Public Policy and Administration Research
ISSN 2224-5731(Paper) ISSN 2225-0972(Online)
Vol.13, No.4, 2023

Policies for Protecting Digital America and Critical Infrastructure Industries Against 21st-Century Cyberattacks

Jakob Mincey[1], Binh Tran[2*]

1. School of Liberal Arts, Georgia Gwinnett College, Lawrenceville, GA 30043, USA
2. School of Science and Technology, Georgia Gwinnett College, Lawrenceville, GA 30043, USA

* E-mail of the corresponding author: btran5@ggc.edu

Abstract

Cyberattacks are rapidly evolving into a more sophisticated means of assault against countries, organizations, and individuals. The rapidly growing capabilities of cyberattacks, which may be conducted by either domestic or foreign malicious actors, underscores the potential devastation to a targeted nation's institutions and its people. These attacks can be deployed against critical industries to cripple a nation's economy, infrastructure, and citizens. Such an attack against a foreign nation could represent an act of modern warfare that equivalates to the 20th-century use of nuclear weapons. Therefore, to combat the potentially devastating cyberattacks of the 21st century, the United States government must pursue cybersecurity policies to protect its critical infrastructure industries and national security. This study seeks to determine the most effective cybersecurity policy when comparing the implementation of a white-hat hacker U.S. task force, cybersecurity regulations on critical infrastructure industries, implementation of cybersecurity awareness curriculum in K-12 public schools, and the federal implementation of a digital consumer privacy protection law. Results show that significant cybersecurity regulations targeting critical infrastructure industries represent the best policy approach for protecting those industries.

Keywords: *Digital America, Cybersecurity, Cyberattack, Critical Infrastructure Industries*

DOI: 10.7176/PPAR/13-4-05
Publication date: June 30th 2023

1. Introduction

The advancement of information technology coupled with the evolution of globalization accentuates the need for a secure digital society. In the increasingly fragile digital ecosystem (Hacker One, 2022), experts across the globe utilize advanced malicious techniques that are developed to disrupt business operations and steal the valuable data of individuals and organizations. Growing hardware and software techniques, such as malware-injected USB drives, offensive AI algorithms, and sophisticated Distributed Denial-Of-Service (D-DOS) attacks, expand the versatility of cyberattacks and the capabilities of hackers. With these new capabilities, the number of cyberattacks increases each year, with a 38% increase in global cyberattacks in 2022 compared to the previous year (Anderson, 2023).

Costs associated with cyberattacks are on the rise. In 2022, the average costs for a U.S. organization data breach were $9.44 million (IBM, 2022). While many cybercriminals target U.S.-based private businesses, some cyberattacks are directed against U.S. critical infrastructure organizations, strategically coordinated by foreign actors. In 2021, the Russia-based group DarkSide stole 100 gigabytes of data and spread vicious ransomware throughout the business networks of Colonial Pipeline, a vital U.S. oil pipeline originating in Houston, Texas. This attack resulted in a $5 million paid ransom and the stalling of transportation for roughly 15 million barrels of oil (Tsvetanov & Slaria, 2021). These critical infrastructure attacks represent the arduous process of holding foreign states responsible for national security-threatening cyberattacks initiated from within their borders.

Cyberattacks have given new meaning to 21st-century warfare. Cyberwarfare allows foreign governments to disrupt critical services and infrastructure with malicious code and to distill chaotic discourse among populations with digital disinformation. From 2014 to 2018, the Ukrainian energy sector experienced dozens of cyberattacks issued by foreign actors in Russia. Some of the attacks created temporary blackouts for hundreds of thousands of Ukrainian citizens (Maliarchuk et al., 2019). Since Russia invaded Ukraine in 2022, there have been over 250 documented cyberattacks by their government against Ukraine (Cyber Peace Institute, 2022).

The rise of cyberattacks and the techniques used to breach both private and public domestic organizations highlight how the United States is ill-equipped for the potentially catastrophic cyberattacks of the 21st century. In 2021, the U.S. government spent $8.64 million on cybersecurity for its federal agencies outside of the Department of Defense. This is significantly lower than the previous four years and represents a 53% decrease from 2020 spending (Petrosyan, 2022). Even if Congress approves a more significant cybersecurity budget for federal agencies, the United States government must engage in innovative ideas to promote and strengthen national cybersecurity.

A devastating cyberattack against another country is a consequential catalyst of change for international relations and the laws of war. It will encompass varying exclusive cyber techniques combined with a sophisticated plan of attack. For example, a foreign government with dangerous political desires, such as the expansion of territory or the disruption of presidential elections, may first target the critical infrastructure sites of major cities to produce widespread blackouts; implement a D-DOS attack on emergency response services to flood emergency hotlines; distribute a sophisticated disinformation campaign on social media sites to inflict confusion and panic among the affected populations; and target government surveillance and communication channels to delay a military response. Therefore, the U.S. government must prepare for scenarios involving devastating, intricate cyberattacks, beyond investing in cybersecurity measures for federal agencies. This paper will outline four policy proposals that each strengthen national cybersecurity prevention and mitigation efforts for federal government consideration.

Implementation of a U.S. White-Hat Hacker Taskforce and support for verified third-party organizations to challenge cybersecurity systems

One of the best methods for companies to identify whether a critical system is vulnerable to cyberattacks is for the company to attack its own systems. This type of good-faith attack is committed by ethical security hackers, commonly referred to as white-hat hackers, who aim to identify system vulnerabilities (Kaspersky, 2022). These individuals are expert IT professionals who either studied in the cybersecurity field with a desire to become an ethical security hacker, or they may have been malicious hackers that violated ethical standards, commonly known as black-hat hackers, who decided to turn over a new leaf. White-hat hackers typically work for vendors or as independent security researchers, and their job is to assess vulnerabilities and report them to the proper authority so that they can be patched (Wilson et al., 2016).

Private companies may elect to hire white-hat hackers to function as cybersecurity agents who periodically assess company security measures. Federal agencies like the Federal Bureau of Investigation (FBI) hire ethical tech experts to become “cyber special agents” who evaluate system vulnerabilities and investigate cybercrimes (FBI, 2014). However, the most common utilization of ethical hackers is through bug bounty programs, where companies pay freelance cybersecurity researchers and professionals to find security bugs within their secure systems. Notable companies that offer bug bounty programs include Apple, Amazon, Android, Microsoft, Facebook, Google, Intel, and Mozilla (Bugcrowd, 2023). The quality and quantity of bug bounty programs have increased significantly in the past few years. Microsoft awarded $13.7 million in bounties to over 330 security researchers across the globe in 12 months from 2021-2022 (Microsoft Security Response Center, 2022). GitLab awarded over $1 million in bounties across 221 valid reports in 2022, nearly four times higher than the bounties distributed in the year prior (Malcolm, 2022). Some companies like HackerOne, Bugcrowd, and Synack have been established to function as brokers between white-hat hackers and companies seeking to evaluate network and device security measures (Doubleday, 2018). The U.S. government has also utilized bug bounty programs across multiple federal agencies. In 2016, the Pentagon hosted a crowdsourced vulnerability disclosure program called “Hack the Pentagon,” which recently launched its third iteration in 2022 (Haworth, 2023). The program is designed to crowdsource ethical hackers to find bugs in Department of Defense (DoD) systems.

The U.S. government currently hires ethical hackers in select agencies, operates bug bounty programs, and utilizes verified third-party organizations that work with white-hat hackers to discover DoD vulnerabilities. So far, bug bounty programs have been instrumental in reducing system vulnerabilities across a variety of industries. However, companies that deploy bug bounty programs, like Apple, may choose to neglect vulnerability reports or refuse to pay white-hat hackers what they believed is owed (Albergotti, 2021), which hurts the overall viability of this crowdsourced practice.

This proposal argues that the president should establish a white-hat hacker task force that recruits the nation’s top cybersecurity professionals to evaluate the security systems of government institutions and critical infrastructure industries. With a designated task force, members can strategically attack these entities and provide risk assessment analyses on a need-to-know basis. These IT professionals will be U.S. government employees who are appropriately compensated, thoroughly vetted, and who follow all applicable government procedures relating to national security. In doing so, the U.S. government eliminates any potential issues with utilizing crowdsourced programs, such as a drop in the volume of ethical hackers that assess for vulnerabilities, the surge of false reports generated to bog down review systems, or the potential evaporation of allocated funds. Programs that utilize verified bug bounty organizations, such as the “Hack the Pentagon” initiative, should continue to exist and expand to appropriate federal agencies. A combined approach that authorizes a white-hat hacker task force and that continues to support third-party ethical hacking programs is the ideal solution for protecting critical infrastructure industries.

Significant cybersecurity regulations on U.S.-based critical infrastructure industries

Regarding federal regulations for cybersecurity and privacy measures, the U.S. government has not deployed any significant cybersecurity regulations on business entities operating in the United States (IT Governance, 2023). Consequently, there are no major cybersecurity regulations on the critical infrastructure industries that represent targets to malicious actors who may administer a catastrophic cyberattack. Outside of privacy laws that dictate how health and financial institutions should protect and distribute collected information within their systems, the only significant cybersecurity statutes are the Federal Information Security Modernization Act of 2002 and its 2014 amendments, and the Cybersecurity Information Sharing Act of 2015. The former implemented security controls for federal agency information systems, and the latter enabled private companies and government entities to coordinate and share cyber threat information (Enterprise Engineering Solutions, 2023). Therefore, critical infrastructure entities are solely responsible for the cybersecurity measures they implement within their organizations, even with the expectation that these entities will be primary targets of future cyberattacks that jeopardize national security and American livelihood.

A major argument for cybersecurity regulations lies in the prevalence of social engineering. Social engineering is the manipulation of an individual to divulge confidential information to be used for illegal purposes. Examples of social engineering include scareware that demands payments from frightened individuals, hacking into someone’s email account, tailgating authorized users to access protected systems, phishing private information, Domain Name System (DNS) spoofing, bait advertisements, physical breaches on individuals’ devices, pretexting, watering hole attacks that identify an individual’s web surfing patterns, and even attempts of quid pro quo (Pilette, 2021).

Social engineering techniques are nearly prevalent in all forms of cyberattacks, including malware-based attacks. In Q2 of 2021, a majority of cyberattacks against organizations and over 90% of cyberattacks against individuals utilized social engineering techniques (Positive Technologies, 2021). In recent U.S. history, major cyberattacks against critical infrastructure companies have featured some form of social engineering. The 2021 Colonial Pipeline ransomware attack transpired due to a leaked password from an ex-employee and an inactive Virtual Private Network (VPN) account (Tsvetanov & Slaria, 2021). The 2020 SolarWinds hack, which jeopardized the systems of over 30,000 companies and government institutions, was a supply chain breach orchestrated by malicious actors who uploaded malicious code onto the widely used Orion network management system (Temple-Raston, 2021). It was later reported that SolarWinds was likely breached a year prior using a compromised Microsoft 365 account (Oladimeji & Kerner, 2022), though Microsoft has denied such claims (Novinson, 2021). Nevertheless, while the original exploit of SolarWinds and affiliated company systems may not be identifiable, the exploit likely utilized some deployment of social engineering techniques.

Outside of social engineering methods, malware-based attacks that utilize exploits like zero-day vulnerabilities represent additional cyberattack strategies that must be secured through cybersecurity regulations. Zero-day vulnerabilities are dangerous vulnerabilities malicious hackers discover and utilize before the vendor becomes aware of them. As such, no patches for the vulnerabilities are available and no defense measures are in place. The 2021 SolarWinds hack and the 2021 Kaseya ransomware attacks were both supply chain breaches conducted utilizing zero-day vulnerabilities (Oladimeji & Kerner, 2022; Nichols, 2021).

In each example of recent U.S. cyberattacks, all but one were orchestrated by foreign hacking groups operating in Russia; the 2021 SolarWinds hack was perpetrated by Chinese hackers (Goodin, 2021). These examples highlight how critical infrastructure cyberattacks conducted by malicious foreign operators jeopardize U.S. national security.

From multi-factor authentication on company logins to the use of temporary passwords and digital certificates, there are dozens of potential cybersecurity provisions that applicable federal agencies should consider when regulating critical infrastructure industries. If Congress does not desire to create a new federal agency, the powers of the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS) should be expanded so that it may generate, implement, and review federal cybersecurity regulations. These regulations should not be designed nor implemented to restrict the free-market liberties shared by these organizations. Rather, they should promote industry growth, strengthen the defensive capabilities of each organization, and protect the national cyberspace; a vital strategy to combat the potential dangers of a multifaceted and catastrophic 21st-century cyberattack.

Investment and support for cybersecurity awareness curriculum implemented in K-12 public schools

Under the premise that social engineering is ubiquitous in almost all cyberattacks, the U.S. government can prevent such techniques by educating future generations on increasingly dangerous and prevalent cyberattacks. Prevention can be correlated with the success of corporate security awareness training programs that are implemented to reduce business security breaches (Proofpoint, 2021). The curriculum of cybersecurity courses must instruct students on basic social engineering techniques and ways to circumvent them, and the structure of the course should be sensitive to the education level of the students. Not only would these courses assist students in protecting their personal information, digital profiles, and devices, they would instruct students on the potential consequences of social engineering techniques that could become catalysts of a major cyberattack.

Educating young students on the dangers of phishing techniques, password reuse, communication with unknown sources, and other dangerous online activities, will lead to them utilizing what they learned throughout their personal lives and into their future career industries. Out of practicality, this policy proposal recommends that the cybersecurity awareness curriculum should coincide with currently established and related IT curricula, such as typing, internet browsing, digital citizenry, and basic IT-level courses. The curriculum should be instructed within a semester-long course that is a requirement for school transition and graduation.

Many school programs across the nation, including the local Gwinnett County, Fulton County, Forsyth County, and Barrow County school districts in Georgia, are framing IT-related curricula into lessons on digital citizenship. Digital citizenship can be defined as the quality of online habits and consumption patterns of technology that affect individuals and their communities (Gwinnett County Public Schools, 2020). Lessons on digital citizenry instruct students on recognizing their digital footprints, maintaining online safety, and communicating online respectively and effectively. The goal of these courses is to help students become good digital citizens both at home and in school.

At many Georgia schools, including Paul Duke STEM High School in Gwinnett County, course developers are fitting digital citizenship curriculum into an introduction to information technology courses throughout K-12 schools. Teachers are also encouraged to merge digital citizenship lessons across school curricula to instruct students who cannot or choose not to enroll in IT courses (Gwinnett County Public Schools, 2020). Other states including Virginia, New York, and California are also implementing digital citizenship curricula (Song & Sridhar, 2021). So far, implementation of these types of IT-related courses is strictly at the state and local government levels. Utilizing these statistics helps show that the implementation of such programs proves the feasibility of implementing cybersecurity awareness courses in K-12 public schools (U.S. Institution of Diplomacy and Human Rights, 2023).

Outside of the United States, educators in foreign countries are hard at work to improve digital citizenship and overall IT courses in pre-college education. In South Korea, Minjeong Kim and Dongyeon Choi developed a youth digital citizenship scale to provide clear feedback for the successful integration of digital citizenship lessons with pre-college education. This study measures the digital citizenship skills that youths should develop, suggests the necessary competence and education that cultivates digital citizenship, and argues that such education should be integrated into both schools and society (Kim & Choi, 2018). The developed five-factor SAFE model consists of Self-identity in the digital environment, Activity in online environments (measuring reasonable activity and social/cultural engagement), Fluency in the use of digital tools, and Ethics for a digital environment. The SAFE model digital citizenship scale was measured using teacher participants to study varying implications for educating students to become active digital citizens (Kim & Choi, 2018).

In Taiwan, Yacine Atif and Chien Chou argue that for broad public and private participation in developing digital citizenship competencies, innovative educational approaches, pedagogical methods, and routine practices that foster digital literacy must be researched and implemented. The authors highlight the growing gap of digital citizenship competency across various education levels that continues to increase with a lack of unified policies (Atif & Chou, 2018). Authors Lile Ghemri and Shengli Yuan argue that modular teaching, alongside the implementation of instructional material into different subjects, is the best approach to teaching mobile privacy and security in IT-related disciplines. Utilizing multiple-choice questions relating to mobile device security and application privacy from 24 sampled students across two IT courses, the authors find that the students score better on exams and prefer this modular approach in class (Ghemri & Shengli, 2018). While the study measures students in IT-related fields at the college education level, the modular approach represents a practical solution for instructing K-12 students on cybersecurity and digital citizenship topics.

The federal government's role in this proposal is to place additional regulations for the instruction of cybersecurity curriculum on current and future federal programs for K-12 public schools. In areas where the federal government cannot invest, it should support all efforts conducted by state and local governments. Implementation of these lessons should not come directly from the federal government. With the current push from various U.S. states for digital citizenship courses in K-12 public schools, cybersecurity awareness curricula should be implemented within already established digital citizenship curricula. These courses will prepare students for the modern digital age as technology becomes even more integrated into their daily lives.

This cybersecurity education program is especially important for current and upcoming generations. A 2004 study published in *The Journal of Consumer Affairs* shows that while student respondents reported being less technologically challenged compared to non-student respondents, non-students are more likely to protect their online information than students (Milne et al., 2004), likely due to the students' increased use of online sources. The future of protected critical infrastructure industries lies in the knowledge and resilience of next-generation employees who enter the industry already aware of cybersecurity threats.

Strengthening consumer data privacy laws and regulating company-collected, private data distribution

An easy approach to gaining information through social engineering is finding an individual's private online data or purchasing the data from a company database. In the United States, there are currently no national consumer data privacy laws that prohibit companies that bulk collect consumer data from sharing and selling the data they collect. There are also no federal protections for notifying consumers whose data is breached or exposed by malicious actors who attack companies for the collection of consumer data (Klosowski, 2021). Currently, applicable privacy laws are separated based on industry, and they regulate only certain aspects of the collection and distribution of consumer data. The Health Insurance Portability and Accountability Act (HIIPA), the Fair Credit Reporting Act (FCRA), the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), the Electronic Communications Privacy Act (ECPA), the Children's Online Privacy Protection Rule (COPPA), the Video Privacy Protection Act (VPPA), and the Federal Trade Commission Act (FTC Act) represent the few federal privacy laws currently applicable in the United States. These laws provide extraordinarily little consumer protection for children and the records that are held by health services and financial institutions. However, they do provide restrictions on certain tools used for government surveillance (Reynolds, 2017).

The lack of modern consumer data privacy laws assists domestic and foreign companies' efforts to profit from consumer data. Consequently, it opens the door for malicious actors to collect information on Americans for social engineering purposes (Germain, 2021). These actors can purchase bulk collections of consumer data or steal information from less secure, third-party buyers. This information can either be used for personal motives or could be given to foreign governments that seek to gain information on important institutional officials and their known associates. To challenge these threats, the federal government should seek a bipartisan resolution that will prohibit the sale of consumer data without consumer input. While this resolution will see heavy blowback from corporate lobbyists who profit from these transactions, it is a crucial step for overall national security to protect the consumer data of Americans.

Good models for a national consumer data privacy law are the California Consumer Privacy Act (CCPA) and its California Privacy Rights Act (CPRA) amendments. The CCPA gives Californian consumers the right to know if personal information is collected by a business, the right to delete personal information collected, the right to opt out of the sale of personal information where applicable, the right to opt in to the sale of personal information of consumers under the age of 16, the right to non-discriminatory treatment for exercising these rights, and the right to initiate a private cause of action for data breaches. The CPRA amends aspects of the CCPA and gives consumers the right to correct inaccurate personal information and the right to limit the use and disclosure of sensitive information (Office of the Attorney General, 2023).

The CCPA and CPRA laws are ideal for national implementation since they give consumers the choice to opt in or opt out of the distribution of their private data. They also give consumers the right to potentially seek damages if a company fails to adequately protect against a data breach, which encourages companies to invest in better cybersecurity measures. This modernized and strict consumer privacy law will protect Americans from corporate greed and strengthen national security against malicious actors who seek to use or distribute consumer data for cyber intrusion purposes.

2. Reflecting on the policy solutions

Protecting the cybersecurity of critical infrastructure industries must become a priority for U.S. actors responsible for the health and stability of U.S. national security. These four proposals represent different policy options for applicable U.S. actors to consider. Regardless of the potential weaknesses of the policies, each proposal possesses unique capabilities for increasing institutional cybersecurity measures. Therefore, the research design will measure each policy proposal to determine which policy generates the most effective critical infrastructure cybersecurity.

Implementation of a U.S. white-hat hacker task force would help evaluate institutional cybersecurity measures. However, the growing success of crowdsourced bug bounty programs may result in a tax-dollar-driven task force that cannot compete with the skills of freelance IT professionals. Investment and support for cybersecurity awareness courses in K-12 public schools should be implemented for national security purposes and to assist young students in navigating the digital age securely. However, the variables needed to consider the effects on national security are too varying to postulate, and there is no guarantee that students will carry the cybersecurity lessons taught in school into their future career industries.

Strengthening consumer privacy laws and regulating company-collected, private data distribution is an important policy proposal in the interests of individual American security. However, the intense lobbying efforts conducted by organizations that profit from consumer data distribution may be too difficult to overcome. Additionally, there is no guarantee that data sold to third-party organizations will lead to malicious actors obtaining the data and using it for cyberattack purposes.

Given the policy positions above, significant cybersecurity regulations on critical infrastructure industries represent the best solution to ensure national security against future cyberattacks. Compared to the other three policies, this proposal is the most effective approach for preventing and mitigating the potentially catastrophic cyberattacks of the 21st century. This approach requires cooperation between the private institutions that must adhere to federal regulations and the public institutions that create and implement the regulations.

3. Hypothesis and Method

The implementation of federally regulated cybersecurity policies on critical infrastructure industries increases industry protections against future cyberattacks. This study measures how the implementation of a white-hat hacker U.S. task force, cybersecurity regulations on critical infrastructure industries, K-12 public school education on cybersecurity techniques, and federal implementation of digital consumer privacy laws each affect the safety of critical infrastructure industry networks and connected technologies. The policy that is most effective for the federal government to pursue is determined by the results of this study. Given the semester-long scope to accomplish this task, the process used for this study is a mixed methods approach utilizing descriptive statistics and a selection of applicable qualitative case studies. The effectiveness of the policies is determined by measuring if the case study representing each policy meets any of these seven requirements for a safer cyber environment: threat identification and management; vulnerability identification and management; identity management and access control practices; data security and privacy protection practices; threat awareness and security training; cyber threat information sharing; and the use of incident response plans, risk assessments, or related reports.

4. Data collection and analysis

The effectiveness of a U.S. white-hat hacker task force is represented by data from the Department of Defense's Vulnerability Disclosure Program (VDP). The VDP is a program that utilizes white-hat hackers (ethical hackers), who are employed through security firms like HackerOne, to ethically hack sectors under DoD jurisdiction to discover security vulnerabilities. The data used for this study comes from a 2022 annual report published by the Department of Defense Cyber Crime Center (DC3). This 2022 report shows the effectiveness of targeting and mitigating vulnerabilities in federal agency systems, with 6,346 vulnerabilities mitigated in 2022 and 44,758 vulnerabilities detected since the program's launch (DC3, 2023).

The Federal Information Security Modernization Act of 2014 provides a solid blueprint to measure the effectiveness of cybersecurity regulations on critical infrastructure industries. This law passed by the U.S. Congress authorizes the Department of Homeland Security to administer the implementation of cybersecurity policies for Federal Executive Branch civilian agencies, oversee agency compliance with administered policies, and assist the Office of Management and Budget (OMB) in developing these policies (CISA, 2023). Agency compliance is determined with an annual report issued by the inspector general of each agency or an independent external auditor. This study measures the current regulations issued by the OMB, without taking into consideration the agency's regulatory power to establish future guidelines. Per the fiscal year 2023-2024 inspector general document on reporting metrics, FISMA requires agencies to meet the cybersecurity standards set in multiple key areas, ranging from risk management to the use of incident response plans.

To measure the effectiveness of pre-university cybersecurity education in preventing targeted cyberattacks, this study will equivalate the measurement of K-12 sex education on preventing cases of adolescent pregnancy and STIs. The lack of quantitative data for the prevalence of pre-university cybersecurity education courses and the effectiveness of digital citizenry programs positions the study to require this alternative case study for measurement. To do so, a research design that measured the results across 66 studies of comprehensive risk reduction and 23 studies of abstinence education. From there, it was assessed that such curricula represented an effective strategy to reduce adolescent pregnancy, HIV, and STIs, based on the reduction of measured outcomes such as sexual activity, use of protection, and the number of sex partners (Chin et al., 2012). When correlated to cybersecurity awareness, these results show that such courses would, at least, improve student awareness of the dangers and prevalence of cyberattacks before entering their prospective industries.

The California Consumer Privacy Act and its California Privacy Rights Act amendments work as applicable case studies for measuring the effectiveness of digital consumer privacy laws on critical infrastructure cybersecurity. These laws give more power to consumers over their digital data, allow consumers to seek damages if harmed in a data breach, and limit corporate use and disclosure of sensitive information. This study will seek to answer whether such privacy laws correlate to stronger cybersecurity practices. When analyzing the state law's effects on institutions under its jurisdiction, results can extend to the federal level to analyze the law's effectiveness in protecting against cyberattacks.

Table 1. Key areas of measurement for cybersecurity practices and the results of each described policy

Key Areas of Measurement	White-Hat Hacker Taskforce	Cybersecurity Regulations	K-12 Cybersecurity Education	Digital Consumer Privacy Law
Threat identification and management		**X**	**X**	
Vulnerability identification and management	**X**			
Identity management and access control practices		**X**		**X**
Data security and privacy protection practices		**X**		**X**
Threat awareness and security training	**X**	**X**	**X**	
Cyber threat information sharing	**X**	**X**		
Incident response plans and risk reports	**X**	**X**		

5. Results and Discussion

Out of the four described policy positions, K-12 cybersecurity education programs represent one of the least effective strategies in strengthening the cybersecurity of critical infrastructure industries. Utilizing the correlated sex education case study, these courses are useful for keeping students aware of the dangers of sexual activity and allow students to identify threats caused due to sex, such as STIs. For cybersecurity purposes, K-12 education can help students become aware of and identify cyber threats. However, basic K-12 cybersecurity curricula will not prepare students in detecting and managing vulnerabilities. It does not promote better access control practices, privacy protection practices, or cyber threat information sharing between entities. It also does not prepare students for creating incident response plans or other cyber reports.

A federally implemented, digital consumer privacy law also lacks substantial application for cybersecurity purposes. Due to its limited scope, a digital privacy law protecting consumers would only apply to identity management and privacy protection practices. As seen with the consumer protection laws in California, businesses that operate under such laws are vulnerable to government action for non-compliance and civil suits for failing to protect consumer data from corporate data breaches. Therefore, businesses will increase protection practices in compliance with state law and are likely to increase identity management and access control practices to avoid potential data breaches. However, this is an inadequate cybersecurity policy when measured in other key areas represented in Table 1.

The implementation of a U.S. white-hat hacker task force shows promise of an effective cybersecurity strategy, but it does not represent the most effective policy approach for the U.S. government to pursue. The purpose of bug bounty programs like the VDP, which utilizes white-hat hackers, is to identify and help mitigate potential vulnerabilities that cybercriminals may target. In the case study used for this paper, ethical hackers are required to report their findings to DC3. This promotes the sharing of cyber threat information between the entities that find ethical hackers, the entities that hire ethical hackers, and the entities that share similar vulnerabilities. By utilizing outside ethical hackers, the institutions become aware of potential cyber threats and will likely strengthen systems and train employees to mitigate detected vulnerabilities. However, the use of ethical hackers does not increase the identification and management of real-time threats, nor does it guarantee any positive changes to an institution's access control or privacy protection practices.

Federally imposed cybersecurity regulations remain the best policy approach to prevent and mitigate devastating cyberattacks. As seen with the policy provisions of the Federal Information Security Modernization Act of 2014, the federal government can successfully create, implement, and audit the cybersecurity policies of applicable institutions. Regulations can include a wide range of policies that affect the strength of an institution's cyber protections. In the case of FISMA, federal agencies are regulated to have the required capacity to identify and manage real-time threats; follow OMB-designated access control and privacy protection practices; provide cyber threat and security training to applicable employees; share cyber threat information with other federal agencies and affected private entities; and to create incident response plans.

The only key area not explicitly regulated under FISMA is the use of ethical hackers to identify and manage potential vulnerabilities (CISA, 2023). However, with the regulatory powers given to the OMB, key areas such as this can be remedied with additional requirements. Regardless of regulatory capabilities for future application, this policy is the most effective based on its present-day provisions. Therefore, cybersecurity regulations on critical infrastructure industries represent the best policy for protecting these industries and the national cyberspace.

6. Limitations and Future research

This study is the result of a four-month, semester-long endeavor to identify the most effective policy to protect digital America and its critical infrastructure. A sufficient collection of quantitative data from private and public institutions, which determine the effects of adopted cybersecurity provisions, could not be obtained within this timeframe. As a result, a qualitative and case study approach is utilized for measuring the effectiveness of each policy. With this qualitative approach and the use of descriptive statistics, the research design measures policy effectiveness based on the presence of key areas of measurement in each policy under consideration; it does not determine the viability of adopted cybersecurity provisions.

Furthermore, the absence of studies that measure the effectiveness of adopted IT and digital citizenry courses on the cybersecurity skills of students in K-12 public schools resulted in the use of a correlating case study on the effects of sex education curricula on adolescent pregnancy, HIV, and STI prevalence. However, this correlation cannot fully equate the results of effective sex education to effective cybersecurity education. For example, students may be more eager to learn new concepts and participate in sex education courses due to their natural desires for sexual activity, and a similar driving interest for students may be absent in cybersecurity education. However, for this study, the correlation of sex education between cybersecurity education represents an ideal case study for measuring the effects of K-12 cybersecurity education on protecting critical infrastructure.

While this paper determines that cybersecurity regulations represent the best policy solution to protect critical infrastructure industries, this subject requires far more research as quantifiable data becomes more readily available. Future researchers are encouraged to seek quantifiable data from institutions willing to share such information as this policy option is pursued. These efforts should determine the effectiveness and viability of different cybersecurity regulations, and they should measure the effectiveness of all cybersecurity regulations on critical infrastructure industries, issued within a set timeframe. If pursuing a comparable case study approach to reevaluate the most effective policy determined in this study, future researchers are encouraged to seek out or develop case studies that determine the effectiveness of teaching cybersecurity topics in K-12 public schools on the cybersecurity skills utilized and understood by students.

7. Conclusion

A multifaceted and foreign government-initiated cyberattack against U.S. critical infrastructure industries has the potential to become the modern-day equivalent to the 20th-century nuclear bombings on Hiroshima and Nagasaki—a coordinated attack that permanently alters the landscape of global norms, international relations, and modern warfare. Whether this kind of cyberattack occurs, and if it will be deployed against the United States, cannot be factually predicted at this time. However, it is the responsibility of the U.S. government to prepare for potentially devastating cyberattacks aimed at undermining its national security, which is dependent on the operational stability of its critical infrastructure industries. The best policy approach to prevent and mitigate these efforts is to federally regulate cybersecurity policies on U.S. critical infrastructure industries.

Regardless of future efforts to improve this study, there should be enough available data for U.S. politicians to recognize the need for a strong cyber defense. Increasing cyber defensive capabilities is key for combatting future cyberattacks. It is the responsibility of United States politicians, its citizens, and its industries to cooperatively pursue, regulate, or implement cybersecurity policies that protect national security and digital America.

References

Albergotti, R. (2021, September 9). *Apple pays hackers six figures to find bugs in its software. Then it sits on their findings*. Washingtonpost.com. https://www.washingtonpost.com/technology/2021/09/09/apple-bug-bounty/

Anderson, J. L. (2023, January 20). *Global cyberattacks increased 38% in 2022*. Security Magazine. https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022

Atif, Y., & Chou, C. (2018). Digital citizenship: Innovations in education, practice, and pedagogy. *Journal of Educational Technology & Society, 21*(1), 152–154. http://www.jstor.org/stable/26273876

Bugcrowd. (2023). *Public bug bounty program list*. https://www.bugcrowd.com/bug-bounty-list/

Chin, H. B., Sipe, T. A., Elder, R., Mercer, S. L., Chattopadhyay, S. K., Jacob, V., Wethington, H. R., Kirby, D., Elliston, D. B., Griffith, M., Chuke, S. O., Briss, S. C., Ericksen, I., Galbraith, J. S., Herbst, J. H., Johnson, R. L., Kraft, J. M., Noar, S. M., Romero, L. M., & Santelli, J. (2012). The effectiveness of group-based comprehensive risk-reduction and abstinence education interventions to prevent or reduce the risk of adolescent pregnancy, human immunodeficiency virus, and sexually transmitted infections: two systematic reviews for the Guide to Community Preventive Services. *American Journal of Preventive Medicine*, *42*(3), 272–294. https://doi.org/10.1016/j.amepre.2011.11.006

Cybersecurity & Infrastructure Security Agency. (2023, February 10). *FY 2023-2024 inspector general federal information security modernization act of 2014 (FISMA) reporting metrics*. https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf

Cyber Peace Institute. (2022). *Cyber dimensions of the armed conflict in Ukraine*. https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf

Department of Defense Cyber Crime Center. (2023). *Vulnerability disclosure program 2022 annual report*. https://www.dc3.mil/Portals/100/Documents/DC3/Missions/VDP/Annual%20Reports/2022/VDP-2022-Annual-Report-Final.pdf

Doubleday, J. (2018). Pentagon unleashes more white-hat hackers on DOD's 'high-value assets.' *Inside the Pentagon, 34*(43), 5–5. https://www.jstor.org/stable/90025788

Enterprise Engineering Solutions. (2023). *Cybersecurity laws and regulations in U.S. [2023]*. https://www.eescorporation.com/cybersecurity-laws-and-regulations-in-us/

Federal Bureau of Investigation. (2014, December 29). *Seeking tech experts to become cyber special agents*. https://www.fbi.gov/news/stories/fbi-seeking-tech-experts-to-become-cyber-special-agents

Gwinnett County Public Schools. (2020). *Digital citizenship at Paul Duke STEM*. https://www.gcpsk12.org/domain/3985

Germain, J. M. (2021, February 4). *Is 2021 the year cyberattacks force privacy laws to grow some teeth?* TechNewsWorld. https://www.technewsworld.com/story/is-2021-the-year-cyberattacks-force-privacy-laws-to-grow-some-teeth-87008.html

Ghemri, L., Shengli, Y. (2018). Increasing students' awareness of mobile privacy and security using modules. *Journal of Learning and Teaching in Digital Age, 4*(2), 1-9. https://files.eric.ed.gov/fulltext/EJ1325039.pdf

Goodin, D. (2021, July 13). *SolarWinds 0-day gave Chinese hackers privileged access to customer servers*. Arstechnica.com. https://arstechnica.com/gadgets/2021/07/microsoft-says-hackers-in-china-exploited-critical-solarwinds-0-day/

Hacker One. (2022, September). *6th annual hacker-powered security report*. https://www.hackerone.com/reports/6th-annual-hacker-powered-security-report

Haworth, J. (2023, February 13). *U.S. government announces third hack the Pentagon challenge*. Portswigger.net. https://portswigger.net/daily-swig/us-government-announces-third-hack-the-pentagon-challenge

IBM. (2022, July). *Cost of a data breach report 2022*. https://www.ibm.com/downloads/cas/3R8N1DZJ

IT Governance. (2023). *Federal cybersecurity and data privacy laws directory.* https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws

Kaspersky. (2022, May 11). *Black hat, white hat, and gray hat hackers – definition and explanation.* https://www.kaspersky.com/resource-center/definitions/hacker-hat-types

Kim, M., & Choi, D. (2018). Development of youth digital citizenship scale and implication for educational setting. *Journal of Educational Technology & Society*, *21*(1), 155–171. http://www.jstor.org/stable/26273877

Klosowski, T. (2021, September 6). *The state of consumer data privacy laws in the U.S. (and why it matters)*. Nytimes.com. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Malcolm, N. (2022, December 19). *Why 2022 was a record-breaking year in bug bounty awards*. About.gitlab.com. https://about.gitlab.com/blog/2022/12/19/why-2022-was-a-record-breaking-year-in-bug-bounty-awards/

Maliarchuk, T., Danyk, Y., & Briggs, C. (2019). Hybrid warfare and cyber effects in energy infrastructure. *Connections, 18*(1/2), 93–110. https://www.jstor.org/stable/26948851

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *The Journal of Consumer Affairs, 38*(2), 217–232. http://www.jstor.org/stable/23860547

Microsoft Security Response Center. (2022, August 11). *Microsoft bug bounty programs year in review: $13.7M in rewards*. https://msrc.microsoft.com/blog/2022/08/microsoft-bug-bounty-programs-year-in-review-13-7-in-rewards/

Nichols, S. (2021, July 6). *Kaseya ransomware attacks: What we know so far*. Techtarget.com. https://www.techtarget.com/searchsecurity/news/252503633/Kaseya-ransomware-attacks-What-we-know-so-far

Novinson, M. (2021, February 5). *Microsoft: No evidence SolarWinds was hacked via Office 365*. Crn.com. https://www.crn.com/news/security/microsoft-no-evidence-solarwinds-was-hacked-via-office-365

Office of the Attorney General. (2023, February 15). *California Consumer Privacy Act (CCPA)*. Oag.ca.gov. https://oag.ca.gov/privacy/ccpa

Oladimeji, S., & Kerner, S. M. (2022, June 29). *SolarWinds hack explained: Everything you need to know*. Techtarget.com. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Petrosyan, A. (2022, September 12). *U.S. government: proposed cyber security spending 2023*. Statista. https://www.statista.com/statistics/675399/us-government-spending-cyber-security/

Pilette, C. (2021, July 26). *What is social engineering? A definition + techniques to watch for*. Norton.com. https://us.norton.com/blog/emerging-threats/what-is-social-engineering

Positive Technologies. (2021, September 22). *Cybersecurity threatscape: Q2 2021*. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2021-q2/

Proofpoint. (2021, July 27). *Enterprise cybersecurity solutions, services & training.* https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2022.pdf

Reynolds, G. (2017). *Ethics in Information Technology* (6th ed.). CENGAGE Learning Custom Publishing.

Song, J. S., & Sridhar, D. (2021, June 15). *How states can support the next generation of digital citizens*. Iste.org. https://www.iste.org/explore/how-states-can-support-next-generation-digital-citizens

Temple-Raston, D. (2021, April 16). *A "worst nightmare" cyberattack: The untold story of the SolarWinds hack*. Npr.org. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Tsvetanov, T., & Slaria, S. (2021). The effect of the Colonial Pipeline shutdown on gasoline prices. *Economics Letters*, *209*, 110–122. https://doi.org/10.1016/j.econlet.2021.110122

Tunggal, A. T. (2022, December 27). *What is an incident response plan?* Upguard. https://www.upguard.com/blog/incident-response-plan

United States Institute of Diplomacy and Human Rights. (2023, February 23). *What is digital citizenship and why is it important?* https://usidhr.org/what-is-digital-citizenship-and-why-is-it-important/

Wilson, A., Schulman, R., Bankston, K., & Herr, T. (2016). Who discovers vulnerabilities? *Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications* (pp. 7–8). New America. http://www.jstor.org/stable/resrep10484.6