://perma.cc/4GC3-UVSQ] (explaining how small business data breaches leave consumers vulnerable; thus, creating a domino effect of data breaches impacting entities the consumer is affiliated with).

22. *Cf.* Ehlinger, *supra* note 18 (inferring that without assistance from industry regulation or legislation, small businesses and their patrons will continue to be severely impacted. For example, cyber insurance was once only reserved for big corporations with large budgets that small companies do not have).

23. *See generally* Baer, *supra* note 21 (elaborating on the effects that cybersecurity practices have on wealth discrimination in America and other social justice issues).

24. *See* INST. FOR ECON. DEV. & CTR. FOR BUS. RSCH., THE UNIV. OF TEX. AT SAN ANTONIO, AFRICAN-AMERICAN BUS. ENTER. RSH. SURV. 8, https://www.bexar.org/DocumentCenter/View/13054/View-the-AABE-Survey-Appendix?bidId [https://perma.cc/KE8B-GHPC] (compiling data on businesses seeking certification under the S/M/WBE program or other minority enterprise titles because of the benefits derived from those certificates).

owned businesses were based in Texas.[25] In 2016, the eight million minority-owned businesses contributed $1.4 trillion to the U.S. economy.[26] S/M/WBE contributed to those numbers and further represents 97% of employer firms in the San Antonio area.[27] The San Antonio Economic Development Office has implemented a program that assists S/M/WBE in attaining city contracts, thereby helping stem their development and community reach.[28] In 2019, 54% of city contract dollars were paid to S/M/WBE applicants in comparison to only 10% in 1992 illustrating a historic underutilization of city contract money going to S/M/WBEs.[29] Although S/M/WBEs are a vital part of San Antonio's economy and serve several thousands of San Antonio area minority residents, they are still impacted by cyberattacks which put their success at risk.[30]

B. San Antonio is Equipped to Ensure Small Businesses Have Effective Cybersecurity

Texas is ranked highly among other states in cybersecurity growth due to San Antonio's reputation as one of the largest cybersecurity hubs in

25. *See* Jan Ross P. Sakian, *How Can San Antonio Help Develop Minority-Owned Businesses?*, TEX. PUB. RADIO (Oct. 10, 2017, 5:17 PM), https://www.tpr.org/post/how-can-san-antonio-help-develop-minority-owned-businesses [https://perma.cc/45W8-B8P9] (recognizing that these U.S. Department of Commerce statistics make the business-friendly state a leader for entrepreneurs with diverse backgrounds).

26. *See id.* (illustrating the positive contribution minority-owned businesses have had on the Texas and U.S. economies).

27. *See* CITY OF SAN ANTONIO ECON. DEV. DEP'T, 2019 ANNUAL REP. 8 (2019), https://www.sanantonio.gov/Portals/0/Files/EDD/Media/EDD-AnnualReport.pdf [https://perma.cc/AY7G-NKYU] (highlighting the City of San Antonio's Economic Development Department's statistics and accomplishments for 2019).

28. *See generally* Shari Biediger, *San Antonio City Contracts: Where Small Businesses Made Big Gains in 2017*, SAN ANTONIO REP. (Feb. 21, 2018), https://sanantonioreport.org/san-antonio-city-contracts-where-small-business-made-big-gains-in-2017/ [https://perma.cc/LZA8-XSXL] (reporting on the S/M/WBE program's progress from 1992 to 2015 in reducing purchase disparities).

29. *See* CITY OF SAN ANTONIO ECON. DEV. DEP'T, CITY OF SAN ANTONIO, SMALL BUSINESS OFFICE ANNUAL REPORT 2 (2020), https://www.sanantonio.gov/Portals/0/Files/SBO/SBO-AnnualReport-FY2020.pdf [https://perma.cc/6436-P8LS] (reporting annual statistics relevant to economic development in San Antonio).

30. *See* Flahive, *supra* note 17 (identifying a small city near San Antonio, Texas that was subject to a cybercriminal attack due to the lack of personnel and funds); *see also* San Antonio, Tex., Ordinance 77758, ch. 16, art. X, § 16-252 (explaining the historical challenges S/M/WBE businesses have faced and the scope and impact of the ordinance).

the United States.[31] San Antonio has premier access to the Department of Defense's (DOD) assets such as the F.B.I. Cyber Division, Texas Branch of the National Security Agency (NSA), the United States Sixteenth Air Force headquarters—responsible for intelligence gathering and cyber warfare operations—and the U.S. Air Force 668th Cyber Wing.[32] Regarding education, The University of Texas at San Antonio has the number one cybersecurity undergraduate program in the United States and six universities in San Antonio have NSA Center of Excellence designations, which enables them to specialize in cybersecurity research and education.[33] Furthermore, with regard to the private sector, San Antonio is home to 140 cybersecurity firms with forty of those firms being headquarter operations.[34] San Antonio also ranks second, behind Washington D.C., as having the most certified cyber professionals spread across cyber insurance firms, defense contractor firms, cloud computing firms, and startups.[35] San Antonio has a robust cybersecurity community capable of correcting S/M/WBE disparities in cybersecurity's framework and procedures which have an adverse effect on the minority population.[36]

---

31. *Cf. The Cybersecurity Capital of Texas*, SAN ANTONIO ECON. DEV. FOUND., https://www.sanantonioedf.com/ industries/cybersecurity/ [https://perma.cc/8CFD-469B] (last updated Sept. 27, 2020) (highlighting factors that make San Antonio a central hub for cybersecurity).

32. *See id.* (listing the governmental cybersecurity resources and agencies based in San Antonio that make the city a robust community of cybersecurity assets).

33. *See Business Facilities' 15th Annual Rankings: State Rankings Report*, BUS. FACILITIES (July 24, 2019), https://businessfacilities.com/2019/07/business-facilities-15th-annual-rankings-state-rankings-report/ [https://perma.cc/L6XU-BT38] (highlighting Texas as top ranked in cybersecurity growth and potential).

34. *See id.* ("San Antonio is now billing itself as the 'Cyber City,' and with good reason. San Antonio's cybersecurity industry is mature and growing stronger.").

35. *See id.* (explaining how the San Antonio cybersecurity centers aim to build an environment where industry, government, and academia can come together to solve issues surrounding cybersecurity, while advancing research, education, and workforce development); *see also* King, *supra* note 16 ("Superior training and education, combined with close proximity to cybersecurity offices and installations of the National Security Agency, the Federal Bureau of Investigation, the Department of Homeland Security and the U.S. Air Force, have helped the San Antonio area amass the highest concentration of cybersecurity professionals outside of Washington, D.C.").

36. *See generally* San Antonio Chamber of Com., *Cybersecurity San Antonio: The Ecosystem*, CITY OF SAN ANTONIO, https://www.sachamber.org/get-involved/cyber/ecosystem/ [https://perma.cc/3ECB-KQVL] (explaining how the CyberSecurity San Antonio program

C. Impact of Data Breaches and a Lack of Cybersecurity

In 2015 and 2016, San Antonio suffered costly cybercrimes targeted at businesses and individuals.[37] In 2016, 133 data breaches were reported on an individual level with individuals losing $130,912.[38] In comparison, there were twenty corporate data breaches causing a loss of $67,510.[39] Additionally, over seventy-one identity theft cases were reported, causing a loss of $310,591.[40] Although these numbers do not directly reflect small businesses in San Antonio, they do reflect the general impact of cybercrime on the community.[41] If a small business experiences a data breach, it can impose a domino effect on the community.[42] For instance, if a patron's personal data is breached as a result of a small business data breach, it could essentially cause additional data breaches for the patrons' other business associations.[43] Data breaches negatively affect small businesses in numerous ways, including the grave possibility of consequential bankruptcy.[44]

I. HISTORY

A. Small Businesses Are Vital to the Success of Federal, State, and Local Economies

(CSSAtx) unites and strategizes with the community to address core focus areas, including innovation and economic development).

37. *See* Kristen Mosbrucker, *Exclusive: What Local Businesses Told the FBI about Cyber Crime*, SAN ANTONIO BUS. J. (July 5, 2017), https://www.bizjournals.com/sanantonio/news/2017/07/05/san-antonio-businesses-told-fbi-about-cybercrime.html [https://perma.cc/AA62-56UQ] (analyzing FBI Internet Crime Complaint Center data for San Antonio in 2015 and 2016).

38. *See id.*

39. *See id.* (examining cyber security data gathered by FBI that reflected increases in the number of data breaches occurring in San Antonio).

40. *See id.* (reporting identity theft monetary losses in 2016).

41. *See generally id.* (discussing the impact of cybercrime on business entities).

42. *See* Baer, *supra* note 21 (explaining how one business's data breach can ultimately contribute to additional data breaches for other business entities).

43. *See, e.g., id.* ("The insecurities not only mount, but compound: an insecurity in one dimension of life (let's say payment systems at a retailer) reverberates through other aspects like cell phone and bank account security. This means that, as with many other aspects of daily life, the most vulnerable Americans are hit the hardest.").

44. *See* Ehlinger, *supra* note 18 (urging the need for cyber insurance for small companies to guard against cyberattacks).

It is evident that the top ten largest businesses in the United States contribute significantly more to the economy than do small businesses.[45] For example, Microsoft "is the most valuably traded company in the U.S.," with a $1.1 trillion market cap and more than 140,000 full-time employees.[46] Apple Inc. closely follows Microsoft, employing 137,000 full-time employees; followed by Amazon with 800,000 full-time employees primarily in their warehouse and transport/delivery services.[47] Yet it is small businesses that truly contribute to the growth of the economy.[48]

The federal government defines small businesses as those with fewer than five hundred employees.[49] Most new businesses start out as small businesses, thus firmly placing small businesses at the forefront of job generation.[50] Between 1977 and 2000, small businesses created over seventy million jobs in their first year.[51] However, by 2002, thirteen million of these jobs disappeared due to small businesses closures.[52] Overall, small businesses create more jobs than larger businesses and primarily assist in boosting the economy by filling in gaps within the labor market regarding underprivileged communities.[53] Small businesses employ a higher percentage of certain populations including minorities, individuals with a high school degree or less, high school aged

45. *See generally* Russell Shor, *10 Largest Companies in The US by Market Capitalisation*, FXCM (May 4, 2020, 4:22 PM), https://www.fxcm.com/markets/insights/10-largest-companies-in-the-us-by-market-capitalisation/ [https://perma.cc/M5VT-MV2U] (acknowledging that companies with the highest market cap, high volume of full-time employees, and an enormous credit line, along with their owners, contribute significantly to the current state of the economy).

46. *See id.* (reporting market cap data for the largest companies in the U.S.).

47. *See id.* (identifying the ten largest U.S. companies by market cap and number of full-time employees to illustrate their contribution and dominance in the U.S. economy).

48. *See* BRIAN HEADD, SBA OFF. OF ADVOC., AN ANALYSIS OF SMALL BUSINESS AND JOBS 4 (2010), https://www.sba.gov/sites/default/files/files/an%20analysis%20of%20small%20business%20and%20jobs(1).pdf [https://perma.cc/A7DH-KGBB] (explaining how small firms are pivotal to the growth of the economy, especially when rebounding from a recession).

49. *See id.* at 4 (clarifying that one-half of the private sector is populated by small businesses, with fewer than 500 employees, and the other half by large businesses).

50. *Cf. id.* (contending that small businesses tend to be a disruption in the economy when they are unsuccessful; but also give rise to an uptick in the economy due to job creation).

51. *See id.* at 7 (emphasizing the impact of small business job creation between the first and fifth year and the resulting fifty-seven million jobs that remained).

52. *See id.* (illustrating that while small businesses create new jobs, they also contribute to significant job losses resulting from small business closures).

53. *See id.* at 6 (highlighting the various ways small businesses fill niches in the labor market compared to larger businesses).

workers, and disabled workers.[54] At the state level, small businesses have just as much of an impact on the economy as their larger counterparts.[55]

As of May 2020, small businesses in Texas constituted a little over 99% of all the businesses in the state.[56] There are over 4.8 million small business employees making up 45% of the private labor in the state.[57] Although eighteen thousand small businesses started generating seventy-five thousand new jobs in the fourth quarter of 2018, over fifteen thousand small businesses dissolved within that same time frame, resulting in a loss of sixty-four thousand jobs.[58] While small businesses can be the starting point of a positive economy, they may also negatively impact labor creation.[59] Small businesses in Texas continue to serve underprivileged communities which is reflected in the over 866,000 women-owned small businesses and the over one million minority-owned small businesses.[60]

The data detailing small business's impact on the Texas economy classifies small businesses as those with 500 or less employees; however, Texas classifies small businesses as those with less than 100 employees due to those businesses making up most of the entrepreneurial sector of

54. *See id.* (identifying that small businesses employ 65.9% of the Hispanic population, 63.8% of high school-aged workers, 59.4% of disabled workers, and 63.2% of individuals possessing a high school degree or less).

55. *See generally* U.S. SMALL BUS. ADMIN. OFF. ADVOC., TEXAS SMALL BUSINESS ECONOMIC PROFILE 177 (2020), https://cdn.advocacy.sba.gov/wp-content/uploads/2020/06/04144220/2020-Small-Business-Economic-Profile-TX.pdf [perma.cc/XLQ3-ZNYP] [hereinafter SMALL BUSINESS ECONOMIC PROFILE] (identifying statistical data that illustrates the positive impacts that small businesses have had on the economy).

56. *See id.* (defining small businesses as those employing less than 500 employees).

57. *See id.* (providing data from the beginning of the COVID-19 pandemic, resulting in lower statistics than pre-pandemic data).

58. *See id.* (indicating that newly formed small businesses contribute to job loss nearly as much as they contribute to job creation).

59. *Compare id.* (expounding on the fact that small businesses began the creation and destruction of the state economy), *with* HEADD, *supra* note 48, at 6 (illustrating how small businesses affect the economy in terms of growth and pitfalls compared to larger businesses at the federal level).

60. *See* GOVERNOR'S OFF. ECON. DEV. & TOURISM, OFFICE OF THE GOVERNOR'S SMALL BUSINESS HANDBOOK 68 (2019), https://gov.texas.gov/uploads/files/business/2019_Governors_Small_Business_Online_Handbook.pdf [https://perma.cc/Z5F9-KHYY] (advertising the statistics of successful small businesses in an attempt to persuade potential business owners to incorporate their businesses within the state).

the economy.[61] Whether a small business is classified as consisting of 100 employees or 500 employees, it does not change the small business's impact on the Texas economy.[62] In fact, as of 2012 small businesses consisting of 100 or less employees produced an estimated economic impact of $844 billion in gross output impacting the retail trade, construction, professional-scientific and technical services, and health and social services sectors the most.[63] Furthermore, small businesses generally provide greater training to a broader segment of the population than larger firms, ensuring skilled labor even if the business does dissolve.[64]

The impact of small businesses on the local economy mirrors that of the state level, but at a smaller ratio.[65] For example, in the San Antonio-New Braunfels Metropolitan Statistical Area (MSA), small businesses with fewer than 100 employees made up 10% of the total employment in the first quarter of 2019.[66] Furthermore, small businesses with less than 500 employees in the first quarter of 2019 made up over 55% of the total employment.[67] A 2008 study showed small businesses with less than

61. *See* THOMAS TUNSTALL ET AL., UNIV. TEX. SAN ANTONIO INST. FOR ECON. DEV. & CTR. FOR BUS. RSCH., SMALL BUSINESSES AND THEIR IMPACT ON TEXAS 4 (2016), https://gov.texas.gov/uploads/files/business/small_business_study_texas_office_of_governor.pdf [https://perma.cc/ENQ8-VHFL] (detailing the impact of small businesses with less than 100 employees on the economic sector in Texas).

62. *See id.* (providing similar data showing that small businesses with fewer than 100 employees represented nearly 98% of the private businesses in Texas as of 2012).

63. *See id.* (indicating the magnitude of impact SBF100 firms have on the Texas economy); *see also* SMALL BUSINESS ECONOMIC PROFILE, *supra* note 55 (introducing similar data showing a positive impact on the economy due to small businesses with less than five hundred employees).

64. *See* TUNSTALL ET AL., *supra* note 61 (indicating that small businesses have a more significant impact on their communities than larger businesses).

65. *See generally* MAYA HALEBIC & STEVE NIVIN, SABÉR RES. INST., SMALL BUSINESS STUDY: A PROFILE OF SMALL BUSINESSES IN SAN ANTONIO METRO AREA 7 (2012), http://www.sahcc.org/wp-content/uploads/Small-Business-Study_A-Profile-of-Small-Businesses-in-San-Antonio-Metro-Area1.pdf [https://perma.cc/BD2H-VXHG] (detailing that in the entire year of 2008, small businesses with less than one hundred employees represented a majority of the private businesses and contributed to a quarter of the overall employment).

66. *See Metropolitan Statistical Area Profiles*, TEX. LAB. MKT. INFO., https://texaslmi.com/EconomicProfiles/MSAProfiles [https://perma.cc/4QTE-RUFL] (distinguishing that the San Antonio-New Braunfels MSA is composed of eight counties that include Bexar, Comal, Atascosa, Guadalupe, Kendall, Medina, Bandera, and Wilson County).

67. *See id.* (implying that small businesses may even be more vital to the local economy since the jobs created in the first quarter by small businesses made up over half of the total employment); *see also* SMALL BUSINESS ECONOMIC PROFILE, *supra* note 55 (describing small

one hundred employees made up 97% of private firms and accounted for over 30% of non-rural employment, illustrating how important small businesses are to local economies.[68] The entrepreneurial, economic, and social growth of the MSA relies on small business growth; without it, unemployment goes up and the economy slows down.[69]

It is imperative that the federal, state, and local levels focus on assisting small businesses in being successful because of their effects on the economy.[70] Dangers that would cause small businesses to close, such as cyberattacks, provide a sufficient reason for the government to assist, educate, and regulate small businesses regarding cybersecurity.[71]

B. General Dangers in the Cyber World for Businesses

Cybercrime is the "use of computer technology or the internet to gain unauthorized access to information for exploitive or malicious purposes."[72] Cybersecurity risks include threats to vulnerable information and any related consequences caused by, or resulting from, unauthorized access, disruption, or destruction of such information.[73] Theft of confidential information or intellectual property provides lucrative opportunities for cybercriminals when stealing data from businesses of any size.[74] Over fifty percent of American companies are subject to critical data breaches through an employee's smartphone or

businesses in Texas with five hundred employees or less accumulating just under half of the total employment in 2020).

68. HALEBIC & NIVIN, *supra* note 65 (accounting for over 225,000 jobs, just over 31% of the overall private sector jobs).

69. *See id.* (explaining the overall effects small businesses have on the economy).

70. *Cf.* 6 U.S.C. § 659 (A) (2018) (authorizing the Secretary of Homeland Security to assist small businesses concerned with cyberattacks or cybersecurity).

71. *See* Christine Myers, *Do I Really Need to Worry About Cybersecurity for My Business?*, U.S SMALL BUS. ADMIN. OFF. ADVOC. (Aug. 1, 2018), https://advocacy.sba.gov/2018/08/01/do-i-really-need-to-worry-about-cybersecurity-for-my-business/ [https://perma.cc/9FUH-8VGF] (discussing the biggest threats facing small businesses concerning the weaknesses in their cybersecurity measures).

72. Courtney King, *Cybersecurity: Protecting Data Systems,* COMPTROLLER.TEX.GOV (Mar. 2019), https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/cybersecurity.php [https://perma.cc/MG76-CPXP] (defining the term cybersecurity while expanding on how cybersecurity threats affect private companies, governments, individuals, and consumers).

73. *See* 6 U.S.C. § 659 (A) (2018) (illustrating the meaning behind cyber threats and how information can be modified and destroyed, resulting in devastating consequences).

74. *See* King, *supra* note 72 (defining the term cybersecurity while expanding on how cybersecurity threats affect private companies, governments, individuals, and consumers).

tablet due to cybercriminals becoming more diverse in how they attack businesses.[75] Cybercriminals are using ransomware, coin-mining, supply chain attacks, viruses, phishing, spyware, and mobile malware to steal data.[76] Ransomware attacks constitute hackers planting malicious code inside businesses' information technology (IT) systems, exploiting unsophisticated or out of date cyber defenses, and rendering all the IT systems down until the business pays a ransom to receive back access or stolen data.[77] Technological developments have increased the amount of data shared between consumers and corporations, providing cybercriminals with additional avenues for exploitation.[78]

There are thirty million small businesses in the United States that are vulnerable to cyberattacks.[79] In 2017, the quantity of data stolen from small to mid-sized businesses doubled from 2016, exceeding more than nine thousand records.[80] In 2017, fifty-eight percent of data breaches involved small businesses resulting in losses between $7,000 and $32,000.[81] At best, a data breach could create an uphill battle to deal with the consequences of rebuilding customer trust, securing future

75. *See 2017 Ponemon Institute Study Finds SMBs are a Huge Target for Hackers*, CISION: PR NEWSWIRE (Sept. 19, 2017, 5:00 AM), https://www.prnewswire.com/news-releases/2017-ponemon-institute-study-finds-smbs-are-a-huge-target-for-hackers-300521423.html [https://perma.cc/2REA-HPWQ] (criticizing how critical data is accessible 24/7 with worldwide interconnected devices).

76. *See* KRAMER & BUTLER, *supra* note 10 (discussing how businesses are unable to cope with the wide variety of attacks due to the lack of resources and education on prevention).

77. *See* Marc Ramirez, *Hackers Breach 20 Texas Government Agencies in Ransomware Cyber Attack*, DALL. MORNING NEWS (Aug. 17, 2019, 4:05 PM), https://www.dallasnews.com/business/technology/2019/08/17/hackers-breach-20-texas-government-agencies-in-ransomware-cyber-attack/ [https://perma.cc/5NXG-JZ87] (acknowledging that hackers conduct coordinated attacks on businesses that utilize fundamental or out-of-date security systems allowing them to disrupt and control their IT systems).

78. *See generally* Ehlinger, *supra* note 18 (indicating that cybercriminals target small businesses in the hopes of discovering a weakness linked to a larger corporation).

79. *See Preparing Small Businesses for Cybersecurity Success: Hearing on S.228 Before the Comm. on Small Bus. and Entrepreneurship*, 115th Cong. 3 (2018) [hereinafter *Hearing on S.228*] (opening statement of Hon. Benjamin L. Cardin, Ranking Member, and U.S. Senator from Maryland) (illustrating the total amount of small businesses at risk for data breaches).

80. *See 2017 Ponemon Institute Study Finds SMBs are a Huge Target for Hackers*, *supra* note 75 (identifying the quantity of stolen PII contained within company records obtained during a data breach).

81. *See Hearing on S.228*, *supra* note 79, at 8 (testimony by Daniel Castro, Vice President of Information Technology and Innovation Foundation) (expounding on how small businesses encounter the same threats as large businesses, except that small businesses experience higher volumes of cyberattacks—such as malware and phishing—due to their vulnerability).

funding, and complying with regulations; at worst a data breach could cause a small business to shut down.[82] With small businesses being so vital to the growth and health of the economy, it is imperative that they receive assistance to deal with these threats.[83]

1. Why Smaller Businesses Are Unequipped to Withstand a Cyberattack Compared to Larger Businesses

The immediate aftermath of a cyberattack threatens an organization's ability to function and access vital information, consequently destroying its patrons' trust and jeopardizing the organization's overall survival.[84] The greatest threat to any business, whether it be large or small, is the financial costs resulting from the data loss.[85] The loss of business accounted for almost forty percent of the average total cost of a data breach.[86] Additionally the consequences following a data breach, such as the regulatory and legal fees associated in the recovery of the lost data, contribute to a higher cost up to two years after a data breach occurs.[87] Larger businesses are more equipped to address cyberattacks compared to their smaller counterparts.[88] Large businesses can: (1) obtain their

82. *See id.* at 2 (opening statement of Hon. James E. Risch, Chairman, U.S. Senator from Idaho) (explaining the consequences of a data breach on both small businesses and the economy).

83. *See id.* at 9–11 (testimony by Daniel Castro, Vice President of Information Technology and Innovation Foundation) (noting that innovation and job growth stem from the success and survival of small businesses).

84. *See generally Cybersecurity Insurance*, *supra* note 14 (strategizing incident responses, best practices, and education for data sharing concerning the assistance of private organizations).

85. *See* Geraldine Strawbridge, *5 Damaging Consequences of a Data Breach*, METACOMPLIANCE (Feb. 25, 2020), https://www.metacompliance.com/blog/5-damaging-consequences-of-a-data-breach/ [https://perma.cc/K58U-DQV5] (emphasizing the financial hardships resulting from a data breach, and the potential economic impacts on a company's share price within the market).

86. *See* Heather Landi, *Average Cost of Healthcare Data Breach Rises to $7.1M, according to IBM Report*, FIERCE HEALTHCARE (Jul. 29, 2020, 12:58 PM), https://www.fiercehealthcare.com/tech/average-cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report [https://perma.cc/ML7P-7F6M] (illustrating the financial losses that organizations can suffer because of a data breach).

87. *See generally* PONEMON INST., *supra* note 3 (highlighting the average distribution of data breach costs in the years following a breach).

88. *See New Survey Shows a Majority of Small Businesses Believe They are a Likely Target for Cybercrimes; More than a Quarter have Experienced Data Breach in Last Year*, CISION: PR NEWSWIRE (Oct. 23, 2019, 1:43 PM), https://www.prnewswire.com/news-releases/new-survey-shows-majority-of-small-businesses-believe-they-are-a-likely-target-for-cybercrimes-more-than-a-quarter-have-experienced-data-breach-in-last-year-300944168.html [https://perma.cc/G2EX-

own cybersecurity team, security automation, and formal incident response team, (2) acquire cyber insurance, (3) access assets to shake off any financial loss, and (4) afford to pay any ransom to get stolen data back if a data breach were to occur.[89]

Smaller businesses either lack an IT staff altogether or do not have a big enough IT budget to implement efficient cybersecurity.[90] Furthermore, small businesses would rather pay the extortion fee for lost data because the legal fees, forensic fees, data restoration costs, loss of revenue, and extra expenses far outweigh the extortion payment itself.[91] Smaller firms are at a disadvantage in implementing cybersecurity protocols as they lack the financial, legal, and technical resources possessed by larger firms.[92] However, ultimately large and small businesses tend not to take cybersecurity seriously.[93] Larger companies possess the capital to install cybersecurity safeguards yet fail to due to so, whereas smaller companies believe they're not at risk and lack the required education and resources needed to implement cybersecurity measures properly.[94]

One of the best ways businesses can learn how to guard and combat against cyberattacks is to share information amongst each other about any data breaches they may have experienced.[95] However, few businesses are willing to share cybersecurity information citing potential liability issues concerning the disclosure of trade secrets and the exposure of

QQGB] (discussing how larger companies are better equipped to handle a data breach due to their funds, resources, and IT personnel).

89. *See* PONEMON INST., *supra* note 3 (highlighting the average distribution of data breach costs in the years following a breach).

90. *Cf.* Ehlinger, *supra* note 18 (commenting on how businesses who can afford the luxury of an IT budget or IT personnel should invest in cybersecurity insurance).

91. *See id.* (illustrating the associated costs and financial impact of a cyberattack).

92. *See* John Suek & Michael Perez, *Spotlight: Banks face Growing Cybercrime Threat*, FED. RSRV. BANK OF DALL., https://www.dallasfed.org/research/swe/2019/swe1904/swe1904e [https://perma.cc/5JR5-CVJY] (acknowledging that in 2019, 43% of data breaches occurred in small businesses, emphasizing how ill-equipped small businesses are when confronted by a cyberattack).

93. *See generally* Myers, *supra* note 71 (explaining how some small businesses ignore cybersecurity because they lack computer proficiency, assume that third-party vendors possess all necessary compliance measures, and fail to prioritize consumer data protection).

94. *See* Neto et al., *supra* note 4 (using the Capital One data breach to demonstrate how even the most prominent companies are ill-prepared to manage and handle cybersecurity risks).

95. *See* King, *supra* note 16 (describing the ability to react to an attack, prevent it, and respond efficiently requires information sharing among banks and other businesses).

security system procedures.[96] Traditionally, these businesses have believed that firewalls, antivirus software, passwords, and third-party cloud computing companies sufficiently guarded against any potential cyberattack.[97] Without more, they are vulnerable and the perfect prey for cyber attackers.[98]

II. ANALYSIS

A. Regulations Governing Cybersecurity Standards

1. Federal Regulations Implementing Data Security

Seventy percent of Americans feel their data is less secure today than in the last decade and only four to six percent of Americans actually understand how their data is being used.[99] Personal data breaches can cost individuals, businesses, industries, and governments millions of dollars in financial losses and identity theft.[100] The effects in regard to the *LabMD* and *Equifax* cases show how pivotal it is to have sound data protection and cybersecurity regulations in place at the federal, state, and local level.[101]

---

96. *Cf. id.* (identifying the hesitations among financial institutions to share information due to legal consequences and possible competitive advantages).

97. *See id.* (expounding how businesses generally rely on software or third-party vendors to safeguard their data).

98. *See generally* Rob Verger, *Your Anti-Virus is Not Enough*, POPULAR SCI. July 7, 2017, 7:45 PM) https://www.popsci.com/antivirus-software-protect-your-computer/ [https://perma.cc/7R9W-FZQS] (identifying how anti-virus software has become less effective given the complexity of our current technological landscape).

99. *See* TEX. PRIV. PROT. ADVISORY COUNCIL, REPORT 1 (2020), https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/TPPAC%20Interim%20Report%2087th.pdf [https://perma.cc/5HPQ-8A65] [hereinafter REPORT] (illustrating how far business, industry, and the internet have advanced data collection to the point where people are uninformed about why their data is collected, where it is stored, and how it is used).

100. *See* Neto et al., *supra* note 4 (reporting the statistics among data breaches to illustrate that any industry is susceptible to a data breach).

101. *See* F. Paul Pittman & Mark Williams, *U.S. Cybersecurity Standards to Get Tougher and More Specific: FTC and NYDFS Lead the Way*, WHITE & CASE (Sept. 9, 2020), https://www.whitecase.com/publications/alert/us-cybersecurity-standards-get-tougher-and-more-specific-ftc-and-nydfs-lead-way [https://perma.cc/VE8P-MH7N] (addressing that LabMD failed to address the loopholes regarding the security of consumer information. However, the U.S. Court of Appeals for the 11th Circuit ruled against the FTC, holding that their regulations were not specific enough to warn LabMD of the importance of implementing cybersecurity measures); *see also* FED. TRADE COMM'N, PRIV. & DATA SEC. UPDATE 6 (2019), https://www.ftc.gov/system/

There are federal regulations created and enforced by government agencies that regulate entire industries with regard to their cybersecurity framework and protection of consumer data.[102] For example, the Health Insurance Portability and Accountability Act (HIPAA) is a law the health care industry must follow, and the Gramm-Leach-Bliley (GLB) Act regulates federal financial institutions.[103] HIPAA is enforced by the U.S. Department of Health and Human Services, which regulates and develops standards regarding the protection and disclosure of an individual's health information and privacy rights.[104]

The GLB Act, 15 U.S.C.A. § 6801, requires financial institutions to implement reasonable security policies and send consumers initial and annual privacy notices that allows them to opt out of sharing their information with unaffiliated third parties.[105] These reasonable security policies need to: (1) ensure security and confidentiality of customer records, (2) protect against anticipated threats, and (3) guard against unauthorized access.[106] Both HIPAA and GLB are codified as United States statutes and are implemented industry-wide.[107] Both of these regulations have brought data security to the forefront of the conversation, yet still do not do enough to enforce cybersecurity defenses

files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf [https://perma.cc/J7PY-9G8Y] (alleging that Equifax failed to implement the necessary safeguards to address the foreseeable vulnerabilities regarding the security of consumer information. The U.S. Court of Appeals for the 11th Circuit ruled for the FTC and its new regulation that specified that procedures and protocols be implemented to prevent accessibility to consumers' personal data on store computer systems).

102. *See* KRAMER & BUTLER, *supra* note 10 (explaining the difference between regulations enforced by law and regulations null until accepted and passed as law by states).

103. *See generally* Neto et al., *supra* note 4 (discussing the mandatory industry regulations by law).

104. *See generally* OFF. FOR CIV. RTS., U.S. DEPT. OF HEALTH & HUM. SERV., SUMMARY OF THE HIPAA PRIVACY RULE 1-3, https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/H4NB-D52L] (last modified May 2003) (addressing the standards used within the Privacy Rule).

105. *See* FED. TRADE COMM'N, PRIV. & DATA SEC. UPDATE at 7 (reviewing the FTC's guidelines and how they have progressed to requiring more efficient cybersecurity practices).

106. *See* 15 U.S.C. § 6801 (2020) (stating the standard guidelines of the GLB Act).

107. *See generally* Neto et al., *supra* note 4 (introducing other federal regulations such as the Sarbanes Oxley Act, Dodd-Frank Wall Street Reform, and the Consumer Protection Act of 2010).

that would prevent future data breaches, putting consumer personal data at risk.[108]

Additional federal regulations that affect the private sector's data security include the Children's Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), Computer Fraud and Abuse Act (CFAA), and the Video Privacy Protection Act (VPPA).[109] COPPA regulates commercial online services such as websites and mobile apps that collect personal identifiable information (PII) from children under the age of thirteen ensuring parents/legal guardians are notified when their children's PII could be collected or used.[110] The FCRA focuses on limiting how people's consumer reports and credit card account numbers can be used as well as certain procedures for disposing of that information.[111] Furthermore, the CFAA criminalizes unauthorized access—such as computer hacking—to protected computers in an effort to obtain national security data, a financial institution's records, consumer reporting agencies consumer profiles, and any U.S. government department or agency information.[112] Last, the VPPA prohibits video service providers, such as Hulu, Netflix, and Amazon Prime, from disclosing consumer PII without their consent and regulates when such PII should be destroyed.[113]

---

108. *See generally id.* (discussing the reasonableness standard set out in both regulations is ambiguous and still does not truly warrant good cybersecurity practices in those industries to guard consumer's personal data).

109. *See* REPORT, *supra* note 99, at 5 (showing how the federal government has codified regulations that limit companies practices on the use and disclosure of private personal information).

110. *See* Ieuan Jolly, *U.S. Privacy and Data Security: Overview*, THOMSON REUTERS PRACT. L., https://1.next.westlaw.com/Document/I03f4d7afeee311e28578f7ccc38dcbee/View/FullText.html?originationContext=knowHow&transitionType=KnowHowItem&contextData=%28sc.DocLink%29 [https://perma.cc/TGR3-LJNM] (pointing out that the FTC is the primary enforcer for COPPA and expands its enforcement to internet connected toys and other devices in the "Internet of Things").

111. *See id.* (expanding on the FTC, in accordance with the FCRA, the Red Flag Rule was implemented which requires financial institutions and creditors that fall under the FRCA to develop a system to identify warnings and risks of identity theft).

112. *See id.* (categorizing protected computers as any with internet connections since they could be used in interstate or foreign commerce).

113. *See generally* REPORT, *supra* note 99, at 5 (discussing the federal laws in place that guard against commercial entities in the private sector collecting, releasing, using, or disposing of consumer PII); *see also* Jolly, *supra* note 110 (detailing how video service providers must also provide notification and authorization from consumers before releasing to using their information that would expose it to third parties).

The federal regulations above provide the private sector with information on what data to protect, their obligations in protecting that data, and ensure that consumer PII is at the forefront of businesses security policies.[114] However, very few of these regulations provide actual guidance on the cybersecurity necessary to protect consumer PII.[115] For example, the regulations in place do not provide businesses with information on what the best cybersecurity strategies are to reasonably protect the data within the scope of their business, where to find resources to educate or assist them, nor information on which third-party cybersecurity service providers to turn to for help.[116]

2. Federal Agencies Implementing Policies and Programs to Develop Cybersecurity Framework

Federal agencies have stepped in to provide a variety of guidance and resources to help businesses structure cybersecurity frameworks to guard against data breaches putting consumers' PII in jeopardy.[117] For example, the U.S. Department of Commerce has implemented the National Institute of Standards and Technology (NIST), which has become renowned for developing the NIST Cybersecurity Framework, especially in the financial industry.[118] The NIST Cybersecurity Framework provides a risk-based approach which collects and cross-references other commonly accepted information security standards that businesses can use to develop a comprehensive information security program.[119] A majority of the federal programs reference or base their material off of the NIST Cybersecurity Framework even though the

114. *See generally State Data Security Laws*: *Overview*, *supra* note 11 (listing the different federal regulations that implement the data that needs to be protected but leaves a gap in how to best protect that data).

115. *See generally* Jolly, *supra* note 110 (describing multiple federal regulations in place designed to show what data needs to be protected, but not how to protect it).

116. *See generally* REPORT, *supra* note 99, at 4 (stating federal regulations limited implication of cybersecurity practices does not apply to every business).

117. *See generally State Data Security Laws*: *Overview*, *supra* note 11 (providing details on the different businesses who do not have the knowledge, resources, or guidance on how to best adhere to the regulations).

118. *See generally id.* (stating how widely adopted the framework is in the United States); *see also* Neto et al., *supra* note 4 (displaying how the NIST Cybersecurity Framework is especially being utilized by the financial industry).

119. *See generally State Data Security Laws*: *Overview*, *supra* note 11 (stating that FTC cross-references business misrepresenting the Privacy Shield with different programs).

framework is not currently enforced on any business or industry by federal law.[120] While the NIST Cybersecurity Framework does not alone carry the force of law, it must be adopted by states or industries.[121]

Furthermore, the Cybersecurity & Infrastructure Security Agency (CISA)—a subagency for the Department of Homeland Security—strives to build a strong national cybersecurity infrastructure by collaborating and providing information and resources to the federal government, agencies, state/tribal/local governments, and private sector entities on cybersecurity posture.[122] Through federal law, the CISA has established the National Cybersecurity and Communications Integration Center which in turn established a multi-directional, cross sector sharing of information related to cybersecurity as a federal to civilian interface.[123] The main goals for the National Cybersecurity and Communications Integration Center are to: (1) address cybersecurity risks and incidents to federal and non-federal entities in real time; (2) share information related to cybersecurity threats, risks, and incidents; (3) conduct integration and analysis of the risks and incidents above; and (4) upon request provide technical assistance, risk management support, and incident response to federal and non-federal entities.[124] The National Cybersecurity and Communications Integration Center consists of federal entities, sector specific agencies, civilian and law enforcement agencies, non-federal entities such as state, local, and tribal governments, information sharing and analysis organizations, and cybersecurity specialists.[125] The CISA National Cybersecurity and Communications Integration Center is one of

120. *See Hearing on S.228*, *supra* note 79, at 18 (testimony of Russell Schrader, Executive Director of National Cyber Security Alliance) (establishing ways in which programs trying to establish a particular cybersecurity system for a specific business or industry incorporates the NIST Cybersecurity Framework).

121. *See generally State Data Security Laws*: *Overview*, *supra* note 11 (showing that states must choose to adopt the framework if they wish to implement it).

122. *See Cybersecurity Insurance*, *supra* note 14 (informing that CISA ultimately strives to be an open resource for any entity to use regarding education, incident response, best practices, or data sharing for cybersecurity).

123. *See* 6 U.S.C. § 659 (A) (2018) (crafting a security blanket to supplement cybersecurity measures for all).

124. *See id.* (adopting a philosophy in whatever action they take to be fluent in assisting federal or non-federal entities, being able to move across different sectors, and cover anything related to cybersecurity, whether that be cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and/or warnings).

125. *See* 6 U.S.C. § 659 (D) (2018) (providing the functions and the general composition of The Center).

the major players in enhancing cybersecurity protection and data security by creating an environment that implements public to private sector collaboration on strategy and information sharing.[126]

In addition to CISA, the National Cyber Security Alliance (NCSA) is a nonprofit public-private partnership attempting to strengthen national cybersecurity through awareness and education with collaboration.[127] The NCSA believes that due to cybersecurity being an economic, security, and social issue, collaboration among industries and sectors is the best way to make the general cybersecurity framework more effective.[128] The Department of Defense and the Department of Homeland Security both offer online cybersecurity training programs the public can access through their Defense Security Service and Cyber Awareness Resources and Training.[129]

The Federal Trade Commission (FTC) is an independent federal agency charged with protecting consumers and enhancing competition within the United States economy.[130] The FTC's primary authority stems from the Federal Trade Commission Act which prohibits unfair or deceptive practices in the marketplace.[131] This allows them to enforce a variety of sector specific laws including those which would prevent consumers from danger and allow them to take full advantage of the benefits offered in the marketplace.[132] Although the FTC is not

126. *See generally* 6 U.S.C. § 659 (C) (2018) (distinguishing itself from other programs because this is codified in a federal statute, and it solidifies the United States Government inclination to create a collaborative information sharing environment to address the modern and ever-changing problems of cybersecurity).

127. *See Hearing on S.228*, *supra* note 79, at 15 (statement of Russell Schrader, Executive Director of National Cyber Security Alliance).

128. *See id.* at 15 (statement of Russell Schrader, Executive Director of National Cyber Security Alliance) (explaining how this cybersecurity framework would better allow small businesses to protect their customers, employees, and assets).

129. *Cf.* U.S. GOV'T ACCOUNTABILITY OFFICE, DEFENSE CYBERSECURITY: OPPORTUNITIES EXIST FOR DOD TO SHARE CYBERSECURITY RESOURCES WITH SMALL BUSINESSES 11 (2015), https://www.gao.gov/assets/680/672724.pdf [https://perma.cc/FMT3-SRAR] (explaining resources that the top federal security agencies offer for public use).

130. *See* FED. TRADE COMM'N, PRIV. & DATA SEC. UPDATE, at 1 (explaining that that the FTC'S two goals have remained the same in protecting consumers' personal information and ensuring that the consumers have in the benefits of products offered).

131. *See id.* (elaborating on how the FTC uses its authority and has brought forth hundreds of privacy and data security cases).

132. *See id.* (providing examples of sector specific laws such as the Gram-Leach-Bliley Act or the Truth in Lending Act).

specifically designed to implement cybersecurity and data protection policies, it has taken on the role of preventing deceptive or unfair labor practices in the collection, use, processing, protection, and disclosure of consumer personal data through its enforcement powers.[133] Therefore, the FTC is pivotal to regulating businesses' cybersecurity policies and has brought over seventy cases against companies that have engaged in unfair practices putting consumers' data at risk.[134]

As of 2019, in response to the Equifax case, the FTC has strengthened its standard with regard to data security safeguards businesses must implement.[135] This standard traditionally required reasonable security policy and procedures; however, it now requires businesses to implement a comprehensive security program, obtain robust biannual assessments of the program, and submit annual certifications by a senior officer about the company's compliance with the order.[136] Ultimately, the FTC is changing their policies on data protection to mirror those already implemented by states such as New York.[137]

Federal regulations and agencies have done well to create more programs and infrastructure to support the data security regulations already in place.[138] However, despite the FTC's updated regulations and policies calling for more specified and efficient cybersecurity—like the NIST Cybersecurity Framework's blueprint for businesses in the financial industry—there has not been a lot of progress in developing specific guidance on cybersecurity infrastructure to protect consumer's

133. *See generally* Jolly, *supra* note 110 (responding through adjudication and other enforcement actions, the FTC has been able to implement data security standards).

134. *See* FED. TRADE COMM'N, PRIV. & DATA SEC. UPDATE, at 2 (expounding on the FTC filing cases against Equifax, which charged them with failing to design and implement safeguards under the GLB Act that would address foreseeable internal and externals risks to consumer data).

135. *See id.* at 2, 6 (citing the Equifax case as one where the court ruled against the FTC because its reasonable standard was ambiguous and did not clearly show a business what it exactly had to do to meet the standard).

136. *See id.* at 5 (detailing the process businesses have to abide to in order to comply with the FTC and their guidelines).

137. *See generally* Pittman & Williams, *supra* note 101 (comparing the NYDFS Cybersecurity Regulation that has imposed stricter compliance obligations with the cybersecurity of financial institutions).

138. *See generally id.* (affirming the future of United States mandated cybersecurity, but the necessity for specified infrastructure).

PII from being breached.[139] For example, in 2020, the United States took an average of 186 days to identify a breach, fifty-one days to contain a breach, and experienced the highest data breach costs in the world at $8.64 million on average.[140]

The healthcare industry incurred the highest cost from data breaches in 2020, despite being one of the most regulated and assisted industries in terms of federal regulations and federal agency guidance.[141] Ultimately the federal regulations, policies, and procedures currently in place are effective at stating what kind of consumer data needs to be protected, what kind of notification regarding the use of consumer data needs to be provided, and some comprehensive plans and councils in place to encourage collaboration to come up with an effective cybersecurity framework.[142] If the United States is incurring the highest data breach cost in the world, having one of its most regulated industries incurring the highest data breach costs, and taking almost three quarters of a year before a data breach is contained, then clearly the legislation and regulations in place to guide an effective cybersecurity framework are not working.[143]

3. State Regulations That Adopt or Enhance Federal Data Security Laws Already in Place

In addition to federal regulations, there are a number of states that contain their own data security laws that businesses (small or large) must

139. *See generally* REPORT, *supra* note 99, at 10 (laying out the regulations and policies of the FTC but omitting any policies for the potential of consumers' personal information being breached).

140. *See* PONEMON INST., *supra* note 3 (explaining that healthcare has continuously incurred the highest average breach costs).

141. *See* PONEMON INST., *supra* note 3 (identifying the health industry costing $7.13 million globally and the financial industry costing $5.85 million globally, both the costliest industries from a data breach in the world).

142. *See* REPORT, *supra* note 99, at 4 (distinguishing between federal and state laws along with agency regulations requiring system and data protections for a variety of industry silos. However, most businesses that do not have the IT resources to funnel through the limited cybersecurity guidance, do not know what kind of cybersecurity framework to establish).

143. *See id.* (relating the general concerns surrounding privacy and cybersecurity to the ongoing complaints and breaches that occur in the United States).

abide by in order to guard consumers' personal data.[144] Traditionally, state data security laws have only required a notification procedure for businesses that fall under certain criteria to report a data breach.[145] Other than that, states have traditionally been absent in regulating any strict data security standards or cybersecurity programs that businesses should follow to guard consumer data.[146] Currently state data security laws either require businesses to take reasonable data security measures to protect consumers' personal information or they require businesses to develop and maintain specific data security measures that are tailored to that business or industry to protect consumers' data.[147]

For example, in Washington, D.C., data security legislation only calls for businesses that license, hold, own, collect, or handle PII of a D.C. resident to implement reasonable security safeguards to protect it from unauthorized use.[148] The statute further details the logistics and requirements for businesses to report a data breach and when it is mandatory to provide identity theft protection services in the case that the PII compromised consists of tax identification numbers or social security numbers.[149] Many states, including Texas, discussed *infra*, passed legislation that only requires businesses to adopt reasonable data security measures because it allows for flexibility on matters that are constantly evolving and changing.[150] Furthermore, there is generally not a "one size fits all" cybersecurity policy to enforce on businesses that could

144. *See generally State Data Security Laws*: *Overview*, *supra* note 11 (affirming that states must follow federal regulations along with their own laws when it comes to the protection of personal data).

145. *See id.* (describing states' general approach to cybersecurity laws regulating businesses for fear of inflexibility or being too restrictive on businesses).

146. *See id.* (showing the discrepancy between the requirements of state data security laws for businesses).

147. *Id.*

148. *See* D.C. CODE § 28-3851 (2020) (including language to tailor the reasonable security safeguards to the nature and amount of the PII as well as the nature and size of the business itself).

149. *See id.* (expounding on the detailed requirements that involve notifying the government and people affected by the breach. However, no helpful nor specific regulations regarding the prevention of breach of PII from occurring in the first place is included).

150. *See State Data Security Laws*: *Overview*, *supra* note 11 (implying the ambiguity in the reasonableness standard due to it being a case by case basis that depends on size and complexity of the business as well as the sensitivity of the data it collects).

address their security needs in protecting patrons' PII.[151] Additional arguments for the reasonable measures approach are that it allows businesses to follow risk-based approaches to cybersecurity rather than focus on compliance, and ensures policies do not become outdated or increase the risk of being exploited.[152]

The reasonable cybersecurity policy requirement creates an ideology that businesses will create policies that react to cyberattacks and then follow compliance in response to it rather than follow specific regulations that aim to prevent data breaches from occurring in the first place.[153] Furthermore, businesses that do not have the cybersecurity expertise or lack cybersecurity personnel all together—such as small businesses—need additional guidance and specific regulations.[154] It is evident that specific regulations of cybersecurity policy requirements are necessary due to the alarming number of cyberattacks occurring every year effecting PII.[155] There is a fine balance between enforcing specific regulations that ensure a proactive approach to preventing data breaches and not constricting all businesses to replicate the same policies that open the door to cyberattacks.[156]

---

151. *Compare id.*, *with See* Pittman & Williams, *supra* note 101 (criticizing the reasonable security compliance standard failure to provide guidance on what reasonable security actually entails).

152. *See State Data Security Laws*: *Overview*, *supra* note 11 (recognizing twenty-two states that have adopted reasonable data security measure statutes).

153. *Compare id.* (enforcing a reasonable approach, allowing an entity to implement a cybersecurity policy with bare-minimum security standards to ensure compliance with data security regulations—which can be, and is being, satisfied with a response plan rather than the arguably preferrable preventative/protection plan for PII), *with Cyber Attacks & Defenses for Small Business*, SBDCNET NAT'L INFO. CLEARINGHOUSE (July 24, 2018), https://www.sbdcnet.org/small-business-cybersecurity/cyber-attacks-threats-defenses-small-business [https://perma.cc/GDX2-2YTG] (demonstrating how proactive approaches to cybersecurity—cybersecurity defenses—help mitigate the risks and threats of a cyberattack to ensure data and information is protected).

154. *See State Data Security Laws*: *Overview*, *supra* note 11 (stating that the downfall of the reasonable security regulation is those businesses that lack the knowledge or resources of how to implement a cybersecurity policy. The reasonableness standard provides no insight on what to specifically implement).

155. *See* IDENTITY THEFT RES. CTR., 2019 END-OF-YEAR DATA BREACH REPORT 1 (2019), https://notified.idtheftcenter.org/s/resource [https://perma.cc/QRW3-AXJZ] (stating the increase in data breaches by 17% from 2018 to 2019).

156. *See generally State Data Security Laws*: *Overview*, *supra* note 11 (contrasting the generally adopted reasonable security standard approach, working to mitigate security issues post-breach, with the small "but growing" movement of implementing proactive security measures).

Ohio's data security legislation is unique in that the Ohio Data Protection Act mandates a reasonable cybersecurity policy but incentivizes specific compliance through the legislation's safe harbor provision.[157] The safe harbor provision provides an affirmative defense to a tort action against an entity for a data breach that effects PII, as long as: (1) the entity's cybersecurity policy reasonably protects PII; and (2) contains administrative, technical, and procedural safeguards, or complies with a recognized cybersecurity framework (such as the NIST Cybersecurity Framework).[158] Therefore, Ohio strikes the balance of incorporating the flexibility of 'reasonable security' while adding a benefit to businesses that take the extra measures not specifically required for compliance.[159]

On the other hand, Oregon requires particular safeguards to supplement its reasonable data security measures to ensure the protection of the data's confidentiality, integrity, and security.[160] These additional specific requirements include administrative, technical, and physical safeguards which range from training and developing cybersecurity policy to protecting against unauthorized access.[161] Additional and further specified data security obligations are imposed on device manufacturers with devices connected to the internet.[162] Furthermore,

157. *See* REPORT, *supra* note 99, at 7 (commenting on the implication of the Ohio Data Protection Act in preventing data breaches and its effect on businesses it regulates).

158. *Compare id.* (discussing Ohio's incentivizing businesses in the most practical way by implementing specific data security policies, enforced by civil liability and fines); *with State Data Security Laws*: *Overview*, *supra* note 11 (acknowledging the existence of the safe harbor provision provided in Ohio's data security law, which also contains "administrative, technical, and procedural safeguards to protect personal information . . . ").

159. *See* REPORT, *supra* note 99, at 7 (recognizing that the security measures implemented by Ohio allow the businesses in that state to comply with the reasonable measures of security. This means that personal information will be protected at least at a bare minimum, but each business alone can implement even stricter regulations which seem too high of a bar for some, but beneficial for others).

160. *See* OR. REV. STAT. ANN. § 646A.622 (2020) (setting forth "safeguards to protect consumer privacy"); *see also State Data Security Laws*: *Overview*, *supra* note 11 (listing the particular reasonable data security measures that Oregon has implemented by statute to protect against cyberattacks on an organization's personal data).

161. *See* OR. REV. STAT. ANN. § 646A.622 (2020) (setting forth "safeguards to protect consumer privacy"); *see also State Data Security Laws*: *Overview*, *supra* note 11 (listing the particular reasonable data security measures that Oregon has implemented by statute to protect against cyberattacks on an organization's personal data).

162. *See* OR. REV. STAT. ANN. § 646A.813(1)(c) (2020) (describing the "reasonable security features" required of manufactures of connected devices); *see also State Data Security*

the businesses that comply with industry security safeguards such as HIPAA or the GLB Act will fall under a safe harbor provision similar to Ohio's.[163] Oregon's data security legislation also provides compliance relief for small businesses with fewer than 100 employees who comply with the necessary data security safeguards in accordance with the small business's size, nature of the business, and sensitivity of the PII collects.[164]

The New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) passed in July 2019, is similar to Oregon's 'reasonable security policy' standard but has additional requirements.[165] These additional obligations under the SHIELD Act can be satisfied by complying with the existing and recognized data security safeguards set forth by the GLB Act, HIPPAA, the New York Department of Financial Services Cybersecurity Regulations (NYDFS) or other federal or New York administered regulations.[166] Additionally, regulated businesses are required to implement administrative, technical, and physical

---

Laws: *Overview*, *supra* note 11 (discussing the data security features manufacturers must equip connected devices with to provide another layer of defense for consumers' PII).

163. *Compare State Data Security Laws*: *Overview*, *supra* note 11 (describing the affirmative defense to a tort action in response to a data breach, provided by the safe harbor provision of the Ohio Data Protection Act), *with* REPORT, *supra* note 99, at 1 (describing the affirmative defense to a tort action in response to a data breach, provided by the safe harbor provision of the Ohio Data Protection Act).

164. *See State Data Security Laws*: *Overview*, *supra* note 11 (addressing how Oregon requires small businesses—businesses with one hundred or fewer employees—to follow regulations to protect against cyberattacks but, due to their small size, scope, and complexity, are provided relief); *see also Cyber Security: Protecting Your Small Business: Hearing Before the S. Comm. on Healthcare and Tech.& the Comm. on Small Bus.*, 112th Cong. 12 (2011) [hereinafter *Cybersecurity Hearing*] (statement of Hon. Mac Thornberry, representative in congress from the State of Texas) (testifying to the struggle small businesses face in meeting regulations, supporting the relaxation of state data cybersecurity legislation for small businesses regarding specific data security requirements).

165. *See State Data Security Laws*: *Overview*, *supra* note 11 (describing the similar specific data security safeguards required in both Oregon and New York, both offering guidance to small businesses); *see also* Mark H. Francis, *Will New York Be the Next State to Adopt Robust Data Privacy and Security Laws*, HOLLAND & KNIGHT (July 9, 2019), https://www.hklaw.com/en/insights/publications/2019/07/will-new-york-be-the-next-state-to-adopt-robust-data-privacy [https://perma.cc/7XES-BAK4] (explaining the recently passed cybersecurity legislation in New York, effectively expanding cybersecurity obligations throughout the state).

166. *See State Data Security Laws*: *Overview*, *supra* note 11 (outlining the additional security measures certain New York entities must take to comply with New York cybersecurity obligations).

safeguards to fall under compliance with the SHIELD Act.[167] The SHIELD Act, like the Oregon legislation, provides relief for small businesses, defined as businesses with less than fifty employees, less than three million dollars in gross annual revenue in the last three fiscal years, or less than five million dollars in year-end total assets.[168] The relief further provides for security safeguards in accordance with the size of the business, nature of activities, and sensitivity of the PII collected.[169] All the states that implement specific cybersecurity compliance regulations have exemptions to avoid complex overlap with other non-state enforced cybersecurity regulations or to account for business size.[170]

The specific approach in the regulations ensure that there is a base level of cybersecurity implemented by businesses to guard PII and further promote the wellbeing of the economy in preventing cyberattacks.[171] It is a public benefit to ensure there are specific regulations implementing a baseline cybersecurity standard to protect consumer's data while also realizing and engaging with small businesses who do not have the expertise or fiscal capability to implement some of the specific regulations.[172] However, with business' interstate commerce capabilities and fifty different state cybersecurity regulations ranging from reasonable to specific compliance, it leads to a fragmented level of cybersecurity among the private sector and an increased risk of exposure to PII.[173] This raises the question of whether a comprehensive federal

167. *See id.* (addressing the requirements that regulated businesses have to follow in order to comply with data security laws and protect against any cyberattacks).

168. *See id.* (defining a small business as those with "less than [fifty] employees; less than [three] million in gross annual revenue . . . or less than [five] million in year-end total assets).

169. *See id.* (describing the flexibility the SHIELD Act affords small business to maintain compliance).

170. *See id.* (listing eighteen states that provide specific regulatory safeguards and the exceptions to those, including being an entity already in compliance with federal/industry data security regulations).

171. *See generally id.* (providing information on the regulations required for businesses to follow, including small businesses, to protect personal information); *see also Hearing on S.228*, *supra* note 79, at 4 (opening statement of Hon. Benjamin L. Cardin, Ranking Member, and U.S. Senator from Maryland) (recognizing that small businesses are the heartbeat of the economy and why it is imperative to find ways to protect them from data breaches).

172. *See generally Cyber Attacks & Defenses for Small Business*, *supra* note 153 (asserting the importance of proactive data security regulation requiring specific safeguards for cybersecurity policies).

173. *See* Francis, *supra* note 165 (warning that businesses of "all shapes and sizes [are] fac[ing] increasing regulatory compliance costs and risk exposure" by having to comply with

framework would better serve the interest of protecting PII and reducing the complexity for businesses satisfying compliance?[174]

There are multiple categories of regulations governing the standards for cybersecurity.[175] The regulations previously discussed are those codified and implemented through federal and state laws, programs and policies implemented by federal and state agencies; discussed *infra* are those regulations created by government agencies or industry groups that do not hold the force of law but are merely suggested and written up for state governments, local governments or industries to adopt.[176] For example, the Payment Card Industry-Data Security Standard (PCI-DSS) is a global payment account data security standard implemented from a global forum created in 2006 by American Express, Discover, JCB International, Mastercard, and Visa Inc.[177] Here, the PCI-DSS is not enforced by federal or state law but, because the biggest financial service providers in the world are members of the PCI-DSS Council, this data security standard is still utilized across the industry which impacts most consumers' lives.[178] For example, if a business receives, transmits, or stores credit/debit card information, their financial service provider most likely is in compliance with PCI-DSS.[179]

Furthermore, the National Association of Insurance Commissioners (N.A.I.C.) Insurance Data Security Model Law is a model that would

varying cybersecurity regulations throughout the states in the absence of cohesive federal regulation).

174. *Cf. id.* (questioning whether there is a better regulation strategy, such as federal oversight, to avoid the complexity of a variety of state regulations).

175. *See* Neto et al., *supra* note 4 (writing about businesses' freedom to apply a variety of best practices and the cybersecurity gap created between regulation, businesses, and the IT sector).

176. *See* NAT'L ASS'N OF INS. COMM'R & THE CTR. FOR INS. POL'Y & RSCH., THE NAIC INSURANCE DATA SECURITY MODEL LAW 1 (2020), https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf [https://perma.cc/KX9Y-UNY2] [hereinafter MODEL LAW] (discussing an exemplary model law the federal government has urged—but not required—the states to adopt to further develop cybersecurity measures and programs).

177. *About Us*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/about_us/ [https://perma.cc/8SC4-HDD9] (introducing the form of governance each of the founding members incorporate in their respective data security compliance programs).

178. *Cf. PCI Security Standards Council At-a-Glance*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/documents/At_a_Glance_Role_of_the_PCI_SSC.pdf [https://perma.cc/NGV2-5TM2] (explaining the source of enforcement of PCI-DSS and what entities can comply with those standards).

179. *See id.* (noting the entities that are in compliance with the PCI-DSS and how this affects some businesses).

require insurers and other licensed entities to implement a cybersecurity program to mitigate the potential damage of a data breach, and further lays out procedures that should be followed in the event of a data breach.[180] The N.A.I.C. Insurance Data Security Model Law (Model Law) is simply a model that State Departments of Insurance or state governments can adopt as law which requires baseline thresholds that implement industry-wide data security regulations.[181] The N.A.I.C. created the Model Law in response to "high profile data breaches of insurers and other institutions."[182]

South Carolina became the first state to adopt the N.A.I.C. Model Law, making all licensed insurers in the State of South Carolina abide by its regulations.[183] For example, through the passage of the South Carolina 'Insurance Data Security Act,' licensed insurers are required to maintain an information security program based on continuous risk assessments.[184] This information security program should establish standards intended to mitigate the damage of a potential data breach.[185] To further ensure accountability, licensed insurers must submit their data breach response plan annually to the South Carolina Department of Insurance.[186] In addition, if a cybersecurity event does occur effecting

180. *See* MODEL LAW, *supra* note 176, at 1 ("The NAIC Insurance Data Security Model Law seeks to establish data security standards for regulators and insurers in order to mitigate the potential damage of a data breach. The law applies to insurers, insurance agents and other entities licensed by the state department of insurance.").

181. *See id.* (stating the U.S. Treasury Department has urged the states to promptly adopt this model law and as of June 2020, eleven states have adopted it).

182. *See id.* (pointing out the purpose behind the development of the model law).

183. *See* Amy O'Connor, *Carolina Passes First Insurance Industry Cybersecurity Law*, INS. J. (May 31, 2018), https://www.insurancejournal.com/news/southeast/2018/05/31/490672.htm [https://perma.cc/LP6W-4CZ6] (declaring the South Carolina governor's adoption of N.A.I.C.'s Cybersecurity Working Group's Model Law in the state and its implications for insurance entities operating within South Carolina).

184. *See id.* (delineating what is included in maintaining an information security program, such as overseeing third-party service providers, investigating data breaches, and notifying the appropriate authorities in the case of a data breach).

185. *See id.* (listing the requirements of the cybersecurity policies required to be established, including the protection of the insurance policyholder's sensitive data pre-breach).

186. *See id.* (describing the scope of the insurance industry this model law applies to, and the slightly varying requirements based upon the domicile, structure, and size of the entity).

at least 250 people and results in a reasonable impact on consumers, then it must be reported within seventy-two hours of the occurring event.[187]

B. How Texas Cybersecurity Regulation and Legislation Compares to Other States

Cybersecurity is a critical function for state government.[188] Texas data security legislation primarily works to improve technology and resources, and increase cybersecurity education in order to ensure that state agencies and entities are in compliance with cybersecurity laws to prevent PII data breaches and avoid liability.[189] The Texas Department of Information Resources (DIR) is Texas' lead agency for coordinating information resources, cybersecurity, and data storage across state government.[190] DIR is further responsible for developing cybersecurity standards to ensure state agencies are protecting sensitive PII.[191] This responsibility gives the DIR the ability to establish a system of information security which is used to provide guidance and direction to both state agencies and entities who are, in turn, responsible for their own cybersecurity.[192]

A piece of compliance legislation currently in place includes Texas Government Code § 2054, which requires an information security officer within a state agency to prepare a biennial vulnerability report regarding their handling of sensitive personal information, confidential

187. *See id.* (setting forth the requirements South Carolina insurers must abide by in complying with the security program mandated by the legislation).

188. *See* REPORT, *supra* note 99, at 4 (explaining how the Texas 86th legislature has embraced the need for cybersecurity regulation through the passing of multiple bills).

189. *See id.* at 7–8 (describing the foundation laid by the major legislation passed in the 86th Legislature to accommodate recommended next-steps in regulatory/compliance legislation to increase security and avoid data breaches within the state government and entities).

190. *See* TEX. GOV'T CODE ANN. § 2059.056 (forming the relationship and responsibilities between DIR and the State agencies/entities it assists); s*ee also* REPORT, *supra* note 99, at 7–8 ("The Texas Department of Information Resources (DIR) is Texas' lead agency for coordinating information resources, cybersecurity, and data storage across state government.")

191. *See* REPORT, *supra* note 99, at 1 (discussing the current responsibilities of the Texas Department of Information Resources).

192. *See* TEX. GOV'T CODE ANN. § 2059.056 ("The [DIR] shall establish a network security center to provide network security services to state agencies."); s*ee also* REPORT, *supra* note 99, at 7–8 (recommending further measures be taken in passing other pieces of legislation and by legislatively defining the role of DIR to specific and proactive safeguards for agencies to implement in their cybersecurity procedures, exceeding the currently established check and balance system through DIR).

information, and PII.[193] Additionally, DIR has promulgated Texas Administrative Code § 202 which sets a minimum cybersecurity standards baseline for state agencies and institutions of higher education.[194] The minimum standard articulates responsibilities for agency heads, chief information security officers, and agency staff.[195] To ensure further compliance with state and federal laws in regard to data sharing and data security, the Texas Statewide Data Sharing Exchange Compact was established to create a uniform data sharing and data security agreement for state agencies and institutions of higher education.[196]

There is no parallel legislation in the private sector to ensure there are coordinating information resources or effective cybersecurity standards.[197] Texas Identity Theft Enforcement and Protection Act, codified at Texas Business and Commerce Code § 521.052, is a reasonable cybersecurity policy that requires businesses to implement and maintain reasonable procedures to protect from unlawful use or disclosure of any sensitive PII collected by the business.[198] A business that fails to comply could face a civil penalty of $100 for each individual

193. *See* TEX. GOV'T CODE ANN. § 2054.077 (requiring a biennial report revealing the vulnerability of any software or program of a state agency that is susceptible to "unauthorized access or harm"); s*ee also* REPORT, *supra* note 99, at 1 ("Texas Government Code 2054 requires that agencies handling sensitive personal information, confidential information, or individually identifiable information submit a biennial data security plan.").

194. *See* TEX. ADMIN. CODE §§ 202.20–202.22 (setting forth the minimum responsibilities of a state agency head, an agency's information security officer, staff of that agency, and procedures for reporting security measures managing security risks); s*ee also* REPORT, *supra* note 99, at 1 ("DIR has promulgated Texas Administrative Code 202 which sets a minimum baseline for cybersecurity standards for state agencies and institutions of higher education.").

195. *See* TEX. ADMIN. CODE § 202.20–202.22 (enumerating the respective responsibilities of the agency head, information security officer, agency staff).

196. *See* REPORT, *supra* note 99, at 2 (implementing data sharing is a key resource that is underutilized by government agencies and private sector entities amongst each other that could be beneficial in preventing cyberattacks by creating a "more efficient and effective method of data sharing.").

197. *Compare* TEX. BUS. & COM. CODE ANN. §§ 521.001–521.152 (requiring a reasonable effort to comply with loosely defined security standards), *with* TEX. ADMIN. CODE §§ 202.20–202.22 (detailing the responsibilities of agency personnel at various levels and describing the procedures for data maintenance, security measures to be taken, how to respond to and report a data breach).

198. *See* TEX. BUS. & COM. CODE ANN. § 521.052 (setting the low and insufficient 'reasonable' cybersecurity standard, as it is the only Texas legislation pertaining to private sector businesses).

that should be notified and for each consecutive day no action is taken to notify those individuals.[199] That is as far as Texas legislation goes to ensure businesses have a proper cybersecurity framework in place to prevent and combat breaches of PII.[200] Texas legislation regulating cybersecurity practices in the private sector only goes as far as describing what data businesses can maintain and what procedure is to be followed in reporting a data breach.[201]

For example, the Student Data Privacy Act, Texas Medical Record Privacy Act, and the Texas Biometric Privacy Act regulates the PII of a specific group of people that can be maintained and used by businesses.[202] The Identity Enforcement and Protection Act provides who, what, and when businesses will notify consumers or the state of a data breach and report it to the appropriate state officials.[203] The Texas Cybersecurity Council, created by DIR, is meant to benefit the state entities rather than entities in the private sector who require the extra cybersecurity regulation and guidance.[204] Under Texas Government Code § 2059.058, the DIR is only authorized to provide cybersecurity assistance to nongovernment agencies such as a school district, hospital district, water district, state legislature, political subdivision of the state, or a public junior college.[205]

---

199. *See* TEX. BUS. & COM. CODE ANN. § 521.151 (imposing civil penalties for those who fail to meet the 'reasonable' standard set by the Identity Theft Enforcement and Protection Act).

200. *See* TEX. BUS. & COM. CODE ANN. §§ 521.001–151 (creating an insufficient line of defense for cybersecurity breaches in the private sector).

201. *See* REPORT, *supra* note 99, at 5 (painting the current and insufficient landscape that is Texas legislation on data security policies in place to protect PII in Texas' private-business sector).

202. *See id.* at 4–5 (comparing privacy laws; the Texas Medical Record Privacy Act applies greater regulation than HIPAA and the Texas Biometric Privacy Act limits the use of a person's biometric identifier).

203. *See* TEX. BUS. & COM. CODE ANN. § 521.053 (indicating the required notification when a data breach occurs).

204. *See Texas Cybersecurity Council*, TEX. DEP'T INFO. RES., https://www.dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=133 [https://perma.cc/2SBR-GEGP] (explaining that the "DIR" created the Texas Cybersecurity Council to develop an enduring partnership between the private and public sector to ensure protection of critical infrastructure. Additionally, providing a collaboration between the private and public sector that can be instrumental for developing better cybersecurity practices to protect citizens PII, especially in the private sector where businesses need the guidance).

205. *See* TEX. GOV'T CODE ANN. § 2059.058 (remarking on the authorized provisions under the Texas Govt. Code).

Texas is tied for the second highest number of internet crime victims in the U.S. resulting in Texans losing an estimated $221 million.[206] USAA, headquartered in San Antonio, Texas, monitors attempts by cybercriminals to gain unauthorized access to both its systems and members accounts.[207] USAA headquarters is home to the Cyber Threat Operations Center that runs twenty-four hours a day focusing on detecting threats, analyzing them, and reverse engineering malicious software.[208] As evident with USAA Cyber Threat Operations Center, private sector entities are targeted and successfully breached at a greater rate than government entities exploiting PII and not all private entities, especially small businesses, have the capacity, knowledge, or fiscal ability to deter them with their own cybersecurity policies.[209] Of course, government agencies and entities collect a plethora of sensitive PII that needs to be given the resources to do so, regulated, and safeguarded.[210] However, it is negligent for a state to only utilize specific and targeted regulation for state agencies when a majority of the private sector can also benefit from specific regulation for guidance in implementing

206. *See* REPORT, *supra* note 99, at 4–5 (stating data from the Federal Bureau of Investigation's 2019 Internet Crime Report).

207. *See generally* Madison Iszler, *At USAA, Cybersecurity is a '24/7 Problem'*, SAN ANTONIO EXPRESS-NEWS, https://www.expressnews.com/business/technology/ article/At-USAA-cybersecurity-is-a-24-7-problem-13376369.php [https://perma.cc/3JAJ-AH7X] (last updated Nov. 8, 2018, 7:08 PM) (establishing USAA as one of the largest financial/insurance institutions in the country and as a pivotal private sector entity that can stand on its own in data security policies due to its resources).

208. *See id.* (referencing a constant vigilance held by the Cyber Threat Operations Center, ready to defend against all potential attack).

209. *See* IDENTITY THEFT RES. CTR., 2019 END-OF-YEAR DATA BREACH REPORT, (2019), https://notified.idtheftcenter.org/s/resource [https://perma.cc/QRW3-AXJZ] (summarizing the data breaches that were reported in 2019 and showing that there were less data breaches that occurred in the government entities compared to private sector entities); *see also Hearing on S.228*, *supra* note 79, at 3 (opening statement of Hon. Benjamin L. Cardin, Ranking Member, and U.S. Senator from Maryland) (upholding the fact that small businesses are not as knowledgeable nor capable to implement effective cybersecurity that state entities can due to the resources and regulation they have which could factor into them experiencing less data breaches in 2019).

210. *See Texas Cybersecurity Council*, *supra* note 204 (explaining that the "DIR" created the Texas Cybersecurity Council to develop an enduring partnership between the private and public sector to ensure protection of critical infrastructure. Additionally, providing a collaboration between the private and public sector that can be instrumental for developing better cybersecurity practices to protect citizens PII, especially in the private sector where businesses need the guidance).

cybersecurity policies considering PII within the private sector is at a greater risk than in state government's care.[211]

Ultimately, Texas current regulations through the Identity Theft Enforcement and Protection Act is not enough to ensure small businesses are satisfying their duty to protect consumers' sensitive PII.[212] All over the country, there are insurance providers, banks, financial firms, law firms, marketing firms etc., that classify as small businesses and collect PII through the course of everyday business without the same capabilities of USAA.[213] These small businesses need the guidance, structure, and direction—through regulation—to implement cybersecurity policies despite not having the same resources as large businesses.[214]

Ohio's reasonable cybersecurity regulation approach with incentives for businesses to implement specific compliance through the safe harbor provision is an effective method to ensure small businesses or businesses not collecting sensitive PII are not over regulated.[215] However, it still is not enough to ensure businesses are fulfilling their duty to protect consumer data.[216] New York's SHIELD Act is the best overall method to ensure businesses that collect sensitive PII are up to par in protecting

211. *See* IDENTITY THEFT RES. CTR., 2019 END-OF-YEAR DATA BREACH REPORT 2 (2019), https://notified.idtheftcenter.org/s/resource [https://perma.cc/QRW3-AXJZ] (emphasizing that the data shows businesses have some of the highest statistics in breaches for sensitive record exposure).

212. *See generally* TEX. BUS. & COM. CODE ANN. § 521.052 (admonishing that under the Texas Code, businesses' duty to protect sensitive personal data is not enough to actually protect consumers).

213. *See* Iszler, *supra* note 207 (distinguishing how USAA has access to a Cyber Threat Operations Center with a full team whose sole job is to deter cyber threats 24/7 that small businesses do not have access to); *see* Ehlinger, *supra* note 18 (proclaiming how small businesses do not invest many resources to guard against cyberattacks because most do not have the budget for it).

214. *See generally* Ehlinger, *supra* note 18 (providing a solution towards helping small businesses protect their private information through cyber insurance which is now feasible for small businesses to purchase).

215. *Cf.* André Dua et al., *COVID-19's Effect on Minority-Owned Small Businesses in the United States,* MCKINSEY & CO. (May 27, 2020), https://www.mckinsey.com/industries/public-and-social-sector/our-insights/covid-19s-effect-on-minority-owned-small-businesses-in-the-united-states [https://perma.cc/VU25-XR9H] (commenting on the public sector helping small businesses by incentivizing banks to lend to small businesses).

216. *See generally* F. Paul Pittman et al., *U.S. Cybersecurity Standards to Get Tougher and More Specific: FTC and NYDFS Lead the Way*, WHITE & CASE (Sept. 9, 2020), https://www.whitecase.com/publications/alert/us-cybersecurity-standards-get-tougher-and-more-specific-ftc-and-nydfs-lead-way [https://perma.cc/VE8P-MH7N] (describing what future cybersecurity compliance will look like and that it is necessary to align with successful industry recognized standards).

consumer's data, but Texas can modify it to ensure small businesses are covered and satisfying their duty to consumers.[217]

For example, it cannot be mandatory for a small business that collects sensitive PII to comply with an existing data security safeguard such as the GLB Act because it is too burdensome on a small business who does not have the resources nor fiscal means to satisfy compliance.[218] There should be an exception in place for a small business' general compliance with the regulation.[219] Instead, a small business that collects sensitive PII should be mandated to implement administrative, technical, and physical safeguards in accordance with the data that is collected and the resources available to them.[220]

An additional safe harbor provision should be added to offer extra resources and funds to small businesses that voluntarily opt into an existing data security safeguard.[221] This ensures that despite their lack of resources, small businesses are meeting a certain level of compliance and are also supported and encouraged to meet greater compliance standards to protect consumers' data.[222] Furthermore, Texas can ensure the resources given out to small businesses are being utilized by allowing the regulating agency to request a summary report of the cybersecurity policy in place at those small businesses.[223]

---

217. *See generally id.* (explaining that the New York SHIELD Act will expect higher cybersecurity requirements for businesses such as industry standards, however there is room to tweak it for compliance relative to small businesses).

218. *See generally* REPORT, *supra* note 99, at 1, 8 (describing how the Texas Privacy Protection Council, authority given by law, can review the laws governing privacy and protection of PII).

219. *Cf.* Ieuan Jolly, *US Privacy and Data Security Law: Overview*, THOMSON REUTERS PRAC. L., https://1.next.westlaw.com/Document/I03f4d7afeee311e28578f7ccc38dcbee/View/FullText.html?originationContext=knowHow&transitionType=KnowHowItem&contextData=%28sc.DocLink%29 [https://perma.cc/TGR3-LJNM] (comparing to the consequences under the law that can apply to small businesses. The exemptions listed are not necessarily for small businesses but for law enforcement, and health (HIPPA)).

220. *See id.* (contrasting what New York and Oregon state cybersecurity laws implement).

221. *See* REPORT, *supra* note 99, at 1, 8 (relating Ohio's data security law that contains a safe harbor provision that acts as an affirmative defense to tort action if the business implements reasonable cybersecurity measures).

222. *Cf. id.* (comparing the safe harbor provision that could be utilized in Texas cybersecurity law to the one in Ohio's cybersecurity law to incentivize small businesses to improve their cybersecurity).

223. *See* Neto et al., *supra* note 4 (stating that regulatory agencies must ensure that proper cybersecurity compliance frameworks are in place to support local businesses such as the NIST framework).

Overall a lot of current regulations implemented in Texas can be updated to take on more stringent and specific data security regulations such as Texas Insurance Code § 830.004, which requires insurers licensed in the state to complete the N.A.I.C. Own Risk and Solvency Assessment (ORSA) that the Texas Commission on Insurance may request a summary of annually.[224] Nowhere in this statute nor the N.A.I.C. ORSA does it require a standard cybersecurity policy or regulation to protect consumers' sensitive PII collected for insurance purposes.[225] Texas should uphold consumers' privacy and trust by adopting the N.A.I.C. Insurance Data Security Model Law ensuring state licensed insurance providers are accountable for maintaining a data security plan.[226] Furthermore, for insurance providers that qualify as small businesses, an exception should be made to ensure they are not overly regulated but are still mandated to satisfy some level of compliance.[227] The Texas Commission on Insurance may require more oversight to adopt the N.A.I.C Model Law; in fact, it would be an easy transition that ensures accountability for modern-day risks of cyberattacks with the current statute in place.[228]

C. The Lack of Cybersecurity Implemented by Small Businesses Has an Adverse Effect on the Minority Community

As of May 2020, over four million small businesses in Texas make up forty-five percent of the private labor in the State.[229] Over one million minority small businesses in the State represent underprivileged

224. *See* TEX. INS. CODE ANN. §§ 830.004, 830.005 (detailing requirements for ORSA completion along with the possibility of requirements being reviewed annually).

225. *See* NAT'L ASS'N OF INS. COMM'R, NAIC OWN RISK AND SOLVENCY ASSESSMENT (ORSA) GUIDANCE MANUAL 1 (2017), https://www.naic.org/documents/prod_serv_fin_recievership_ORSA-2014.pdf [https://perma.cc/H4D8-JLAZ] (suggesting an insurer refer to the laws adopted by their state of domicile when determining requirements for risk management).

226. *See* MODEL LAW, *supra* note 176, at (emphasizing NAIC's insurance model main priority is to protect consumers' information).

227. *See generally Cyber Attacks & Defenses for Small Business*, *supra* note 153 (explaining certain cyber defenses small businesses need to implement compared to larger businesses).

228. *See generally* TEX. INS. CODE ANN. §§ 830.004, 830.005 (outlining the structure already in place by the regulating entities to transition to the NAIC Model Law); *see generally* MODEL LAW, *supra* note 176, at 1 (referencing the NAIC security model).

229. *See* SMALL BUSINESS ECONOMIC PROFILE, *supra* note 55 (detailing the economic statistics of small businesses).

communities.[230] Furthermore, as of 2019, small businesses make up ninety-seven percent of employer firms in the San Antonio, Texas area.[231] Under the current regulations, small businesses do not have the knowledge, resources, nor government assistance to implement sufficient cybersecurity practices to prevent cyberattacks such as data breaches.[232] Loss of business accounted for almost forty percent of the average cost of a data breach with the other sixty percent coming from cost associated with legal, regulatory, and data retrieval fees.[233]

Therefore, at the rate cyber attackers are targeting small businesses, the lack of cyber readiness adversely affects the minority communities these businesses serve.[234] For example, if a small business experiences a cyberattack such as a data breach, one of the common consequences is for that business to file for bankruptcy.[235] If the small business filing for bankruptcy included medical care, pediatric care, dental care, insurance, legal or financial related services that served the minority community, would possibly result in further financial loss for the minority consumers affected.[236]

---

230. *See* Sakian, *supra* note 25 (describing the disparity in business ownership in the state of Texas).

231. *See* CITY OF SAN ANTONIO ECON. DEV. DEP'T, 2019 ANNUAL REP. 8–9 (2019), https://www.sanantonio.gov/Portals/0/Files/EDD/Media/EDD-AnnualReport.pdf [https://perma.cc/AY7G-NKYU] (listing the details of individual and small business owners and the demographics which make up that portion of the population).

232. *See generally State Data Security Laws*: *Overview*, *supra* note 11 (comparing New York, Ohio, and Oregon's cybersecurity laws that are not meant to regulate or assist small businesses in implementing their own effective cybersecurity. Rather those states just provide exceptions to the main regulations large businesses can implement because they have the resources to).

233. *See* PONEMON INST., *supra* note 3 (emphasizing percentages of costs associated with data breaches for a small business owner).

234. *See Why the Future Success of Our Economy Depends on the Expansion of U.S. Minority-Owned Business*, MINORITY BUS. DEV. AGENCY, https://archive.mbda.gov/news/blog/2016/11/why-future-success-our-economy-depends-expansion-us-minority-owned-business.html [https://perma.cc/65BK-WXJ7] (correlating the success of small minority owned businesses leads to an increase in community investment).

235. *Compare* Ehlinger, *supra* note 18 (stressing that a severe consequence for a small business suffering a cyberattack is to file for bankruptcy); *with New Survey Shows a Majority of Small Businesses Believe They are a Likely Target for Cybercrimes; More Than a Quarter Have Experienced Data Breach in Last Year*, *supra* note 88 (acknowledging out of the small businesses surveyed, 25% of them filed for bankruptcy).

236. *Cf. Hearing on S.228*, *supra* note 79, at 2, 5 (explaining that cybersecurity risks are existential threats to small businesses causing them to go bankrupt).

The pressing issue to solving this problem is the lack of statistical data on the number of minority-owned small businesses affected by cyberattacks.[237] Why don't we care to look out for our small minority business owners that are essential to our communities?[238] There is a logical connection between the lack of cybersecurity in small businesses and the way it affects consumers and the negative effect on minority-owned businesses and the minority consumer communities they serve.[239] However, without accurate data about how the lack of cybersecurity affects businesses and consumers, it is hard to create targeted solutions to the problem.[240]

III. SOLUTION

A. Federal Level

The biggest threat to small business is their lack of awareness, education, and resources in place to deal with a data breach or cyberattack.[241] For example, a small business owner of a marketing company expressed that she wanted to retain assistance to address her cybersecurity but did not know who would qualify as a good third-party cybersecurity provider or IT person.[242] The owner proceeded to question why there was not a certified cybersecurity credential for experts like

237. *See generally* King, *supra* note 16 (recognizing that the general lack of data collected on cybersecurity measures stems from the federal government industry classifying system not classifying cybersecurity as an industry yet).

238. *See generally* Dua et al., *supra* note 215 (emphasizing that minority owned small businesses may be most at risk, additionally, addressing how COVID-19 made those vulnerabilities worse).

239. *See* Kiersten E. Todt, *Small Businesses Barely Survive Cyberattacks—The US Must Help to Secure Them*, THE HILL (May 7, 2021, 1:31 PM) https://thehill.com/opinion/cybersecurity/552296-small-businesses-barely-survive-cyber-attacks-the-us-must-help-to [https://perma.cc/9MRV-NJ4W] (emphasizing that small businesses are the weak link in the economy's supply chain. Further, small businesses have limited resources and are not able to invest in cybersecurity and that 80% of America's businesses have fewer than ten employees).

240. *See* King, *supra* note 16 (emphasizing cybersecurity is a relatively new field, so an industry has not been established to analyze and publish data).

241. *See* Myers, *supra* note 71 (emphasizing that small businesses only have two options since they lack the awareness and education, that is to find a way to implement the necessary security measures or retain an outside resource to do it for them, yet many do not do either).

242. *See id.* (referring to small business owners' lack of knowledge on where to even find help for cybersecurity and if that help is the 'right' help they need).

there are for CPAs or licensed insurance brokers.[243] Additionally, an owner of a paving company (small business) knows little about computers in general, and relies on ineffective methods of cybersecurity in QuickBooks and other cloud software.[244] These two examples show the need for government regulation of small business cybersecurity standards as well as access to resources that contain the tools to implement sufficient cybersecurity practices.[245]

At the federal level the U.S. Small Business Administration (SBA) is the point of contact for providing the resources and conducting the research necessary to assist small businesses in implementing effective cybersecurity policies.[246] Currently, the SBA does little to offer direct guidance in implementing cybersecurity for small businesses when it is one of the more severe threats small businesses face consistently.[247] The SBA currently offers a thirty-minute online class that provides a program covering cybersecurity concepts for small businesses which are outdated and do not guide small businesses on how, when, and what kind of cybersecurity they should be implementing.[248]

The SBA should be developing a low-cost, vendor-neutral certification program for small business employees who serve as their designated

243. *See id.* (discussing issues within regulation for small companies and why there are not individuals that are certified to assist with issues in the cyber security field for small business owners).

244. *See generally id.* (distinguishing the necessity of small businesses, like a construction company, to have good cybersecurity posture yet lack the capability and resources to do so).

245. *See id.* (recognizing the gap between the government's goal of wanting effective cybersecurity across the board, yet the cybersecurity regulation in place does not educate or assist small businesses to comply).

246. *See Small Business Assistance*, TEX. ECON. DEV. [https://perma.cc/85SR-CM8B] (discussing the economic assistance the SBA provides for small businesses and it being the main federal resource dedicated to small businesses).

247. *See id.* (stating the resources SBA offers include: information around loan disbursement, advocacy efforts, and business relationships, but not necessarily information on how to implement systems of security).

248. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, DEFENSE CYBERSECURITY: OPPORTUNITIES EXIST FOR DOD TO SHARE CYBERSECURITY RESOURCES WITH SMALL BUSINESSES, at 11; *see Preparing Small Businesses for Cybersecurity Success: Hearing Before the Comm. on Small Bus. and Entrepreneurship*, 115th Cong. 2, 6 (2018) (explaining new solutions the SBA can implement for cybersecurity training programs those small businesses can utilize since none of the current SBA cybersecurity training are effective. Disregarding the current SBA thirty-minute cybersecurity training because it is poor quality, the advice is impractical for small businesses to implement, and simply not helpful in educating on the main cyberthreats small businesses actually face).

cybersecurity experts allowing those employees to be professionally certified and qualified to handle cybersecurity issues.[249] Furthermore, SBA should develop a free online cybersecurity boot camp that shows concrete steps small businesses can take to develop a basic cybersecurity program addressing the most critical and persistent threats.[250] This bootcamp would not require any prior knowledge and the SBA should consistently update the content to keep up with the evolving cyberthreats small businesses face.[251] Depending on the type of sensitive PII a small business collects, participating in this boot camp should be a prerequisite to receiving an SBA loan.[252] In addition, SBA should be utilizing their ground offices spread across the country, known as Small Business Development Centers (SBDC), and their personnel in getting them trained and certified to educate other small businesses owners on cyber habits when starting a new business.[253]

The Small Business Cybersecurity Enhancement Act would also prepare SBDCs to receive information on cyber threats and breaches as they occur to guide small businesses in their response in real time.[254] Furthermore, the SBA should assist small businesses by establishing a cybersecurity cooperative, which would identify and evaluate cybersecurity products and services for its members; thereafter, participating small businesses would receive negotiated rates on those

249. *See Hearing on S.228*, *supra* note 79, at 2, 6 (outlining a program that allows small businesses to have a resource to help themselves by gaining access to cybersecurity personnel they often don't have).

250. *See generally id.* (creating another option for small businesses to help themselves if they are unable to afford personnel that are certified to meet their cybersecurity needs).

251. *See generally id.* (ensuring the boot camp is repeated as often as necessary, so small businesses can receive training to mitigate common cybersecurity threats).

252. *Cf. id.* at 6 (introducing a solution to the lack of cybersecurity knowledge with a fee boot camp with incentives that help all parties involved; if the SBA were to require a small business to take this course, it ensures that businesses educate themselves on cyber threats and on how to implement effective cybersecurity while also having an assurance that the small business receiving the loan is less likely to succumb to a cyber threat that would decrease the chance of that business being successful and repaying the loan).

253. *See id.* at 1 (stating that the Small Business Cyber Training Act should include a provision ensuring that SBDCs are utilized to offer cybersecurity advising to small businesses).

254. *See id.* (discussing the propositions to be covered throughout the duration of the hearing).

products and services.[255] This would allow for small businesses to: (1) receive greater value for their investment; (2) know which of the qualified products to use; and (3) increase the overall cybersecurity of small businesses across the country.[256]

The little data that is collected about how small businesses are affected by cyberattacks and data breaches is mainly done by private entities with no real push from the federal government to collect data.[257] This is due to cybersecurity being a relatively new field that has yet to be defined as an industry by the federal government's North American Industry Classification System—the standard federal agencies use to collect, analyze, and publish statistical data related to the business economy.[258] As soon as it is defined as an industry, there should be a federal initiative through the SBA and FTC to ensure data is collected on small business data breaches/cyberattacks, the effects on small businesses, and its effects on their patron's data.[259]

Furthermore, the FTC Cybersecurity for Small Business Campaign must be utilized since the FTC is the lead federal agency in ensuring consumer protection and charging those that violate its standards.[260] This could be a collaborative effort with SBA, the CISA, and the National Cybersecurity Communications Integration Center for the government to private entity collaboration.[261] Additionally, there should be an effort to simplify and tailor the version of the NIST framework for small

255. *See id.* (promulgating a solution for small businesses, like the owner of a marketing business, to find third party cybersecurity services that can be trusted if they don't have the capabilities to implement services themselves).

256. *See id.* (expounding on the ability to ensure that small businesses are receiving first class cybersecurity tools to implement which strengthens the overall cybersecurity posture of the private sector).

257. *Cf.* King, *supra* note 16 (addressing the failure of the federal government to start researching and collecting data through its federal agencies due to the cybersecurity industry not being registered as one).

258. *See id.* (discussing the issues surrounding an emerging field where there is yet to be firm regulation).

259. *See* Pittman et al., *supra* note 216 (adhering to the FTC being the head federal agency charged with enforcing cybersecurity requirements, protecting consumer's data, and in leading small business cybersecurity research).

260. *See* FED. TRADE COMM'N, PRIV. & DATA SEC. UPDATE, at 15 (outlining the updates and emphasizing that the FTC under which cybersecurity falls).

261. *See id.* at 16 (noting the work that is done alongside DHS, NSIT, and SBA above to develop the Cybersecurity for Small Business Campaign).

businesses so that there may be a blueprint to implement a renowned cybersecurity safeguard.[262]

B. State Level

Although regulations are burdensome, they are necessary because they can help improve a business's ability to detect a data breach/cybersecurity threat and respond appropriately.[263] Future legislation regarding cybersecurity regulation should be written broadly enough to adapt to new technology and business standards, yet specific enough to ensure efficiency in protecting Texan's sensitive PII.[264] Furthermore, the Texas Cybersecurity Council—being an enduring partnership between private and public industry—should have a larger role in creating resources to assist small businesses cybersecurity development.[265] This could be achieved through a variety of ways including state agency oversight/collaborations such as DIR, utilization of public universities as local/ground facilitators of resources such as Texas A&M University System Cyber Response Team, or the UTSA National Security Collaboration Center/UTSA Small Business Development Center.[266] These are all resources the state can organize and get out to these small businesses in need.[267]

---

262. *See id.* at 12 (proposing a NIST privacy framework that guides small businesses through privacy risks).

263. *See generally* PONEMON INST., *supra* note 3 (finding that government regulation can help improve a business's ability to detect a data breach, evaluate their risk in order to satisfy compliance, and continue to create solutions); *see also* Pittman et al., *supra* note 216 (contrasting how burdensome cybersecurity regulation is with the benefit of it providing a clear path to the price measures, processes, and controls for effective cybersecurity).

264. *See* REPORT, *supra* note 99, at 12 (promoting a balance between future legislation addressing current issues, but still being broad enough for the evolution of those issues and mindful to not contradict the legislation already in place).

265. *See Texas Cybersecurity Council*, *supra* note 204 (pointing out that "the Texas Cybersecurity Council represents the acknowledgment that cybersecurity initiatives cannot rely on government alone").

266. *See id.*; *see also Texas A&M University System Cyber Response Team*, TEX. A&M UNIV. SYS. OFF. OF INFO. & TECH., https://it.tamus.edu/blog/texas-am-university-system-cyber-response-team/ [https://perma.cc/D79J-P4B7] (introducing how the Texas A&M System Security Operations Center and Cyber Response Team responds to cyber incidents within the recent framework of the Texas Division of Emergency Management).

267. *See Hearing on S.228*, *supra* note 79, at 1 (indicating the necessity for small businesses to realize the resources available to them).

To further advance resources such as cybersecurity personnel and training, Texas can contribute to small businesses through the Skills Development Fund.[268] This fund is administered by the Texas Workforce Commission and aims to provide training dollars for Texas businesses and workers with the help of the public community and technical colleges, local workforce development boards, and economic development partners.[269] The collaboration of these entities already in place makes it easier for small businesses to develop cybersecurity training that they could utilize and provide access to professionals that can conduct and explain the importance of cybersecurity.[270] This could be a resource that can incentivize small businesses if the voluntary safe harbor provision is complied with.[271]

Furthermore, one of the greatest issues inhibiting targeted assistance and development of cybersecurity practices for small businesses is the lack of data collected on small businesses encountering cyberattacks.[272] For example, a business is required to report a data breach that affects 250 people to the Office of the Texas Attorney General as regulated by the Texas Identity Theft Enforcement and Protection Act.[273] An open records request from the Office of the Texas Attorney General of data breaches in 2020 reported 325 breaches of businesses.[274] The open

268. *See* CLIFF MORTON & BUS. SERV. CTR., CITY SAN ANTONIO ECON. DEV. DEP'T 22 (2011) https://www.bexar.org/DocumentCenter/View/190/San-Antonio-Small-Business-Resource-Guide-PDF [https://perma.cc/PE6U-4NGC] (listing the funding available through the state and its uses).

269. *See id.* (emphasizing the organization and purpose of the funds and the administrator of the funds available in Texas).

270. *Cf. id.* (appealing to the reason why this fund is established which is to provide businesses with funds and resources through other entities that can help develop and train their workforce).

271. *Cf.* TEX. PRIV. PROT. ADVISORY COUNCIL., REPORT 7–8 (2020), https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/TPPAC%20Interim%20Report%2087th.pdf [https://perma.cc/5HPQ-8A65] (implying another incentive for small businesses to utilize the proposed Texas safe harbor provision).

272. *Cf.* King, *supra* note 16 (affirming the reason why the government does not have an initiative to conduct research on cybersecurity and ultimately how cybersecurity affects small businesses).

273. *See* TEX. BUS. & COM. CODE ANN. § 521.052 (outlining requirements for data breaches through the law in the state of Texas).

274. *See generally* OFF. OF TEX. ATT'Y GEN., PIC R 007756, ALL DATA BREACH REPORTS SUBMITTED ELECTRONICALLY JAN-DEC 2020 (2020) (reporting on data breaches that were submitted electronically in compliance with Texas statutes).

records report provides the business name; type of entity; date the data breach is discovered, when it began, and when it ended; the type of personal information involved; if a law enforcement agency is contacted; the number of Texans effected; and the remedial measures taken.[275]

All the information provided supports the overall statistics identifying the consequences of a data breach, including the average time between when a data breach is discovered, when it started, and when it actually ended.[276] Yet, a request showing how many small businesses have reported a data breach to the state, whether these businesses were small businesses, or how many of the data breaches were form the San Antonio metropolitan area cannot be fulfilled.[277] With small businesses being so pivotal to the Texas economy and its communities, it should be imperative that this information is collected to better understand how to support these businesses.[278] The State should be utilizing its research institutions in higher education to collect and analyze the data being provided.[279] The State's public flagship university systems already have programs and institutions in place to assist small businesses, such as the UTSA Small Business Development Center, where state funding can be applied towards advancing this research vital to small business's survival.[280]

275. *See generally id.* (providing information allowable by statute on data breaches reported within the state of Texas).

276. *See* PONEMON INST., *supra* note 3 (explaining that the 2020 U.S. average to identify a data breach is 186 days, and 51 days to contain the breach for an average total of 237).

277. *See* E-mail from June B. Harden, Assistant Att'y Gen., Assistant Pub. Info. Coordinator for the Tex. Off. of the Att'y Gen., to author (Jan. 6, 2021) (on file with *The Scholar: St. Mary's Law Review on Race and Social Justice*) (reflecting opens record requests and the conversation which followed).

278. *See* TUNSTALL ET AL., *supra* note 61 (providing data that shows that small businesses in 2012 had an economic impact of $844 million in gross output).

279. *Cf.* REPORT, *supra* note 99, at 3 (implying that Texas already has a close relationship when collaborating with different state agencies regarding data sharing and cybersecurity strategy, and that the State is the best entity to look to for research since it already provides its public institutions with the funding).

280. *See Welcome to UTSA Small Business Development Center*, UNIV. TEX. SAN ANTONIO, https://sasbdc.org [https://perma.cc/BTB2-XZLQ] (providing a resource for small businesses where they can access a multitude of things from confidential business advising to research resources).

C. Local Level

Small businesses in San Antonio make up over ninety-seven percent of private firms and over a quarter of the total employment.[281] As previously stated, small businesses play a vital role in local job market growth as well as the wellbeing of the people, programs, and community.[282] For example, Jefferson Bodega is a small local corner store on the Westside of San Antonio, Texas that gives back to the community by organizing toy, school supplies, food, and voter registration drives; it also teams up with other small businesses to showcase them on their storefront.[283] This is just one example of how successful small businesses are giving back to the community which has supported them while simultaneously lifting other small businesses along the way.[284]

Due to how essential small business are, a myriad of resources have been developed for them to overcome their economic instability; however, no organized solution to assist them with cybersecurity threats has yet to be implemented.[285] This is due to both small businesses not

281. See HALEBIC & NIVIN, *supra* note 65, at 7 (providing information about the employment by firms with less than 100 employees in the San Antonio area).

282. *See Why the Future Success of Our Economy Depends on the Expansion of U.S. Minority-Owned Business*, *supra* note 234 (identifying the investment small businesses and small minority owned businesses make in the community).

283. *See* @jeffersonbodega, INSTAGRAM (Sep. 9, 2020), https://www.instagram.com/jeffersonbodega/ [https://perma.cc/PF8M-VTBW] (setting the example by showcasing other businesses); *see also* @jeffersonbodega, INSTAGRAM (Oct. 5, 2020), https://www.instagram.com/jeffersonbodega/ [https://perma.cc/PF8M-VTBW] (giving back to the community through service events); *see also* @jeffersonbodega, INSTAGRAM (Nov. 29, 2020), https://www.instagram.com/jeffersonbodega/ [https://perma.cc/PF8M-VTBW] (assisting the community during a time where people are not financially stable by setting up a toy drive).

284. *See* @sanantoniogold, INSTAGRAM (Dec. 15, 2020), https://www.instagram.com/sanantoniogold/ [https://perma.cc/CFY9W4PG] (expressing gratitude for the business' community by organizing a food drive at the elementary school next door for at-need students who rely on school breakfast/lunch for the holidays and would not get that over the holiday break).

285. *See San Antonio MBDA Business Center*, MINORITY BUS. DEV. AGENCY, https://www.mbda.gov/business-center/san-antonio-mbda-business-center [https://perma.cc/97W9-AWKT] (promoting their proven track record of service and advocacy for small minority owned clients assisting in securing over $185 million in loans and bonds); *see also Welcome to UTSA Small Business Development Center*, *supra* note 280 (providing entrepreneurs access to business advising, training programs, and a referral network); *contra The Community Cyber Security Maturity Model*, CIAS, https://cias.utsa.edu/the-ccsmm.html [https://perma.cc/A3U9-VSAE] (representing a cybersecurity model designed for communities, not specifically small businesses, but is the only effective resource that could contribute to small businesses).

understanding how threatened they are by cyberattacks and there not being one entity for them to go to for cybersecurity assistance.[286] San Antonio has all the tools necessary to implement a 'one-stop shop' that will deliver resources and information to small businesses that can be utilized to educate and implement effective cybersecurity practices.[287] With public education institutions taking the lead on this initiative by collaborating with private entities, the resources and information being passed down to small businesses will be coming from experts and top researchers in the field.[288]

For example, San Antonio has already begun to foster growth and development of the local cybersecurity industry by implementing the San Antonio Chamber of Commerce Cybersecurity Council, Business Against Theft Network (BAT-NET) and the Southwest Texas Fusion Center.[289] The San Antonio Chamber of Commerce Cybersecurity Council aims to provide support and advocacy for legislative issues impacting the cybersecurity industry and create initiatives to meet future industry needs through collaboration with academic institutions, the private sector, and the military.[290] BAT-NET is a business crime alert program provided, at no cost, by the San Antonio Police Department (SAPD) for businesses in the San Antonio area.[291] It provides a two-

286. *See* Ehlinger, *supra* note 18 (recognizing that cyberattacks often have severe consequences for small businesses, mostly due to a lack of resources available to them).

287. *See Business Facilities' 15th Annual Rankings: State Rankings Report*, *supra* note 33 (displaying all the cyber infrastructure San Antonio has in place—second behind Washington D.C.—making it known as "Cyber City").

288. *Cf. UTSA National Security Collaboration Center*, UNIV. TEX. SAN ANTONIO, https://nscc.utsa.edu/ [https://perma.cc/52RU-VYUQ] (emphasizing the credentials UTSA already has including four National Center of Excellence designations from the NSA, making it more than capable of being the lead resource option for small businesses to seek out).

289. *See Southwest Texas Fusion Center*, CITY OF SAN ANTONIO, https://www.sanantonio.gov/Southwest-Texas-Fusion-Center [https://perma.cc/P9PL-LK3Y] (listing new development and growth in the area of cybersecurity); *see also Cybersecurity Council*, SAN ANTONIO CHAMBER COM., https://www.sachamber.org/get-involved/cyber/ [https://perma.cc/JJ8Q-TXT4] (describing steps taken to create and enhance business cybersecurity); *see also SAPD and Business Community*, CITY OF SAN ANTONIO, https://www.sanantonio.gov/SAPD/SAPD-and-Business-Community [https://perma.cc/4RMW-52GK] (offering information for citizens and business owners alike).

290. *See Cybersecurity Council*, *supra* note 289 (promulgating the importance of government assistance to the development of the industry through cybersecurity workforce and recruitment).

291. *See SAPD and Business Community*, *supra* note 289 (introducing the steps law enforcement is taking at the local level to address cybercrime and how it is affecting small businesses rather than just individuals and larger businesses).

way communication between police and business concerning current business crime alerts and includes cybercrime that effects small and large businesses.[292] The Southwest Texas Fusion Center is a working group of regional and national agencies, managed by SAPD, that serves as a threat center for information/intelligence and public safety with a central focus on cyber integrity.[293] These local government initiatives and small business collaborations are the necessary legislative backing and resources small businesses need to be successful in cybersecurity.[294]

The institutions include the federal law enforcement/intelligence agencies, cyber military assets, six universities with NSA Center of Excellence designation, and the 140 cybersecurity firms in the private sector that call San Antonio home.[295] The University of Texas at San Antonio (UTSA) is the one institution that has the resources and established relationships to assist small businesses cybersecurity.[296] UTSA is one of the few universities in the nation to hold four National Center of Excellence designations from the NSA and DHS, further solidifying its dominance as a leader in cybersecurity.[297] It can be the

292. *See id.* (explaining the two-way relationship between the BAT-NET and the San Antonio police department).

293. *See generally Identifying Cyber Threats and Computer Crime in South Texas*, ARMA SAN ANTONIO, https://armasanantonio.org/event-3577706 [https://perma.cc/6S5C-44N7] (implying that the internet research tools utilized to establish metrics of internet-connected devices and vulnerability-related information can be used to monitor any cybercrime threats towards businesses); *see also Southwest Texas Fusion Center*, *supra* note 289 (indicating the capability and information it can provide to assist in creating this model resource for small businesses to use through its public and private partners throughout the South-West Texas region).

294. *See generally Southwest Texas Fusion Center*, *supra* note 289 (describing the importance of legislative action for small business protection).

295. *See NSA Designates UTSA a National Center of Academic Excellence in Cyber Operations*, UTSA TODAY (Oct. 26, 2021) https://www.utsa.edu/today/2018/06/story/NSA-CyberDesignation.html [https://perma.cc/YBW3-BEFK] ("The University of Texas at San Antonio (UTSA) has been designated by the National Security Agency (NSA) as a National Center of Academic Excellence in Cyber Operations Fundamental (CAE-Cyber Operations) for 2018 through 2023.").

296. *See Business Facilities' 15th Annual Rankings: State Rankings Report*, *supra* note 33 (establishing the cyber resources already based in San Antonio, Texas); *compare with UTSA National Security Collaboration Center*, *supra* note 288 (leading the way due to already established relationships with all the above cyber leaders in San Antonio).

297. *See NSA Designates UTSA a National Center of Academic Excellence in Cyber Operations*, *supra* note 295 ("Receipt of the CAE-Cyber Operations designation makes UTSA one of the few universities in the nation to hold three National Center of Excellence designations from the National Security Agency, further solidifying its dominance as a leader in cybersecurity.").

"one-stop shop" where small businesses can go to for resources and assistance on establishing effective cybersecurity with the collaboration of three centers UTSA is already home to.[298]

First, the UTSA Small Business Development Center (SBDC) is a part of the South-West Texas Border Small Business Development Center Network where entrepreneurs have access to business advising, quality training programs, and an extensive referral network.[299] Furthermore, small businesses have access to research resources and workshops specifically designed for small businesses.[300] For example, UTSA's SABDC hosted a COVID Business Town Hall, Cybersecurity in a Time of COVID-19, which focused on protecting small businesses and their remote working environments from cyberattacks during the pandemic.[301] The UTSA's SBDC already consists of experts who understand the economic and logistical hardships small businesses face thereby keeping those hardships in perspective when collaborating with the next two centers that provide the cybersecurity resources.[302]

Second, the UTSA National Security Collaboration Center (NSCC) has created an ecosystem to engage government, industry, and academia to tackle the nation's greatest cybersecurity threats.[303] Its goal is to be the nation's premier supplier of cyber-ready workforce tailored to provide innovative solution for the national security challenges facing

298. *See Cyber Security: Protecting Your Small Business Before the S. Comm. on Healthcare and Tech.& the Comm. on Small Bus.*, 112th Cong. (2011) (explaining that small businesses should be going to one trusted source that has a harmonized message for the type of effective cybersecurity they should be implementing).

299. *See generally Welcome to UTSA Small Business Development Center*, *supra* note 280 (demonstrating the multiple avenues for connecting with other small businesses through the program).

300. *See id.* (supporting small businesses through their corporate affiliates that provide business advising and training events that could be geared towards cybersecurity and how it is implemented on a larger scale).

301. *See generally COVID Training*, UNIV. TEX. SAN ANTONIO, https://txsbdc.org/businessrecovery-register/ [https://perma.cc/6ZJM-AMV9] (partnering with the State of Texas Cybersecurity Coordinator and Southwest Texas Fusion Center representative to educate small businesses on cyber vulnerabilities they face and ways to stay resilient to them).

302. *See Welcome to UTSA Small Business Development Center*, *supra* note 280 (relating to other federal, state, and local SBA's, all have the personnel experienced with what small business budgets look like, the fiscal position they are in, and what they can spare to afford).

303. *See UTSA National Security Collaboration Center*, *supra* note 288 (explaining the purpose of the Universities' new National Security Collaboration Center (NSCC)).

U.S. Government, the state of Texas, and the private sector.[304] With the network of relationships that the NSCC has already built, it is now easier to collaborate with small businesses to develop a cybersecurity framework.[305] Third, the UTSA Center for Infrastructure Assurance and Security (CIAS) has worked on community security since 2002.[306] Despite the essential focus of cybersecurity at the federal level on critical infrastructure, cybersecurity at the state and community levels has lacked, making it arguably the weak link in the nation's cybersecurity chain.[307] The Community Cyber Security Maturity Model (CCSMM) is a coordinated scheme, providing communities and local jurisdictions with a framework to identify what is needed to build a cybersecurity program that will prepare, detect, respond, and recover when a cyberattack occurs.[308] This framework is versatile; no matter the industry, CCSMM can adjust to help small businesses develop their cybersecurity framework.[309]

Here, the UTSA SBDC, NSCC, and CIAS accomplish so much individually. However, if all three divisions combined their services to assist small businesses in implementing effective cybersecurity practices, small businesses would need to look nowhere else to find that help.[310] The SBDC develops cost effective training specifically geared for small businesses, because it knows the economic and logistical challenges that

304. *See id.* (listing the mission statement of the UTSA National Security Collaboration Center).

305. *See id.* (noting the NSCC embedded partners with Dell Technologies, Army Research Laboratory, Air Force Research Laboratory, National Security Agency, 16th Air Force, Air Force Life Cycle Management Center (Cryptologic and Cyber Systems Division), Air Force Chief Data Science Office, Texas Department of Information Resources, U.S. Secret Service, plus an additional thirty partners have signed on to locate within the NSCC once the new facility opens).

306. *The Community Cyber Security Maturity Model*, *supra* note 285

307. *See id.* (emphasizing that small businesses are the only area of cybersecurity that isn't supported at the government level despite so many consumer and government contracts going through small businesses).

308. *See id.* (describing how it works to prepare and defend against cyber-attacks).

309. *See id.* (showing the versatility of the CCSMM in how it can incorporate other frameworks such as the NIST Cybersecurity Framework, National Initiative for Cybersecurity Education, and the Cybersecurity Workforce Framework).

310. *See generally Cybersecurity Hearing*, *supra* note 164, at 7–8 (statement of Rep. Mac Thornberry, Member, H. Cyber Sec. Taskforce) (urging the idea that one resource is needed for small businesses to go to where they can receive advising on all facets of effective cybersecurity which the three UTSA centers combine to represent).

small businesses face.[311] NSCC already has established relationships with cybersecurity experts in the government, military, and private sectors.[312] Finally, the UTSA CIAS has developed the technical framework that small businesses can use to shape their cybersecurity.[313] UTSA is the solution for small businesses' cybersecurity needs due to its reputation as the undisputed leader in cybersecurity education in the San Antonio community and South Texas region, through its three established, foundational centers.[314] These centers along with the UTSA cybersecurity program's ability to create internship opportunities for their students to assist small businesses in implementing cybersecurity is a great way to provide the necessary personnel that small businesses do not have access to.[315]

To further ensure small businesses are implementing effective cybersecurity policies to protect consumers' data, at the local level, the city can use tax breaks to incentivize small businesses to use these resources.[316] For example, the San Antonio Tax Phase-In Program helps new or expanding companies gain a stronger foothold in their initial years by creating a tax abatement.[317] This tax abatement helps promote business expansion, attract new businesses, and assist the city's overall economic development strategy.[318] A similar tax phase-in could be

311. *See UTSA Small Business Development Center*, *supra* note 280 (showing the various ways a small business can receive cost friendly cybersecurity assistance).

312. *See generally UTSA National Security Collaboration Center*, *supra* note 288 (listing the many organizations tied to NSCC).

313. *See The Community Cyber Security Maturity Model*, *supra* note 285 (noting CIAS's ability to provide communities with a structure that prepares and assists those communities in creating a cybersecurity framework).

314. *See generally UTSA National Security Collaboration Center*, *supra* note 288 (leading the way, UTSA's cyber security programs collaborate with academia, government, and industry to protect America's national security).

315. *See Table of Experts: Cybersecurity Professionals on Handling a Data Breach*, *supra* note 20 (finding the largest cybersecurity vulnerability for small businesses is either the lack of cybersecurity personnel or comparable IT resources to large businesses); s*ee generally UTSA National Security Collaboration Center*, *supra* note 288 (keeping with UTSA's vision to be the national supplier of cybersecurity's workforce, implementing an internship program to assist small businesses is the best way to supply personnel to small businesses while also giving students practical experience before entering the real world).

316. *See* Myers, *supra* note 71 (proposing a tax incentive to offset the cost of compliance or implementing the cybersecurity system).

317. *See* CLIFF MORTON & BUS. SERV. CTR., *supra* note 268 (implementing a tax abatement on real or personal property that can be used for improvements for up to ten years).

318. *Id.*

given to small businesses that implement effective cybersecurity using the resources UTSA provides.[319] This, in turn, would ensure San Antonio consumers' data are protected and improve the overall economic development of the city by protecting small businesses.[320]

D. Small Businesses and Their Minority Counterparts

Despite all the education, advising, and resources from the UTSA collaboration, small businesses still face a huge challenge in implementing cybersecurity due to not having a dedicated staff for information technology (IT) nor any room to budget for cybersecurity.[321] The fees associated with cyberattack/data breaches make it more essential than ever for small businesses to have cyber insurance despite being generally reserved for larger businesses.[322] A Ponemon Institute research study found that post data breach; 51% of businesses used cyber insurance to cover the cost of third-party consulting and legal fees, 36% of businesses used it to cover the cost of restitution to the victims, and 10% used it to cover the cost of extortion or ransomware.[323] Currently, only about 40% of small to medium size businesses buy the coverage.[324] This is largely due to small businesses not investing enough resources upfront to secure their business from a cyberattack, making it increasingly difficult to qualify for cyber insurance.[325]

Furthermore, when a small business starts applying for cyber insurance, they are met with a ten to twenty-five page questionnaire regarding the IT processes, control, and system that is being

319. *See also* Myers, *supra* note 71 (introducing the implementation of compliance regulations and using incentives, such as tax breaks, for small businesses that comply).

320. *See generally Metropolitan Statistical Area Profiles*, *supra* note 66 (explaining small businesses with five hundred or less employees making up over half of the employment in the San Antonio-New Braunfels Metropolitan Statistical Area).

321. *See* Ehlinger, *supra* note 18 (stating the challenge it is for small businesses to implement cybersecurity or fend off cyberattacks without a dedicated staff to do so or IT budget).

322. *See id.* (ending a cyberattack is expensive. A small business must pay extorsion fees, legal fees, lose business from interrupted operations, etc.).

323. *See* PONEMON INST., *supra* note 3 (detailing the breakdown of the cost for cybersecurity breaches for businesses).

324. *See* Ehlinger, *supra* note 18 (reporting on the number of businesses that purchase the coverage throughout the state).

325. *See id.* (explaining how cost affects whether small businesses purchase cyber insurance. Small businesses consider the cost of the insurance and the cost incurred to meet cyber insurers requirements prior to qualifying for insurance).

implemented.[326] Small businesses do not know how to answer insurance application questionnaires without hiring a consultant to lay out all the business's risks which would make them ineligible.[327] However, small businesses need to access cyber insurance due to the financial detriment a cyberattack pose without it.[328] Cyber insurers should be making the application for eligibility more lenient depending on the size of the business, industry, and weight of the potential risk.[329] Insurers should still be able to mitigate risks by offering reduced prices for the cyber insurance coverage if the small business does implement the cybersecurity measures usually required for eligibility.[330]

In addition to the current lack of accessibility to knowledge, assistance, resources, and cyber insurance to combat the threat of a cyberattack, small businesses—and businesses in general—further the risk by failing to communicate amongst each other when a cyberattack occurs.[331] Most businesses do not disclose the details of cyberattacks amongst each other for fear of exposing confidential business practices, giving the competition an upper hand, or losing reputation.[332] Yet businesses need to share that information quickly, efficiently, and regularly because one vulnerability taken advantage of in one business could be the same

326. *See id.* (demonstrating the lengths a small business must meet to acquire cybersecurity insurance).

327. *See* Judy Shelby, *Cyber Insurance: Insuring for Data Breach Risk*, THOMSON REUTERS PRAC. L., https://1.next.westlaw.com/Document/Iabe04ecd7a6f11e498db8b09b4f043e0/View/FullText.html?originationContext=document&transitionType=DocumentItem&contextData=(sc.RelatedInfo)#co_anchor_a550473 [https://perma.cc/D7WD-P48D] (establishing how hired counsel assists business in applying for insurance).

328. *See* Ehlinger, *supra* note 18 (indicating costs covered by insurers for a cyberattack on a small business, such as the legal fees, forensic fees, data restoration costs, and extra expenses the business might incur to deal with the interruption in the operation of their business).

329. *See id.* (outlining what can be scaled down for small businesses such as the number of questions asked and the requirements needed for eligibility).

330. *See* Shelby, *supra* note 327 (listing the requirements to apply for cyber insurance).

331. *Cf.* Neto et al., *supra* note 4 (relating companies do not share information regarding effective cybersecurity measures and potential cyberattacks, thus creating an impediment to understanding how cyberattacks occur).

332. *See* ANDREW NOLAN, CONG. RSCH. SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES 32–33 (2015) (detailing the myriad of legal liability a business may face if they share their cyber-information, including privacy, antitrust, negligent tort law, shareholder derivative suits, and breach of express and implied contracts).

vulnerability ten other businesses may have.[333] From a security standpoint, businesses that work together to share information regarding their cybersecurity policies and threats help to mitigate the overall risk of a cyberattack.[334] It is the main reason BAT-NET is a vital resource SAPD has implemented to help facilitate the information sharing that will mitigate an attack from threatening all businesses.[335]

1. What We Do Not Know About Small Minority-Owned Businesses' Cybersecurity

Through research and data collected, the government realized the disparity between small minority-owned businesses and their counterparts in receiving government contracting opportunities.[336] Research shows minority-owned firms are less likely than non-minority-owned firms to receive the capital necessary to make their business goals a reality.[337] The Brookings Institution 2018 Small Business Credit Survey shows that large banks approve around 60% of loans sought by white small business owners, 50% of those sought by Hispanic small business owners, and just under 30% of those sought by black small business owners.[338] This research has encouraged implementing programs that ensure government contracts are issued to small, minority-

333. *See* King, *supra* note 16 (reporting how easily businesses can fall victim to cyberattacks and how financial companies recognize efficient, quick, and regular information sharing is crucial to defend against cyberattacks).

334. *See id.* (insinuating that teamwork, rather than competing, is what is necessary for small businesses to decrease the cyberattack threat).

335. *See SAPD and Business Community*, *supra* note 289 (explaining how SAPD uses BAT-NET to help local business prevent business crimes).

336. *See Minority Entrepreneurs*, U.S. SENATE COMM. ON SMALL BUS. & ENTREPRENEURSHIP https://www.sbc.senate.gov/public/index.cfm/minorityentrepreneurs [https://perma.cc/6DUL-CNV8] (acknowledging as the numbers of minority owned business in the United States increases, there has been a reduction in minority business grant recipients).

337. *See Why the Future Success of Our Economy Depends on the Expansion of U.S. Minority-Owned Business*, *supra* note 234 (sharing the difficulties minority-owned firms have in acquiring funding).

338. *See* Sifan Liu & Joseph Parilla, *Businesses Owned by Women and Minorities Have Grown. Will COVID-19 Undo That?*, THE BROOKINGS INST. (Apr. 14, 2020), https://www.brookings.edu/research/businesses-owned-by-women-and-minorities-have-grown-will-covid-19-undo-that/ [https://perma.cc/5UFU-Z3JZ] (laying out the percentage difference amongst small business owners in accessing capital with respect to race).

owned businesses at the federal, state, and local levels.[339] In addition, the programs ensure minority-owned businesses have greater access to capital, allowing the economy to enjoy employment, community investment, and innovation that small, minority-owned businesses bring.[340]

Ensuring all small businesses have access to federal contracts, to capital, and to technical assistance needed for success is a top priority for the U.S. Senate Small Committee on Small Business and Entrepreneurship.[341] Yet there is not any data or research collected on the lack of knowledge, resources, or community impact cyberattacks have on small minority-owned businesses.[342] It has been shown that cyberattacks can be detrimental to the survival of a small businesses lacking cybersecurity.[343] If, "diverse small-business ownership is [truly] essential to our nation's continued economic success and growth," then the only answer is for the government to invest in and fund research on how small minority-owned businesses are affected by cyberattacks.[344] No matter the size, the industry, nor the ethnicity, cybersecurity will be a factor in any business and the problems and solutions need to be addressed now.[345]

339. *Cf. Why the Future Success of Our Economy Depends on the Expansion of U.S. Minority-Owned Business*, *supra* note 234 (expressing the importance of the Minority Business Development Agency's mission to grow and expand minority-owned firms).

340. *Cf. id.* (sharing how Minority Business Development Agency has created partnerships and programs to assist minority entrepreneurs in accessing alternative sources of capital).

341. *See Minority Entrepreneurs*, *supra* note 336 (stating the mission of the Committee on Small Business and Entrepreneurship is ensuring small business have access to capital, technical assistance, and federal contracts).

342. *Cf.* E-Mail from June B. Harden, *supra* note 277 (demonstrating the lack of information on data breaches of small, minority-owned businesses and the lack of access small, minority-owned business have to government records of cybersecurity data).

343. *See* Ehlinger, *supra* note 18 (commenting cyberattacks have severe consequences, like bankruptcy, for small businesses which lack resources).

344. *Minority Entrepreneurs*, *supra* note 336.

345. *See* PONEMON INST., *supra* note 3 (graphing data from businesses all around the world which experience enormous, expensive, and severe cyberattacks. The research shows cyberattacks likely will not slow down).

CONCLUSION

Larger companies have a greater focus on cybersecurity due to the large number of individual consumers that may be affected if a successful cyberattack were to occur.[346] Therefore, the combination of federal/state legislation and industry regulation toward large businesses, critical infrastructure, and government agencies shows a lack of acknowledgement for the dangers small businesses face from cyberattacks.[347] The government's investment in small businesses shows how important small businesses are to the economy; they create numerous jobs and support local communities.[348] Despite the lack of resources, knowledge, regulation, and assistance against cyberattacks, small businesses prevent cyberattacks by implementing a proactive cybersecurity approach.[349] Without that support, the consequences facing small businesses post cyberattack are detrimental to their survival.[350]

Specifically, in Texas, the legislation regarding cybersecurity in the private sector only regulates what data can be maintained and the procedure for reporting a data breach.[351] There is too much reliance on large businesses, which have the capabilities and resources to implement effective cybersecurity without requiring additional assistance, unlike small businesses that need help.[352] However, with revamped regulation and funding from the University of Texas at San Antonio's Small Business Cybersecurity Center, Texas can balance out small businesses'

346. *Cf.* Iszler, *supra* note 207 (admitting to experiencing over 12 million possible cyberattacks in one day during the week).

347. *See generally* Neto et al., *supra* note 4 (noting the lack of regulatory compliance at the local level in comparison to highly, federally regulated institutions).

348. *See* SMALL BUSINESS ECONOMIC PROFILE, *supra* note 55 (reasoning small businesses are important because they make up over forty percent of Texas business as of May 2020).

349. *See Hearing on S.228*, *supra* note 79 (emphasizing that in 2017, over fifty-eight percent of data breaches involved small businesses).

350. *See* Ehlinger, *supra* note 18 (indicating that cyberattacks often lead to a small business going bankrupt).

351. *See* TEX. BUS. & COM. CODE ANN. § 521.052–53 (regulating how data is maintained and the steps businesses must follow upon a data breach).

352. *See* Ehlinger, *supra* note 18 (reporting large companies are the presumptive targets for cybercrime, however it does not remove the substantial threats of cyberattacks on small businesses. Small business are good targets for intermediate cyberattacks attempting to infiltrate a third-party company.)

stress by complying with the law.[353] If the same initiative is provided to small businesses, they could access capital and government contracts; then, small businesses would no longer be the weak link in the nation's cybersecurity posture.[354]

353. *See generally Texas Cybersecurity Council*, *supra* note 204 (informing on the collaboration of the Texas Cybersecurity Council with government, higher education, and private sector entities to combat cyberattacks. It is the same collaboration necessary for small businesses to combat cyber threats).

354. *See generally The Community Cyber Security Maturity Model*, *supra* note 285 (promoting a collaboration of entities which a small business could trust to produce comprehensive best cybersecurity practices and a singular source for cyber information and resources).