Risk At Rest: How is the United States Government keeping our data secure?

Exploring security of a nation in cyberspace

Global Politics Engagement Activity Internal Assessment (SL)
February, 2025
Word Count: 1952

Growing up around digital technology for numerous years showed me the vastness of the internet, and helped me gain valuable skills that have shaped my view of the world. Several years back I picked up an interest in ethical hacking - breaking into devices and making them perform actions they were never intended to do: gain an advantage in a video game, access files that I didn't have explicit permission to, manipulate another device remotely. I have personally seen how easy it can be for a bad actor to perform malicious actions. A hacker could shut down an entire supply chain due to countless factors I will cover in this paper. As a single individual, if I gain physical access to a laptop, I can easily hack a device and remotely access the device within a few seconds. If I can do that, then so can an entire nation with hundreds of professionals whose job is to gain access to these devices. They can do significantly worse, and they have. What has always surprised me was how the public and private sector seemingly never learn from their mistakes, so recently I started wondering, how is the United States Government trying to secure our data? This idea stems from the belief that the most effective way of protecting national security, and individual privacy, is through actions taken by an authoritative body, and in this case, the United States government. Throughout this paper I will cover the national effect of data breaches and ransomware across the private and public sectors on national policies, and connecting how this idea relates to concepts of internal sovereignty, interdependence, and development.

In efforts to expand my knowledge of this topic, and actively engage with it, I chose to conduct interviews and attended a webinar. I reached out to two professionals in the field as their expertise are highly specific to the topic I chose, and conducted both over zoom, and attended a virtual webinar over zoom. I started out by interviewing Dr. Josephine Wolff, an associate professor of cybersecurity policy at Tufts University, using the information from that interview

to inform the following interview with Mrs. Jillian Burner, a cybersecurity advisor at the Cybersecurity & Infrastructure Security Agency (CISA). I attended a webinar called, "Demystifying AI in the SOC", conducted by James Taral, a cybersecurity consultant, hosted by SANS Institute, a leader in cybersecurity education and training. In my interview with Dr. Wolff, I learned about the effect of Inter-Governmental Organization (IGO) level policies like General Data Protection Regulation (GDPR), and she brought my attention to the Network and Information Systems (NIS) directive, which also affects cybersecurity across the EU. A significant takeaway from the interview was pivoting my research away from just data breaches towards investigating ransomware – a type of malware, or malicious software, designed to steal information, then prevent the affected person from accessing that information. The intent of this malicious software is to ransom the stolen information in exchange for monetary compensation. Using what I learned from that interview, I conducted an interview with Mrs. Jillian Burner, who heavily informed, and reinforced, the research I have collected. The intent of the interview was to get an understanding of CISA, an agency created during the Trump administration, oriented around improving the security of the nation at a physical, and a cyber level. Beyond that, she informed me of regulations across the nation, the prevalence of ransomware, and the importance of cybersecurity from a private and public perspective. I attended a webinar covering the use of Artificial intelligence (AI) in the Security Operations Center (SOC). A SOC is a term used to refer to a cybersecurity department, where the goal is maintaining the security of the devices in an organization. The reason for attending this webinar was understanding the future of cybersecurity, and how novel technologies will play a role in bolstering the security of the nation. The webinar informed me of standards used across the globe and how the industry as a whole is shifting towards embracing AI across cybersecurity.

The main difficulty of cybersecurity is the prevalence of interdependence in the form of private corporations and their ties to public institutions. In cybersecurity, the defense of infrastructure is as strong as the weakest link. A clear example is a breach in 2024 where state sponsored hackers gained access to the US Department of The Treasury through a compromised third party vendor, who had the ability to remotely control workstations at the department (Egan). The hack was performed by hacker's sponsored by another nation, which puts tension on an international scale due to the infringement of another nation's security, and as such sovereignty. The federal government has specific standards they are required to adhere to due to policies passed at a federal level; however, private companies are not beholden to such regulations, they are given recommendations that aren't heavily enforced. This unequal enforcement of security leaves all parties involved at risk, but companies have less incentive to implement these recommendations.

The federal government for the United States respects the internal sovereignty of States by allowing them to specify laws surrounding cybersecurity in their state, leading to differing regulations by state (Appendix B). This disjointment of regulations has little impact for most corporations, but a downside is that there is no enforcement of these laws at a national level, so most consequences of violating these laws are negligible or even non-existent (Appendix A). Bringing the enforcement of the regulations will increase the incentive for companies to comply with cybersecurity standards. A notable example is the network and information systems (NIS) Directive – legislation passed in the European Union (EU) with the intent of boosting cybersecurity in the EU – have played a role in bolstering cybersecurity for MNCs and nations alike, the effect being seen in the US with major corporations having higher requirements for cybersecurity. Bringing cybersecurity to the national level would likely benefit the nation as a

whole, but it is unlikely to happen due to pressures of internal sovereignty of states and lobbying efforts of MNCs to keep regulation at a minimum.

The struggle with regulations in general is they often restrict the abilities of corporations, specifically MNCs, which is why companies spend millions on lobbying in the United States, with nearly $200 million spent by technology companies in 2024 alone according to Open Secrets, a non profit that tracks the movement of money in US Politics. Regulations increase operating costs for businesses, increase time to present a minimal viable product (MVP) to market as the product is required to be secure, and add friction to accessing required resources within a company as more security is needed to keep those resources secured. What often goes overlooked initially is how a cybersecurity incident could affect a businesses operating capacity, whether by shutting down a manufacturing plant or disrupting the supply chain, taking precautions and setting up plans before hand, whether by choice or by requirement of regulation, can benefit a company in the long term financially (Appendix B). The benefit of regulations aren't often seen until after an incident occurs, where a company often suffers financially or reputationally. In 2024 a data broker – a corporation whose business is to sell personal information to public and private institutions – suffered a data breach resulting in the breach of 2.9 billion records containing sensitive information, and due to the reputational harm, were forced to shut down.

Why should the average person care about a company suffering from a data breach or a ransomware attack? A data breach is an incident where a company's data gets leaked onto the internet, while a ransomware attack is when an attacker uses that information to extort companies, and even individuals. The emphasis there is individuals. If a company suffers from a data breach, the customers get negatively affected; whether an individual has control over that

corporation, they often see a brunt of the attack. Leaked personal information can be used to open a loan in their name, use credit card information to make unauthorized purchases, or extort the person with highly sensitive information that someone could mistake as a person they know.

Cybersecurity has historically been a continuous cat and mouse chase; as hackers get more advanced, so do defenders in order to stay secure. A major criticism of regulation is the failure of it to keep pace with the rapidly changing landscape of cybersecurity. Regulations have historically been sluggish in regulating evolving technologies. The explosion of the internet is still struggling to be regulated, AI evolving at a rate surpassing anything in history is unlikely to see regulatory actions against it for a significant period of time. However, the benefit of regulations is that they place the blame on a specific party, as the focus on who is at fault when a security incident occurs is vague at best, leading to inaction for all parties involved; they hold organizations accountable.

Efforts have been made in politics pertaining to legislations regarding cybersecurity, primarily at a State level. Congress operates at a slower rate compared to state governments, leaving rapidly evolving landscapes like cybersecurity to the states. Most states have legislation regarding cybersecurity in one manner or another, often in terms of disclosures when an incident occurs. California has been a trailblazer in terms of legislation; the passage of the California Consumer Privacy Act (CCPA) – a legislation focused on privacy oriented policies, and cybersecurity related policies – was a major step for regulations in regard to bolstering cybersecurity for any business operating in California, and as such MNCs, were forced to improve their defenses. The legislation varies between states, but most corporations comply with the strictest regulations as it results in compliance with every state (Appendix A). The federal government has passed legislation on cybersecurity; however, the effects are limited to the

federal government. Federal agencies are required to comply with the NIST standard, a cybersecurity standard created by the National Institute of Standards and Technologies with the goal of setting a minimum requirement for the government and organizations to be secure (Appendix C). A criticism voiced by professionals is that most standards lack newer ideas, so simply meeting the requirement doesn't constitute them being secure. While a fair criticism, it gives a baseline for companies to expand on the idea, as a notable portion of organizations don't even meet the expectations of these standards. A concerning number of incidents occur because of simple mistakes like poor password hygiene – reusing the same password in multiple places, and using compromised login information. Companies who meet the standards are less likely to suffer from these well documented issues. In efforts to improve cybersecurity without the involvement of regulators, congress passed the Cybersecurity and Infrastructure Security Agency (CISA) Act. CISA is a part of the Department of Homeland Security with a focus on securing critical infrastructure both on a physical and a cybersecurity level (Appendix B). The agency often engages in consulting with a focus on being preemptive. A major flaw with most regulations across the nation is the focus on the results of a security incident, and little on preventing it in the first place.

There is a sizable chunk of actions the government can take to improve cybersecurity across the nation, but few are easy and most take exorbitant amounts of time and money to implement. The landscape of cybersecurity is always changing, and the introduction of AI will greatly accelerate it; massive bureaucracies like federal agencies and federal regulators take immense amounts of time to adjust to change. Regulations aren't the silver bullet to making critical infrastructure more secure, it will set a precedent of how it should be handled, in both the public and private spheres.

Works Cited

Egan, Matt. “China-Backed Hackers Breached US Treasury Workstations | CNN Business.” CNN, Cable News Network, 31 Dec. 2024, www.cnn.com/2024/12/30/investing/china-hackers-treasury-workstations/index.html.

“What Is GDPR, the EU’s New Data Protection Law?” GDPR.Eu, 29 Aug. 2024, gdpr.eu/what-is-gdpr/.

“The NIST Cybersecurity Framework (CSF) 2.0.” Nist.Gov, National Institute of Standards and Technology, 26 Feb. 2024, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

“Electronics MFG & Equip Lobbying Profile.” OpenSecrets, 2024, www.opensecrets.org/federal-lobbying/industries/summary?cycle=2024&id=B12.

NPD Closure, 2024, nationalpublicdata.com/.

“Cybersecurity and Infrastructure Security Agency Act of 2018.” Library of Congress, 2018, www.congress.gov/bill/115th-congress/house-bill/3359.

Appendix A

Josephine Wolff Interview

September, 2024

Zoom

Me: How influential is GDPR on US policy and how companies treat cybersecurity?

Wolf: I think it’s quite influential how they think about certain pieces of data protection and autonomy.The things that GDPR mandates have made a huge difference for Multinational companies and companies that do business in the EU. Like, giving people the option to receive

all of their data, and informing them of what use the data is being collected for. I think in terms of security it's a little less clear that it's been hugely influential. I would say that… The NIS directives have been a more influential piece.

Me: What are your thoughts on the United States adopting a federal level of Data Protection? For example, expanding on State Legislation like CCPA across the country.

Wolff: Maybe, but it's been pretty hard seeing it go through congress. I wouldn't say we've made a ton of progress.

Me: With the disjointed regulation in the US, how difficult do you feel it makes for companies trying to comply with them?

Wolff: I think generally most large companies appear to the strictest standards because that is easier than doing 50 different things. If you do that hardest thing you are generally in compliance with most things.

Me: How Influential are database breaches in pushing policies around preventing further security incidents?

Wolff: In the past they were influential because they were a newer phenomenon, and there was more of a sense there was oh my gosh there is a really big deal. I think nowadays ransomware attacks on critical infrastructure have done more to drive it.

Me: Do you have any regulations passed recently to regulate information companies can collect?

Wolff: There aren't really laws regulating how much information companies can collect.

Me: Recently there has been a data breach of the City of Columbus where the mayor claimed the data was either encrypted or corrupted. A cybersecurity researcher showed the public how serious the breach was and that the mayor was lying, and in response the city sued him. What are your thoughts on companies and the government lying to save face?

Wolff: We know that's illegal. It would violate deceptive business practices under the FCC.

Me: How should the US government deal with data breaches with companies? For example with fines and sanctions to encourage better standards because there is a risk or collaboration and standards to encourage better security out of good faith.

Wolff: I mean ideally you would want to see all of the above.

Me: What incentives outside of monetary risks are there for companies to have secure data protections?

Wolff: Well I mean you could be worried about regulator action or angry customers.

Appendix B

Jillian Burner Interview

October, 2024

Zoom

Me: What Is Cisa?

Burner: We were founded in 2018, a fairly new agency. We are a part of the department of homeland security. Our mission & vision is to defend today, secure tomorrow, and we do that through helping mitigate, understand, and build resilience across critical infrastructure across the US.

Me: What is the primary goal of CISA?

Burner: To help critical infrastructure defend themselves against cybersecurity and physical security attacks.

Me: Does CISA act as an SOC for the government?

Burner: "...when we're talking about critical infrastructure, we're talking private & public infrastructure. 80% of critical infrastructure is privately owned & operated, so we have to build relationships, share information, and get out there and really meet with private entities to get on the same page and understand the risks they're facing in terms of cyber threats and physical security threats, and there are 16 sectors of critical infrastructure, and that includes government agencies, education, finance, transportation, energy, waste water / waste treatment, healthcare facilities. There are 16 of those, both private & public.

Me: Have you seen companies reach out to CISA?

Burner: Yes, yeah. We're in a lot of their incident response plans, like we are documented as a third party for them to call. When they are dealing with an incident, and we really have a lot of outreach we do on a regular basis to make sure that organizations are aware of the services that we offer. We can come on site and conduct assessment. We really like to partner with

organizations left of boom, which is prior to an incident, so they understand the resources we have, and a relationship built, and can help fill in where they need us in terms of incident response coordination, if that were ever to happen; which is, we are telling organizations to plan for it to happen. We try to engage prior, and help them become more resilient, to fend off and reduce the impact of any cyber incidents that they may have or physical incidents, and then we also offer capabilities during incident response and then we can also help after actioning and kind of get them back to an operational state.

Me: So it's mainly preventative and not reactionary?

Burner: Yes, we try to be preventative and make sure organizations are taking advantage of the resources that we offer, and offer guidance to help them continue to mature their program. Cybersecurity is definitely a journey, it's not a one and done, you continually have to keep maturing the program especially as the threat actors and cyber criminals change their tactics, it's a continual care and feeding type situation.

Me: What have you seen that has been the most common weakness for organizations in terms of cybersecurity?

Burner: I will say, probably one of the things that we are seeing threat actors exploit the most, or the most frequently in the incidents that we are aware of and get called in to assist with, usually start out because of compromised credentials. So, it is password hygiene that we speak quite a bit about, and securing those accounts, which comes down to password hygiene, and not reusing passwords, so when users reuse their passwords for personal life & work life, it just takes one of those to get compromised for all of them to get compromised. We encourage folks to use a

password manager; we encourage organizations to offer that to the employees, and we also encourage Multi-Factor Authentication to be enabled wherever possible for every single account. Multi-Factor is not a bulletproof solution, but it is an extra step that can slow the bad actor down or if they are opportunistic, and looking for a low hanging fruit, they will move on to another account they can compromise more easily.

Me: What's the biggest concern for organizations when it comes to a security incident? The loss of data, financial loss, PR?

Burner: That depends on the organization, but usually for the organization it is the operational impact. If there's an operational impact, organizations can't make money. Depending on the industry, if it's a manufacturing industry, every day that they can't manufacture whatever they're trying to manufacture and sell, they lose money. In the healthcare industry, every day you can't properly treat patients or you can't access medical records, there's an impact to that. It just depends on the industry, and threat actors use a double extortion method; they try to hit and cause an impact regardless of the organization. We're seeing ransomware [as] the most prolific type of attack that we see because it is so cripping regardless of the organization that you are in. They want to ransomware the information so you can;t access it, you can operate. The chances of them getting the money have increased and then they exfiltrate the data to extort the victims again, whether it be employee data, customer data, sensitive data, personally identifiable data, healthcare data, they want to do that reputational data, and they want to extort the organizations a second time saying 'if you pay me x amount of money we won't post the data online'. The first one is the ransom to pay them to get your data back, and the second extortion is for them not to post the data online.

Me: How big of an increase have you seen in terms of ransomware.

Burner: I think we have seen a jump in ransomware in this double extortion tactic year over year. We have unfortunately seen an increase in not only the ransomware ransomware activity, but also the money that cybercriminals are able to make. Every year the FBI, the internet complaint crime center (IC3), do stats on what's been reported to them and I believe the impact due to cybercrime was like 12.5 billion dollars last year. They have stats from 2019 to 2023, and you can see the significant increase in the profit of that cyber crime. Unfortunately, covid there were a lot of scams and compromises, imposters, and fishing emails that caused compromised credentials, that then caused exfiltration and data breaches in the organizations.

Me: Is the average person really concerned about their data being breached since most of their data is online?

Burner: I think folks have an expectation that their data is probably out there, that being said there are still things that you can do to protect your identity. You don't want loans taken out in your name, you don't want accounts opened up in your name, and we do recommend credit freezing, and there's actually I think been a slight uptick in kids. So [kids] under 18 and their information is being stolen and they don't realize it until they turn 18 and they go to buy a car, they go to apply for a loan, because their social and their credit aren't being monitored because you don't expect anything to be there, and elderly fraud that increases year after year. There's still damage that could be done and there's still things you need to do to protect yourself.

Me: Are there any recognized standards enforcing the protection of data?

Burner: In healthcare there is HIPAA, if you're a publicly traded company the SEC has some requirements in terms of expectations on how to handle data. Ohio actually has some laws, ORC 1347, in terms of notifications and what should be made public if data is breaches. In terms of following standards to prevent breaches, NIST has a framework that's pretty widely adopted by government, public, and private sectors. There's [other] standards; people can become SOC Certified, ISO certified. I think those have historically been adequate if you're dealing with an organization and they say, well we meet this standard, but I think a lot of organizations are asking for more, in terms of what they see in contracts and how they manage third parties, just because you have a secure SOC and hold the data with physical securities wrapped around it, the threat actors and cyber criminals are finding other ways to get into the network, so there are standards but I personally think there can be work done to prove you've met certain requirements. It doesn't talk about multi-factor authentication and some other things.

Appendix C

Demystifying AI in the SOC Webinar

October 14, 2024

Zoom

My Question: Are standards often shaped based off of existing regulations, or are regulations often adoptions of standards into law? What I mean is, to my knowledge, NIST compliance isn't a requirement for organizations throughout the United States; however, it contains several sections related to regulations passed in the country.

Response: NIST only formally established legal requirements for US federal entities. That's their mandate. Other groups, like state governments, etc, can choose to adopt their standards, but that's a choice. But some states have decided to use NIST. Other states use CIS, and other standards. Very few standards are actually required by law, especially outside of government agencies.