INSTITUTE FOR HOMELAND SECURITY

Toward a More Effective Policy Model for Data Breach Reporting in the Texas Healthcare System

Institute for Homeland Security

Sam Houston State University

Alexander Kinney

ABSTRACT

Hospital data breaches have been escalating in recent years commanding the attention of policymakers. In addition to putting healthcare facilities in financial and legal jeopardy, data breaches undermine the healthcare system by threatening public trust. In 2023, Texas legislators amended the Business and Commerce Code to adjust data breach reporting practices in response to this growing threat. This amendment introduces new reporting requirements that impact healthcare facilities in several ways. The aim of this technical paper is to provide policymakers and healthcare administrators an introduction to the issue of data breaches and suggest additional improvements to this law. In what follows, I will provide a brief overview of the background and significance of data breaches in the healthcare system, define the types of data breaches that most commonly impact the healthcare system and review existing regulatory policies governing data breach responses. I will then provide an overview of Senate Bill 768 and suggest several ways that future legislation can strengthen reporting and response requirements in the future.

INTRODUCTION

Background and Significance of Data Breaches in Healthcare

The digital transformation of the healthcare industry has paved the way for a remarkable shift in service provision and quality of care (Set et al., 2020). Where once this this industry operated through purely paper-based systems, nearly all healthcare facilities now rely on electronic health record systems. In addition to improving access to treatment, electronic health record systems and their associated cloud services have simplified the patient experience, reduced costs, and increased efficiency across the healthcare system. Unfortunately, this digital turn has also caused healthcare organizations to become a prominent target for malicious actors. The digitization of data, decentralization of storage, and mobile accessibility of vital information can lead to unexpected privacy breaches. Additionally, software vulnerabilities and simple human error can compound issues of data security. Collectively, these issues complicate patient services and reduce trust in the contemporary healthcare system.

As compared to other sectors, healthcare organizations experience more frequent and costly attacks to their data infrastructure (Liu, Musen, & Chu, 2015). Over the past two decades, over 250 million people have been affected by a healthcare system-related data breach (Set et al., 2020). In 2023 alone there were just over 500 data breaches in healthcare organizations (see PrivacyRights, 2024). According to an IBM report, the average cost of a data breach was $4.45 million in 2023–a number that has increased 15% across the previous three years (IBM, 2024). This figure also does not consider the elevated costs for healthcare organizations due to unique compliance challenges, remediation expenses, insurance premium hikes, and liability suits. As Murray-Watson (2023) notes, the average cost of data breaches for healthcare organizations have escalated to an all-time high of $10.1 million.

Beyond these fiscal considerations, data breaches reduce public trust in the healthcare system (Moffit & Steffen, 2017). Major insurance providers and hospitals suffer reputational harm from these events that can lead patients to consider switching their providers (Ke, Wang, & Foutz,

2022). These harms are only escalated when the public perceives that a healthcare organization could have responded to a data breach better or even prevented it completely (Perera et al., 2022). Diminished trust in our nations' healthcare organizations also has downstream effects on the quality of patient care by elevating worker stress and/or redirecting resources to mitigation efforts that could have otherwise been targeted at improving the patient experience.

In recent years, policymakers have made strides in responding to data breaches by rolling out a suite of new legislation and regulatory tools aimed at improving confidentiality, security, and system-wide resilience. By developing more robust regulatory frameworks for addressing data breaches, policymakers hope to achieve a dual of reducing organizational risks while also incentivizing them to invest in improved security countermeasures (Hovav & Gray, 2014). However, these laws have varied in their effectiveness (Schuessler et al., 2017). In the healthcare sector specifically, efforts to strengthen laws concerning data breach transparency and reporting accountability have long been championed by state governments with the federal government following their lead. While most states now have laws on the books in the effort to reduce privacy risks, there are also regulatory disparities across the country. As such, opportunities remain to improve regulations concerning data breach incident responses and preparedness.

Problem

Practitioners note that the COVID-19 pandemic escalated the propensity for healthcare organizations to be targeted by cyberattacks (Muthuppalaniappan & Stevenson, 2021). Not only has there been an escalation in healthcare data collected in the wake of this global catastrophe, insufficient resourcing and staffing capacity during this period attracted an unprecedented number of cyberattacks exposing the deficiencies in healthcare system data integrity protocols. While a substantial number of states now have legislation focused on responding to data breaches, legal observers have noted that current regulatory frameworks are inconsistent due to their state-level focus and are less comprehensive on prevention protocols (Agelidis, 2016). As health care facilities are disproportionately impacted by data breaches, strengthening policies even at the state level can have a palpable impact the financial and reputational integrity of this sector.

Research Objective

This past legislative session, Texas lawmakers passed Senate Bill 768 which shortened the window of time that healthcare facilities had to report a data breach from 60 days to 30 days. This bill represented an additional step forward in a longstanding effort to move beyond HIPAA and develop a more stringent data breach notification framework in the state. In what follows, this paper will contextualize the nature of data breaches as a social problem by examining system and human factors that can lead to information exposure. It will then cover existing policy responses at the federal and state level with a focus on their effectiveness. Then, this paper will describe the lineage of Texas policies addressing data breach reporting in the healthcare system and describe opportunities that exist for S.B. 768 to be strengthened in future legislative work to address the healthcare system vulnerabilities. Specifically, this paper will advocate for a holistic policy approach (see Solove & Hartzog, 2022) that incorporates additional measures aimed at

risk mitigation and prevention to support the solid foundation for data breach response outlined in S.B. 768.

CONTEXTUALIZING DATA BREACHES IN THE HEALTHCARE SYSTEM AS A SOCIAL PROBLEM

Definition, Causes, and Types of Data Breaches

Defined, a data breach is a "security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so" (Kahn et al., 2019, p. 2). There are a multitude of contextual factors that associated with data breach incident. These include: 1. Whether there was intent behind the data breach, and 2. What vulnerability was exploited. When an incident is the result of a malicious act where there is a specific intent to cause harm to an organization this is considered an *intentional* data breach. When an incident is the result of an accidental action or process and is without malicious intent, this is considered an *unintentional* data breach. Likewise, there are different loci of vulnerability where data can be breached. These include both physical points of access and digital points of access. Each factor requires unique approaches to prevention and mitigation efforts.

Intentional Data Breaches

There are several forms of intentional data breaches. Hacking, or the unauthorized entry to a data system by an individual or a group of individuals, is the most common form of an intentional data breach in the United States (Holtfreter & Harrington, 2015). These can be conducted by organizational "insiders" who have preexisting knowledge of data system infrastructure, state-sponsored actors that are external to the organization, or terrorists (Kahn et al., 2019). Preventing intentional data breaches tend to be the most high-profile incidents as they typically have the largest financial impact and can be international in scope (Cheng, Liu, and Yao, 2017). Though more constrained in their consequences, the theft of a hard drive or physical computer can also precipitate a data breach (Ogie, 2016). Additionally, as these incidents can be the result of both external and insider threats, they can require more complex prevention protocols and command more resources.

Unintentional Data Breaches

Unintentional data breaches are slightly less common, but still prevalent (Bennett, Bennett, and Griffiths, 2010). When people do not follow best practices for cybersecurity including using strong passwords or locking down monitors when away from their desk data leakages can occur. Likewise, hard drive sharing can lead to similar outcomes. Improperly vetted or unlicensed software can also inadvertently contain programming faults that increase exposure to databases that can unintentionally prompt a data breach. Collectively, these incidents may receive less public attention but are highly consequential. They are also preventable through appropriate trainings and corporate data management protocols.

The Direct Costs of a Data Breach in the Healthcare System

Data breaches can have a staggering on the financial wellbeing of individuals, organizations, and national economies (Sharma, Oriaku, & Oriaku, 2020). Upon disclosing a data breach, organizational values are likely to go down (Tripathi & Mukhopadhyay, 2020), and shareholder values take a major hit (Gatzlaff & McCullough, 2010). Additionally, not all data breach events elicit the same magnitude of financial impact. When a data breach involves the loss of confidential data, as the vast majority of healthcare information is classified, the aforementioned financial impacts of a data breach are amplified (Campbell et al., 2003). As such, there are several *direct costs* associated with these events that healthcare facilities must navigate (Choong et al., 2016). These include detection and escalation costs, notification costs, and post-breach service costs (Fowler, 2016).

Detection and Escalation Costs

Detection and escalation costs refer to the amount of money that it takes for a healthcare facility to investigate a data breach and engage with crisis management teams to begin remediation efforts (Algarni & Malaiya, 2016). This involves financial commitments to hire a third-party forensic team to detect the scope of the breach and identify the data that was lost. It also encompasses the costs of hiring legal representation and formulate a communication strategy in conjunction with corporate leadership to notify public stakeholders (Fowler, 2016). Detection and escalation costs are the initial direct financial costs associated with a data breach.

Notification

Notification costs are incurred by organizations as they work to identify who was affected and inform them that they have been the victim of a data breach. Likewise, there are costs associated with engaging with state agencies and lawmakers to disclose an incident (Fowler, 2016). These costs can vary depending on where a breach occurs, and the methods employed to notify victims. Notification costs are incurred when a healthcare facility sets up website advertisements and employs individuals to coordinate email, phone, and postal mail efforts to let individuals know that their information was compromised.

Post-Breach Services

The costs that are associated with legal and consulting fees, paying fines to regulators and distributing awards in lawsuits, mitigating identity theft and fraud for victims through monitoring services are considered post-breach costs (Fowler, 2016). Additionally, health care organizations may need to institute targeted service cost reductions as a preventative effort to incentivize patients to stay loyal. Often, facilities will have to revise their cybersecurity programs which can be particularly costly. The magnitude and scope of a data breach influences not only how many post-breach services facilities are expected to finance, but also how much they cost. It is not uncommon for post-breach services to be the most financially demanding direct cost associated with a data breach (Choong et al., 2016; Fowler, 2016).

The Indirect Costs of a Data Breach in the Healthcare System

Beyond the financial costs associated with these events, data breaches have wide ranging social consequences that impact the healthcare system. These are more commonly referred to as the *indirect costs* associated with a data breach (see Choong et al., 2016). Though difficult to quantify, they can impact the long-term survival of a healthcare facility if improperly managed (Fowler, 2016). Indirect costs include business loss, reduced employee productivity, diminished brand value, and victim harms.

Business Loss

Victims of data breaches experience stress, anxiety, and psychological trauma. Even more concerning, the exposure of patient data has been used to physically harm individuals (Wairimu & Fritch, 2022). Research finds that healthcare system data breaches are more likely to experience these negative outcomes because of the personal nature of information loss (Labrecque et al., 2021). Healthcare data is particularly valuable to cybercriminals as it allows them to leverage information that could be embarrassing or stigmatizing if made public. Data illicitly acquired from healthcare facilities can be used by cybercriminals to engage in other crimes such as identity theft, fraud, harassment, stalking, and blackmail (Wairimu & Fritch, 2022). Unsurprisingly, victims of data breaches are more likely to consider moving on to another service provider further exacerbating the strains placed on healthcare facilities as the work through mitigation efforts (Ke et al., 2022).

Reduced Employee Productivity

Data breach mitigation efforts can also cost a healthcare facility in employee time and effort. Employee effort is often reallocated toward breach mitigation tasks that include the providing interviews to forensic teams, developing action and accountability plans, and working to select among external stakeholders to assist in post-breach response. Research also finds that data breaches in healthcare facilities elevate employee stress. (Fauzi et al., 2021). Hospital productivity has been shown to experience declines in the wake of a data breach which acts as a "shock" to patient care delivery (Lee & Choi, 2021, p. 1). This can disrupt critical processes of care and increase patient mortality in the immediate aftermath of these incidents (Choi & Johnson, 2019).

Diminished Brand Value

Data breaches are a public relations nightmare for healthcare facilities that erode public trust (Liu et al., 2018). Efforts to remediate reputational damage is not always a successful endeavor and threaten organizational survival (Talesh, 2018). Temporary shutdowns of healthcare facilities are common during the immediate aftermath of a data breach and in the most extreme cases, they can close their doors permanently (Hope, 2023). Small and midsize healthcare facilities have the most to lose as they often lack the resources to weather a public relations storm. This contributes to the downstream impacts on opportunities for patient care in rural and suburban areas.

CURRENT POLICY APPROACHES TO MITIGATING DATA BREACHES IN THE HEALTHCARE SYSTEM

Federal Laws Concerning Data Breaches

Despite increasing momentum to implement a cohesive cybersecurity legal system at the national level (Kosseff, 2023), there are currently no federal laws that broadly address data breach incidents. Likewise, the vast majority of the legal provisions that are applicable to data breaches focus on post-incident remediation efforts rather than pro-active preventative solutions (Marcus, 2018). However, several existing federal laws have specific provisions that address data breaches in the healthcare system. Some notable provisions include the Breach Notification Rule embedded in the Health Insurance Portability and Accountability Act (HIPAA), The Health Breach Notification Rule in the Health Information Technology for Economic and Clinical Health (HITECH) Act, the FTC Safeguards Rule in the Gramm-Leach-Bliley (GLB) Act.

HIPAA Breach Notification Rule

The HIPAA Act is the flagship federal law governing the security of healthcare data. Enacted in 1996, the purpose of this law is to place stipulations on the transfer of healthcare information in order to restrict the unauthorized collection and dissemination of personally identifiable information. It also provides patients with rights regarding to access and control over their own healthcare information. HIPAA contains several important provisions that are germane to data breaches, but the most direct element is the Breach Notification Rule. According to the U.S. Department of Health and Human Services (2024), the Breach Notification Rule requires healthcare entities and their business associates to notify specific parties that there has been a data breach. This includes not only individuals that were directly affected by the breach, but the media and the Secretary of the Department of Health and Human Services in the event that the breach affected over 500 individuals.

HITECH Health Breach Notification Rule

The HITECH Act was enacted as a part of the broader American Recovery and Reinvestment Act in 2009 to promote the adoption and use of novel health information technologies. The Health Breach Notification Rule embedded in this legislation HIPAA broadened the requirements for notifying affected parties that are affected by a data breach and also expanded the penalties associated with non-compliance. One of the more controversial, but novel changes advanced by the HITECH Act was the requirement that the Health and Human Services Department establish a public portal to review breach summaries on its website. Nicknamed the "HIPAA Wall of Shame" this was proposed to increase public transparency and operate as a deterrent that was designed to incentivize healthcare organizations to invest in preventative measures (Alder, 2024).

The FTC Safeguards Rule

The FTC Safeguards Rule is embedded within the non-healthcare specific GLB Act which requires financial institutions to explain their information-sharing practices to their customers

and safeguard their data (Federal Trade Commission, 2024). However, many healthcare organizations also offer financial products or services. When they do, they also fall under the purview of the FTC Safeguards Rule which requires businesses to implement measures to safeguard consumer data. Notably, they must keep an information security program that has administrative, technical, and physical safeguards of information. It also must be written and be formulated through risk assessment exercises. Regular staff trainings on this program are also expected to take place and a regular review of program protocols is required.

State Laws Concerning Data Breaches

The vast majority data breach laws are implemented at the state-level. While all 50 states have a notification law, these laws vary in their requirements vary and in scope leading to little consistency across the nation. Additionally, legislators have only recently began to revise notification laws to incorporate more provisions aimed at prevention to compliment robust standards of mitigation. This in turn, leads to additional variability in how healthcare organizations are expected to safeguard consumer data given multi-state providers are simultaneously beholden different jurisdictional requirements. Only 18 U.S. states have a comprehensive data privacy law on the books that lays out specific corporate expectations on how to manage sensitive information in order to reduce the likelihood of a data breach. As such, revising existing laws remains a key priority for state legislators (Strauss & Lamont, 2023). According to a report issued by the National Conference of State Legislators, several common trends have emerged in recent attempts to revise state-level data breach laws (NCSL, 2022). These include:

- Attempts to establish a timeframe for reporting or shorten an existing timeframe.
- Increase accountability in government agencies for reporting a data breach.
- Provide entities with protections in the event that they can demonstrate that their security factors were appropriate despite a breach occurring.
- Broaden the scope of what constitutes "personal information" given the rise of third-party health trackers and biometric data collection tools.

Challenges Implementing Data Breach Law in the Healthcare System

Despite recent efforts, there is mixed evidence that data breach laws are effective at all. For instance, Schuessler et al., (2017) found that data breaches incidents increased in frequency and escalated in cost even after a state passes a data breach law. This is largely because organizations find it difficult to comply with these laws (Talesh, 2018). In the healthcare sector specifically, organizations point to two intersecting issues that contribute to non-compliance: 1. There is a lack of regulatory clarity which makes compliance difficult to assess and, 2. History points to a low likelihood of enforcement undermining the incentives to comply (Pavankumark et al., 2021). These "human factors" that lead to vulnerabilities and risks are often an aside during the legislative process because policymakers are too often focused on cybersecurity rather than data security (Solove & Hartzog, 2022, p. 14). As such, data security experts have recently argued that hat overcoming this challenge will require policymakers to take a *holistic approach* to future legislative efforts (Solove & Hartzog). The holistic approach shifts the regulatory focus away

from data breaches to data processing. In line with this approach, data security laws should be redesigned to incentivize proactivity rather than reactivity, establish acceptable parameters of compliance rather than mandating specific measures, broaden accountability to all actors that contribute to data leaks, and promote simplified security norms rather than specific security practices. Collectively, these broad tenets offer a roadmap for simultaneously improving organizational compliance and reducing data breaches incidents.

TOWARD A MORE COMPREHENSIVE POLICY MODEL FOR DATA SECURITY IN THE TEXAS HEALTHCARE SYSTEM

Overview of Healthcare Data Privacy Law in Texas

In 2001, the Texas legislature passed the Texas Medical Records Privacy Act (TMRPA) which created a new chapter of the Health and Safety Code dedicated specifically to outlining data security and compliance expectations for healthcare facilities. This law signaled that in the state's opinion, HIPAA did not go far enough to protect personally identifiable health information (Alder, 2023). While HIPAA only applies to a narrower set of providers and businesses, the TMRPA expanded their definition to include a variety of unconventional industries including sports teams, website owners, IT service providers, and even representatives in the legal field. Moreover, it also applies to non-Texas specific entities that do business in the state *and* to victims of data breaches of a business operating under the jurisdiction of the state but that reside outside of Texas.

In 2011, Texas lawmakers went even further, passing House Bill 300 that amended the Health and Safety Code in response to the federal HITECH act. The increasing digitization of health records required additional protections on patient data due to novel risks associated with online data security. H.B. 300 outlined new disclosure and authorization requirements that aimed to increase transparency. It also banned commercial activities with digitized personally identifiable health information. It also empowered patients to have quicker access to their own health records if they are stored in an electronic format. Finally, it escalated penalties for non-compliance.

S.B. 768: Strengthening Data Breach Reporting Requirements in Texas

For over a decade, subsequent efforts to build on the TMRPA were mostly minor clarifications to terminology and employee training requirements (Alder, 2023). This changed during the 2023 legislative session when lawmakers passed Senate Bill 768 which specifically established new data breach reporting requirements for healthcare facilities across the state. This landmark law revised the Business and Commerce Code to require that businesses notify the attorney general within 30 days of a data breach involving at least 250 Texas residents and provide specific information about the breach (Parker, 2023). This is down from a 60-day window of and a victimization threshold of 500 Teas residents–a standard that mirrored the requirements in HIPAA (Freer, 2023). Additionally, S.B. 768 institutes a new requirement that the attorney general post the affected healthcare facility to a publicly available online listing. Those that do not comply are subject to a financial penalty not exceeding $50,000. The passage of this law brought the standards in Texas in line with a few other states, namely Colorado, Florida, Maine,

and Washington, that have moved their reporting deadline down from the federal standard (Borgia & Austin, 2023). Notably, it does not offer any state agency, institution, or officer additional authority.

Building on S.B. 768 to Improve Data Protection in the Healthcare System

It is anticipated that healthcare data privacy will remain a topic of interest to lawmakers in future legislative sessions (see Patrick, 2024). With the rise of artificial intelligence and its increasing impact on corporate data security, S.B. 768 represents a new standard to build upon. Additionally, other states continue to move in different directions regarding healthcare information privacy (Borgia & Austin, 2023). This will undoubtably impact patient expectations for relief and standards of breach mitigation in the public sphere. Drawing on the holistic approach to data breach response and information security (Solove and Hartzog, 2022), there are several avenues where this legislation can be strengthened.

First, the current regulatory framework is primarily focused on post-breach services, and light on outlining standards of compliance that promote proactive measures to prevent data breaches from occurring at the outset. It is notable that Texas also passed another, more comprehensive data privacy law in the previous legislative session that contained some of these types of measures including specific data hygiene practices and the establishment of a new enforcement division (see Neas, 2024). However, healthcare facilities were explicitly excluded from this legislation. As a result, there is an opportunity to build in additional protections for patients by porting some of these standards into the healthcare system.

Next, risk management approaches advocate for setting what are known as data security "defaults" in policy that operate as a state-endorsed standard (Solove and Hartzog, 2022, p. 162). In contrast to a requirement, defaults bring state-private partnerships into the fold by recommending specific data management tools. Put differently, the state can (and should) clarify specific tools including software, technologies, and practices that organizations can adopt to comply with the law. Organizations have the option to deviate from defaults if they wish to innovate in their security protocol, either for financial or accountability reasons. However, defaults introduce an important accountability standard. They give healthcare facilities a working compliance standard, while also giving them the freedom to innovate. This has the dual benefit of reducing regulatory ambiguity that is a source of risk-taking and also standardizing a mechanism for enforcement should a non-default be identified as the culprit in a data breach.

Finally, policymakers should take seriously that data breaches are a systemic problem and that the failure of one organizational protocol likely means that other organizational protocols are compromised. Keeping a public record of healthcare facility data breaches is commendable for establishing opportunities to seek victim relief, however a holistic approach also advocates for transparency measures that keep organizations informed that their peers have been compromised. Building out additional compliance measures and systems that encourage organizational decision makers to stay informed would help to reduce data breaches from occurring. Likewise, it may also improve mitigation efforts in the long run as noted vulnerabilities are shared among peer facilities.

CONCLUSION

Data breaches are a serious social problem that uniquely impact healthcare facilities in a variety of ways. While strides have been made in Texas to position the state as a leader in healthcare facility data security, there are opportunities for future legislative efforts could build on this foundation. This paper provides a technical overview of data breaches by covering the formal and indirect costs associated with these incidents, describing key federal laws and state efforts to address them, and contextualizing the challenges associated with policy implementation.

REFERENCES

Agelidis, Y. (2016). Protecting the Good, the Bad, and the Ugly: "Exposure" Data Breaches and Suggestions for Coping with Them Privacy Law. Berkeley Technology Law Journal, 31, 1057–1078.

Alder, S. (2023, November 5). What is the Texas Medical Records Privacy Act? The HIPAA Journal. https://www.hipaajournal.com/texas-medical-records-privacy-act/

Alder, S. (2024, January 11). What is the HITECH Act? 2024 Update. The HIPAA Journal. https://www.hipaajournal.com/what-is-the-hitech-act/

Algarni, A. M., & Malaiya, Y. K. (2016). A consolidated approach for estimation of data security breach costs. 2016 2nd International Conference on Information Management (ICIM), 26–39. https://ieeexplore.ieee.org/abstract/document/7477530/?casa_token=gsYFGS-QGukAAAAA:_b4nY2TyyiJuXpXFJJOoVOlnw_LQBOzEPQEIBNoUxW0qNOFPKZMLmjIE_9PHWqw93m2RHMOUZNiO

Bennett, K., Bennett, A. J., & Griffiths, K. M. (2010). Security considerations for e-mental health interventions. Journal of Medical Internet Research, 12(5), e1468.

Borgia, M., & Austin, P. (2023). Data Breach Notification Law Update. https://www.dwt.com/blogs/privacy--security-law-blog/2023/06/texas-data-breach-notification-law-update

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer Security, 11(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Cheng, L., Liu, F., & Yao, D. (Daphne). (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. WIREs Data Mining and Knowledge Discovery, 7(5), e1211. https://doi.org/10.1002/widm.1211

Choi, S. J., & Johnson, M. E. (2019). Do Hospital Data Breaches Reduce Patient Care Quality? (arXiv:1904.02058). arXiv. https://doi.org/10.48550/arXiv.1904.02058

Choong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. Journal of Marketing Development and Competitiveness, 11(1). https://articlearchives.co/index.php/JMDC/article/view/4360

Fauzi, M. A., Yeng, P., Yang, B., & Rachmayani, D. (2021). Examining the Link Between Stress Level and Cybersecurity Practices of Hospital Staff in Indonesia. Proceedings of the 16th International Conference on Availability, Reliability and Security, 1–8. https://doi.org/10.1145/3465481.3470094

Federal Trade Commission. (2024, May 23). Gramm-Leach-Bliley Act. Federal Trade Commission. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Fowler, K. (2016). Data breach preparation and response: Breaches are certain, impact is not. Syngress. https://books.google.com/books?hl=en&lr=&id=m5SZBgAAQBAJ&oi=fnd&pg=PP1&dq=fowler+2016+data+breach&ots=8uszmr1o8Q&sig=NoLwpXcsxLhAux2baq0apI-5bGk

Freer. (2023). New Texas Law Shortens Data Breach Notification Period. https://www.texmed.org/Template.aspx?id=62558

Gatzlaff, K. M., & McCullough, K. A. (2010). The Effect of Data Breaches on Shareholder Wealth. Risk Management and Insurance Review, 13(1), 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Holtfreter, R. E., & Harrington, A. (2015). Data Breach Trends in the United States. Journal of Financial Crime, 22(2), 242–261.

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. Communications of the Association for Information Systems, 34(1), 50.

IBM. (2023). Cost of a data breach Report 2023 | IBM. https://www.ibm.com/reports/data-breach

Ke, J., Wang, W., & Foutz, N. Z. (2022). My Data or My Health? Examining Patients' Response to a Healthcare Data Breach. Examining Patients' Response to a Healthcare Data Breach (February 2, 2022). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4029103

Khan, F. S., Kim, J. H., Moore, R. L., & Mathiassen, L. (2019). Data Breach Risks and Resolutions: A Literature Synthesis. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/14/

Kosseff, J. (2023). Upgrading Cybersecurity Law. Houston Law Review, 61(1), 51–90.

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. Journal of Business Research, 135, 559–571. https://doi.org/10.1016/j.jbusres.2021.06.054

Lee, J., & Choi, S. J. (2021). Hospital productivity after data breaches: Difference-in-differences analysis. Journal of Medical Internet Research, 23(7), e26157.

Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. Jama, 313(14), 1471–1473.

Marcus, D. J. (2018). The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. Duke Law Journal, 68(3), 555–593.

Moffit, R. E., & Steffen, B. (2017). Health care data breaches: A changing landscape. Maryland Health Care Commission, 1–19.

Muthuppalaniappan, M., LLB, & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. International Journal for Quality in Health Care, 33(1), mzaa117. https://doi.org/10.1093/intqhc/mzaa117

NCSL. (2022). 2022 Security Breach Legislation. https://www.ncsl.org/technology-and-communication/2022-security-breach-legislation

Neas, C. (2024, June 7). Texas law sets new data security rules for businesses, expands privacy protections. KXAN Austin. https://www.kxan.com/news/texas/texas-law-sets-new-data-security-rules-for-businesses-expands-privacy-protections/

Ogie, R. (2015). Bring your own device: An overview of risk assessment. IEEE Consumer Electronics Magazine, 5(1), 114–119.

Patrick, D. (2024). 2024 Interim Legislative Charges.

Perera, S., Jin, X., Maurushat, A., & Opoku, D.-G. J. (2022). Factors affecting reputational damage to organisations due to cyberattacks. Informatics, 9(1), 28. https://www.mdpi.com/2227-9709/9/1/28

PrivacyRights.org. (2024). Data Breach Chronology | Privacy Rights Clearinghouse [dataset]. https://privacyrights.org/data-breaches

S.B. 768.

Schuessler, J. H., Nagy, D., Fulk, H. K., & Dearing, A. (2017). Data Breach Laws: Do They Work? Journal of Applied Security Research, 12(4), 512–524. https://doi.org/10.1080/19361610.2017.1354275

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. Healthcare, 8(2), Article 2. https://doi.org/10.3390/healthcare8020133

Sharma, N., Oriaku, E. A., & Oriaku, N. (2020). Cost and Effects of Data Breaches, Precautions, and Disclosure Laws. International Journal of Emerging Trends in Social Sciences, 8(1), 33–41.

Solove, D. J., & Hartzog, W. (2022). Breached!: Why Data Security Law Fails and how to Improve it. Oxford University Press.

Strauss, L., & Lamont, K. (2023). The year that was in state data privacy. https://iapp.org/news/a/the-year-that-was-in-state-data-privacy

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. Law & Social Inquiry, 43(2), 417–440. https://doi.org/10.1111/lsi.12303

Tripathi, M., & Mukhopadhyay, A. (2020). Financial Loss due to a Data Privacy Breach: An Empirical Analysis. Journal of Organizational Computing and Electronic Commerce, 30(4), 381–400. https://doi.org/10.1080/10919392.2020.1818521

United States Department of Health and Human Services. (2009, September 14). Breach Notification Rule [Text]. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Wairimu, S., & Fritsch, L. (2022). Modelling privacy harms of compromised personal medical data—Beyond data breach. Proceedings of the 17th International Conference on Availability, Reliability and Security, 1–9. https://doi.org/10.1145/3538969.3544462

AUTHOR BIOGRAPHIES

Alexander B. Kinney, Ph.D., is an Assistant Professor in the Department of Criminal Justice and Criminology at Sam Houston State University. His research unpacks the dynamics of social control in gray markets, uses automated text modeling algorithms to study the logics of deviant behavior, and theorizes punishment in a cross-historical context. Recently, his work has been published in *Social Problems*, *Crime & Delinquency*, and *Law & Policy*, among other journals.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Kinney, Alexander (2024) Toward a More Effective Policy Model for Data Breach Reporting in the Texas Healthcare System. (Report No. IHS/CR-2024-1023). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/23TR9