Would Increased Regulation Reduce the Number of Information Breaches?

Mark L. Huson  
Texas A&M University-San Antonio, USA  
mlhuson@tamsua.tamu.edu

Barbara Hewitt  
Texas State University, USA  
Bh05@txstate.edu

Abstract

Private Personally Identifiable Information (PII) is increasingly stored and lost by a variety of organizations. The retail, healthcare, technology, banking, and gaming industries as well as many government agencies have been particularly hard hit by high visibility security breaches that compromised millions of individual’s records. Decisions to protect information are not always based on good risk management practices and can often be affected by the need to comply with an industry or government regulation. We examine the effectiveness of regulation within several industries to determine whether increased regulation would result in a reduction in information compromises.

1. Introduction

This century has seen an increase in security breaches affecting personal data from organizations such as Egghead, Citigroup, EBay, Travelocity [1], TJX Corporation [2], Target, Home Depot [3], JP Morgan Chase [4], Anthem, [5], and the Office of Personnel Management (OPM) [6] for the United States government. The loss of this data has resulted in major financial burdens as companies and agencies contend with resolving security issues while notifying customers, paying fines, and taking losses in reputation and business. The TJX breach, widely believed to be the result of weak wireless security, will ultimately cost the corporation between $256 million and $4.5 billion when all the impacts are included [2]. Most breaches involve far fewer personal records and can be statistically analyzed. According to the Ponemon Institute, the average security breach for businesses in all sectors results in a cost of $51 (India) to $201 (United States) per record, with medical sector records being the most expensive, while retail and public records cost the least per capita. The average cost of a breach ranges from $1.37 million in India, to $5.85 million in the United States, with an average of approximately 29,000 records per breach [7].

The total cost for many breaches have yet to be determined, including Target, Michael’s, and Neiman Marcus. Damage to these corporations extends beyond the immediate financial loss, into other areas of operation. There is a loss in the trust and confidence of consumers and the costs and other impacts on the financial industry to replace compromised credit card numbers. We also see the start of the managerial impact. Gregg Steinhafel was asked to step down as CEO of Target, following their late 2013 security breach. The information compromised in these breaches is often sold to individuals around the world, blurring any geographic component to the crime.

Government organizations are not immune to compromise. Over the years there have been several compromises of military veterans’ information, with millions of veterans affected. During congressional hearing on the security of veterans’ personal information, it was revealed that the records of more than 20 million veterans had been compromised in a series of attacks from 2010 to 2013 [8, 9]. Government civilians are also at risk. In April 2015, OPM announced the compromise of 4.2 million current and former federal worker records that occurred from late 2014 and early 2015. The attackers are presumably from China, [10, 11]. During the investigation into this breach, OPM discovered the compromise of an additional 21.5 million records related to government and contract employees seeking security clearances. This breach included information of 1.8 million non-applicants, predominately spouses and co-habitants of the applicants [6].

The need for companies to develop comprehensive risk management programs evolves as rapidly as the technology it is designed to secure. Risk assessment and risk management are often viewed, like most security efforts, as having a poor return on investment. As a result, many companies forgo conducting a complete risk management process to discover and address the shortcomings of their security posture. This is due in part to the “negative externalities” of losses due to cyber security lapses [12]. While the cost of protection such as free credit monitoring is paid by the company, many other expenses are often borne by the individuals whose
information was compromised or financial institutions who must replace the credits cards for each compromised account.

For some organizations, including government agencies such as the VA and OPM and health care institutions, regulations require specific steps and controls to protect information, such as implementing risk management programs and developing policies regarding the handling and safeguarding of information. The Federal Information Security Management Act (FISMA) states in section 3544(b),

Each agency shall develop, document, and implement an agency-wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source… [13].

This research examines the current legal and regulatory requirements for different industries. We then explore the potential impact of these regulations on information protection at organizations. We also explore whether changes in the statutory and regulatory environment would provide potential benefits to these organizations by decreasing the likelihood of a breach.

2. Current Legislative and Regulatory Requirements

The general structure of the legal environment both government and commercial entities face in the United States is that laws are written and passed by congress, signed into law by the president, and then implemented through regulations written and supervised by government agencies. The laws are usually written to address a specific industry or type of information. Sometimes industries self-regulate to protect information, such as the Payment Card Industry Security Standards Council.

For the purposes of this work, we focus on the industries of payment card and credit card handling, government agencies, financial institutions, and health care. The specific laws and regulations we address are the Payment Card Industry Digital Security Standards, Federal Information Security Management Act, Graham-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act. The following sections address each area.

2.1. Payment Card Industry Data Security Standard (PCI DSS)

PCI is an industry standards organization founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. It has developed standards for the credit card industry for protecting card holder data. There are three sets of standards. The first is PCI PIN Transaction Security which affects device manufacturers. PCI PA-DSS is a standard for use by software developers. PCI DSS is the most commonly used standard, which affects all entities that process credit cards as a means of payment.

The PCI DSS standards are prescriptive and include best practices for protecting card holder data in the form of 12 requirements [14]:

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied default passwords and settings
3. Protect stored cardholder data (encrypt stored data)
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

Card accepting organizations are evaluated for compliance with these twelve steps.

2.2. Federal Information Security Management Act (FISMA)

FISMA provides a framework for protecting federal (U.S. government) computer systems. Implementation guidance is provided by the National Institute of Standards and Technology (NIST) with the principle documents being Federal Information Processing Standard (FIPS) 199, which provides categorization guidelines for information systems, FIPS-200, which provides minimum security requirements by addressing seventeen areas of controls, and NIST Special
Publication (SP) 800-53 which lists recommended security controls based on the security category of the information system [15, 16, 17]. As stated earlier, federal agencies are required to have a risk management program. This program is based on a risk assessment of the systems and information the management plan addresses and should implement controls in the seventeen areas: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity [16]. FISMA also includes reporting requirements described in NIST SP 800-37. Federal agencies are required to provide continuous monitoring of their systems and can use the results of that monitoring to meet the annual FISMA security control assessment requirement. Each agency receives an annual grade on FISMA compliance.

The FISMA risk management framework defines a six step process for managing the security lifecycle of systems and information. A graphical representation of the framework, along with the supporting NIST documentation is provided in Figure 1.

2.3. Graham-Leach-Bliley Act (GLBA)

The Graham-Leach-Bliley Act of 1999 removed the restriction on financial institutions to perform only one type of service for customers (banking, investment, and insurance), allowed those institutions to market or share customer information (with the ability of customers and consumers to “opt-out”), and provided for the protection of the private information of those same customers and consumers. The term “financial institutions” has a broad interpretation that includes real estate appraisers, tax return preparers, non-bank loan or mortgage lenders, banks, financial advisors, and others.

One requirement of GBLA is known as the safeguards rule and it sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information [19]. This rule requires financial institutions under the Federal Trade Commission (FTC) to develop and
implement an information security program containing
the following elements [19]:
1. Designate an employee or employees to
coordinate the institution’s information
security program.
2. Identify reasonably foreseeable internal
and external risks to the security,
confidentiality, and integrity of customer
information that could result in the
unauthorized disclosure, misuse, alteration,
destruction or other compromise of such
information, and assess the sufficiency of
any safeguards in place to control these
risks.
3. Design and implement information
safeguards to control the risks identified
through a risk assessment, and regularly
test or otherwise monitor the effectiveness
of the safeguards’ key controls, systems,
and procedures.
4. Oversee service providers by taking
reasonable steps to select and retain service
providers that are capable of maintaining
appropriate safeguards for the customer
information at issue; and requiring your
service providers by contract to implement
and maintain such safeguards.
5. Evaluate and adjust your information
security program in light of the results of
the testing and monitoring.

Other federal regulations affect the practices of
financial institutions but do not directly address the
protection of private information.

2.4. Health Insurance Portability and
Accountability Act (HIPAA)

Passed in 1996 and administered by the Department
of Health and Human Services (HHS), HIPAA uses two
rules to address security concerns under the act. The
Privacy Rule addresses use and disclosure of
individually identifiable health information. One goal
of the rule is
to assure that individuals’ health information is
properly protected while allowing the flow of health
information needed to provide and promote high
quality health care and to protect the public’s health
and well-being [20].
This rule limits when protected information can be used
or disclosed to those instances specifically mentioned
under the rule and when the subject of the information
has given their authorization in writing.
The second rule is the Security Rule, which defines
what information is covered, and what administrative,
physical, and technical safeguards must be in place to
protect electronic protected health information. Those
entities with access to this information must:
1. Ensure the confidentiality, integrity, and
availability of all e PHI they create,
receive, maintain or transmit;
2. Identify and protect against reasonably
anticipated threats to the security or
integrity of the information;
3. Protect against reasonably anticipated,
impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

HIPAA is non-prescriptive in that it allows the
covered entities (clinics, doctors, hospitals, etc.) to
determine the appropriate security measures based on
the size complexity and capability of the entity, its
technical, hardware, and software infrastructure, the
costs of the security measures, and the likelihood and
potential impact of the risks to the protected information
[21, 22]. HHS does provide some guidance on the
process all entities should use in determining how to
comply with the Security Rule requirements. The
recommended process is:
1. Assess current security, risks, and gaps
2. Develop an implementation plan by
reading the security rule, reviewing the
addressable implementation specifications
and determining the security measures
3. Implement the solutions
4. Document the decisions made
5. Reassess periodically

These steps essentially represent a risk assessment
process and a decision by the entity as to what security
measures should be implemented to safeguard the
information based on the entity’s ability to implement
the safeguard.

3. The Effectiveness of Regulations

How effective are regulations? There is no simple
answer. The usual dimensions for evaluating
regulations include whether the regulation accomplishes
its goals and whether it is being followed or not. The
regulations studied here are not a panacea for all security
woes, but there is evidence that they do provide some
amount of protection.

In a study about the impact of laws on security
breaches, Romanosky, et al., determined after a law was
introduced there was a 6.1 percent reduction in data
compromises [23]. Verizon’s 2010 study reported that
PCI compliant organizations were 50% less likely to be
attacked [24]. Clearly some regulations do contribute to
the goals they are designed to address.

But regulations are not always followed. When the
TJX Corporation data breach occurred, the company
was in compliance with only 3 of the 12 PCI DSS requirements covering encryption, access controls, and firewalls [25]. During the time period reported on in congressional testimony, the VA Office of the Inspector General (OIG) repeatedly reported on security issues which contributed to the compromise of more than 20 million records [9]. Similarly, the OPM compromise, which resulted in the loss of at least 4 million and as many as 21.5 million records also occurred after repeated reports of failures to comply with regulatory requirements [10]. The breach was discovered after the OPM installed a program to detect breaches. The cause of the breach is the stolen credentials of a government contractor [26].

Even though HIPAA has been in place for over 10 years now and HITECH was introduced in 2009 was made enforceable in 2013, many health care breaches occurred recently. As many as 80 million American’s personal identifiable information was compromised when Anthem a health insurance company was compromised between December 2014 and January 2015 [5]. While early reports indicated that the data was not encrypted, more recent reports indicated that Anthem had encrypted the data. Anthem stated this was a sophisticated attack; however, the attack actually included a social engineering attack where at least 5 key employees provided their credentials during a phishing attack including the database administrator whose credentials had been used to encrypt the data and later by the hackers to unencrypt it. University of California Los Angeles (UCLA) Health Systems (HS) reported a security breach on May 5, 2015 [5]. Over 4.5 million records of both patients and providers were compromised. The data acquired by the hackers in this breach included names, social security numbers, medical record numbers, and date of birth. The data was not encrypted. While HIPAA does not explicitly require encryption, the health care organization must provide an explanation for why the organization chose not to encrypt the data as well as a reasonable and acceptable alternative that was used instead of encryption [20].

4. Arguing Both Sides

What is a regulation? Webster’s defines regulation as “the act of regulating” or “an authoritative rule dealing with details or procedure,” as in a safety regulation, or “a rule or order issued by an executive authority or regulatory agency of a government and having the force of law” [29].

4.1. What Makes a Good Regulation?

The failures to protect private information call to question whether regulation is a viable way to ensure information is safeguarded. Common sense would suggest that a good regulation is one that was effective (achieved its goal or objective), required minimal burden on the affected entities (simple to implement, low cost), and that would be followed by all organizations within the target population.

However; not all regulations achieve these goals, but they and the enacting legislation provide the means for government to address social and societal concerns regarding the protection of private information. For example, HIPAA was first introduced in August 1996 but health care organizations were not required to comply with the Privacy Rule until April 2003 and the Security Rule in April 2005. Unfortunately, problems with enforcement still exist over ten years later and the backlog of complaints is tremendous with only 8000 of the 23,000 complaints from 2008 being investigated. Many individuals were skeptical as to whether HIPAA would be too cumbersome or expensive, or would not provide any value or impact [28]. In the end, it has been fortified by both the Health Information Technology for Economic and Clinical Health Act (HITECH) and the American Recover and Reinvestment Act that were passed in 2009 to increase the penalties for violations of HIPAA and strengthen requirements. Many healthcare organizations have been fined under the new ruling including CVS Caremark for $2.25 million, Cignet Health Center for $4.35 million, Alaska Department of Health and Social Services for $1.75 million [28], and more recently Cancer Care Group for $750 thousand [29]. While these rules and penalties are strong encouragers for health care organizations to secure the patient records, healthcare organizations are still experiencing many breaches.

4.2 Why Regulate?

What are reasons to regulate? Hart argues that the concept of regulation covers both criminal and tort law, and that in the presence of negative externalities, it makes sense for government or the courts to discourage a laissez-faire attitude towards one’s behavior [30]. Hart also mentions the differences in regulating behaviors when contractual relationships may exist. Regulations restrict the contract, but can be desirable in the following cases: asymmetric information; bounded rationality; the judgement proof problem; commitment problems; and influencing tastes. All play a role in the area of information security. Corresponding examples are: the holder of information knowing more about the risks than the owner; the belief that one’s information
will never be compromised; the resources necessary to bring suit might not be available to those suffering loss; public outcry regarding information breaches; and regulations proposing products from a limited number of vendors as prescriptive controls.

In a market free of regulation, the loss of PII represents a large negative externality for the individuals whose records are compromised in a breach, while the organizations collecting and maintaining such information have little incentive, other than market pressure and reputation, to address the loss of information. In highly competitive industries market pressure would likely be sufficient to force organizations to respond without regulation (assuming consumers were informed of the breaches). In less competitive industries such pressure would be less effective. Verizon reports that 69% of consumers would be less inclined to do business with a breached organization [31].

Regulations provide uniformity by establishing a set of minimum requirements to be met. As Payne describes it, “it forces those who don’t do anything to at least do something” [32]. His article lists two other benefits of regulation, the economic impact of improved customer confidence and increased awareness of security issues at the executive management level of regulated organizations. This uniformity is brought about through auditing and enforcement mechanisms that strongly influence industries to follow their protective mandates. The consequences of non-compliance vary. Government regulations stipulate fines and/or jail time for non-compliance while self-regulating industries determine their own penalties, which may include fines and/or other sanctions. For example, PCI DSS can exclude entities from direct participation in credit card processing. This affects the bottom-line of any company found in violation through lost sales or the need to arrange for a payment handling service that can accept credit card payments.

Regulation can also ensure that less capable entities receive guidance to improve the security of the information they handle. The more prescriptive regulations, such as PCI DSS, require designated policies, procedures, and technical controls, giving organizations specific steps, such as implementing a firewall, to protect information [14].

Finally, regulations provide standards that can be used to make side-by-side comparisons of the methods used to protect information, resulting in consumers’ ability to make a “better” choice for private data protection. Just like a Better Business Bureau rating, organizations would be able to tout their regulatory compliance to potential customers.

### 4.3 Reasons Not To Regulate

The dark side of regulations must also be considered when deciding whether to regulate or not. Regulations can have a significant cost impact. For example, it was estimated that the changes to the HIPAA security rule update published in 2013 would have an impact of $100M on the health care industry [22]. Payne notes the expense is borne by both the regulator (tax dollars to audit and regulate compliance) and regulate (corporate dollars to document and remain in compliance) [32]. As Hart might point out, some corporations might choose not to comply due to the disparity between compliance costs and possible penalties, based on the proof of judgement problem [30].

Payne also explains that there are problems with deciding what to regulate in terms of rigor and level of detail, determining what metrics to use, and setting the boundaries of responsibility for systems connected to the Internet.

Even when regulations are followed, compliance does not guarantee that data will not be compromised. In fact, common wisdom is that we have reached the point where it isn’t “if” but “when” organizations will experience a data breach. For example Target, Neiman Marcus, Home Depot, Michaels were all PCI DSS compliant but were still victims of major security breaches [33]. While Home Depot was in compliance, some argue that they used a loop-hole in the PCI DSS regulations. A former employee states that security managers raised concerns about security issues as early as 2008 citing outdated software and inadequate security policies. In April 2014, the company finally addressed these issues and took precautions by encrypting the credit card data stored on its systems but full implementation did not occur across all stores until September 2014, after the systems had already been compromised. Hackers had planted malicious software that allowed them to steal millions of credit card records [34].

Data breaches are regulation agnostic. While PCI organizations have probably been the most visible, (Target, Neiman Marcus, P.F. Chang’s, Home Depot, etc.), government (VA, OPM, etc.), financial (JP Morgan), and healthcare (Anthem, Premera, and UCLA HS) organizations have all experienced the loss of private information. The disparity in approach and specificity of the various regulations highlights the difficulty in creating effective regulations. Whether detailed and prescriptive (PCI), thorough and broad (FISMA), or broad and descriptive (HIPAA), each has its failing.

The regulatory process usually allows exceptions or grace periods for entities found short of the requirements. From a practical perspective, it would be
economically disruptive to both individual organizations and markets if such exceptions were not granted. And once given, when should the exception or grace period be revoked? TJX Corporation, the VA, and OPM all were allowed to continue operations with known shortcomings in their security profiles. What choice is there? Should failure to comply result in a shutdown in operations? Before saying yes, consider Verizon’s estimate that only 20% of businesses are in PCI compliance [31]. But Verizon also points out, compliance does not represent the complete story. A comparison across the 12 PCI requirements show that companies that fail to maintain compliance are more likely to be breached. The data suggests a strong correlation between non-compliance and increased susceptibility to data compromise. At the same time, compliance does not guarantee that no data breach will occur (though Verizon’s after breach forensics analysis showed that none of the set of compromised companies they examined was fully compliant). When it comes to a government agency, should the business of government stop if systems are found to be out of compliance? Are all measured aspects of compliance equal, or are some more directly indicative of security problems. What of the citizens who potentially rely on the services provided by the government entity? For example, should veterans be denied treatment if the VA is not in FISMA compliance? Or should other government agencies be unable to manage their personnel due to OPM’s non-compliance?

Our arguments against regulation really fall into just a few categories:

- **Cost:** it is expensive both to be regulated and to regulate
- **Practicality:** it can’t be completely effective, and forcing compliance is often not possible
- **Difficulty:** we don’t know how to write and measure effective regulations

The observed reduction in data compromises would suggest that we need regulation, but how much?

5. **Forever Vulnerable**

In their 2015 PCI Compliance Report, Verizon states, “No organization can ever be fully secure. “Secure” is an absolute and it is not possible to say with certainty that a breach cannot occur. To do so you’d need to have complete knowledge of all threats, established and emergent” [31].

As we’ve seen, compliance with regulatory standards results in a reduced likelihood of compromise. We need regulation. The standards and metrics, as well as the guidelines for implementing controls to meet the regulatory requirements are necessary to establish a baseline expectation. However, we may never be fully compliant with the standards we have.

We’ve also seen that non-compliance can lead to problems, but compliance is not a guarantee of security. We are not prepared to deny businesses and government agencies the ability to operate due to non-compliance. Nor can we prove that compliance will lead to no data compromises.

What can we do? Adding regulations to improve security might be tempting to some. What specifically would be regulated? Would they be replacements for or additions to current regulations? Would they be detailed and prescriptive or descriptive and non-specific? What impact would they have on companies and regulatory bodies? Would they reduce the likelihood of data breaches in cost effective ways?

We don’t know the answers to these questions for many of our current regulations as their total cost and effectiveness are not yet known. Perhaps our best option would be to standardize regulatory requirements across industries as much as possible. This could reduce the regulatory burden by allowing security professionals to apply their skills in a more standardized way and by establishing common requirements for regulatory bodies. Regardless, we are going to see more data compromises. As Verizon observed, “secure” is an absolute which we cannot proclaim without complete knowledge, which we will always lack.

Several other issues would need to be addressed within any new regulations especially when it comes to sanctions, such as responsibility and accountability. For example if an organization complied with the regulation but was breached would they be liable for being compliant? Would compliance prevent or reduce the liability incurred? Accountability is an especially tricky issue with the constant change of personnel at all levels within organizations. Who is accountable if a decision made years ago is the root cause of a data breach today?

We did not try to answer all of these questions in this paper. We recognize that work remains to address these in any new or revised regulations. Regardless of what regulations we might create, there doesn’t appear to be a need for an “increase” in regulation, only for an increase in the effectiveness of regulation.

6. **Conclusion**

We’ve examined the regulatory environment as it relates to the compromise of personally identifiable information. While the industries examined have different regulations, each with its own approach to addressing information security, all face the same problem. Compromises will happen, regardless of the
regulations. Though compliance may be an issue in some of the more spectacular breaches, there are operational and economic reasons to allow even non-compliant entities to continue operating. Even with evidence that some regulation can reduce losses due to data compromise, there is no indication that an increase in regulation would result in fewer compromises.

7. References


