American Academic Scientific Research Journal for Engineering, Technology, and Sciences
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
http://asrjetsjournal.org/

Fighting Cybercrime with Zero Trust

Kiran Sharma Panchangam Nivarthi[a]*, Ganesh Gatla[b]

[a]*31108 Algonquin Trail, Chisago City, MN, 55013, USA*
[b]*480 Meadowhill Drive, Alpharetta, GA, 30004, USA*
[a]*Email: Kiransnandu@gmail.com*, [b]*Email: Ganeshgatla73@gmail.com*

Abstract

Zero Trust Architecture focuses on securing critical data and access paths by eliminating trust as much as possible by "assuming breach." It establishes trust every time a user tries to access an asset in the system by questioning the premise that users, devices, and network components should be implicitly trusted based on their location within the network. We have chosen Zero Trust to help reduce the impact of cybercrime and establish baseline security practices. It is a dramatic paradigm shift in the philosophy of securing our infrastructure, networks, and data, from verifying once at the perimeter to continually verifying each user, device, application, and transaction. Trust in humans is essential to forming connections; however, trust in network connections can create dangers and potential security gaps in the digital world. In a hyper-connected world, anyone can launch an attack virtually and participate in cybercrime by violating the trust of systems or networks. The cost of not implementing good security practices is evident in the growing number of data breaches and ransomware attacks that erode consumers' trust in tech and online space. Considering Zero Trust and Zero Trust Architecture developed by the National Institute of Standards and Technology (NIST) should help reduce the impact of cybercrime and protect the crown jewels in cyberspace from a malicious insider or an external attacker.

Keywords: Cybercrime; Zero Trust; Zero Trust Architecture; Cybersecurity; Network Security.

1. Introduction

Cybercrime, as the name indicates, involves computers, a computer network, or a networked device. Phishing, malware attacks, data breaches, and ransomware attacks are just a few examples of current cyber threats, while new types of cybercrime are constantly emerging [1]. Over the last decade, technological advances have connected the world more digitally than ever. Criminals use digital transformation to target weaknesses in online systems, infrastructure, and networks. Due to this, there is a significant impact on the economic and social aspects of individuals and businesses worldwide. Since cyberspace has no borders, threats and attacks can come from any location at any time. Criminals, victims, and technical infrastructure span multiple jurisdictions bringing many challenges to protect, investigate, and prosecute these crimes.

---

* Corresponding author.

Research published by Israeli cyber-intelligence firm KELA in Q3-2022, hackers sell access to 576 corporate networks worldwide for a cumulative price of $ 4 million, fueling attacks on the enterprises [2]. Based on the reports from the U.S. Treasury Department released recently, the U.S. financial institutions observed nearly $1.2 billion in costs associated with ransomware attacks in 2021, which is a 200% increase over the previous year [3].

The exponential growth in infrastructure and complexity as we operate several internal, remote, and other local networks and cloud services. This paper explores the definitions of Zero Trust, the History of Zero Trust, and the challenges in implementing Zero Trust architecture. This paper will traverse whether the implementation of Zero Trust must consider incentivizing or taking a penalty-based approach and the challenges in auditing the performance of Zero Trust by the regulators. This paper will also analyze the efforts required to achieve Zero Trust by incentivizing and understanding how it can be adopted at the federal and state levels while measuring the effectiveness of such implementation. Finally, it will consider the options on enforcement and private right of action before concluding with the necessity to implement Zero Trust to improve cybersecurity posture.

2. What is Zero Trust?

Zero Trust security operates under the "assumed breach." It establishes trust every time a user tries to access an asset in the system by questioning the premise that users, devices, and network components should be implicitly trusted based on their location within the network. It applies a "least privilege" principle, giving the user the least access possible, and requiring additional validation before stepping up access privileges [4].

Trust in humans is a basic necessity and essential to forming connections; however, trust in network connections can create dangers and potential security gaps in the digital world. *John Kindervag,* a Forrester alum, coined the term Digital trust [5] in 2009; that centers on the belief that trust is a vulnerability, and security must be designed with the strategy, "Never trust, always verify," which goes hand-in-hand with the concept of "Trust but verify."

3. History of Zero Trust

Although the term *"Zero Trust"* is relatively new, the concept has been present in cybersecurity for longer than it has been named [6]. The perimeter-based approach has always been the default security posture before the enterprise cloud adoption started to enhance or expand the perimeter for cybersecurity experts to rethink their defensive stance. As in the sports analogy, "the best defense is a good offense."

In 2018, NIST released 800-207 Zero Trust Architecture, offering guidelines on Zero Trust's core components. Which established the logical components [7] of Zero Trust as listed below:

- **Policy Engine (PE)** – The PE provides the final decision in granting access to a resource
- **Policy Administrator (PA)** – The PA establishes access to a resource
- **Policy Enforcement Point (PEP)** – PEPs serve as a system gateway for activating, monitoring, and terminating connections between authorized users and their access resources.

On May 12, 2021. President Joe Biden issued an Executive order on *Improving the Nation's Cybersecurity*, [8] in which he specifically stated, "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments to defend the vital institutions that underpin the American way of life." He also stated, "The Federal Government must adopt security best practices; advance towards Zero Trust Architecture; Develop a plan to implement Zero Trust architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST)."

On September 7, 2021, upon release of the executive order, the Office of Management and Budget (OMB) released a draft of a national strategy for moving the U.S. Government towards a Zero Trust architecture. The Cybersecurity and Infrastructure Security Agency (CISA) also released its Cloud Security Technical Reference Architecture and Zero Trust Maturity Model to guide and assist agencies in their implementation planning [9].

4. Implementation of Zero Trust

Government agencies are ahead of corporations in adopting and implementing Zero Trust security architecture, with 72% of government organizations already utilizing a Zero Trust framework compared to 56% of companies, according to a report released by Okta [10].

4.1 Challenges of implementing Zero Trust

When implementing Zero Trust at the federal government level or on enterprise networks, several challenges may arise that reduce the solution's effectiveness. To list a few:

- Legacy systems rely on "implicit trust;" this concept conflicts with the core principle of adaptive evaluation of trust within a Zero Trust Architecture (ZTA) [11].
- Lack of support throughout the enterprise, possibly from leadership, administrators, or users, as the mindset required for Zero Trust must be embraced fully for any solution to be successful [12]. The pervasive need for Zero Trust concepts to be applied throughout the environment, scalability, performance, and monitoring requires resources because multiple perimeters require continuous authentication and authorization before accessing data or applications.
- Absolute Zero Trust is not achievable due to complex administrative duties; administrators and defenders may become fatigued with constantly applying default-deny security policies and always assuming a breach is occurring. If the Zero Trust approach falters, its cybersecurity benefits will significantly degrade or eliminate [13].
- Organizations, government agencies, and departments often implement cloud IaaS, PaaS, and SaaS, from numerous cloud providers. Zero Trust approaches center around security policy, and the consistent application of that policy in a multi-cloud environment is a non-trivial undertaking [14].

5. Achieving Zero Trust

"Our adversaries are constantly adapting, and so must we. Zero Trust principles are the core of how our federal

agencies must evolve to meet today's cybersecurity demands. Our draft national Zero Trust strategy will push agencies in the right direction and help make a more coherent federal cybersecurity posture." Said Chris Inglis, National Cyber Director [15].

5.1 Investing toward Zero Trust and growth in the market

Demand for products that support Zero Trust is on the rise. Research firm Markets and Markets projects that the global Zero Trust security market will grow from $19.6 billion in 2020 to $51.6 billion by 2026. The market's significant factors include the growing frequency of target-based cyber-attacks and increasing data protection and information security regulations. In January 2022, the U.S. Defense Information Systems Agency (DISA) awarded a $6.8 million contract to Booz Allen Hamilton to execute Thunderdome Prototype, a Zero Trust security platform that it said aligns with a May 2021 executive order from the White House aimed at improving the nation's cyber security [16].

The U.S. Department of Agriculture (USDA) recently received $4.4 million from the Technology Modernization Fund (TMF) [17] to invest in a Zero Trust cybersecurity architecture, given the agency's role as a shared service provider and a significant source of public-facing government services.

The U.S Government must raise awareness through the broad spectrum of policy tools available, from public training and awareness campaigns through the marketplace to federal funding incentives to targeted regulatory action by using the "carrot and stick" approach. Effective, lasting digital transformation can only be achieved through a sustained government commitment by promoting strategic coherence, sustained financial investment, and effective management and oversight.

5.2 Adoption by Government agencies

The federal CIO council began to look at Zero Trust almost five to six years before the EO 14028, trying to figure out what it meant for them and decide on how to adopt it. However, the COVID-19 pandemic and the increase in telework accelerated the timelines [18]. One reason the government has been ahead of industry counterparts is federal mandates regarding Zero Trust. Agencies have until the end of September 2024 to meet five Zero Trust goals: identity, devices, networks, applications, and data. As the Executive order on Zero Trust defines, incremental improvements to security do not give us the protection we need. Federal government and organizations must make bold changes and significant investments to defend the vital institutions that serve Americans in the form of utilities, emergency services, or day-to-day operations.

While the executive order does not provide funding on its own, according to the report, 87% of government agencies have seen an increase in their budget to support these Zero Trust initiatives. Specifically, 16% reported a significant increase, and 71% reported a moderate budget increase. Agencies can also apply to the TMF for funding to enact Zero Trust initiatives [19]. The TMF is a promising funding source for agencies' implementations of Zero Trust. TMF is an innovative funding vehicle, authorized by Section 4(a) of the Modernizing Government Technology Act of 2017, that gives agencies additional ways to quickly deliver services to the American public and better secure sensitive systems and data [20].

5.3 Adoption by States

September 2024 may be an unrealistic goal to expect the federal government and all the agencies to implement Zero Trust; the state and local governments are pursuing the cloud more aggressively, using their StateRAMP certification process to find secure and vetted third-party products. State governments, in particular, sit in a real sweet spot right now: boasting higher budgets and talent pools than local governments, with none of the bureaucratic mess of the feds. With a more efficient size and scope of government to work with, we could conceivably see many states successfully execute their transition to Zero Trust by 2024 – carrying out the spirit of the White House's mission and helping to drastically narrow government security gaps for attackers to exploit [21].

6. Analysis

Cybercrime will cost companies an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015, at a growth rate of 15 percent yearly [22]. This past year, there were 847,376 complaints, up from 791,790 in 20220; numbers correlate to a 7% increase. The amount lost from the complaints, which largely stems from scams like extortion, identity theft, and data breaches, went up from $4.2 billion to $6.9 billion last year (2021) [23].

6.1 Measuring the effectiveness of Zero Trust

The passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2021 amended the Homeland Security Act of 2002 to establish stringent timelines for reporting a cybersecurity incident within 72 hours of discovery and within 24 hours of making a ransom payment. Although the bill recommends establishing a Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency (CISA), the challenges of resources, training, and awareness at both federal and state levels still exist and would continue to prove a daunting task for CISA to implement the Zero Trust methodology. In general, Security strategies and implementation are iterative. They may require multi-year planning for implementation to achieve the desired state because they are time-consuming or impactful due to the technical debt.

However, no single research could directly correlate the reduction in breach costs by implementing or adopting Zero Trust. There have been multiple [24] independent and industry-specific research that help us understand the underlying cost benefits if Zero Trust is implemented.

One such independent research conducted by the Ponemon Institute, sponsored by IBM, has studied breaches across 537 organizations, 17 countries, and 17 different industries on adopting Zero Trust and its impact in reducing the cost of breaches. Costs for those with Zero Trust depend on the level of maturity for two consecutive years (2021 and 2022).

The average breach cost was $5.04 million in 2021 for those with no Zero Trust approach. The average breach cost was $3.28 million in the mature deployment stage. This cost difference of $1.76 million between mature Zero Trust organizations and organizations without Zero Trust is 42.3%. The difference between early-stage Zero Trust (average cost of a breach $4.38 million) and mature stage ($3.28 million) was $1.10 million, for a

cost difference of 28.7% [25].

A similar survey in 2022 revealed that in early adoption state organizations that were beginning to implement a few practices, the average cost of a data breach was $4.96 million, and the cost was $1.51 million more than breaches at mature organizations (average cost of a breach $3.45 million), a difference of 35.9%. Comparatively, between 2021 and 2022, The average cost of a data breach was $4.15 million at organizations with Zero Trust deployed, while the cost of a breach was an average of $5.10 million at organizations without Zero Trust deployed. The difference was USD 0.95 million, representing a 20.5% savings for organizations with Zero Trust deployed [26].

6.2 Developing a workforce and building awareness

Zero Trust skill development and awareness must be developed via dedicated school curricula aimed at inter/multi-disciplinary covering technical and non-technical aspects; the government must also consider providing scholarships and grants for relevant programs. This should help develop dedicated career paths and an effective pipeline of future employees, particularly for the public sector, by providing executive and operational training, including certifications that can be created in partnership with academia, the private sector, and civil society.

The government must foster an environment that stimulates basic and applied research in cybersecurity across sectors and various stakeholder groups. Such initiatives include, for example, ensuring that national research efforts support the objectives of the National Zero Trust Strategy; developing Zero-Trust-focused R&D programs in public research organizations; effective development and dissemination of new findings, baseline technologies, techniques, processes, and tools [27].

7. Enforcement

The most common approach in enforcing new regulations or policies is driven by the fear-based rather than the incentivized system. U.S. laws are a combination of federal, sectoral, and state laws. Let’s explore the tangible options (carrot and stick) to enforce Zero Trust through industry-specific regulations or at a national level by authorizing federal agencies to perform audits and incentivize good hygiene or punish bad behavior.

7.1 Incentivizing good behavior

Post Covid-19 pandemic, the U.S. Government has announced multiple grants and funding opportunities to state and local governments to include cybersecurity, including the 2021 American Rescue Plan [28] and the 2021 Infrastructure Investment and Jobs Act [29]. The government should distribute these grants conditional upon demonstrating good cyber-hygiene by implementing cybersecurity best practices and extending the rules to align with the NIST 800-27: Zero Trust Architecture [30] or CISA’s draft Zero Trust maturity model [31], serving as a baseline.

The federal government is one of the largest acquirers of software technologies. Utilizing the acquisition

contracts and purchase agreements to drive cybersecurity requirements specifically articulated to the organizations aligned with Zero Trust standards to enhance the supply chain security to avoid attacks like Solar winds or colonial pipeline attacks.

7.2 Industry-Specific enforcement

The sector-specific adoption of Zero Trust can be considered by penalizing for the violations if the businesses or organizations fail to demonstrate prioritization of cybersecurity through alignment with a commonly accepted Zero Trust NIST framework or CISA ZTA draft as these standards mature.

The financial industry is heavily dependent on the latest trends in information technology; cybersecurity is the most significant and integral part of financial regulatory compliance. Since the rapid evolution of FinTech is influencing the regulatory environment in many economic sectors, industry-specific regulations, such as PCI-DSS, SOX, and GLBA, could be enhanced to include Zero Trust architecture to thwart state-sponsored hackers by adding the requirements of MFA and SSO to all endpoints on sensitive applications that include payment systems. Office of the Comptroller of the Currency (OCC), NY Department of Financial Services (DFS), Consumer Financial Protection Bureau (CFPB), or Federal Trade Commission (FTC) could enforce the ZTA requirements to the financial industry.

The healthcare sector can make amendments to Health Information Technology for Economic and Clinical Health (HITECH) Act [32] to consider any violation against Health Insurance Portability, and Accountability Act (HIPAA) should be fined if the entity fails to demonstrate the implementation of NIST ZTA or CISA's ZTA practice. The U.S. Department of Health and Human Services and the Office for Civil rights (OCR) could be the enforcers regarding the healthcare sector enforcement of ZTA.

7.3 Federal Trade Commission regulatory enforcement

The Federal Trade Commission enforces federal consumer protection laws that prevent fraud, deception, and unfair business practices. The Commission also enforces federal antitrust laws prohibiting anticompetitive mergers and other business practices that could lead to higher prices, fewer choices, or less innovation [33]. FTC is well suited and has longstanding experience and expertise to administer the enforcement of ZTA. FTC's authority can take action based on the breach occurrence and failure to prove the ZTA implementation. The biggest challenges FTC might face are resources constraint and "how to audit the ZTA implementation?"

7.4 Auditing Zero Trust Architecture

Applied policies can create borders, boundaries, and network segmentation because each asset is fingerprinted before it is allowed to communicate in a Zero Trust environment, as it is based on its cryptographic identity to differentiate between good or malicious traffic. The Zero Trust Maturity Model audit checklist [34] developed by CISA can be utilized by regulators to audit the implementation of Zero Trust capabilities in organizations through the five pillars of Zero Trust development: identity, device, network/environment, application workload, and data. For example, Access controls policies, risk assessment reports, network perimeter is

periodically assessed, or access to information resources is granted via SSO or MFA.

7.5 Private Right of Action

Limiting the recovery to "actual damages," requiring a heightened "knowing or reckless" liability standard for most statutory provisions and including a "willful and repeated" offense standard to sue for more administrative violations [35]. Considering all the following recommended elements [36] to be added to the private right of action:

- heightening liability standards,
- limiting what provisions are enforceable through private lawsuits,
- providing for notice and an opportunity to cure before bringing suit,
- raising standards for pleading cases,
- placing limits on damages,
- shifting costs and fees, and
- setting limits on class actions.

8. Conclusion

Zero Trust must be considered as a journey rather than a destination. Governmental agencies and businesses must accentuate the need to regulate and implement Zero Trust security practices and to either incentivize good practices or impose penalties or sanctions for violating regulations. Small and medium businesses lack the financial resources and skillset to combat cybersecurity and ransomware attacks. A Better Business Bureau survey found that for small businesses — which make up more than 97% of total companies in North America — the primary challenge for more than 55% of them to develop a cybersecurity plan is a lack of resources or knowledge [37].

The Zero Trust approach in this paper provides the capability and capacity building while raising awareness at the national level to ensure resources are streamlined, efforts are measured, and accountability is established. Generally, Return on Investment (ROI) [38] is crucial for Zero Trust implementation. The return is the avoidance or minimization of consequences of destructive incidents in terms of time, money, services, privacy, intellectual property, or an individual's safety.

Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. Ultimately, the trust we place in our digital infrastructure should be proportional to how reliable and transparent that infrastructure is and the consequences we will incur if that trust is misplaced [39].

References

[1] ˈERPOL, "Cybercrimes cross borders and evolve rapidly," 01 June 2022. [Online]. Available: https://www.interpol.int/en/Crimes/Cybercrime. [Accessed 23 November 2022].

[2] Toulas, "Hackers selling access to 576 corporate networks for $4 million," BleepingComputer.com logo, 31 October 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/hackers-selling-access-to-576-corporate-networks-for-4-million/. [Accessed 24 November 2022].

[3] Vicens, "Ransomware costs top $1 billion as White House inks new threat-sharing initiative," CyberScoop, 01 November 2022. [Online]. Available: https://www.cyberscoop.com/ransomware-payments-cost-treasury/. [Accessed 25 November 2022].

[4] rcedes Cardona, "The Trend Toward A Zero Trust Model for Security," Mimecast, 19 July 2022. [Online]. Available: https://www.mimecast.com/blog/the-trend-toward-a-zero-trust-model-for-security/. [Accessed 16 November 2022].

[5] Cunningham, "A Look Back At Zero Trust: Never Trust, Always Verify," Forrester, 24 August 202. [Online]. Available: https://www.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/. [Accessed 18 November 2022].

[6] ional Institute of Standards and Technology, "Zero Trust Architecture," *SP800-27,* pp. 2-3, August 2020.

[7] . General Services Administration, "Zero Trust Architecture (ZTA)," *Buyer's Guide,* pp. 2-3, June 2021.

[8] ted States Executive Office of the President Joseph R. Biden, "Exec. Order No. 14028, Improving the Nation's Cybersecurity," *86 Fed. Reg. 26633 (2021),* pp. 26633-26647, 12 May 2021.

[9] ce of Management and Budget, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," *M-22-09,* pp. 2-3, 26 January 2022.

[10] TA, "The State of Zero Trust Security 2022," September 2022. [Online]. Available: https://www.okta.com/sites/default/files/2022-09/OKta_WhitePaper_ZeroTrust_H2_Campaign_.pdf. [Accessed November 2022].

[11] ersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," pp. 3-4, June 2021.

[12] ional Security Agency, "Embracing a Zero Trust Security Model," *Guidance on Zero Trust Security Model,* pp. 6-7, 25 February 2021.

[13] ional Security Agency, "Embracing a Zero Trust Security Model," *Guidance on Zero Trust Security Model,* pp. 5-6, 25 February 2021.

[14] palto, "Zero Trust Guidance for the US Federal Government," *The Zero Trust Journey for Federal Agencies: The Next Phase,* pp. 2-3, 09 April 2020.

[15] ce of Management and Budget, "Draft Federal Strategy For Moving the U.S. Government Towards a Zero Trust Architecture," 07 September 2021. [Online]. Available: https://www.whitehouse.gov/omb/briefing-room/2021/09/07/office-of-management-and-budget-releases-draft-federal-strategy-for-moving-the-u-s-government-towards-a-zero-trust-architecture/. [Accessed November 2022].

[16] Violino, "Why companies are moving to a ‘zero trust’ model of cyber security," CNBC, 01 March 2022. [Online]. Available: https://www.cnbc.com/2022/03/01/why-companies-are-moving-to-a-zero-trust-model-of-cyber-security-.html. [Accessed November 2022].

[17] . General Services Administration, "Technology Modernization Fund Announces Investments to

Modernize Major Systems at USDA and NARA," 23 May 2022. [Online]. Available: https://www.gsa.gov/about-us/newsroom/news-releases/technology-modernization-fund-announces-investments-to-modernize-major-systems-at-usda-and-nara-05232022. [Accessed November 2022].

[18] Errick, "Government Implementing Zero Trust Architecture Faster than Corporations," Nextgov, Washington D.C., 2022.

[19] TA, "The State of Zero Trust Security 2022," September 2022. [Online]. Available: https://www.okta.com/sites/default/files/2022-09/OKta_WhitePaper_ZeroTrust_H2_Campaign_.pdf. [Accessed November 2022].

[20] President's National SecurityTelecommunications Advisory Committee, "Zero Trust and Trusted Identity Management," NSTAC, Washington D.C., 2022.

[21] Schiappa, "The Federal Government's Path to Zero-Trust Security," Sophos, 08 November 2021. [Online]. Available: https://www.govtech.com/sponsored/the-federal-governments-path-to-zero-trust-security. [Accessed November 2022].

[22] Mclean, "2022 Must-Know Cyber Attack Statistics and Trends," Embroker, 11 November 2022. [Online]. Available: https://www.embroker.com/blog/cyber-attack-statistics/. [Accessed November 2022].

[23] Brook, "Cybercrime Cost U.S. $6.9 Billion in 2021," Digital Gaurdian, 02 September 2022. [Online]. Available: https://digitalguardian.com/blog/cybercrime-cost-us-69-billion-2021. [Accessed November 2022].

[24] Tero, "Defining Metrics to Successfully Manage Your Zero Trust Implementation Plan," Illumio, 11 August 2020. [Online]. Available: https://www.illumio.com/blog/zero-trust-metrics. [Accessed November 2022].

[25] M, "Cost of a data breach 2021," IBM, New York, 2021.

[26] M, "Cost of a data breach 2022: A million-dollar race to detect and respond," IBM, New York, 2022.

[27] rnational Telecommunication Union, "Guide to Developing a National Cybersecurity Strategy," in *Strategic Engagement in Cybersecurity*, Geneva, 2021.

[28] U.S.C 9001, "American Rescue Plan Act of 2021," *PUBLIC LAW 117–2*, pp. 4-245, 11 March 2021.

[29] U.S.C 101, "Infrastructure Investment and Jobs Act," *PUBLIC LAW 117–58*, pp. 429-1039, 15 November 2021.

[30] ional Institute of Standards and Technology, "Zero Trust Architecture," *SP 800-27*, pp. 2-3, August 2020.

[31] ersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," pp. 1-4, June 2021.

[32] . Department of Health & Human Services, "HITECH Act Enforcement Interim Final Rule," 17 February 2009. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html. [Accessed November 2022].

[33] eral Trade Commission, "Enforcement," [Online]. Available: https://www.ftc.gov/enforcement. [Accessed November 2022].

[34] A, "Zero Trust Maturity Model audit checklist," [Online]. Available: https://cdn.ttgtmedia.com/rms/pdf/cisa_zero_trust_maturity_model_audit_checklist_download.pdf.

[Accessed November 2022].

[35] okings, "Bridging the gaps: A path forward to federal privacy legislation," Brookings, Washington D.C, 2020.

[36] ernance Studies, "Bridging the gaps: A path forward to federal privacy legislation," Brookings, 2020.

[37] Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime Magazine, California, 2020.

[38] anization of American States (OAS), "National Cybersecurity Strategies: Lessons learned and Reflections from the Americas and Other Regions," Global Partners Digital, 2022.

[39] ted States Executive Office of the President Joseph R. Biden, "Executive Order No. 14028, Improving the Nation's Cybersecurity," *86 Fed. Reg. 26633 (2021)*, pp. 26633-26647, 12 May 2021.