Protecting Data Privacy in Response to Data Breaches

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Juan Chavez

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Travis Elliot, Department of Engineering and Society

Introduction

Employee concerns with monitoring systems involve the security of their data that is collected. The social construction of technology (SCOT) framework can be applied to these concerns about data collection and storage and used to analyze improvements in data security. SCOT is theory of technological advancement that argues that human action shapes technology. Specifically, this paper will use SCOT to analyze how health data breaches have affected companies' data collection systems and the technologies they use.

SCOT and Data Storage

Pinch and Bijker (1984) theorized SCOT by looking at the evolution of bicycle design and how it was affected by the needs of different groups, such as women and race cyclists. SCOT states that technology evolves from social groups rather than scientific advancements. This is due to interpretive flexibility, which means that different groups may have different meaning or interpretations of technological artifacts (Pinch & Bijker, 1984). This results in diverse user groups having different needs and problems with the technology, which ultimately leads to distinct technical solutions. For example, women had a dressing problem with the high-wheeled Ordinary bicycle resulting in a new bicycle design with pedals on the same side (Pinch & Bijker, 1984). Thus, a specific problem arises for a social group with the existing design technology, which results in modifications of that design to solve the problem. Closure in technology arises when interpretive flexibility diminishes creating stability in the technological artifact. Two closure mechanisms Pinch and Bijker (1984) describe are rhetorical closure, which results when social groups view their problems being solved by the new design, and closure by problem redefinition, in which a design that has its conflicts can be stabilized by solving a different or new problem.

Privacy concerns have led to the development of new methods to secure collected data. Yang et al. (2020) presented an enhanced differential privacy system for student health monitoring using smart wearable devices. Differential privacy is a process where information about a dataset is shared by describing patterns within the data while keeping individual data points private. The proposed method adds extra shielding to the data to ensure no important information is leaked. This protection occurs during the transmission of data from an app connected to a smartwatch to a database for storage. This new method supports Pinch and Bijker's social construction of technology (SCOT) by showing how students, the social group, affect the technology of a socio-technical system.

SCOT can be applied to describe the sociotechnical relationships of a monitoring system, specifically the student health monitoring system discussed in the Yang et al. (2020) study. For that system, the students are the social group, and the problem is that current smart wearable devices do not have secure enough data collection and transmission due to limitations in size and wireless communication being susceptible to data interception. Thus, there was concern about the vulnerability of students' data, so the proposed method addresses this problem and increases their data security.

Background on Privacy Concerns of Monitoring Systems

Multiple studies have investigated how specific employee privacy concerns affect their attitude toward monitoring systems. For example, Carpenter et al. (2018) looked into how the three concerns of perceived employee accountability (PEA), perceived employee vulnerability (PEV), and employee distrust (EDT) affect employee attitudes toward biometric data being collected for authentication technology. PEA is the employees' view that they will be held to more stringent standards when monitored using biometrics. PEV encompasses how much the employees believe their biometric data is at risk. Lastly, EDT entails the concern that employers will use biometric data for unintended reasons. The study found that concerns about PEA and PEV were associated with a negative attitude toward the biometric system while EDT did not have a significant effect (Carpenter et al., 2018).

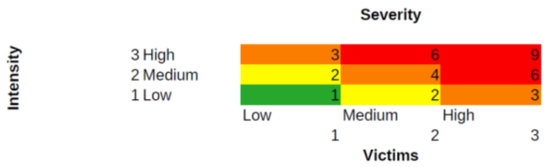
The second study is based on Communication Privacy Management (CPM) theory which argues there is a private information boundary created when individuals pick and choose what information of theirs, they disclose and to whom (Petronio, 1991). Boundary turbulence occurs when there is disagreement on what information should be disclosed in a relationship which often affects the trust in the relationship. With employee monitoring, boundary turbulence may occur when employers and employees disagree on what employee data should be collected. They investigated how information boundary concerns affect trust in employee monitoring. They found that concern about the organizational infringement (COI) and perceived amount of monitoring (PAM) significantly reduced trust in employee monitoring policy (TEMP), and only COI significantly reduced trust in employee monitoring members (TEMM) (Chang et al., 2015). COI can consist of privacy infringements which is why it reduces trust. PAM affects TEMP because employees may get uncomfortable when they perceive the policy as excessive.

These two studies show the concerns employees have with monitoring systems. Both studies reinforce the claim that employee data security is a significant concern and affects employee attitudes towards monitoring systems.

Research Question and Methods

With a monitoring system that collects health data of employees, there must be careful consideration by the employer on how to ensure the security of the data. This is already a significant concern of employees as shown by the background research. Once digital data storage became more popular around the turn of the century, external data breaches became more prevalent and more significant. For example, 79 percent of breached records between 2010-2017 were from network servers, and in this same timeframe, the number of breach reports increased every year except in 2015 (Mccoy & Perlis, 2018). Thus, data security has risen in importance. The question that arises is: How have data breaches affected the way in which companies collect & store health data? To answer this question, I will perform a historical analysis of how companies responded to health data breaches.

Specifically, I will look at four different health data breaches since 2010 and assess them using Wairimu & Fritsch's (2022) modified Privacy Risk Analysis Methodology (PRIAM) assessment method. This method describes the harms and effects of data breaches by considering the scale of victims, the irreversibility of the harm caused, and the type of privacy harm done. The method provides a severity score for physical, financial, psychological, societal, and dignity harm. The matrix, in Figure 1, shows the different severity scores that can be given based on the intensity and scale of the harm.



Severity

Intensity	Low 1	Medium 2	High 3
3 High	3	6	9
2 Medium	2	4	6
1 Low	1	2	3

Victims

Figure 1. Severity Score Matrix (Wairimu & Fritsch, 2022)

In Figure 1, the color of the score corresponds to the level of privacy harm severity with green being negligible, yellow being limited, orange being significant, and red being maximum. Once I have described the event using the PRIAM method, I will analyze the response and changes made to the data security system by the company that was involved with the breach. I will compare these responses and see how data security system technologies have changed over time.

Case Analysis

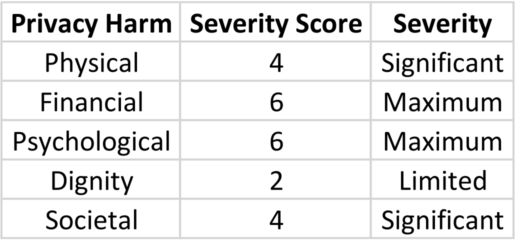
When analyzing the data security systems of healthcare companies, the four main social groups usually involved are the company itself, its employees, its customers or users, and the government. The company prefers the security system to be strong enough to provide adequate security to their customers' data to attract more customers while not being too secure to the point where it becomes too expensive. Similarly, employees want the data protected but not difficult to use. The customers need the system to be the most secure possible since their data is at risk. Lastly, the government wants to protect the rights of their citizens who are the customers. I expect the occurrence of a breach will result in changes in each group's interpretation of the security system, pushing toward wanting to make improvements since a breach means the system failed.

Utah Department of Health Breach Analysis

One of the first health data breaches caused by hacking into servers since 2010 was the Utah Department of Health Breach in 2012. Seven hundred eight thousand individuals were affected, with names and other medical information being accessed. However, only 280,000 records contained social security numbers. A hacker gained access to a new server that still had the factory password and then downloaded the patient personal information (Stewart, 2013). Table 1 shows the severity score I gave for each privacy harm using the PRIAM method.

Table 1

Utah Department of Health Breach Severity Scores



Privacy Harm	Severity Score	Severity
Physical	4	Significant
Financial	6	Maximum
Psychological	6	Maximum
Dignity	2	Limited
Societal	4	Significant

Physical harm was given a score of four since it was unlikely that a threat would result in danger since the hacker was in Europe, far away from the victims. Financial harm was a six as there was a great chance of identity theft for the victims that had their social security numbers breached, which was about a third of the victims. Psychological harm was at six because all the victims most likely had some stress due to the breach. Dignity harm was a two as the data hacked would not have caused much harm to their dignity, and the scale of victims was relatively low. Lastly, societal harm was at a four since their medical information was breached, the victims' societal reputations could have been affected.

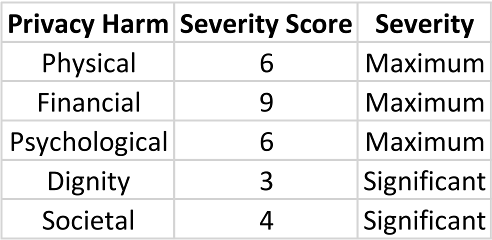
This breach did not involve a company as the owner of the system; instead, there was a government organization system owner. Thus, profits were not a factor when creating the security system, and the security system could have been more secure. The system failed and resulted in a breach affecting the citizens the government was responsible for. The Utah legislature recognized this and allocated $4.4 million for security upgrades (Stewart, 2013). The upgrade included funding for a new office of security within the Department of Health that was supposed to be dedicated to privacy and security and focused on areas, such as data risk assessment, data security training, and systems development (McGee, 2013). While this was not an improvement in technology, this new office addressed areas of weakness present in their system.

Community Health Systems Breach Analysis

Community Health Systems (CHS), a hospital operator, was subject to a breach in 2014 consisting of 4.5 million affected individuals (DuBois, 2014). Personally identifiable information (PII), such as names, birthdates, social security numbers, and addresses were compromised. Hackers infiltrated a server with weaker security measures that was not meant to be connected and that contained other credentials. Once the server went online, the attackers used a bug to access the entire system allowing them to copy and transfer data (Kennedy, 2014). Table 2 shows the severity scores for this breach.

Table 2

Community Health Systems Breach Severity Scores



Privacy Harm	Severity Score	Severity
Physical	6	Maximum
Financial	9	Maximum
Psychological	6	Maximum
Dignity	3	Significant
Societal	4	Significant

Physical harm was a six since addresses were exposed. There was a possibility that the hacker could have threatened the victims. Financial harm was a nine as there was a high chance of identity theft for the victims since social security numbers were compromised. Psychological harm was at a six, with all the victims potentially having been distressed due to the breach.

Dignity harm was a three because the data hacked would not cause much harm to victims' dignities. Lastly, societal harm was at a three since the information stolen was unlikely to affect the societal reputations of the victims.

CHS used OpenSSL’s software that contained a bug the hackers exploited to breach the system. Thus, the first upgrade was for CHS to install the patch to the software system (Ragan, 2014). No other additional security measures were implemented until the U.S. Department of Health and Human Services (HHS) created a corrective action plan that CHS agreed to implement. The security measures required in the plan were for CHS to create an internal monitoring and risk management plan, conduct a risk analysis, update their procedures to be up to standard, and begin employee training on security threats (Office for Civil Rights, 2020).

Anthem Breach Analysis

The largest health data breach since 2010 was the Anthem Inc. breach in 2015 that resulted in 78.8 million compromised records, which included current and former enrollees in their health insurance plans since 2004. PII was stolen as well as employment and income information (California Department of Insurance). The attack occurred using phishing emails that downloaded malware when opened by employees giving the attackers remote access to many of Anthem’s systems (McGee, 2017). Table 3 shows the severity score for this breach.

Table 3

Anthem Breach Severity Scores

Privacy Harm	Severity Score	Severity
Physical	6	Maximum
Financial	9	Maximum
Psychological	9	Maximum
Dignity	3	Significant
Societal	6	Maximum

Physical harm was a six since the hackers could have made physical threats with the addresses they stole. However, the hackers could not have endangered every victim of the breach. Financial harm was a nine as there was a high chance of identity theft for all the victims due to the hackers having access to their social security numbers. Psychological harm was at nine because all the victims could have been distressed due to the breach. Dignity harm was a three as the compromised data would not have caused much harm to the victims' dignities. Lastly, societal harm was at a six since the hackers could have released victim income and employment data to affect their societal reputation.

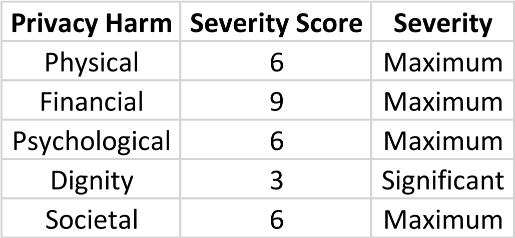
Anthem understood that, to maintain its position as a leading health insurance provider, it must make security improvements. Thus, following the breach, Anthem implemented different measures to bolster its system. These measures included two-factor authentication for remote access logins, which requires employees to provide a second form of identification when logging in using their username and password, usually a separate code sent to a cell phone via text. Additionally, they gave more resources to their security event and incident management teams to help identify future breaches more quickly (McGee, 2017). The Anthem breach also showed the importance of other security strategies and measures lacking from Anthem’s system, such as employee training about phishing, data encryption, and improved monitoring and detection tools (McGee, 2015). The breach resulted in most of these measures being implemented by other companies, completely overhauling data security. The Anthem breach is still the largest healthcare data breach by number of people affected (HIPPA Journal). Thus, this breach had a significant impact on the implementation of newer technologies into data security systems.

Banner Health Breach Analysis

Lastly, the Banner Health breach in 2016 affected 3.7 million individuals. Hackers initially gained access to card processing systems at one of Banner's food outlets and then accessed other data servers (McGee, 2016). They initially attained all the card information from the processing systems and later retrieved patient PII and some clinical information, such as physician names and information on claims. Table 4 shows the severity score for this breach.

Table 4

Banner Health Breach Severity Scores



Privacy Harm	Severity Score	Severity
Physical	6	Maximum
Financial	9	Maximum
Psychological	6	Maximum
Dignity	3	Significant
Societal	6	Maximum

Physical harm was a six since addresses were exposed. Real physical threats could have been made by hackers to some of the victims. Financial harm was a nine since the attackers stole card information, and there was a high chance of identity theft for the victims who had their social security numbers exposed. Psychological harm was at six because the breach may have stressed all the victims. Dignity harm was a three as the data hacked would not have caused much harm to the victims' dignities. Lastly, societal harm was at a six since hackers could have released patient clinical information to affect the victims' societal reputations.

Afterward, Banner Health improved its card data security as well as its cyber threat and risk monitoring (Alltucker, 2018). Additionally, Banner Health agreed to implement a corrective action plan that the U.S. HHS created to secure protected health information (PHI), similar to the one given to Community Health Systems. Plan obligations included conducting a risk analysis, developing a risk management plan, and updating its policies and procedures to meet federal standards (Office of Civil Rights, 2023).

Discussion

This study investigated how data breaches affect the social construction of data security systems. As expected, after every breach, organizations considerably improved their security system. The breaches resulted in a lack of stability in the data security system. Once the systems failed, each relevant group viewed the design as inadequate and, for different reasons, wanted improvements. Non-governmental organizations in charge of the system made upgrades to maintain their reputation as secure companies, to keep customers, or they were required to do so by the government. When a government agency was the owner of the system, the decision to make improvements was primarily to ensure the security of citizen data resulting in a more immediate investment in security, such as in the Utah case. A secondary reason could have also been to maintain the citizens trust in the government. The customers' or citizens' greatest concern is that their data will be secure in the future, so they understandably want improvements in the system. When companies did not provide adequate upgrades as judged by the government, they were required to make further improvements and changes in policies to meet standards with a corrective action plan. Initially, I overlooked government intervention in these cases; however, their intervention is justified because data privacy and security are heavily regulated, especially in the healthcare industry. Ultimately, a data security system will have closure, which is when relevant groups view a technological problem as being solved, if there are no breaches following the improvements since there will be little to no interpretive flexibility.

While there may be closure, these cases show that these data security systems were not up to standard. For example, Anthem did not have two-factor authentication, data encryption, or employee training on phishing when these technologies and strategies had already been widely available. Thus, there should have been some interpretive flexibility on the company's end since its system was vulnerable. This showed the importance of having a data security system that is as strong as possible since it will be more cost-effective in the long term. While a more secure system is more costly to develop and create, a breach in the system will result in significantly more costs from lawsuits and government fines. For example, in the Anthem breach, the settlement alone was nearly $40 million, considerably more than the cost of developing a secure system (Davis, 2020). Thus, initially investing in a more secure data security system would be beneficial for all social groups.

Conclusion

By analyzing four different breaches in the 2010s, I understand how they affected the social construction of data security systems. All four breaches resulted in improvements in the data security system since the relevant social groups viewed the system as having failed, especially the organization involved. In some cases, the government was involved to ensure those organizations made sufficient improvements. In the future, companies or organizations should strive to create highly protected data security systems prior to a breach because this will lead to closure and will actually keep customer data secure.

References

Alltucker, K. (2018, March 30). *Banner Health warns of possible "negative findings" from federal data breach probe*. The Arizona Republic. https://www.azcentral.com/story/money/business/health/2018/03/29/banner-health-warns-possible-negative-findings-federal-data-breach-probe/470032002/

California Department of Insurance. (n.d.). *Consumer information on Anthem Blue Cross data breach*. Insurance.ca.Gov. Retrieved March 12, 2023, from https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm

Carpenter, D., McLeod, A., Hicks, C., & Maasberg, M. (2018). Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers*, *20*(1), 91–110. https://doi.org/10.1007/s10796-016-9667-5

Davis, J. (2020, October 1). *Anthem Settles with 44 States for $40M Over 2014 Breach of 78.8M*. HealthITSecurity. https://healthitsecurity.com/news/anthem-settles-with-44-states-for-40m-over-2014-breach-of-78.8m

DuBois, S. (2014, August 18). *Community Health Systems data breach affects 4.5M*. The Tennessean. https://www.tennessean.com/story/money/industries/health-care/2014/08/18/community-health-systems-data-breach-affects-m/14228457/

HIPPA Journal. (n.d.). Healthcare Data Breach Statistics. *HIPAA Journal*. Retrieved March 13, 2023, from https://www.hipaajournal.com/healthcare-data-breach-statistics/

Kennedy, D. (2014, August 19). *CHS Hacked by Heartbleed (Exclusive to TrustedSec)*. TrustedSec. https://www.trustedsec.com/blog/chs-hacked-heartbleed-exclusive-trustedsec/

McCoy, T. H., Jr, & Perlis, R. H. (2018). Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017. *JAMA*, *320*(12), 1282–1284. https://doi.org/10.1001/jama.2018.9222

McGee, M. K. (2013, April 8). *Post-Breach: Utah Boosts Info Security*. Data Breach Today. https://www.databreachtoday.com/post-breach-utah-boosts-info-security-a-5663

McGee, M. K. (2015, February 10). *Protecting Against Anthem-Like Attacks*. Data Breach Today. https://www.databreachtoday.com/protecting-against-anthem-like-attacks-a-7896

McGee, M. K. (2016, August 3). *Banner Health Breach Affects 3.7 Million*. Bank Info Security. https://www.bankinfosecurity.com/banner-health-breach-affects-37-million-a-9304

McGee, M. K. (2017, January 10). *A New In-Depth Analysis of Anthem Breach*. Bank Info Security. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Office for Civil Rights. (2020, September 22). *HIPAA Business Associate Pays $2.3 Million to Settle Breach Affecting Protected Health Information of Over 6 million Individuals*. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/chspsc/index.html

Office for Civil Rights. (2023, February 2). *Banner Health Resolution Agreement and Corrective Action Plan*. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner-health-ra-cap/index.html

Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. *Communication Theory*, *1*(4), 311.

Pinch, T., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. Social Studies of Science, 14, 399–441. doi: 10.1177/030631284014003004

Ragan, S. (2014, August 19). *Heartbleed to blame for Community Health Systems breach*. CSO Online. https://www.csoonline.com/article/2466726/data-protection-heartbleed-to-blame-for-community-health-systems-breach.html

Stewart, K. (2013, April 29). *Report: Utah's health data breach was a costly mistake*. The Salt Lake Tribune. https://archive.sltrib.com/article.php?id=56210404&itype=CMSID

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

Yang, M., Guo, J., & Bai, L. (2020). A Data Privacy-preserving Method for Students' Physical Health Monitoring by Using Smart Wearable Devices. *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and*

Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 29–34. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00021