Editors: Michael Lesk, lesk@acm.org | Jeffrey MacKie-Mason, jmm@umich.edu

Protecting Patient Data—The Economic Perspective of Healthcare Security

Juhee Kwon | City University of Hong Kong
M. Eric Johnson | Vanderbilt University

Data breaches have become a staple of the news cycle. Over the past 10 years, there have been so many breaches that the coverage for any particular breach often quickly fades. But every year, a few breathtaking failures find their way to the front page and span multiple news cycles. For the healthcare industry, the recent Anthem breach affecting 80 million individuals received multiday coverage, sending shock waves through a nervous public and highlighting the growing threat facing healthcare. For years, researchers have been predicting that the healthcare industry would become the next target for wide-scale attacks.[1] While the financial sector steadily stiffened its security, healthcare's relatively immature level of security made many organizations easy targets. It was only a matter of time before healthcare firms' rich source of vulnerable personal information would attract criminals.

This breach epidemic in healthcare led us to explore the impact of the new US regulatory regime and market forces to better understand the effectiveness of different security investment strategies.

Security in Healthcare

Healthcare data has fueled diverse frauds from simple financial identity theft to more sophisticated schemes involving fraudulently obtained medical care, fake billing, and black markets for stolen pharmaceuticals and equipment.[2] Such diverse fraud models make healthcare data lucrative on black markets, where sensitive information is traded through underground websites and chat rooms.

The impact on patients goes well beyond traditional financial identity theft. Unlike with a credit card, once patients' data is exposed, they can't simply cancel a single 16-digit card number. Moreover, damages could be life-threatening to victims if erroneous information contaminates their personal healthcare records. This is the case when others use identity information to fraudulently obtain care. Given the impact to individuals, the media and general public often question why healthcare organizations don't better protect private healthcare data.

Healthcare firms' security issues, as well as the related challenges of organizational maturity and compliance, apply to organizations in many industries. Economists blame market failures for the underinvestment in security. For example, customers often shoulder the costs of security failures. In imperfectly competitive markets in which firms significantly control pricing, consumers might not be able to fully pass these costs back to firms, and thus, firms are rationally tempted to underinvest in security.

In addition, it's difficult for customers to evaluate a firm's security efforts or performance. This information asymmetry further reduces a firm's interest in investing in security—something economists call a *moral hazard*. This is particularly true in US healthcare. Observers have noted that patients in some markets have only a few hospitals from which to choose[3] and little security information on which to base their choice. Moreover, the US third-party payment system via insurance and government further insulates healthcare providers from patients, exacerbating moral hazards in the sector. The result is an industry whose organizations don't prioritize security and subsequently become easy targets.

Copublished by the IEEE Computer and Reliability Societies

US Regulations

Security experts hoped that the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act would nudge the industry toward better security practices and ultimately reduce breaches. The heart of HITECH is a set of financial incentives (provided by Centers for Medicare & Medicaid Services) to expedite the adoption of electronic health records (EHRs). Indeed, these incentives have dramatically increased EHR adoption. According to a recent report, EHR adoption has increased fivefold since 2009, rising to 83.2 percent of hospitals in 2014 (see Figure 1).[4]

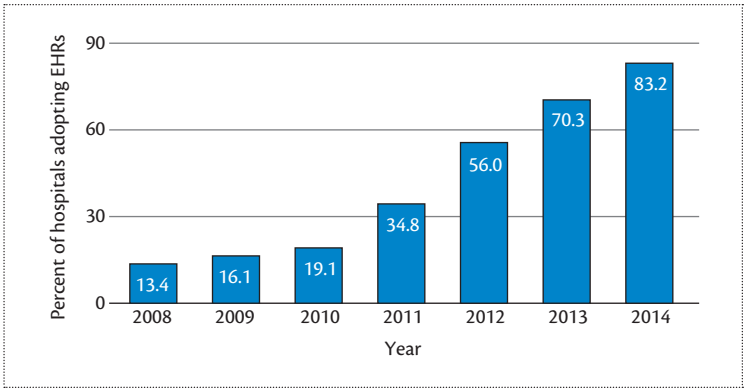

Figure 1. Trends in the adoption of electronic health records (EHRs). (Source: www.healthit.gov.[4]) Respondents included acute care, general medical and surgical, general children's, and cancer hospitals owned by private/not-for-profit, investor-owned/for-profit, or state/local government entities and located within the 50 US states and the District of Columbia.

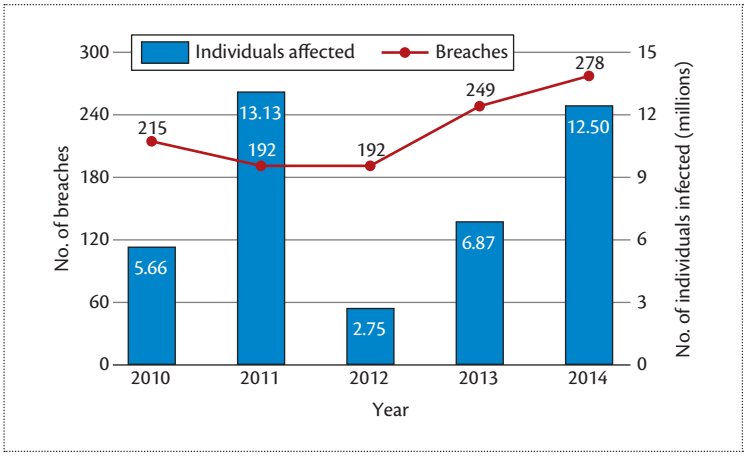

Figure 2. Healthcare data breach trends. The bars and line depict the trends in affected individuals and the number of healthcare data breaches from 2010 to 2014. (Source: US Department of Health and Human Services.)

However, the legislation also contains regulatory and market mechanisms to address security investment failures. For example, it requires organizations to conduct risk assessments and put teeth into violations of longstanding Health Insurance Portability and Accountability Act rules, increasing penalties to as much as US$1.5 million per breach incident based on the severity. It also requires providers that experience a breach to notify impacted individuals within 60 days of discovery. If the breach impacts more than 500 people, providers must report it to media organizations and the US Department of Health and Human Services (HHS), which posts announcements to its website,[5] sometimes referred to as "the wall of shame." Notification reduces information asymmetry, and both the breach notification process itself and related fines impose significant costs.

When the HITECH breach-reporting rules went into effect, security professionals predicted a spike in breach announcements as newly adopted processes uncovered more breaches and organizations rushed to disclose and avoid penalties. By the end of 2010, 215 breaches affecting more than 5.6 million Americans were reported to HHS's wall of shame.[5] After the initial disclosures, many hoped that improved security investment would reduce breaches. However, the announcements haven't slowed—2014 was one of the worst years since the HITECH-mandated disclosures started in 2009, with the most breach incidents (line in Figure 2) and the second highest number of individual records (bars in Figure 2). Today, more than 40 percent of reported data breaches arise from the health sector (see Figure 3), with a marked shift in past years from business to healthcare.

Impact of Security Strategies

Skeptics often argue that compliance with mandated security standards has little to do with actual security performance. Given the heterogeneity of organizational security resources and operational maturity, we conjectured that security investments and compliance need to be tailored to an organization to successfully improve

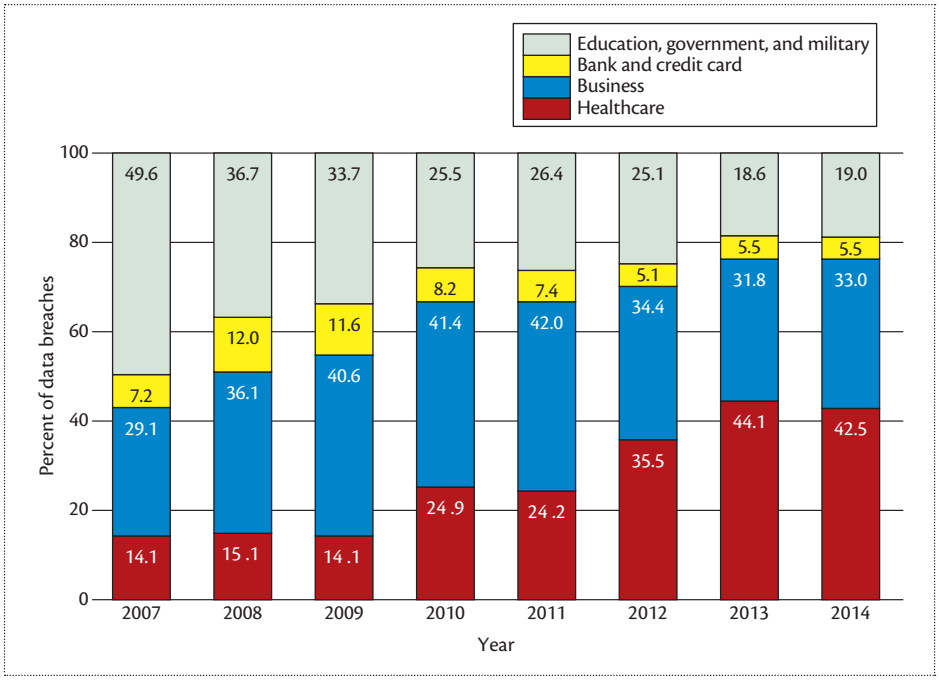

Figure 3. Data breach trends for industries. Of all data breaches, the proportion of healthcare data breaches steadily increased, while those of the other industries declined from 2007 to 2014. (Source: Identity Theft Resource Center.)

security. To explore the impact of regulatory regimes, we conducted several studies.

Operational Maturity

In one of our first projects, we examined how relationships among actual data protection, compliance, and security resources vary with a healthcare provider's operational maturity.[6] We considered organizations that maintained and regularly updated a security plan *operationally mature*. Using data from 243 hospitals, we found that the impact of security investments indeed varied depending on an organization's operational maturity.

Compliance with state and federal IT security mandates significantly improved actual security in *operationally immature* organizations, but surprisingly, it didn't have any effect on operationally mature organizations. We also found that operationally mature organizations were more motivated by breach occurrences than by compliance with federal and state security standards. By contrast, operationally immature organizations were more motivated by compliance than security.

We concluded that in operationally mature organizations, security investments were more strategically planned and executed for both compliance and actual security. Strategic plans—along with periodic reviews—enabled organizations to learn of potential new risks and evaluate their own security posture. As a consequence, organizations' security resources were better targeted to address their specific needs and the environments in which they operate.

In a related project, we found evidence that proactive security investments are more effective than reactive ones.[7] Examining the security investment decisions and breach history of 2,386 US hospitals over five years, we found that proactive investments were associated with lower security failure rates than investments made in reaction to breaches. Combining this data with the costs of breach disclosure and security program costs, we showed that proactive investments are more cost effective than reactive investments. In other words, hospitals lowered their security costs while providing more effective protection, and patients experienced less harm from having their private data exposed. Interestingly, we also found proactive, voluntary security investments had more impact than those driven solely by regulatory compliance.[7]

HITECH's Effect

More recently, we examined HITECH's longitudinal impact. As we noted, the major thrust of HITECH is a sequence of financial incentives to encourage EHR adoption. Hospitals and doctors are eligible to receive millions of dollars for adopting and attesting to their meaningful use of certified EHR technologies. These financial incentives, linked to a certification mechanism called *meaningful-use* attestation, have been a key policy initiative of the Obama administration to ensure effective technology adoption and the protection of patient healthcare data.

The incentive program consists of three stages with increasing requirements: stage 1 for capturing patient data and sharing the data with patients, stage 2 for advanced clinical processes, and stage 3 for achieving better healthcare outcomes. As part of stages 1 and 2, hospitals and doctors must conduct a security risk analysis. Stages 1 and 2 went into effect in 2011 and 2014, respectively; stage 3 is currently being finalized. Eventually, eligible healthcare organizations that haven't adopted and attested to meaningful use of EHRs will see financial penalties. Since 2011, many healthcare organizations have attested to their meaningful use of EHRs and received billions of dollars in financial incentives, as shown in Figure 4.

Meaningful-use attestation as a certification scheme both improves

the hospital security investment calculus and reduces information asymmetry by signaling difficult-to-observe security capabilities. In a statistical analysis of nearly 1,000 US hospitals, we examined whether the security standards of stage 1 meaningful-use attestation actually improved information security performance. In this research context, we had to carefully address potential selection bias issues from observable and unobservable factors. Hospitals with fewer prior breaches might be more likely to attest and subsequently have fewer breaches. In addition, we were concerned about bias resulting from unobservable factors (that is, security culture, skillful staff, well-managed healthcare systems, and so on) that influence both meaningful-use attestation and data breaches, which are simply correlated without any causal relationship. Our analysis approach that employed propensity score-matching and difference-in-differences techniques addressed both potential bias issues.

Propensity score matching pairs meaningful-use hospitals with non-meaningful-use hospitals having similar prebreach observable factors (that is, previous breach experience, size, and so on). We employed a difference-in-differences technique that compared the difference in meaningful-use hospitals' data breaches between pre- and post-breach periods with that of non-meaningful-use hospitals' data breaches. This technique isolated the effect of meaningful-use attestation on data breaches by allowing each hospital to have its own baseline of capabilities (for instance, security culture, skillful staff, well-managed healthcare systems, and so on), which are unobservable in our data.

The results indicate that the systematic and standardized approach of meaningful-use attestation improves the protection of healthcare data as well as the tracking of accidental disclosures often caused by poor data-handling standards. In particular, hospitals that attested to having reached stage 1 meaningful-use standards indeed saw reduced external breaches. However, hospitals that achieved meaningful use also experienced short-term increases in accidental breaches resulting from mishandled data but eventually realized longer-term reductions in such inadvertent disclosures. The increase in accidental breaches in the first year after attestation might seem surprising, but it shows that attestation leads to the discovery of more accidental disclosures (or better compliance with breach notification rules). This discovery then drives improvement, as we see such breaches significantly decreasing over time.[8]

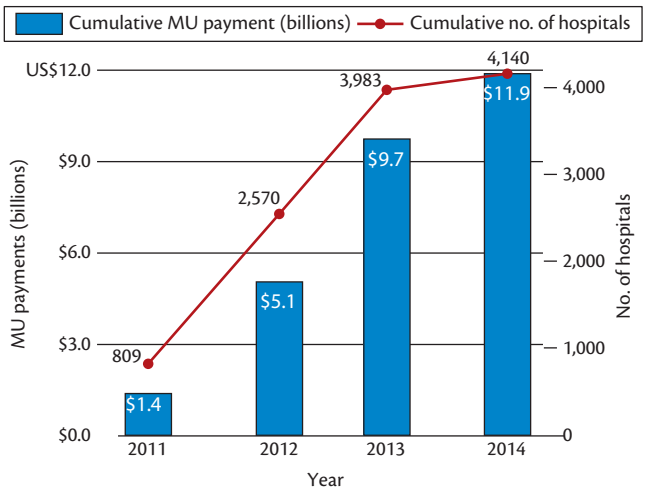

Figure 4. Federal payments to hospitals and the numbers of hospitals attesting to meaningful use (MU) of EHRs. The bars and line depict the cumulative payments to and cumulative numbers of hospitals attesting to MU of EHRs, respectively. (Source: Centers for Medicare & Medicaid Services.)

Patients' Awareness of Security Breaches

HITECH's breach-reporting rules also reduce information asymmetry by giving patients information about security performance. In markets in which patients can choose from among multiple hospitals, security performance information should enable them to make choices based on their security preferences. Our recent research investigated market reaction to data breaches by analyzing both the short-term and cumulative impact of breaches on changes in patient visits. Our analysis addressed potential selection bias in the data. For instance, hospitals with more patient visits likely have more IT resources and, subsequently, better security performance. In addition, hospitals with well-integrated EHRs might achieve both better data protection and more patient visits (this information wasn't included in our data). Thus, data breaches could be correlated with patient visits but not affect them. To mitigate the selection bias issues, we employed propensity score matching and difference-in-differences techniques. After controlling for the selection bias that exists in most organizational performance research, we found that although data breaches didn't affect patients' short-term choices, the cumulative effect of data breaches over three years significantly decreased hospitals' outpatient visits

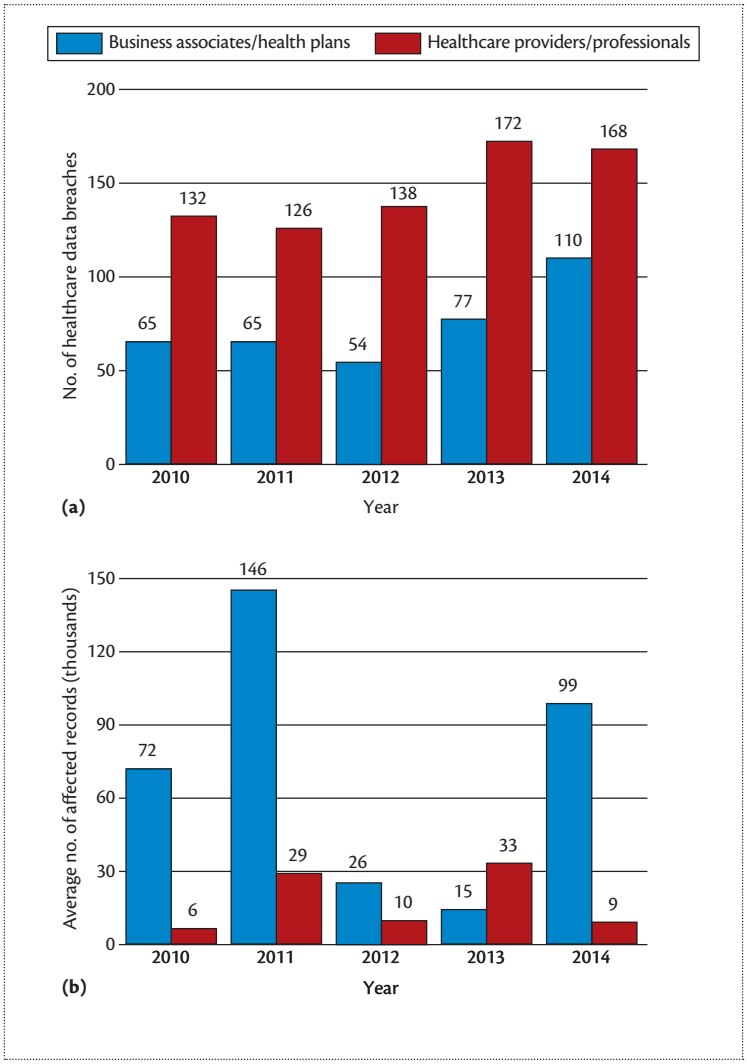

Figure 5. Data breaches and affected records by organization type: (a) the number of data breaches and (b) the average number of affected records. Although data breaches occurred more frequently in healthcare providers than in business associates, the average size of each data breach was much larger for business associates than for healthcare providers. (Source: US Department of Health and Human Services website.)

and admissions in competitive markets.[9] As we might expect, in geographic markets with little hospital choice, patient volumes were unaffected by breaches.

Public Goods

Last, we consider the *public-good* nature of information security as an important economic factor. Economic theory describes public goods as those things that are *nonexcludable* and *nonrivalrous*. That is, when made available, public goods are generally available for the benefit of all, and when consumed by one, they don't impair the consumption by another. Streetlights are a good example of both characteristics.

Although the private provision of security is important for firms operating in competitive markets, security also has strong public-good characteristics. Healthcare data is shared among healthcare providers, business associates, and payers. In this environment, one healthcare organization with high security capability could be adversely affected by a data breach incurred elsewhere in the healthcare network. The value of this public good is typically not realized by any one organization, and thus health organizations again undervalue security investment. On the positive side, security investments can benefit from what economists call *positive externalities*—security investments at any point in the healthcare network benefit all players.[7]

In fact, data breaches have occurred in nearly every part of the healthcare supply chain. Figure 5 shows that although two-thirds of data breaches occurred in hospitals and doctors' offices, the average number of affected records is much larger in breaches arising from business associates such as insurance plan administrators. This finding implies that although occurrences of business associate breaches are relatively low, their potential impact is huge. To date, incentives programs such as HITECH have focused on hospitals and doctors. Given the public-good nature of healthcare security, such programs should be expanded across all types of healthcare organizations.

Despite the ambiguities of healthcare security costs and benefits, market mechanisms can nudge healthcare organizations toward effective, proactive, and voluntary security actions. However, the effectiveness of market mechanisms suffers from the economic forces of the imperfect US healthcare market. Thus, market-driven investments must be supplemented with regulator intervention across all types of healthcare organizations. However, such regulatory intervention should focus on reinforcing the economic impact of information

security rather than simply trying to force specific behavior.

Around the world, governments are taking steps to drive EHR adoption, but with different views on security and privacy. Government-funded incentives supported by national strategies seem to generate the most significant EHR adoption, with notable examples in Nordic countries, the UK, Germany, and Canada.[10] However, policies related to personal data protection vary, such as Canada's Personal Information Protection and Electronic Documents Act, the EU's Data Protection Directive, Hong Kong's Privacy Ordinance, and the UK's National Health Service directives. Although security and privacy norms might vary across countries due to philosophical differences regarding the government's role in the commercial sector, our experience suggests that encouraging self-motivated, proactive investment is an important element of success. ■

Acknowledgments

This research was partially supported by a collaborative award from National Science Foundation award CNS-1329686. The views and conclusions in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the National Science Foundation.

References

1. A. Appari and M.E. Johnson, "Information Security and Privacy in Healthcare: Current State of Research," *Int'l J. Internet and Enterprise Management*, vol. 6, no. 4, 2010, pp. 279–314.
2. L.J. Camp and M.E. Johnson, *The Economics of Financial and Medical Identity Theft*, Springer, 2012.
3. M.S. Gaynor, M.Z. Hydri, and R. Telang, "Is Patient Data Better Protected in Competitive Healthcare Markets?," *Workshop Economics of Information Security* (WEIS 12), 2012; http://weis2012.econinfosec.org/papers/Gaynor_WEIS2012.pdf.
4. D. Charles, M. Gabriel, and M.F. Furukawa, "Adoption of Electronic Health Record Systems among US Non-federal Acute Care Hospitals: 2008-2013," ONC Data Brief, no. 16, Office of the National Coordinator for Health Information Technology, May 2014; https://www.healthit.gov/sites/default/files/oncdatabrief16.pdf.
5. "Breaches Affecting 500 or More Individuals," US Dept. Health and Human Services, 2015; https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
6. J. Kwon and M.E. Johnson, "Health-Care Security Strategies for Data Protection and Regulatory Compliance," *J. Management Information Systems*, vol. 30, no. 2, 2013, pp. 41–65.
7. J. Kwon and M.E. Johnson, "Proactive versus Reactive Security Investments in the Healthcare Sector," *MIS Q.*, vol. 38, no. 2, 2014, pp. 451–472.
8. J. Kwon and M.E. Johnson, "Meaningful Healthcare Security: Does "Meaningful-Use" Attestation Improve Information Security Performance?," *Workshop Economics of Information Security* (WEIS 14), 2014; http://weis2014.econinfosec.org/papers/KwonJohnson-WEIS2014.pdf.
9. J. Kwon and M.E. Johnson, "The Market Effect of Healthcare Security: Do Patients Care about Data Breaches?," *Workshop on the Economics of Information Security* (WEIS 15), 2015; http://weis2015.econinfosec.org/papers/WEIS_2015_kwon.pdf.
10. J. Hiller et al., "Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): US and EU Compared," *Boston University J. Science & Technology Law*, vol. 17, no. 1, 2011, pp. 1–39.

Juhee Kwon is an assistant professor of information systems in the College of Business at the City University of Hong Kong. Contact her at juhee.kwon@cityu.edu.hk.

M. Eric Johnson is the Ralph Owen Dean and Bruce D. Henderson Professor at the Owen Graduate School of Management at Vanderbilt University. Contact him at eric.johnson@owen.vanderbilt.edu.