Issues in Information Systems
Volume 16, Issue II, pp. 185-194, 2015

SECURITY BREACHES IN HEALTHCARE DATA: AN APPLICATION OF THE ACTOR-NETWORK THEORY

Richard D. Stachel, Robert Morris University, rdsst175@mail.rmu.edu
Marilyn DeLaHaye, Robert Morris University, mcdst248@mail.rmu.edu

ABSTRACT

Healthcare data in 2015 is easily accessible and shareable, which is beneficial for those in the healthcare industry as well as those they serve; however, because of the increasing volumes of data accessible on many types of devices, vulnerabilities to breach and theft of that data have been uncovered. This paper applies the Actor-Network Theory (ANT) to describe the relationship among those involved in this data-sharing healthcare environment and to explain the complexities of that environment. It further uses ANT to explain how these complexities lead to vulnerabilities that can then be easily exploited and result in data breaches and subsequent data theft, and it also applies the theory to offer suggestions for mitigating that risk.

Keywords: Healthcare Data Breach, Protected Health Information, Actor-Network Theory, Data Theft

INTRODUCTION

In early 2015, news headlines heralded the discoveries of significant data breaches among large health insurance providers. The Premera Blue Cross cyberattack in March affected approximately 11 million records [12]. One month previous, Anthem Inc., which manages plans for 79 million people, announced it had uncovered a breach of its stored data [17]. While these two events were widely reported in the media, the authors of this paper were interested in uncovering a sense of the real threat involving Protected Health Information (PHI). Their subsequent analysis of breaches involving 500 or more people revealed that there were 278 breaches in 2014. That amounted to a 12 percent increase over 2013, which in itself was a 30 percent increase over the previous year [32]. These data suggest that breaches of PHI represent an increasing threat to healthcare consumers and industry members. Other research indicated that unintentional exposure of private or sensitive information was 83 percent higher in healthcare than in other industries [29]. Not only are the number of occurrences, and the increasing rate of them, concerning, but the subsequent use of that data by cybercriminals also makes it a significant hazard. PHI involves not only health records of individuals but also their social security numbers and dates of birth, which could be exploited for identity theft. In addition, healthcare data is increasingly pervasive and accessible from various and numerous devices [24], and while the theft of credit card data can be damaging, the theft of healthcare data is even more malicious. Credit card issuers offer fraud detection and subsequent alerts. The same is not true of those managing and storing healthcare data. Research conducted by Ponemon Institute [28] indicated that 54 percent of healthcare organizations which reported breaches discovered those breaches one year or more after they had occurred. In addition, another 20 percent were unable to determine exactly when the breaches took place. Because of the evidence indicating an increase in healthcare data breaches, and because of the significant threat they represent, the authors set out to explain why there was such an increase in healthcare data breaches. As a result of their investigation, they uncovered a complex web of individuals, organizations and technology that gather, store and transfer PHI. In their effort to make better sense of this complex web, which in this article they refer to as the *Protected Health Information Network* or *PHI Network*; they conducted research into a theory that could best be applied to explain the interplay of these individuals, organizations and technology.

RESEARCH METHODOLOGY

The authors' work herein is an effort to address one broad but overarching question; what is an appropriate theory that can be applied to describe the complexities of PHI which can lead to vulnerability, security risks and breaches of data? Subsequent to the identification of an applicable theory, the authors will use that theory to describe and analyze the complexities, vulnerabilities and security risk areas. Finally, they will use the theory to suggest modifications to improve security and mitigate breach threats. To address and answer their research question, the authors completed a literature review of key areas including; theories applied to information systems, healthcare-

related data, security of healthcare-related data, breaches of healthcare-related data, cybersecurity and healthcare policy as applied to PHI. Once the authors identified the Actor-Network Theory (ANT) as a suitable framework to explain the complexities of PHI leading to security risks and breaches, they conducted additional reviews of the literature that focused on ANT. Concurrent and subsequent to this literature review, the authors identified and interviewed three Subject Matter Experts (SMEs) in data warehousing, data architecture design and compliance and information-security privacy. Following each interview, the authors further narrowed the focus of their research to arrive at the research question outlined above.

THEORY APPLICATION

Introduction of the Actor-Network Theory

The major element of the authors' question, as previously described, was the identification and application of a theory to explain the complexities of PHI, and further, to use this theory to cast light on how these complexities can lead to vulnerabilities which can be exploited for data breaches and theft. After conducting literature reviews of various theories and their uses in information systems research, the authors chose the application of the Actor-Network Theory (ANT) [3, 7 ,8, 9]. In this section, they introduce and review ANT and its treatment for analysis.

The Actor-Network Theory posits that systems of relations, concepts or environments are composed of hybrid entities [15] both human and non-human. These are considered to be actors within these systems of relations, concepts or environments. The theory was developed in the mid-1980s to explain the involvement and interplay of both sociological and technical actors and processes in the workings of these systems of relations, concepts or environments. The theory involves three underlying constructs. The first of these is agnosticism whereby impartiality is invoked for all actors whether they are individuals, organizations or technology. This construct, therefore, values both human and non-human actors similarly. The second construct is that of generalized symmetry. In that, the viewpoints of the various actors, which could be, but are not necessarily contrary to one another, are set to symmetry or their equivocality is mitigated through the use of conceptual and impartial or unbiased vocabulary. This offers a baseline and level-set of arguments and approaches across actors. The third construct is that of free association. Here, the theory urges the rejection of previous assumptions and distinctions between actors, be they human and sociologically oriented or non-human and technologically oriented.

The three underlying constructs of the theory all argue for impartiality of the actors involved in a network or systems of relations, concepts or environments. As Luppicini [10] ascribed to Law and Hassard, ANT "helps to explain how socio-technical 'humanchine' networks (comprised of humans and technologies as actors) intersect through translation and create agency." However, there is no distinction made between the types of actors involved in these networks or systems whether they are social, natural or technological. Callon refers to the strength of the network as not being determined by any one actor or group of actors but rather by the bonds that tie the actors to one another [15].

Aside from the three underlying constructs of the theory, there are other salient points. The first is the understanding that these networks are not fixed and unchangeable but could involve shifting alliances between actors. The theory further espouses that these networks could, at times, be the antithesis of fixed and unchangeable. Change could be witnessed to the extent of collapse and dissolution of the network. Other networks could then develop and supplant their predecessor. Two, while actors are bound together in the network through *problemitization*, or as an approach to deal with problems, individual actors at times could also be *de-problemtizing* or undermining the stability of the network connections because of shifting loyalties or because of the realization in their worlds that issues exist due to their own initial underlying assumptions of the *problemitization*. Three, the theory posits that actors involved in networks are themselves not solely individual elements but could within their own states be another network, or as Tatnall and Gilding [15] explain citing Callon, "An actor can however, in many ways also be considered as a black-box, and when the lid of the box is opened it will be seen to constitute a whole network of other, perhaps complex associations." The fourth point is that of power. The theorists were cautious to explain power within the network as something that is not wielded autocratically but is rather ascribed to actors from others within the network. Latour [15] argued that just because one or more actors maintained perceived power did not indicate that these specific actors had enough power to affect change. In fact, the power in the network is given to an actor or actors out of the

willingness of other actors to ascribe power. The fifth salient point to be mentioned here, and one closely associated with power, is the realization that actors are active in enlisting others into the network; however:

> The notion that power is an attribute that can be possessed by an actor is an essentialist one, and Latour contends that rather than this, it is the number of other people who enter into the business that indicate the amount of power that has been exercised [15].

Uses of the Actor-Network Theory

Through their literature review, the authors discovered various applications of the Actor-Network Theory. They uncovered applications similar to those under investigation in this article, which would include information systems, security, cybersecurity and healthcare. The authors will concentrate on this literature which they believe applies most directly to ANT in these areas.

Tatnall and Gilding [15] argued for the use of ANT as a framework in information systems research. They claimed that much of the existent research relied too heavily on technology, where ANT provided an explanation that included both humans and machines. "We contend, that actor-network theory can be useful for studies of information system in situations where interactions of the social, technological and political are regarded as particularly important" (p. 962). They further advised the theory could be informative in "computer-based collaborative work, interface design, usability testing, the use of distributed systems within organisations and other areas that involve a consideration of some of the social and political issues in information systems" (p. 962). The authors of this paper will argue that this study fits this scenario, specifically in the area of social and political issues in information systems.

Another key work used herein is that of Luppicini [10] who, in his selective integrative review, compiled descriptions of the use of ANT and subsequent findings in various cybercrime scenarios. He identified 15 articles that used ANT to investigate cybercrime. Those he classified in the following six areas; cyber terrorism, cyber espionage, cyber theft, cybercrime theory, cyber fraud and cyber bullying and harassment. Not only is this work closely connected to the efforts of the authors of this paper, but moreover, Luppicini urged the use of ANT in such situations:

> Taken together, ANT is gradually becoming entrenched in cybercrime research as a theoretical tool to provide a critical perspective on crime and law within techno-social networks, offer alternative theory to compare with exiting theories, explain the complexities of information technological project escalation, and guard against unintended development of Trojan actor-networks that may allow cybercrime to occur.

While Tatnall and Gilding [15] are cited here for their work in applying ANT in information systems research, and Luppicini [10] for his work's application to cybercrime, the authors would also like to point to the research of Singleton and Michael [14] for their use of ANT to explain the network involving healthcare actors. Their study focused on a cervical screening program in the U.K., but it is important to this article because of the involvement of healthcare providers, patients, the government and a government-initiated program.

RESULTS

In this section, the authors will connect the information gathered through their data collection to each of the three underlying constructs of the Actor-Network Theory as well as to the salient points already articulated. They will use the analysis in this section first to support their assertion that ANT applies in this case, and second, to further their claim that ANT can be used to explain the complexity of the PHI Network which can lead to vulnerabilities.

Evidence of the Actor-Network Theory

Before the authors move to identifying the three underlying constructs of ANT in the PHI Network, they believe it is important to establish the understanding of the actors involved in the network. In this discussion, the authors refer to *theDataMap*™ as seen in Figure 1 [25]. This map was developed initially by Harvard University researchers to

identify and explain the actors involved in a patient's data and the flow of that data between actors. It was subsequently expanded upon by others.

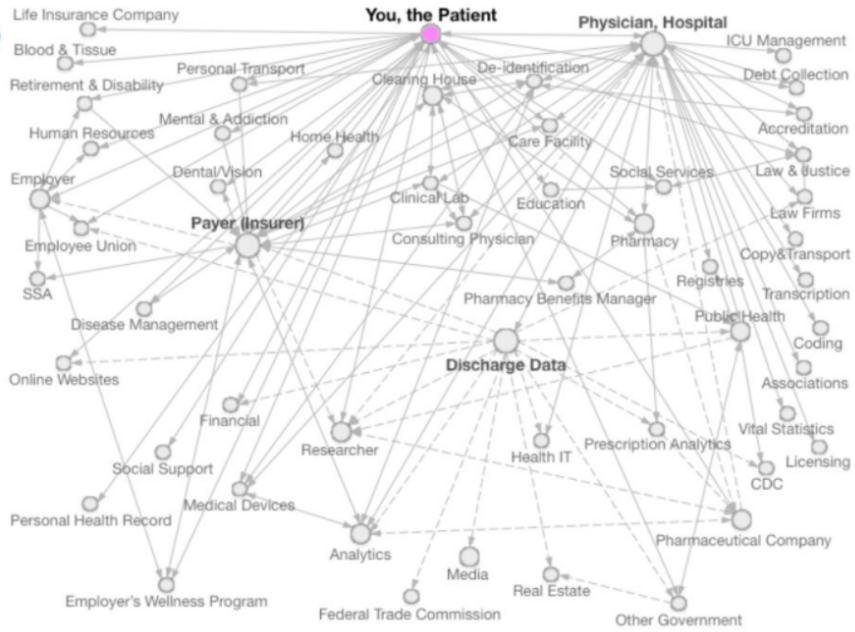

Figure 1. theDataMap™

The authors introduce this map as evidence to the number of actors involved in the collection, storage, transfer and analysis of PHI. In addition, this model depicts the flow of information between actors, and hence, the relationships between them. These actors are human and organizations comprised of both human and non-human actors. However, what is not evident here is the uncovered *black-box* of each actor. If the reader were to imagine the lid being lifted off of any one of the *black-boxes*, there he might find other sets of complexities, as indicated by Callon as cited in Tatnall and Gilding [15]. What is important to realize is that the additional complexities under the lid of the *black-boxes* would include a network of technology or devices that are used to collect, store, analyze and transfer the data between actors. Those are not depicted in theData Map, and if they were to be more clearly defined, they would further complicate an already-complex model.

To substantiate their point that the data map should also include non-human actors, the authors cite research reports and white papers that detail the ubiquitous nature of different types of technology used in data storage or transmission of PHI. A Ponemon Institute study [28] on patient privacy and data security indicated that 65 percent of respondents reported that patient data resided on non-secure databases. In other analyses in the same report, 63 percent of those responding worried that data breaches could occur because of the use of patient registration information on non-secure websites. In addition, 32 percent of respondents identified themselves as members of a Health Information Exchange (HIE). The report identified these as "the mobilization of healthcare information electronically across organizations within a region, community or hospital system." Of those who were members of an HIE, which is a network with in a network, 40 percent were not confident in the security of the data moving through the exchange. The same report indicated that 88 percent of their participants admitted to allowing the use of personal, non-secure mobile devices such as phones and tablets by employees and medical staff as a means of accessing their networks.

Evidence of the use of technology for the collection and storage and/or transfer of patient data between actors can also be witnessed through the uptake of Electronic Health Records (EHRs) by physician practices. Data from the National Center for Health Statistics, Centers for Disease Control and Prevention, U.S. Department of Health and Human Services [31] indicate the adoption levels of EHRs by office-based physicians reached 78.4 percent by 2013. The adoption was driven by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 [21]. The HITECH Act established incentive payments to increase adoption.

Connecting the PHI Network to the Actor-Network Theory

The constructs of the Actor-Network Theory are; agnosticism, generalized symmetry and free association. In this section the authors will present evidence from the PHI Network that connects the network to each construct. The first construct, agnosticism, which is impartiality invoked for all actors, is evident in the PHI Network, the authors argue, by the interest of each actor to participate in the network for a greater good or overall benefit. They contend that this benefit is the coordinated care of patient populations, of which the Agency for Healthcare Research and Quality [23] says the following:

> Care coordination involves deliberately organizing patient care activities and sharing information among all of the participants concerned with a patient's care to achieve safer and more effective care. This means that the patient's needs and preferences are known ahead of time and communicated at the right time to the right people, and that this information is used to provide safe, appropriate, and effective care to the patient.

The Patient Protection and Affordable Care Act (ACA) [22], designed to reduce the increasing cost of healthcare and provide better outcomes, is in itself testimony to the interest of increased engagement in this network. According to Optum [27], an integrated health services system, Population Health Management (PHM), a system and process supported and incentivized through the ACA, is key to providing optimal health-systems performance. Optum states that the cornerstone of this integrated approach is data, which it separates into two sources; claims and clinical. Claims data is created to approve and assure payment of healthcare services and is used by health insurers, but Optum states this data is valuable not only for that purpose but also because it can be analyzed to discover care patterns and to develop insights into population health trends. It also states this data can be used for research, not to mention something more aligned to its original intent, monitoring the cost of care. The clinical data, Optum states, is that which is collected for diagnosis and treatment, and with the use of Electronic Medical Records (EMRs), is becoming a valuable and more complete source of information, "EMRs make a rich store of data available for analysis and are found throughout the continuum of care, including the emergency department, hospital inpatient records, outpatient/ambulatory, physical therapy and radiology areas." To further acknowledge the benefit of this coordination, Shortell, citing Gillies, et al. [13] claimed that health plans with closely linked networks of actors in physician groups, those that actually employ their own physicians, perform better in patient outcomes than non-networked performers, but they had no difference in patient satisfaction.

The evidence is clear regarding the reason providers, be they physicians, hospitals or insurers, are interested in participation in a network of data sharing, or PHI Network, but research indicates that patients are also keen to participate. In a study of Veterans Administration (VA) patients, Zulman, et al. [18] found the majority of respondents in their study were interested in sharing their electronic health information with caregivers and non-VA network providers. Fricton and Davies [5] discovered, in their study of congestive heart-failure patients, that there was interest among care providers, caregivers and patients in sharing electronic health information. To further this point, a study conducted on behalf of the Society of Participatory Medicine [20] claimed that 75 percent of U.S. adults believed it to be very important that their health data be shared across a spectrum of PHI-Network actors.

Generalized symmetry, the second construct of ANT, also applies in the PHI Network. This construct, as previously outlined, indicates that an impartial or unbiased vocabulary is established to mitigate viewpoints among actors. This article already includes many examples of such mitigating vocabulary, such as; *Electronic Health Records*, *HIPPA*, *Population Health Management*, *Protected Health Information*, *patient outcomes*, the *Affordable Care Act*, the *HITECH Act*, and *care coordination*. One can add to that, terms such as; *Accountable Care Organizations* (ACOs) and *meaningful use*. ACOs, according to the Centers for Medicare and Medicaid Services (CMS) [19], are groups, or networks of physicians and other clinicians who participate voluntarily in the management of patient care. *Meaningful use* is a term used specifically with electronic health records, and as indicated previously in this article, has been part of an incentive plan for both physician-actors and hospital-actors from the U.S. government to digitize health records and is envisioned to be rolled out and established in three phases [21]. Language used for generalized symmetry is evidenced throughout this paper and, as such, is credible in its attempt to demonstrate a link between the PHI Network and one of the core constructs of ANT. It also depicts the involvement of both human and non-human, or technology-based, actors.

The third construct of ANT, for which the authors intend to demonstrate connection to the PHI Network, is that of free association or the rejection of a priori assumptions and distinctions between actors. With this construct as it applies to the PHI Network, many see the influence of the ACA as a watershed, but prior to that, the Institute of Medicine Report of 2001, *Crossing the Quality Chasm: A New Health System for the 21st Century* [26] called for a dynamic change in healthcare delivery with the patient at the center of the delivery system. The ACA's passage then ushered in a shift of relationships between actors, as stated by Burkman [2], "A cornerstone of this new approach is patient-centered care as opposed to provider- or disease-centered care." He also acknowledge that technology or non-human actors were central to this paradigm shift, "…electronic databases can be used to monitor such items as the utilization of costly imaging for certain diagnoses or ancillary services by specialists." This paradigm shift has had ramifications on a more individual level. In their article, Epstein and Street [4] claimed the communication dynamic has changed between physician and patient whereby physicians are encouraging patients to take a more active and participatory role in their own healthcare.

The section above reviewed the three constructs of the Actor-Network Theory and offered evidence to indicate that each has applicability in the PHI Network. As the authors indicated, there are other elements to the theory that are evident in this network. One is that of *problemitization*. The PHI Network developed in order to address a problem; that of increasing healthcare costs. The network has formed, perhaps not formally as that of a single organization, but in the strength of the ties between the actors. This was indicated previously in the work by Optum [27] when it referred to the strength of the data in supporting coordinated care. The authors have also noticed areas of *deproblemitizing*. This was the case in the Singleton and Michael research [14], where physicians were reticent to apply government recommendations of cervical screening program to all women indicating it should be customized to specific patients. The authors have also witnessed such *de-problemitizing* among physicians and health organizations in the PHI Network. A survey conducted of physicians by *Medical Practice Insider* [6], revealed that of the nearly 2,000 physicians polled, 55 percent did not plan to move forward with meaningful use guidelines in phase two of the program established by the HITECH Act. In addition, it found that 60 percent of physicians did not consider their EHR to be a worthwhile investment. An article in *Medical Economics* in October 2014 [16] also attested to the slow adherence to the second phase of the program. The *Medical Practice Insider* survey [6] claimed the slowing adoption was due to second-phase requirements of the meaningful use program which stipulated that medical practices entice five percent of their patient population to engage in health-data portals. Similar to what was depicted in the *de-problemitizing* in the Singleton and Michael study [14], some physicians are raising objections because they believe the government plan is applied too broadly without consideration for any customization to population characteristics. Not only are the authors recognizing *de-problemitization* among physician groups, but they have also witnessed the same among some healthcare organizations. As part of the Affordable Care Act, CMS established the Pioneer ACO program and enrolled 32 health systems, but by the end of 2014 only 19 remained [1]. Others exited, according to the *Wall Street Journal* report, because of onerous requirements.

Two other aspects of ANT that can be applied to the PHI Network are those of power and enlistment. Power is not autocratic but rather participatory in that actors within the network knowingly and willingly bestow power to certain members. In addition, members enlist participants in the network. There is evidence of both at work in the PHI Network. The Institute of Medicine [26] called upon a paradigm shift in medical practice, giving acknowledgement to some of the practices and policies initiated later under the ACA. In addition, there are other policies and procedures that have been outlined by the U.S. government that would indicate that it has been bestowed this power from other actors within the network; those include the HITECH Act of 2009, which established the concept of meaningful use and established participation incentives, and previous to that, HIPPA. Not only do these pieces of legislation indicate that there is an actor, in this case the government, wielding power bestowed upon it by others who realize the potential benefits of the network, but it also includes enlistment. Enlistment was also evident in the establishment and enrollment of healthcare organizations in the Pioneer ACO. The mere act of incentivizing participation in meaningful use itself is enlistment. In addition, although the authors cited concerns and dropping participation in the CMS-managed Pioneer ACO, there are other ACOs outside of the Pioneer program, and *Health Affairs* [11] reported in 2015 that the number of participants continued to expand.

Vulnerabilities

In this section, the authors will discuss how the PHI Network represents a vulnerability to the theft of personal health data, because of the sheer number of actors, the number of data transfers between actors and the amount of

data stored among them. Given the enlistment practices of the U.S. government, the amount of healthcare data being stored and transferred between actors is expected to multiply, which according to SANS [30] will lead to vulnerabilities, "an outpouring of electronic protected health information (ePHI) being exchanged online, even more attack surfaces are being exposed in the health care field." In addition, the number of devices connecting data to actors is expected to grow. As indicated earlier in this article, 88 percent of respondents to a survey of healthcare organizations admitted that they allow employees or clinical staff to access their network using mobile devices such as phones and tablets [30]. A report from BitGlass [24] states that 90 percent of healthcare professionals use smartphones for work. One security consultant interviewed by the authors says it is not just the number of the devices alone but also the technology of the devices. "We can store vast amounts on, say an iPad. That means there's more data to be lost if it's stolen. So, we're looking at larger volumes of data than can be carried around."

Beyond this, many medical devices can now transmit data, and the SANS Institute [30] predicts that the healthcare and pharmaceutical industries will be among the industries that experience the highest deployment of Internet-connected devices. It also warns that mobile communication devices and medical devices are not the only vulnerable actors in this system, but they can also be conferencing systems, web servers, printers or security cameras. "Today, almost every network-attached device is shipped from its vendor in an insecure configuration with defaults that can be discovered easily through an internet search." Another vulnerable access point is not a device at all, but data storage, and that is the cloud. The SANS report indicated that 60 percent of respondents were using, or planned to use, cloud storage, and yet 73 percent were worried about data leakage from cloud providers. As it suggests, perhaps they have good reason to be, "Cloud applications, particularly in the form of health care exchanges and medical and pharmaceutical networks, create additional attack surfaces attackers can exploit to gain access to protected patient medical and financial data."

While the authors here have discussed the vulnerabilities around the increased volume of data and the expanding number of devices-as-actors in the network, they have not discussed perhaps the most vulnerable part of the network; humans. When asked to identify the biggest threat to PHI, one SME said, "People. People is the biggest risk." Indeed the authors' analysis of healthcare breaches using data from the U.S. Department of Health and Human Services [31] bears this out. The authors' analysis of breach type for breaches affecting over 500 people between 2009 and March 2015, clearly indicates that theft is the most prevalent, accounting for 50 percent of breaches. Other analyses confirm this finding. BitGlass [24] reports that 68 percent of healthcare data breaches since 2010 were due to theft or lost devices. These data would suggest that it is not technology-related actors in the network but the human ones that are responsible for most of the breach threats. As one informant told the authors, "Your biggest threat when you're looking at it from a day-to-day perspective, are your employees."

APPLYING ANT FOR SUGGESTIONS ON BREACH-RISK MITIGATION

In this section, the authors apply the Actor-Network Theory to offer suggestions on mitigating breach risks of protected health information. These suggestions rely on the three main constructs of the theory to frame the discussion; agnosticism, generalized symmetry and free association, and they use the same data sources outlined in the literature review and methodology sections of this paper to inform the suggestions offered.

When contemplating agnosticism and its role in providing suggestions for breach-risk mitigation, the authors believe the suggestions lie in two broad, interrelated concepts. The first is encouraging increased activity of particular actors in the network and the second is the enlistment of new actors.

Regarding increased activity of particular actors, training and accountability of individuals and staff members involved in the network is a key area of improvement. That training should focus on identifying threat points, such as theft of devices and define the steps individuals can take to lessen those threats. In addition, since some data breaches are engineered by human actors with access to the data, making those actors accountable for their illicit actions is critical. First though, they need to understand what comprises illegitimate use according to their roles.

Another significant area of improvement in risk mitigation is vendor management. Healthcare organizations using PHI should provide stricter guidance to contractors with access to sensitive data, and beyond that, they should insist on tighter data security policies as a cost of doing business. These are costs vendors need to bare if they are interested in working within the industry.

Not only does agnosticism call for improved activity among network participants, but it may also implore further enlistment into the network from new participants who have skills, processes or abilities current members do not possess. Those could include the support of current actors of consumer-facing technologies, such as patient portals or mobile health applications [30], each of which would encourage consumer-actors to take a more active role in their data and its security. The network should also enlist vendors that provide secure cloud options [12], and even more specifically the use of Cloud Access Security Brokers (CASBs) [24]. This will offer a level of security and visibility not achieved by many actors in their current use of cloud solutions.

The final suggestion regarding agnosticism comes not within an organization-actor but in the interplay between actors. Actors need to create greater awareness across the network when a breach occurs. Not only will other actors be better prepared for new and developing threats identified through these communications, but those affected by a breach can take steps to mitigate the damage.

Under the construct of generalized symmetry, the authors believe that the suggestions for risk mitigation all fall under the concept of systems or process improvement. These systems or processes, to be considered part of generalized symmetry, need to become part of the impartial or unbiased vocabulary across actors. One of the suggestions deals with the language and processes already in place. Actors should comply with the already-established standards and regulations developed under HIPPA or by agencies such as the Centers for Medicare and Medicaid Services. Other suggestions deal specifically within an actor's organization. Those include the establishment of policies and procedures to mitigate breaches such as sound audit and risk-management programs. Actors should also take steps toward mandatory encryption of data when transmitted by email, over mobile devices and from databases. Security can also be improved through practical improvements such as a Single Sign-On (SSO) solution [24] to thwart the efforts of hackers who exploit password vulnerabilities. Databases with PHI should require masking of data to determine who can access certain data and from which devices. With a development of a sophisticated schema of data masking, however, parallel databases may be necessary in order to allow multi-layer access while not compromising performance. In addition, sensitive data should be tracked throughout an actor's organization or throughout the network by employing the use of a digital watermark [24]. That would allow actors to determine who has downloaded the data and how they have used it. In general, actors should make any data security easy to deploy and use, and they should assure the resiliency of those systems because threats change and evolve quickly [30].

The third ANT construct is free association, and here, the theory encourages the rejection of a priori assumptions. This paper is based on the rejection of a key primary assumption; that being the one in which hackers infiltrating systems or devices are the most significant threat. The authors have shown that human actors within the network are the biggest threat, and suggestions discussed under agnosticism address this threat through training and accountability. However, organizations in the network need to discard their assumptions that the biggest threats are external. They also need to shift their emphasis away from applying security to devices and apply it more appropriately to securing the data itself. Similarly, instead of solely thinking about the uses of data when designing a database for PHI, organization-actors should design with security as a priority rather than attend to it once they have had a breach threat. In order to more effectively coordinate that, and to raise the status of security, organization-actors should strengthen the role of the Chief Information Security Officer (CISO) [12]. That role frequently reports to a Chief Information Officer (CIO); however, that may be misplaced. The role is not just about technology, but it is also about processes and physical safeguards that tend to be broader than those traditionally considered to be part of a CIO's organization.

CONCLUSIONS

The authors of this paper addressed an area of increasing concern in 2015, that being data breaches of Protected Health Information (PHI). The year began with two significant events, but further analysis indicated there were over 250 breaches in 2014, implying a more significant problem than highlighted in media reports. In an attempt to explain the risks and vulnerabilities, the authors applied the Actor-Network Theory. Much of the paper was focused on proving the relationship between the PHI Network and the Actor-Network Theory. In the opinion of the authors, the three underlying constructs of ANT, agnosticism, generalized symmetry and free association work well in explaining the complexities of the network and the vulnerabilities inherent because of the complexities, as well as offering suggestions for mitigating threat risks. As a result of their work, the authors believe that ANT is an appropriate and useful tool to analyze the actors in the PHI Network, uncover vulnerabilities in the network for data breaches and theft of healthcare data in addition to offering suggestions for security improvement.

REFERENCES

1. Beck, M. (2014, September 25). A Medicare program loses more health-care providers: Hospital systems say rules too stringent in Pioneer Plan set by federal health law. Wall Street Journal. Retrieved from http://www.wsj.com/articles/a-medicare-program-loses-more-health-care-providers-1411685388
2. Burkman, R.T. (2012). Patient-centered care: A new and challenging paradigm in health care. The Female Patient, (37), 14-15
3. Callon, M. (1986). Some elements of a sociology of translation: Domestification of the scallops and the fishermen of St Brieuc Bay. In J. Law (Ed.), Power, Action and Belief: A New Sociology of Knowledge, 196-233. London, UK. Routledge Kegan Paul.
4. Epstein, R.M. & Street, R.L. (2012). The values and value of patient-centered care. Annals of Family Medicine, 9(2).
5. Fricton, J.R. & Davies, D.D. (2008). Personal health records to improve health information exchange and patient safety. In K. Henriksen, K., J.B. Battles, M.A. Keyes & M.I. Grady (Eds.), Advances in Patient Safety: New directions and Alternative Approaches (4). Rockville, MD. Agency for Healthcare Research and Quality.
6. Irving, F. (Ed.). (2015). 2015: End of the road for meaningful use? Medical Practice Insider. Retrieved from http://www.medicalpracticeinsider.com/news/2015-end-road-meaningful-use
7. Latour, B. (1988). The Pasteurization of France. Cambridge, MA. Harvard University Press.
8. Law, J. (1986). On the methods of long-distance control: Vessels, navigation and the Portuguese route to India, in J. Law (Ed.), Power, Action and Belief: A New Sociology of Knowledge, 234-63. London, UK, Routledge Kegan Paul.
9. Law, J. (1986). Editor's introduction: Power/knowledge and the dissolution of the sociology of knowledge, in J. Law (Ed.), Power, Action and Belief: A New Sociology of Knowledge, 234-63. London, UK. Routledge Kegan Paul.
10. Luppicini, R. (2014). Illuminating the dark side of the Internet with Actor-Network Theory: An integrative of current cybercrime research. Global Media Journal – Canadian Edition, ISSN: 1918-5901 (English) – ISSN: 1918-591X (Francais), 7(1), 35-49.
11. Muhlestein, D. (2015). Growth and dispersion of accountable care organizations in 2015. Health Affairs Blog. Retrieved from http://healthaffairs.org/blog/2015/03/31/growth-and-dispersion-of-accountable-care-organziations-in-2015-2/
12. Padmanabhan, P. (2015, March 20). Premera data breach: 3 things healthcare enterprises could do, CIO. Retrieved from http://www.cio.com/article/2899664/data-breach/premera-data-breach-3-things-healthcare-enterprises-could-do.html
13. Shortell, S.M., et al. (1996). Remaking Health Care in America. San Francisco, CA. Josey-Bass.
14. Singleton, V. & Michael, M. (1993). Actor-Networks and ambivalence: General practitioners in the UK Cervical Screening Programme. Social Studies of Science, London, UK, Sage (23) 227-64.
15. Tatnall, A. & Gilding, A. (1999). Actor-Network Theory and information systems research. Proceedings of the 10th Australasian Conference on Information Systems.
16. Terry, K. (2014, October, 23). Meaningful Use 2: A Work in Progress for Physicians. Despite software and patient outreach challenges, many physicians are still determined to attest to stage 2. Medical Economics. Retrieved from http://medicaleconomics.modernmedicine.com/medical-economics/news/meaningful-use-2-work-progress-physicians?page=full.
17. Wayne, A. (2015, March 18). Senators demand Anthem hasten notifications on data breach, BloombergBusiness. Retrieved from http://www.bloomberg.com/news/articles/2015-03-18/senators-demand-anthem-hasten-notifications-on-data-breach.
18. Zulman, et al. (2011). Patient interest in sharing personal health record information: a web-based survey. Annals of Internal Medicine 155(12), 805-810. doi: 10.7326/0003-4819-155-12-201112200-00002.
19. Accountable Care Organizations. (2015). Centers for Medicare & Medicaid Services. Retrieved from: https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/index.html?redirect=/aco
20. Americans Believe Personal Medical Data Should be Openly Shared with Their Health Care Providers. (2015, March 19). PR Newswire on behalf of Society of Participatory Medicine. Retrieved from http://www.prnewswire.com/news-releases/americans-believe-personal-medical-data-should-be-openly-shared-with-their-health-care-providers-300052787.html

21. American Recovery and Reinvestment Act of 2009. (2009). Senate and House of Representatives of the United States of America in Congress assembled.
22. An Act Entitled The Patient Protection and Affordable Care Act. (2001). The Senate and House of Representatives of the United States of America.
23. Agency for Healthcare Research and Quality. (2014). Care Coordination. Retrieved from: http://www.ahrq.gov/professionals/prevention-chronic-care/improve/coordination
24. BigGlass. (2014). The 2014 BitGlass Healthcare Breach Report: Is Your Data Security Due for a Physical?
25. Harvard University, Institute for Quantitative Social Science (IQSS), Data Privacy Lab. (2013). theDataMap. Retrieved from http://www.thedatamap.org
26. National Institute of Medicine. (2001). Crossing the Quality Chasm: A New Health System for the 21st Century. Washington, DC. National Academy Press.
27. Optum. The Four Steps of Population Health Management. Retrieved from https://www.optum.com.
28. Ponemon Institute. (2014). Fourth Annual Benchmark Study on Patient Privacy & Data Security.
29. PriceWaterhouseCoopers. (2014). US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey.
30. SANS Institute. (2014). New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations.
31. U.S. Department of Health & Human Services, Centers for Disease Control and Prevention. National Center for Health Statistics. (2014). Use and Characteristics of Electronic Health Record Systems Among Office-based Physician Practices: United States, 2001-2013. NCHS Data Brief, No. 143.
32. U.S. Department of Health and Human Services, Office for Civil Rights (2015). Breaches Affecting 500 or More Individuals. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf