Legally "Reasonable" Security Requirements: A 10-year FTC Retrospective

Travis D. Breaux
Carnegie Mellon University
Institute for Software Research
5000 Forbes Avenue, 5210 Wean Hall, Pittsburgh, PA 15213
e-mail: tdbreaux@ncsu.edu

David L. Baumer
Department of Business Management
North Carolina State University
2801 Founders Drive, Box 7229, Nelson Hall, Raleigh, NC 27695
e-mail: david_baumer@ncsu.edu

Abstract. Growth in electronic commerce has enabled businesses to reduce costs and expand markets by deploying information technology through new and existing business practices. However, government laws and regulations require businesses to employ reasonable security measures to thwart risks associated with this technology. Because many security vulnerabilities are only discovered after attacker exploitation, regulators update their interpretation of reasonable security to stay current with emerging threats. With a focus on determining what businesses must do to comply with these changing interpretations of the law, we conducted an empirical, multi-case study to discover and measure the meaning and evolution of "reasonable" security by examining 19 regulatory enforcement actions by the U.S. Federal Trade Commission (FTC) over a 10 year period. The results reveal trends in FTC enforcement actions that are institutionalizing security knowledge as evidenced by 39 security requirements that mitigate 110 legal security vulnerabilities.

Keywords. Requirements, security, reasonability, legal compliance, case study.

1 Introduction

In the United States and Europe, businesses employ information technology to reduce costs and automate business practices. This technology includes a complex integration of network hardware and custom and proprietary software that introduces new security vulnerabilities that expose companies to e-crime and identity theft when consumer information is inadequately secured. For example, the 2007 E-Crime Watch Survey found 671 U.S. companies reported that unauthorized access and use of information, systems and networks was among the top three e-crimes that they experienced [CUC07].

Unauthorized access to consumer information can lead to identity theft, which enables perpetrators to open fraudulent bank accounts using the identity of an unsuspecting consumer. Although this negative outcome is difficult to measure, the 2008 Javelin Identity Fraud Survey found that 8.1 million Americans are victims of identity fraud, which amounted to $45 billion in damages [Kim08]. Only 27% of surveyed consumers could rule out data breaches and online transactions as the source of identity theft, because 65% of consumers surveyed never knew how their information was stolen [Kim08].

Government laws and regulations require companies to employ reasonable security measures to reduce private harms such as identity theft due to unauthorized access. The U.S. Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and the broader European Directive 95/46/EC, Article 17, both require that companies employ reasonable or appropriate administrative and technical security measures to protect consumer information [BEP04]. The GLBA is a U.S. Federal law enacted by U.S. Congress in 1998 to allow consolidation among commercial banks. The GLBA Safeguards Rule is U.S. Federal regulation created in reaction to the GLBA and enforced by the U.S. Federal Trade Commission (FTC). The Safeguards Rule requires companies to implement a security plan to protect the confidentiality and integrity of consumer personal information and requires the designation of an individual responsible for compliance. Because these laws and regulations govern consumer personal information, they can lead to new requirements for information systems for which companies are responsible to comply.

The act of compliance includes demonstrating *due diligence*, which is defined as “reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations” [Gar04]. Reasonableness in software systems includes industries standards and may allow for imperfection [Ott09]. Lawyers representing firms and other organizations, regulators, system administrators and engineers all face considerable challenge in determining what constitutes “reasonable” security measures for several reasons, including:

1. Compliance changes with the emergence of new security vulnerabilities due to innovations in information technology;
2. Compliance requires knowledge of specific security measures, however publicly available best practices typically include general goals and only address broad categories of vulnerability; and
3. Compliance is a best-effort practice, because improving security is costly and companies must prioritize security spending commensurate with risk of non-compliance. In general, the costs of improved security are certain, but the improvement in security depends on unknown variables and probabilities outside the control of companies.

In the United States, when evidence of legal non-compliance emerges, i.e., a firm in possession of personally identifying information does not employ reasonable security to protect that information, a regulatory enforcement action ensues in which a regulator files a legal complaint against a company. The legal complaint lists individual violations of relevant laws that are alleged to have occurred with supporting facts; some of these facts describe security vulnerabilities. We define legal compliance as a company’s ability to maintain “a defensible position in a court of law” [BAK06] and we believe reasonable security under the law should prevent or reduce the impact of legal complaints.

This paper reports the results of an empirical, multi-case study to discover and measure the meaning and evolution of “reasonable” security. The study examined 19 regulatory enforcement actions that occurred over a 10-year period and that were conducted by the U.S. Federal Trade Commission (FTC), the independent agency regulating commerce in the United States. This study first examines what constitutes *unreasonable* security by itemizing vulnerabilities identified by the FTC in these regulatory enforcement actions. We define reasonable security using two artifacts: mitigating security requirements that the investigator deduces from examining these vulnerabilities and FTC-imposed remedies. Because legal violations are often pursued in response to resulting damages, this study also estimates the magnitude of private harms experienced by customers during acts of non-compliance.

The remainder of this paper is organized as follows: related work appears in Section 2; the case study design is presented in Section 3 with findings discussed in Section 4; threats to validity appear in Section 5; and we conclude with discussion and summary in Section 6.

2 Related Work

Researchers in requirements engineering have recognized the need to develop new methods and tools to identify privacy and security requirements. Early work includes the adaptation of existing requirements engineering methods, such as problem frames, agent-models, goal-oriented models and use cases to the problem of eliciting security requirements. These adaptations include abuse frames [LNI03], authoritative agents [MMZ07], intentional anti-goals [Lam04] and abuse and misuse cases [SO05, WWH08], respectively. Combined with security patterns [KCC03], these techniques focus elicitation on identifying security vulnerabilities from which mitigating security requirements are derived. Frameworks such as the SQUARE method [MS05], Lee et al.'s ontology-driven method [LGM06] and Haley et al.'s satisfaction argument-driven method [HLM08] all use a similar paradigm, driven by identifying threats to assets and then using specialized techniques to reduce these threats in the form of security requirements. In this paper, we introduce a process for identifying legal and security vulnerabilities that, when exploited by attackers, correspond to legal violations. From these documented security vulnerabilities, we derive mitigating security requirements with the intent to define what constitutes reasonable security under these laws. From a legal case history spanning 10 years, we observe how reasonable security has evolved in the eyes of one U.S. Federal regulator.

Legal compliance is defined as an organization's ability to maintain "a defensible position in a court of law" [BAK06]. In requirements engineering, work to support legal compliance with privacy and security regulations includes research on models, methods and frameworks. Models have been proposed to represent rights, permissions and obligations [BA05] and acts of delegation and permission [MMZ08] and to manage traceability [BA07,GAP07]. Methods include a legal requirements acquisition method, including a technique to balance rights and obligations [BVA06], a method to identify hidden assumptions [DED06], and a requirements prioritization method based upon legal exceptions [BA08]. Frameworks have been proposed to manage traceability between goal models and legal documents [GAP07] and manage accountability and traceability through refinement and delegation [BAS08]. Finally, research in legal requirements has yielded reusable catalogues of privacy requirements [TOP02] and information access constraints [BA08]. Recently, Breaux et al. have demonstrated that criminal court proceedings provide rich sources of security scenarios and abuse cases [BLO09]. This paper extends this body of work by investigating a frequently occurring and *intended* legal ambiguity, what constitutes reasonable security, to help companies avoid or defend against legal complaints from regulators.

Recent industry and legal analysis further illustrates the extent of the problem investigated in this study. The 2008 Data Breach Investigations Report, a survey of over 500 data breaches over a 4 year period by the Verizon Business Risk Team, reports that most of the data breaches studied result from a "combination of events" with 87% of these breaches being avoidable with appropriate security controls [BHV08]. The results of our study show a similar trend, that reasonable security includes a combination of security measures to thwart attacks and prevent or diminish violations of security laws. With an increased incidence of data breaches, regulators will consider such breaches as foreseeable and come to expect companies to implement reasonable and appropriate security measures [Bishop]. Although legal analysis shows that private lawsuits due to data breaches typically fail, the FTC has been successful in settling cases based on an emerging definition of reasonable security [Han08]. Legal experts note that this definition is not uniform across U.S. laws [Cio07, Sie07], is evolving and relies upon a security program, leaving the technical details to be defined by security experts [Sme07]. This paper seeks to bridge this knowledge gap by analyzing the FTC security cases to understand the evolution of reasonable security in terms of technical safeguards, which address documented security vulnerabilities that led to violations of law.

Management and technical standards provide organizations broad guidance in how to plan, implement and monitor security controls. Unlike U.S. laws that require broad security goals to be achieved (e.g., privacy notices, confidentiality, etc.), security standards provide technical guidance that can be used to strategize how to comply with security laws. The Control Objectives for Information and related Technology (COBIT) [ISA07], the ISO/IEC 17799:2005, subtitled ``Code of practice for information security management" [ISO05a] and the U.K. Office of Government Commerce (OGC) Information Technology Infrastructure Library (ITIL) [OGC07] are prominent management standards that describes personnel, process and resource planning. Alternatively, the ISO/IEC 15408:2005, also called the Common Criteria, is a technical standard that describes functional security requirements [ISO05b]. Failing a detailed understanding of what constitutes reasonable security under a regulation governing the healthcare industry, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, organizations are resorting to security standards for guidance [Mer04]. However, the SANS Institute found that the HIPAA Security Rule requirements are not contained in ISO/IEC 17799, including requirements for preventing, monitoring and terminating access to patient health information [Bor03]. Thus, companies cannot arbitrarily rely on security standards to comply with security laws. This paper includes empirical evidence that companies must look at security laws, in addition to standards, to ensure reasonable security in information technology. While this paper considers what constitutes "reasonable security" under the FTC in terms of specific security requirements, future work should consider how this definition of reasonable security aligns with existing security standards. While security laws are written by lawmakers to address significant past or potential commercial failures, security standards are written by industrial trade-groups and independent security bodies. The extent to which a security standard can be used to comply with a law remains an open question [Ott09].

3 Case Study Design

The research reported in this paper employs a descriptive, multi-case study design [Cre03] directed at discovering constructivist knowledge claims and outcomes, as opposed to explanatory case studies that examine underlying causes [Yin03]. This section describes the research questions, units of analysis and case study materials used to conduct this study.

Reasonable security is a non-functional requirement that is periodically adjusted by regulators to address changes in business practices, information technology and public concern. What is "reasonable" depends on multiple, complex, time-dependent factors, such as what vulnerabilities exist in the marketplace, both in products and through the surrounding physical environment in which they are deployed. In this multi-case study, we seek to measure the meaning and evolution of reasonable security across 10 years of regulatory enforcement actions within the United States. This measurement is conducted in terms of regulatory enforcement actions that identify specific vulnerabilities that culminated in legal violations and that lead to remedial obligations. In addition, we consider which security requirements can be used to mitigate these vulnerabilities with the intent to avoid the legal violations in the future. Taken together, reasonable security can be measured by the change in vulnerabilities, obligations and security requirements.

Figure 1 illustrates the legal lifecycle that traces the units of analysis (in bold), which are defined in Section 3.2. The units of analysis include legal vulnerabilities, which if exploited may lead to the private harms, not all of which are observable. Where the FTC observes these harms in newspapers or as consequences of reporting required by other laws and, if the company is deemed culpable, the FTC may produce a regulatory enforcement action. Our case study demonstrates a method to derive remedial obligations, which are high-level goals that require a company to act to reduce legal vulnerabilities, and mitigating security requirements, which address the cited legal vulnerabilities. These artifacts produced by our method comprise a partial representation of what constitutes "reasonable" security.

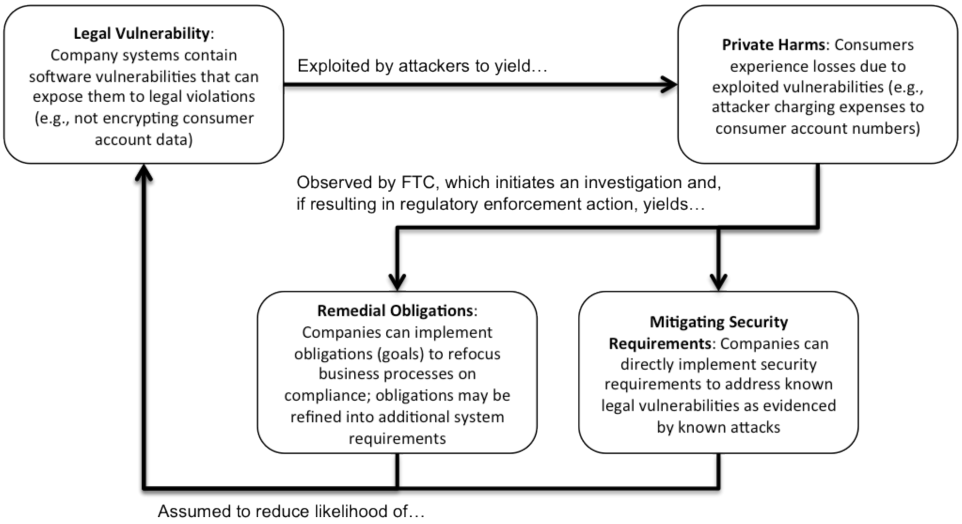
Legal Vulnerability: Company systems contain software vulnerabilities that can expose them to legal violations (e.g., not encrypting consumer account data)
Exploited by attackers to yield…
Private Harms: Consumers experience losses due to exploited vulnerabilities (e.g., attacker charging expenses to consumer account numbers)
Observed by FTC, which initiates an investigation and, if resulting in regulatory enforcement action, yields…
Remedial Obligations: Companies can implement obligations (goals) to refocus business processes on compliance; obligations may be refined into additional system requirements
Mitigating Security Requirements: Companies can directly implement security requirements to address known legal vulnerabilities as evidenced by known attacks
Assumed to reduce likelihood of…

Figure 1: Overview of the analysis procedure to identify requirements, obligations and harms

3.1 Research Questions

The following research questions investigate the non-functional requirement “reasonableness” by identifying security that is *unreasonable*, evidenced by business practices or lack thereof that constitute legal vulnerabilities, private harms and government imposed remedies (see Section 3.2 for definitions of these terms as the units of analysis). The research questions in this study are:

RQ$_1$: What organizational practices constitute legal vulnerabilities that lead to violations of security law?

RQ$_2$: What security requirements can be used to mitigate legal security vulnerabilities?

RQ$_3$: What trends exists, if any, in government enforcement of laws that require reasonable security?

RQ$_4$: What are the private harms and government-imposed remedies for non-compliance?

The answers to RQ$_1$ correspond to documented legal vulnerabilities that affect security. These vulnerabilities, which are extracted using a procedure illustrated in Section 3.3, are used by an analyst to systematically specify mitigating security requirements, which answer RQ$_2$ and directly measure the meaning of reasonable security within the narrow scope of this study. If reasonable security evolves over time, RQ$_3$ asks what trends are observable over the 10 year period studied. We answer this question by examining the results of the deriving the mitigating security requirements to identify any changes in security focus. Finally, because the FTC often responds to failures that result in damages, RQ$_4$ measures both the private harms and the government-imposed remedies that were sought in response to those harms.

We now discuss case study materials and units of analyses that were used to answer these research questions.

3.2 Case Materials and Units of Analysis

This study examined 19 regulatory enforcement actions by the FTC over a 10-year period from 1999-2008 (see Table 1). In Table 1, each case is classified by one of the following types: illegal disclosure (ID), illegal collection (IC) or data breach (DB). The FTC identified these actions as prominent security cases that violate the FTC Act (15 U.S.C. §§41 et seq), governing deceptive and unfair trade practices. If companies post online privacy policies ensuring that consumer information is secure prior to contradictory reports that company internal controls failed to protect such information, these policies may be instruments of deceptive and unfair trade practices under the FTC Act. In addition, the U.S. Gramm-Leach-Bliley Act of 1996 (GLBA) Safeguards Rule (16 C.F.R. §314) and the U.S. Children's Online Privacy Protection Act of 1998 (COPPA) Rule (16 C.F.R. §312), requiring parental consent prior to collecting children’s personal information, both require businesses to post privacy policies ensuring consumers that their information is protected by reasonable security measures. The FTC claims that the legal violations in these security cases could have been avoided with properly implemented security requirements.

Table 1: Nineteen FTC Security Cases Ordered by Settlement Date

Type	Company	Settled
ID	Geocities	02/1999
ID	Toysmart	07/2000
ID	Eli Lilly	05/2002
IC	Microsoft	12/2002
DB	Guess	08/2003
DB	Tower Records	06/2004
ID	Gateway Learning	09/2004
DB	PetCo	03/2005
ID	CartManager	03/2005
DB	BJ’s Wholesale Club	06/2005
DB	ChoicePoint	01/2006
DB	CardSystems Solutions	02/2006
DB	DSW	03/2006
DB	Guidance Software	11/2006
DB	Life Is Good	01/2008
ID	Goal Financial	03/2008
DB	ValueClick	03/2008
DB	Reed Elsevier	03/2008
DB	TJX	03/2008

For each of the cases in Table 1, the materials acquired for this study include the *complaint*, which describes the federal charges against the company, the *agreement* or *judgment*, which describes the remedy to be implemented by the company, and the *press release* by the FTC, which summarizes additional details from the case, including private harms that result from the alleged legal violations.

In case study research, units of analysis describe the elements of data to be collected and analyzed [Yin03]. The following units of analysis, which consist of concepts and their definitions, were identified and documented in the case materials using the analysis procedure described in Section 3.3:

- *Legal vulnerabilities*, which describe specific acts or failures to act that are susceptible to violations of law;
- *Mitigating security requirements*, which describe acts that businesses can take to prevent legal violations.
- *Remedial obligations and refrainments*, which describe acts that businesses must or must not perform to remedy a complaint.
- *Private harms*, which describe acts that negatively affect consumers or positively affect businesses at cost to consumers.

The following analysis procedure provides the analyst a means to identify, classify and extract statements and phrases that represent instances of the above units of analysis. During this acquisition process, we identified heuristics that can be used to reproduce this study and to validate the acquired artifacts; the heuristics are reported in Section 4 with the case study findings. These artifacts represent nominal measures of the range of phenomena described by the units and can be compared to each other to identify similarities and differences using metrics that we developed in prior work [BAB08]. To compensate for errors in subjective interpretation that results from classifying phrases and sentences, multiple analysts must apply the units of analysis to the case study materials during the acquisition process. In the following section, we present each step to acquire these artifacts with examples to illustrate both the ease and difficulty in conducting this analysis.

3.3 Analysis Procedure

The analysis procedure consists of the following steps: (1) identify legal vulnerabilities from complaints; (2) derive mitigating security requirements from legal vulnerabilities;

(3) identify remedial obligations from agreements and judgments for each case selected; (4) identify private harms from press releases and complaints. Figure 2 illustrates these steps in order of application, including the case materials and units of analysis. Each numbered step is completed for all of the cases studied prior to proceeding to the next step to reduce unwanted bias resulting from a preliminary results introduced by completing a single case.

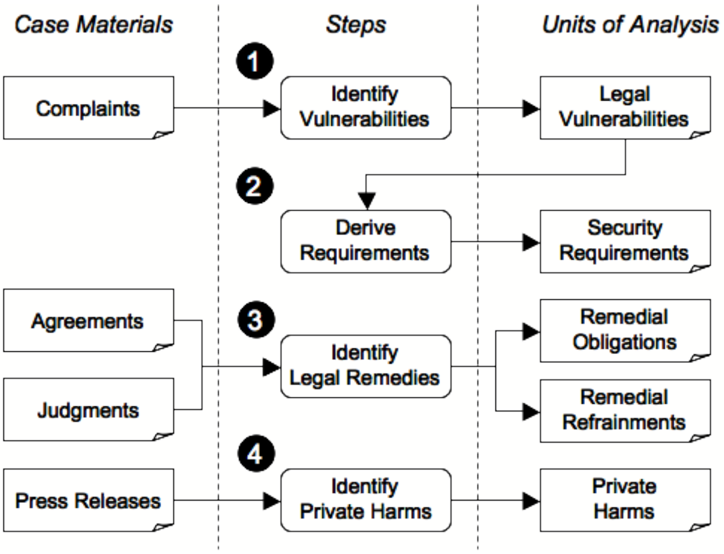

Figure 2: Overview of the analysis procedure to identify requirements, obligations and harms

We now discuss the separate procedures to identify legal vulnerabilities, legal remedies and private harms followed by applying the definitions of the units of analysis to the case materials.

3.3.1 Identify legal vulnerabilities

The analyst identifies legal vulnerabilities by analyzing legal complaints (step 1, Figure 2). The complaints we analyzed are written according the U.S. Federal Rules of Civil Procedure, Rule 10, which requires the plaintiff, such as the FTC, to "state its claims or defenses in numbered paragraphs, each limited as far as practicable to a single set of circumstances" [FRCP]. Legal systems in other jurisdictions that use a similar format, which itemizes legal vulnerabilities in the form of numbered claims and defenses, should be amenable to this type of analysis. Consider the following excerpt from the complaint by the FTC against TJX Companies, Inc. (TJX), FTC File No. 072-3055:

> "7. Since at least July 2005, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks. In particular, respondent:
>
> (a) created an unnecessary risk to personal information by storing it on, and transmitting it between and within, in-store and corporate networks in clear text;
>
> (b) did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to in-store networks without authorization;"

The above excerpt highlights several facts that the FTC alleges in that complaint constitute "unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a)." The first step in the analysis procedure is to itemize each fact that represents a legal vulnerability, in some cases by performing *case-splitting* on individual sentences [BA05], which works as follows: for a sentence with phrases A, B and C, we split "A… B or C" into "A… B" and "A… C". The fact in paragraph (7)(a) above is separated into two legal vulnerabilities (LV) TJX-LV1 and TJX-LV2 as follows using case-splitting:

TJX-LV1: Created an unnecessary risk to personal information by storing it on in-store and corporate networks in clear text.

TJX-LV2: Created an unnecessary risk to personal information by transmitting it between and within in-store and corporate networks in clear text.

From the excerpt, the case "storing it on… networks" was separated from the case "transmitting it between and within… networks" using case-splitting to yield separate vulnerabilities. During this step, every effort is made to preserve the original language and avoid amending the legal vulnerability by introducing or removing information. This preservation ensures that we can reuse this data for later analyses.

3.3.2 Derive mitigating security requirements

The nature of these cases and laws under which the corresponding complaints were charged concern privacy and security claims that were unfair, deceptive or misleading, as evidenced by documented security exploits. Consequently, the legal vulnerabilities identified in the first step are also security vulnerabilities. We derive mitigating security requirements as a means to classify the vulnerabilities and propose a definition of reasonable security that evolves with each case. In our findings in Section 4, we discuss how this evolution unfolds over the 10-year period.

The analyst derives mitigating security requirements from vulnerabilities (see step 2, Figure 2) by beginning with the complete set of vulnerabilities from all cases studied and by sorting the vulnerabilities using the security categories, presented in Table 2. These categories were derived during this case study using grounded analysis, in which theory derived from a dataset if valid for that dataset [GS67]. Because these categories are grounded in the legal vulnerabilities cited by the FTC in this study, this list of security categories may be incomplete for other studies and purposes in other domains. However, several of these categories appear in related work. For example, the categories *Access*, *Consent* and *Notification* appear in the FTC Fair Information Practice Principles and Antón/Earp privacy taxonomy [AE04] and the categories for *Encryption*, *Monitoring*, *Patching*, *Retention*, *Training* and *Verification* have corresponding guidelines in the NIST Information Security Handbook [BHW06].

Table 2: Security categories used for sorting legal security vulnerabilities

Category Keywords		
Access	Monitoring	Retention
Consent	Notification	Training
Encryption	Patching	Verification

Recall the legal vulnerability TJX-LV1 from the previous section. TJX-LV1 can be mitigated in several ways, including: (1) not storing personal information; (2) storing personal information for a limited time; (3) not storing personal information in clear text; and so on. Each strategy reduces risk while potentially interfering with business practices in different ways and adding to costs. For example, the first strategy "not storing person information" likely obstructs a business practice, but reduces risk significantly, whereas the second strategy fits the *Retention* category and reduces risk by reducing availability, but does not address the vulnerability "in clear text" stated in vulnerability TJX-LV1. However, using the *Encryption* category, the analyst can mitigate this vulnerability using the third strategy, which yields security requirement (SR) SR18:

SR18: Require encrypted information during storage.

The security categories help broaden the focus of the analyst's mitigation strategy by encouraging the analyst to consider alternatives and enabling requirements reuse.

Because a single legal vulnerability can present multiple issues to be considered, the analyst must consider each category in the process of deriving security requirements. During reuse, if a subsequent legal vulnerability contains additional detail, the reused requirement may be further refined to address this new detail. Conversely, vulnerabilities with less detail should yield generalized requirements with less detail. Because we are interested in investigating trends over time, we cannot ignore these subtle variations in detail. For example, Guess-LV3 describes a vulnerability that uses the verb "maintain", which can refer to information both in storage and in transit. Security requirement SR17, obtained during this study, is specified more generally to mitigate this second vulnerability.

Guess-LV3: Failed to maintain personal information obtained from consumers in an encrypted format.

SR17: Require encrypted information.

In Section 4, we illustrate how this change in detail corresponds to an evolution in the meaning of reasonable security. In addition, we present examples from the study where the analyst must make assumptions to derive mitigating security requirements.

3.3.3 Identify legal remedies

In the United States, regulatory enforcement actions generally conclude with agreements between the regulator and the company, or judgments against the company. An agreement or judgment contains orders, in the form of actions that are required (obligations) or prohibited (refrainments) by the company for the purpose of remedying the alleged legal violations. The procedure to identify these remedial obligations and refrainments (step 3, Figure 2) employs the method developed by Breaux et al. to identify legal rights, permissions and obligations [BVA06]. Consider the following excerpt from the agreement and consenting order between the FTC and TJX (FTC Case No. 072-3055):

> "IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, ***shall***, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."

The procedure first directs the analyst to identify modal keywords, such as "shall" that indicates an obligation; see Breaux et al. for a list of modal keywords [BVA06]. For the purposes of this study, the remedial obligations (OB) and refrainments (R) were simplified by removing details that enable comparing remedies across different cases. For example, obligation OB25 was acquired from this excerpt:

OB25: Implement a comprehensive information-security program.

The missing detail that was removed in OB25, while unnecessary to broadly compare remedies in this study, is necessary to correctly reason about and implement the intended, government-imposed remedy; a topic that is beyond the scope of this study.

3.3.4 Identify private harms

The procedure to identify private harms (step 4, Figure 2) is applied to legal complaints and press releases by the FTC. For example, the FTC press release for the TJX case described several harms in the following excerpt [FTC08]:

> "An intruder exploited these failures and obtained tens of millions of credit and debit payment cards that consumers used at TJX's stores, as

> well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. Banks have claimed that tens of millions of dollars in fraudulent charges have been made on the cards and millions of cards have been cancelled and reissued."

From these sources, we are concerned with identifying consumer harms to measure the scope of the exploited vulnerability. Complex factors affect the order of magnitude for an exploited vulnerability in terms of *number of affected consumers*. For example, the safeguards at a bank may reduce the threat to their account holders when corresponding account numbers are exposed through a merchant's unprotected information systems. Two exploited vulnerabilities that appear to yield harms in different proportions to each other may have equal or inverse *potential* for harms. For example, a breach similar to the above excerpt can be measured by "actual harms" using the number of consumers affected or fraudulent charges recorded by the bank. The "potential harms," however, may include the total credit limits for these customers that could be used for fraudulent purchases before the bank could take corrective action to halt this criminal activity. Thus, this information is relevant to generally consider the extent of harms but is not adequate to rank vulnerabilities by severity.

4 Study Findings

The multi-case study yielded several important findings that companies can use to understand the meaning and evolution of reasonable security in the United States. These findings are organized chronologically by the date of the final agreement or judgment, called the settlement year, because from the date a legal complaint is filed, the regulatory agency can receive public comments and amend the complaint by adding or removing legal violations.

Table 4 summarizes the number of legal vulnerabilities by security category (the rows) for each year in the study (the columns); empty cells represent zero vulnerabilities under that category and year. Each vulnerability is mapped to a mitigating security requirement: for the 110 vulnerabilities identified, 39 unique mitigating security requirements were derived. The last column contains the row totals for each category of legal vulnerability. We organized the security categories and weighted them by the number of vulnerabilities in each category. From this analysis, we observe the FTC focus across the following broader topics: information handling (access, encryption and retention) ranking highest (53.6%), followed by security process improvement (monitoring, patching, training and verification) ranking second (32.7%) and consumer management (consent and notification) ranking last (13.6%).

During the acquisition of legal vulnerabilities and remedial obligations, we identified several heuristics that cover the range of phenomena described by the units of analysis (see Section 3.2). In each instance, the vulnerabilities were contained in numbered paragraphs with at most 2-3 vulnerabilities stated in each paragraph (see Section 3.3.1). Among the 110 vulnerabilities reported in Table 4, two-thirds or 74 vulnerabilities were all described by two phrase heuristics: "failed to… [act]", "failure to… [act]", and "did not… [act]" where [act] is a domain-specific verb. In the remaining 36 vulnerabilities, the descriptions concern actions performed by companies that led to legal violations. In these cases, the analyst must rely on the paragraph structure, which was found to be sufficient, to identify the corresponding vulnerabilities.

The bottom two rows in Table 4 summarize the number of security cases per year and the mean number of legal vulnerabilities identified per case per year. A linear regression was performed on this data and determined that a statistically significant increase in the number of legal vulnerabilities per case per year (p = 0.024, R^2 = .598, *confidence* = 95%) occurred for these 19 security cases. The statistical means and the y-intercept with slope that approximates this trend are presented in Figure 2. The low R^2 is attributable to the 2002 Microsoft and 2006 ChoicePoint cases, which are landmark cases that incurred an unusually large number of legal vulnerabilities. As illustrated in Table 4 and discussed in the remainder of this section, the upward trend is likely due to a change in security focus and institutionalization (accretion) of security knowledge by the FTC.

Table 4: Distribution of Legal Vulnerabilities by Security Category and Settlement Year[1]

Security Category	Settlement Years from 1999 to 2008								Totals
	‘99	‘00	‘02	‘03	‘04	‘05	‘06	'08	
Access		1	2	3	1	3	15	15	40
Encryption				1		5	3	6	15
Retention						1	2	1	4
Monitoring			3			1	6	3	13
Patching						1	2	3	6
Training			2					1	3
Verification			1	1	4	1	2	5	14
Consent			2						2
Notification	2	2	3		2	2		2	13
Totals	2	3	13	5	7	14	30	36	110
Cases	1	1	2	1	2	3	4	5	19
Vulnerability/ Case	2.0	3.0	6.5	5.0	3.5	4.7	7.5	7.2	5.8

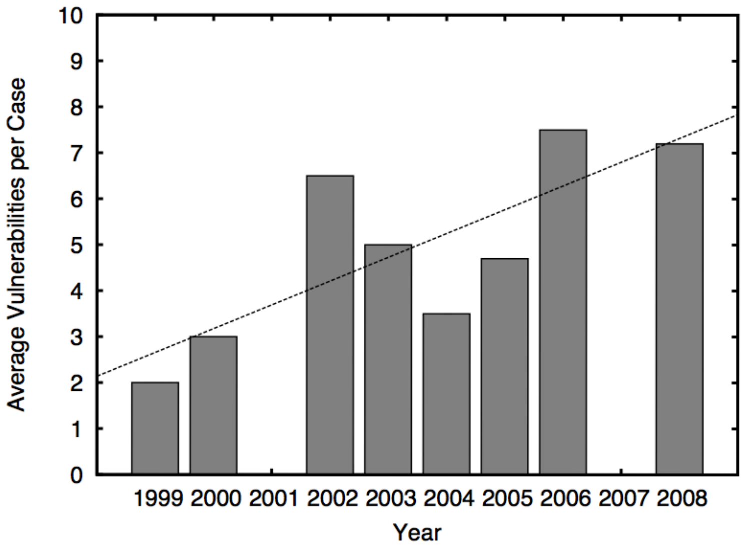

Figure 2: Upward Trend in Mean Number of Vulnerabilities per Case per Year

The remainder of this section presents findings obtained by analyzing the mitigating security requirements. In Section 4.1, we discuss two trends: (1) a shift in focus from consumer management to information handling that is not obvious in Table 4 but is evidenced by changes in the proportion and quality of security requirements; and (2) an increased focus on security process improvement requirements. Finally, we discuss an emerging emphasis on physical security that is dispersed across multiple security cases in Section 4.2.

4.1 FTC Shifts Focus on Security

Over the past 10 years, the security focus at the FTC appears to have shifted from consumer management requirements (consent and notification), towards information handling requirements (access, encryption and retention). Table 5 presents 25 mitigating

[1] The FTC Privacy Initiative lists no cases settled in 2001 and 2007.

security requirements, acquired during step 2 of the analysis (see Figure 2), that comprise the security categories for access, encryption, retention, consent and notification. The columns correspond to the 19 security cases in chronological order, with the settlement years across the bottom row. The shaded portions of the table illustrate that the majority of consumer management requirements (86.4%) correspond to cases prior to 2005, whereas the majority of information handling requirements (73.3%) correspond to cases from 2005 to 2008. A possible explanation for this shift in security focus is the California Security Breach Notification Law (Cal. Civil Code §1798.29), which became effective in 2003 and requires companies to notify consumers whenever their personal information is compromised due to unauthorized access. Today, at least 44 states have enacted similar laws. An increase in consumer data breach notifications, as seen in the ChoicePoint case, may lead the FTC to investigate these breaches under their enforcement authority for unfair and deceptive trade practices. Thus, explaining why the FTC security focus has shifted from notification to information handling and security process improvement.

In addition to the change in focus, we observe an increase in the specificity of mitigating security requirements due to an increased level of detail in legal vulnerabilities. In 2008 alone, we observe four new security requirements: the requirement of unique user ids (SR13), login suspension (SR15), periodic password changes (SR16) and third-party controls (SR18). Prior to 2005, the FTC only cited vulnerabilities from e-commerce web access points (SR3), such as information portals and storefronts. In addition, from 2005 to 2008 the FTC refined their focus on access to distinguish intranet (SR1), Internet (SR2), physical (SR4) and wireless network (SR5) access points in legal complaints. During the same period, encryption (SR21) was refined to distinguish between information in storage (SR22) and information in transit (SR23). Finally, whereas Table 4 appears to show a consistent focus on notification-related vulnerabilities, the breakdown behind Table 5 reveals an 83% decrease after 2004 in user notifications about information use by providers (SR31) and third-parties (SR32). While not a user notification, we do observe a business-to-business notification requirement for third-party companies to notify their information providers about how they use consumer information (SR33). This requirement has important consequences for companies that sub-contract or outsource processing of sensitive consumer information.

Table 6 presents nine mitigating security requirements that comprise the categories for monitoring, patching, training and verification to support security process improvement. The shaded table area shows that the majority of security process improvement requirements (69.4%) were derived from legal vulnerabilities identified between 2005-2008. Consistent with Table 5, where we observe a shift towards access-related requirements, in Table 6 we observe an increase in monitoring for unauthorized access (SR34) during 2005-2008.

Whereas the steps in the analysis procedure described in Section 3.3 to identify legal vulnerabilities and remedial obligations and refrainments rely on phrase heuristics to improve the reliability in the acquisition of these artifacts, the mitigating security requirements are *derived artifacts* that an analyst infers from the acquired vulnerabilities. Consider vulnerabilities CP-LV1 from the ChoicePoint case and RE-LV7 from the Reed Elsevier case, below.

CP-LV1: Accepted for verification purposes documentation that included facially contradictory information, such as different business addresses on federal tax identification documents and utility statements, without conducting further inquiry to resolve the contradiction

RE-LV7: Allowed customers to create new credentials without confirming that the new credentials were created by customers rather than identity thieves

Both vulnerabilities CP-LV1 and RE-LV7 were mitigated by the broadly-stated security requirement SR12 “Require controls to verify physical identity.” The high degree of abstraction and the loss of detail in SR12 is appropriate for this study, because we are interested in discovering broad trends in evolving security requirements across multiple cases as described above and in Tables 5 and 6. That said, these two vulnerabilities describe fairly complex issues. In CP-LV1, for example, the legal vulnerability is that

ChoicePoint did not check the documentation provided by customers for contradictory information (a procedure that can presumably be implemented in software for at least partial automation). In RE-LV7, however, we assume that identity thieves would not use their own identities but instead use fake identities. Therefore, to mitigate this vulnerability SR17 requires that the customer's physical identity only be valid (not fake).

4.2 Emphasis on Physical Security

The multi-case study reveals that physical vulnerabilities, which can be exploited to gain access to consumer information, must be mitigated to ensure that consumers receive a reasonable degree of security. These vulnerabilities were highlighted by the 2006 ChoicePoint and 2008 Goal Financial cases and include the following legal vulnerabilities: (GF-LV2) failing to restrict access to consumer information stored in paper files; authorizing a physical identity using facially contradictory (CP-LV2) or incomplete (CP-LV5) information; (CP-LV8) furnishing consumer information to third-parties beyond the scope of their physical identity or stated need; (CP-LV9) continuing to permit access when a physical identity was found to be inconsistent or invalid; and (GF-LV4) failing to assess the risks of storing consumer information in paper files. Table 7 presents the mitigating security requirements that correspond to these vulnerabilities.
The requirements in Table 7 are not explicit in the security law cited by the FTC in their legal complaints. However, they offer further empirical evidence that physical security is an important component to the FTC's interpretation of reasonable security under the law.

Table 7: Requirements for Mitigating Physical Security-related Vulnerabilities

Vulnerability	ID	Security Category	Physical Security Requirements
GF-LV2	SR4	Access	Require authentication at physical access points
CP-LV5	SR7	Access	Require complete information on physical identity
CP-LV2	SR12	Access	Require controls to verify physical identity
CP-LV8	SR14	Access	Require information access consistent with physical identity
CP-LV9	SR27	Monitoring	Require periodic validation of physical identity
GF-LV4	SR39	Verification	Require physical vulnerability testing

4.3 Scope of Private Harms

Among the 19 security cases studied, only 14 case documents (i.e., complaints and press releases) include explicit references to the magnitude and types of harms experienced by consumers. Figure 3 presents the number of consumers affected for each of the 14 cases in chronology of the case settlement date; the y-axis is logarithmic. The harms affected consumer information stored in paper and electronic files and in database tables, 47% of which included credit card, debit or bank account information. The number of affected consumers ranges from 669 customers in the 2002 Eli Lilly case, involving an e-mail divulging sensitive consumer information, to over 10 million consumers in the 2006 CardSystems Solutions case, which involved unsecured transmissions of credit card data across networks. The cost of these vulnerabilities, for which data is incomplete, includes up to tens of millions of dollars of fraudulent charges reported by banks in the 2008 TJX case. The 2005 CartManager case, where the company illegally sold consumer information to third parties for $9,100 in profit, exposed over 1 million consumers to potential misuse of their financial information. A similar sale of consumer information, which netted $4,600 in profit for the company, was reported in the 2004 Gateway Learning case. For that case, we do not know the number of consumers affected.

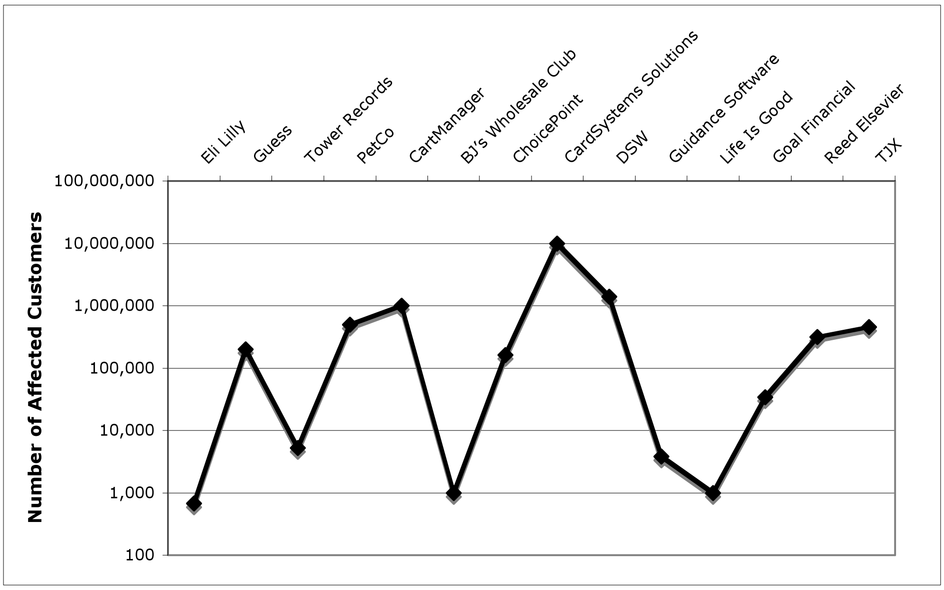

Figure 3: Number of Affected Consumers Harmed by Exploited Vulnerabilities

4.4 Remedial Obligations and Refrainments

The 19 security cases all ended in an agreement or judgment that includes new obligations and refrainments that the defendants are required to implement, in addition to any legal requirements as part of their normal civic responsibility. The study yielded 34 obligations and 18 refrainments. All of these artifacts were identified using the phrase heuristics “it is ordered that…” or “it is further ordered that…”, which precede the remedial obligations. Refrainments (i.e., “shall not”) appeared as supporting statements and exceptions to the obligations. These statements were preceded by the phrase heuristic “provided, however, …” and a condition that should be satisfied before the refrainment was applicable to the company.

Table 8 presents the remedial obligations that comprise the information security program imposed by the FTC in 15 cases. Table 8 shows the remedial obligation ID and description. In general, these obligations require companies to establish (O21) and maintain (O22) a security program by designating appropriate personnel to oversee the program (O23). The program requires companies to identify risks (O24) and design (O26), implement (O27) and monitor (O28) safeguards to control such risks. In addition, companies are required to evaluate (O30) and adjust (O31) the security program in response to risk monitoring and to have qualified personnel conduct annual written reviews (O25). Recently, in six of the 15 cases, companies are also required to ensure service providers, such as sub-contractors, employ reasonable security safeguards (O34).

Whereas only one of the 15 cases was cited for a violation of the GLBA Safeguards Rule (16 C.F.R. §314), most of the remedies in Table 8 align with legal requirements stated in the Rule. Table 8 illustrates how the FTC has institutionalized knowledge of security best practice in at least two additional ways: (1) in the drafting the GLBA Safeguards Rule to conform to such security practices; and (2) in requiring these same security practices as remedial obligations for whenever corporate internal security controls (a) lead to actual or potential data breaches (an unfair practice) or (b) are found to be inconsistent with privacy policies (a false or misleading statement).

Table 8 Obligations for Information Security Program

ID	Remedial Obligation Description	Safeguards Rule
O21	ESTABLISH an information security program for the protection of personally identifiable information collected from or about consumers	§314.3(a)
O22	MAINTAIN an information security program for the protection of personally identifiable information collected from or about consumers	§314.4(a)
O23	DESIGNATE appropriate personnel to coordinate and oversee the program	§314.4(a)
O24	IDENTIFY reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information	§314.4(b)
O25	CONDUCT an annual written review by qualified persons to monitor and document compliance with the program	——
O27	DESIGN reasonable safeguards to control the risks identified through risk assessment	§314.4(c)
O28	IMPLEMENT reasonable safeguards to control the risks identified through risk assessment	§314.4(c)
O29	MONITOR the effectiveness of the safeguards’ key controls, systems, and procedures	§314.4(c)
O30	EVALUATE the information security program in light of the results of the testing and monitoring	§314.4(c)
O31	ADJUST the information security program in light of the results of the testing and monitoring	§314.4(e)
O34	EMPLOY reasonable steps to retain service providers capable of appropriately safeguarding personal information	§314.4(d)

The agreements and judgments, called the *order*, from all 19 cases include routine obligations required to monitor compliance, presented in Table 9. These obligations include the requirement to maintain (O8) and, upon request, provide to the FTC (O9) documents relating to compliance, including a report that describes how the company has complied with the order (O12). In addition, companies are required to deliver the order to current and future principals and employees (O10) and notify the FTC of changes in the corporation (O11). Finally, for the three cases that involve judgments, the FTC takes a more invasive tactic, requiring companies to permit access to offices storing relevant documents (O19) for the purpose of inspecting and copying those documents (O20).

All 18 of the refrainments identified in this study concern consent and notification practices and apply to cases in which a false or misleading statement was made in a privacy policy. In Table 10, these refrainments are presented with the cases in which they were cited by settlement year. The shaded area corresponds to the pre-2005 period where the majority (86.4%) of security requirements concerning consent and notification practices were identified (see Section 4.1, Table 5). From 1999 to 2008, we observe a convergence from 12 different remedial refrainments concerning various consent and notification practices, prior to 2006, to one remedial refrainment (R7) after 2005 that broadly describes misrepresentations of privacy, confidentiality, and security. This is further evidence that the FTC, while emphasizing information handling and security process improvement practices in legal vulnerabilities, has not stopped requiring companies to maintain consistent policies and practices. In addition, 100% of the ten cases that result in refrainment R7 also result in remedial obligation O25, which requires the implementation an information security program.

Table 9: Obligations for Compliance Monitoring

ID	Remedial Obligation
O8	MAINTAIN a print or electronic copy of all documents relating to compliance
O9	PROVIDE a print or electronic copy of all documents relating to compliance to the FTC for inspection and copying, upon request
O10	DELIVER the order to all current and future principals and employees having responsibilities with respect to the subject matter of this order
O11	NOTIFY the FTC of any change in the corporation that may affect compliance obligations arising under this order
O12	PROVIDE the FTC a report about how they have complied with this order
O19	PERMIT the FTC access to any office or facility storing documents
O20	PERMIT inspection and copying of all documents relevant to any matter contained in this order

5 Threats to Validity

Case studies ask broad research questions to examine phenomena that cannot be controlled in a laboratory and thus require the investigator to address threats to construct, internal and external validity and reliability [Yin03]. Threats to validity that arose during the design, conduct and analysis of this multi-case study are now discussed.

Construct validity concerns efforts to reduce subjectivity in the data collection procedure, which can result in bias in the findings. In this study, the 19 cases were selected from a list of 24 cases highlighted by the FTC as representative of their privacy initiative. Five cases were removed from the data collection and analysis procedure that concern overt acts to defraud customers allegedly condoned by corporate management. These acts correspond to deceptive trade practices, whereas the focus of this study is on unfair trade practices and false or misleading statements, wherein companies have fallen short of commercially reasonable security standards. For the ValueClick case that includes both allegedly intentional acts to defraud consumers and failures to implement reasonable security measures, the study was limited to the legal vulnerabilities, private harms and government-imposed remedies that concern reasonable security. In addition, each step in the analysis procedure (see Section 3.3, Figure 2) was completed for all cases prior to beginning the subsequent step to avoid having preliminary findings from the first cases studied disproportionately influence the study of the remaining cases. Furthermore, the derivation of the mitigating security requirements from legal vulnerabilities requires expert knowledge that is variable and subject to bias. To reduce bias, the security categories were employed by the investigator to view each security vulnerability from multiple viewpoints. This enabled the investigator to equally consider alternatives influenced by a broad but finite set of security categories before selecting the most appropriate requirement.

Internal validity concerns causal inferences made during explanatory case studies. In Section 4.1, we infer trends using a statistical regression and proportions but stop short of inferring what events may cause this trend to appear.

To address external validity, which refers to the generalizability of the study findings, we employed replication logic using a standard analysis procedure (see Section 3.3). During this procedure, we sought to reuse mitigating security requirements and remedial obligations and refrainments. To avoid losing critical distinctions that emerge overtime in the specification of security requirements, the reuse procedure sought to avoid generalize requrieemnts for the sake of reuse. For example, a requirement SR21, which requires encryption, was not reused to address the vulnerability mitigated by requirement SR23, which requires encryption *during transit*. This approach enabled us to generalize findings across multiple cases for the purpose of answering our broad research questions, but also enabled us to preserve subtleties necessary to identify changes in security knowledge over time. However, because the FTC cases studied represent the worst offenders, our findings may not represent so-called “near misses”, which yield no enforcement actions by the FTC.

Lastly, the reliability of this study was reinforced through the use of a case study database, which facilitated tool-supported analysis and enabled the comparison of mitigating security requirements and remedies during reuse [Yin03].

6 Discussion and Summary

The multi-case study reported in this paper sought to define and measure the evolution of reasonable security by examining regulatory enforcement actions in 19 security cases under the FTC over the last 10 years. The study findings include a trend wherein the mean number of legal vulnerabilities cited per case per year is increasing. For logistical reasons, we believe this upward trend will likely diminish in proportion to the sophistication of attack scenarios. In other words, the number of vulnerabilities per legal complaint likely corresponds to the complexity of the scenarios being investigated and the available knowledge of security failures applied by regulators during their investigations – an important topic for future study.

The impact of this study on software engineers is two-fold. First, the resulting security requirements provide a partial definition of what constitutes “reasonable security” in attempt to address vulnerabilities cited by the FTC. These requirements can be used to prioritize security reviews of software design and testing to build a case for compliance through due diligence. Second, these requirements and the vulnerabilities they mitigate provide insight into the broader security context to which their software may be deployed. This context is further illustrated by actual violations of law that have cost on the order of millions of dollars across the retail and financial industry. Therefore, while security standards provide general guidance on how to improve software security, legal vulnerabilities (and their mitigating security requirements) provide a current picture of both legal and security risks.

In addition, this study found a shift in focus from consumer management (consent and notification) to information handling requirements (access, encryption and retention) and security process improvement requirements (monitoring, patching, training and verification). This trend is further evidenced by a refinement from early legal vulnerabilities that are broadly stated to historically later vulnerabilities that target specific technological failures with known solutions based on best security practices. An inverse effect is observed in remedial refrainments, in which early refrainments describe specific and varied consent and notification practices while later refrainments are homogeneous and broadly stated.

The remedial obligations imposed by the FTC and described in Section 4.4 provide broad guidance to companies; for example, “establish an information security program” or “maintain documentation relating to compliance.” However, the obligations fall short of explaining *how* companies can ensure that the steps they have taken are consistent with the full extent of these obligations. Because the security requirements that were identified and presented in Tables 5 and 6 only cover the vulnerabilities discovered by the FTC, they may not cover the full range of requirements required to avoid a regulatory enforcement action. Moreover, because the security focus is known to change over time, what constitutes reasonable security also changes. Therefore, we believe future work is needed to identify new tools and techniques that support an agile community of security practice that holistically monitors events and reifies best practice so that industry adapts to the technical requirements necessary to satisfy shifting legal interpretations.

While this study generalizes from multiple cases to deduce a meaningful definition of reasonable security in terms of security requirements that can be applied broadly, companies are encouraged to appreciate the nuances of specific FTC security cases. For example, the following highlights from individual cases were not empirically quantified by this study but were informally observed:

1. The 2002 Microsoft case (FTC Case No. 012-3240) illustrates that company failures to comply with legal security requirements need not result in damages before the regulating agency enforces these requirements by filing a legal complaint.
2. The 2005 CartManager case (FTC Case No. 042-3068) shows that the FTC distinguishes between consumer notification and business-to-business notification of intended information use. Companies that sub-contract or outsource processing of sensitive consumer information may be vulnerable to the same legal violation.
3. The 2008 Reed Elsevier case (FTC Case No. 052-3094) illustrates the potential harms resulting from poor password and account management practices (e.g., by multiple users sharing the same user id), which is expressly regulated for health care providers by the HIPAA Security Rule, §164.312(a)(2)(i).

Finally, because this study derives reasonable security from evidence of *unreasonable* security (i.e., via legal complaints), the mitigating security requirements are likely under representative of the holistic FTC interpretation. To investigate which requirements may be missing from the definition of reasonability presented herein, one may consider performing a conformance or gap analysis between the mitigating security requirements identified in this paper and security standards that represent best practices. The results of this analysis may show which security standards provide coverage for the vulnerabilities identified by the FTC. For the remaining requirements in the "gap," one could then inquire whether these play an important supporting role not amenable to the public vulnerabilities cited by the FTC. In addition, researchers may focus on emerging threats to consumer privacy that may result in new kinds of harms, such as behavioral advertising or consumer data mining.

References

[AE04] A.I. Antón, J.B. Earp. "A requirements taxonomy for reducing Web site privacy vulnerabilities", Requirements Engineering Journal, Spring, 9(3): 169-185, 2004.

[BHV08] W.H. Baker, C.D. Hylender, J.A. Valentine, *Data reach Investigations Report: A Study Conducted by the Verizon Business RISK Team*, 2008.

[BEP04] David L. Baumer, Julie B. Earp, and J.C. Poindexter, "Internet privacy law: a comparison between the United States and the European Union," *Computers and Security*, 23(5): 400-412, 2004.

[Bis06] D.A. Bishop, "To serve and protect: do businesses have a legal duty to protect collections of personal information?", 3 Shidler J. L. Com. & Tech. 7, 2006.

[Bor03] S. Borkin. The HIPAA final security standards and ISO/IEC 17799. *In Collect. Information Security Reading Room*. SANS Institute, July 2003.

[BHW06]P. Bowen, J. Hash, M. Wilson, "Information security handbook: a guide for managers", U.S. National Institute of Standards and Technology (NIST), Special Publication 800-100, Oct. 2006.

[BA05] T.D. Breaux, A.I. Antón, "Analyzing goal semantics for rights, permissions and obligations", *IEEE 14th International Requirements Engineering Conference*, Paris, France, pp. 177-186, Aug. 2005.

[BA07] T.D. Breaux, A.I. Antón, "A systematic method for acquiring regulatory requirements: a frame-based approach, *6th International Workshop on Requirements for High Assurance Systems (RHAS-6)*, Delhi, India, Sep. 2007.

[BA08] T.D. Breaux, A.I. Antón, "Analyzing regulatory rules for privacy and security requirements", *IEEE Transactions on Software Engineering, Special Issue on Software Engineering for Secure Systems*, 34(1): 5-20, January/February 2008.

[BAB08] T.D. Breaux, A.I. Antón, K. Boucher, M. Dorfman, 'Legal Requirements, Compliance and Practice: An Industry Case Study in Accessibility", *IEEE 16th International Requirements Engineering Conference (RE'08)*, Barcelona, Spain, pp. 43-52, Sep. 2008.

[BAK06] T.D. Breaux, A.I. Antón, C.-M. Karat, J. Karat, "Enforceability vs. accountability in electronic policies", *IEEE 7th International Workshop on Policies for Distributed Systems and Networks (POLICY'06)*, London, Ontario, pp. 227-230, Jun. 2006.

[BLO09] T.D. Breaux, J.D. Lewis, P.N. Otto, A.I. Antón, "Identifying legal vulnerabilities and critical requirements using criminal court proceedings", (In Press) *24th ACM/SIGAPP Symposium on Applied Computing (ACM SAC'09)*, Honolulu, Hawaii, March 2008.

[BAS08] T.D. Breaux, A.I. Antón, E.H. Spafford, "A distributed requirements management framework for compliance and accountability", (In Press) Computers and Security, Oct. 2008.

[BVA06] T.D. Breaux, M.W. Vail, A.I. Antón. "Towards compliance: extracting rights and obligations to align requirements with regulations", *IEEE 14th International Requirements Engineering Conference (RE'06)*, Minneapolis, Minnesota, pp. 49-58, Sep. 2006

[DED06] D. Delahaye, J.-F. Etienne, V.V. Donzeau-Gouge, "Reasoning about airport security regulations using the focal environment", *2nd International Symposium on Leveraging Applications of Formal Methods, Verification and Validation*, Paphos, pp. 45-52, Nov. 2006.

[Cio07] C.A. Ciocchetti, "E-commerce and information privacy: privacy policies as personal information protectors," 44 Am. Bus. L.J. 55, Spring, 2007.

[CUC07] CSO magazine, U.S. Secret Service, CERT® Program, Microsoft Corp, "2007 eCrime watch survey", CSO magazine, Sep. 2007.

[Cre03] J.W. Creswell. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches, 2nd ed*. Sage Publications, 2003.

[FRCP] *Federal Rules of Civil Procedure,* revised Dec. 1, 2007.

[Gar04] B.A. Garner, editor. Blacks Law Dictionary, 8th ed., ThompsonWest, St. Paul, Minnesota, 2004.

[GAP07] S. Ghanavati, D. Amyot, L. Peyton, "Torwards a framework for tracking legal compliance in healthcare," *19th Int'l Conf. Adv. Info. Sys. Engr.*, pp. 218-232, 2007.

[GS67] B.C. Glaser, A.L. Strauss. *The Discovery of Grounded Theory,* Aldine Pub. Co., Chicago, IL, 1967.

[HLM08] C.B. Haley, R.C. Laney, J.D. Moffett, B. Nuseibeh, "Security requirements engineering: a framework for representation and analysis. *IEEE Transactions on Software Engineering* 34(1): 133-153, 2008.

[Han08] J.B. Hanson, "Liability for consumer information security breaches: deconstructing FTC complaints against businesses victimized by consumer information security breaches," 4 Shilder J. L. Com. & Tech. 11, 2008.

[ISA07] Information Technology Governance Institute, Control Objectives for Information and related Technology (COBIT), Version 4.1, 2007.

[ISO05a] ISO/IEC 15408:2005. Information technology – Security techniques – Evaluation criteria for IT security, 2005.

[ISO05b] ISO/IEC 17799:2005. Information technology - Security techniques - Code of practice for information security management, 2005.

[Kim08] R. Kim, "2008 Identity fraud survey report: identity fraud continues to decline, but criminals more effective at using all channels", Javelin Strategy and Research, Feb. 2008.

[KMS07] D. Karagiannis, J. Mylopoulos, M. Schwab. "Business process-based regulatory compliance: the case of the Sarbanes-Oxley act," *IEEE Int'l Req'ts Engr. Conf.*, pp. 315-321, 2007.

[KCC03] "Using security patterns to model and analyze security requirements", Proc. 2nd International Workshop on Requirements Engineering for High Assurance Systems (RHAS-2), Kyoto, Japan, pp. 13-22, Sep. 2003.

[Lam04] A. van Lamsweerde, "Elaborating security requirements by construction of intentional anti-models", *IEEE 26th International Conference on Software Engineering*, pp. 148-157, 2004.

[LNI03] L. Lin, B. Nuseibeh, D. Ince, M. Jackson, J. Moffett, "Introducing abuse frames for analysing security requirements", *IEEE 11th International Requirements Engineering Conference*, pp. 371-372, Sep. 2003.

[LMG06] S.W. Lee, D. Muthurajan, R.A. Gandhi, D. Yavagal, G. Ahn, "Building decision support problem domain ontology from security requirements to engineer software-intensive systems" *International Journal on Software Engineering and Knowledge Engineering*, 16(6): 851-884, Dec. 2006.

[MMZ07] F. Massacci , J. Mylopoulos , N. Zannone, "Computer-aided support for Secure Tropos," *Automated Software Engineering*, 14(3): 341-364, Sep. 2007.

[MS05] N.R. Mead, T. Stehney, “Security quality requirements engineering (SQUARE) methodology”, *Proc. Software Engineering for Secure Systems (SESS) --- Building Trustworthy Applications, ACM Software Engineering Notes*, 30(4): 1-7, 2005.

[Mer04] Rebecca T. Mercuri. The HIPAA-potamus in health care data security. *Communications of the ACM*, 47(7):25–28, 2004.

[Ott09] P.N. Otto, “Reasonableness Meets Requirements: Regulating Security and Privacy in Software”, Duke Law Journal, 2009.

[Sie07] K.M. Siegel, “Protecting the most valuable corporate asset: electronic data, identity theft, personal information and the role of data security in the information age.” 111 Penn St. L. Rev. 779, Winter 2007.

[SO05]G. Sindre, A.L. Opdahl, “Eliciting security requirements with misuse cases,” *Requirements Engineering*, 10(1): 34-44, Jan. 2005.

[Sme07] T.J. Smedinghoff, “It’s all about trust: the expanding scope of security obligations in global privacy and e-transactions law”, 16 Mich. St. Int’l L. 1, 2007.

[TOP02] S. Toval, A. Olmos, M. Piattini. “Legal requirements reuse: a critical success factor for requirements quality and personal data protection,” *IEEE Int’l Conf. Req’ts Engr.*, pp. 95-103, 2002.

[FTC08] U.S. Federal Trade Commission, “Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers’ Data”, Mar. 2008.

[OGC07] U.K. Office of Government Commerce, Information Technology Infrastructure Library, Version 3, vols. 1-5, The Stationary Office, Ltd., United Kingdom, 2007.

[WWH08] J. Whittle, D. Wijesekera, M. Hartong, “Executable misuse cases for modeling security concerns,” *IEEE 30th International Conference on Software Engineering*, Leipzig, Germany, pp. 121-130, 2008.

[WM08] M. Weiss, H. Mouratidis, “Selecting Security Patterns that Fulfill Security Requirements”, *IEEE 16th International Requirements Engineering Conference*, pp. 169-172, 2008.

[Yin03] R.K. Yin. *Case study research*, 3rd ed. In Applied Social Research Methods Series, v.5. Sage Publications, 2003.

Table 5: Shift in FTC Focus from Consent and Notice to Information Access, Encryption and Retention

ID	Security Category	Mitigating Security Requirement	Geocities	Toysmart	Eli Lilly	Microsoft	Guess	Tower Records	Gateway Learning	Petco	CartManager	BJ's Wholesale Club	ChoicePoint	CardSys. Solutions	DSW	Guidance Software	Life is Good	Goal Financial	ValueClick	Reed Elsevier	TJX
SR1	Access	Require authentication at intranet access points												●	●			●			
SR2	Access	Require authentication at Internet access points												●		●	●				●
SR3	Access	Require authentication at web access points				●		●													
SR4	Access	Require authentication at physical access points																●			
SR5	Access	Require authentication at wireless network access points										●			●						●
SR6	Access	Require authentication to access data										●									
SR7	Access	Require complete information on physical identity											●								
SR13	Access	Require unique user ids at network access points																		●	●
SR14	Access	Require information access consistent with physical identity											●								
SR15	Access	Require login suspension after multiple, failed login attempts																		●	
SR16	Access	Require periodic password changes																		●	
SR17	Access	Require strong passwords at network access points												●						●	●
SR18	Access	Require third-party controls to protect information																●			
SR21	Encryption	Require encrypted information					●			●		●									
SR22	Encryption	Require encrypted information during storage								●		●		●	●	●	●		●	●	●
SR23	Encryption	Require encrypted information during transit												●						●	●
SR35	Retention	Require periodic information disposal										●			●	●	●				
SR19	Consent	Require user controls to restrict information collection				●															
SR20	Consent	Require user controls to restrict information use				●															
SR28	Notification	Avoid deceptive user notifications																	●		
SR29	Notification	Avoid retroactive policy implementation							●												
SR30	Notification	Require consistent policy and practices			●	●												●			
SR31	Notification	Require user notification of information use		●																	
SR32	Notification	Require user notification of third-party information use	●	●		●			●		●										
SR33	Notification	Require provider notification of third-party information use									●										
		Settlement Year	**'99**	**'00**	**2002**		**'03**	**2004**		**2005**			**2006**				**2008**				

Table 6: Increased FTC Focus on Security Monitoring, Patching, Training and Verification

ID	Security Category	Mitigating Security Requirement	Geocities	Toysmart	Eli Lilly	Microsoft	Guess	Tower Records	Gateway Learning	Petco	CartManager	BJ's Wholesale Club	ChoicePoint	CardSys. Solutions	DSW	Guidance Software	Life is Good	Goal Financial	ValueClick	Reed Elsevier	TJX
SR24	Monitoring	Require monitoring for unauthorized access				●						●		●	●	●	●				●
SR25	Monitoring	Require monitoring to identify vulnerabilities				●															
SR26	Monitoring	Require monitoring to perform security audits				●															●
SR27	Monitoring	Require periodic validation of physical identity											●								
SR34	Patching	Require application vulnerability patching								●				●		●	●			●	●
SR36	Training	Require personnel privacy and security training			●													●			
SR37	Verification	Require application vulnerability testing			●		●	●		●				●	●	●	●		●	●	
SR38	Verification	Require network vulnerability testing																●			
SR39	Verification	Require physical vulnerability testing																●			
		Settlement Year	**'99**	**'00**	**2002**		**'03**	**2004**		**2005**			**2006**				**2008**				

Table 10: Remedial Refrainments for Consent and Notification

ID	Remedial Refrainments	Geocities	Toysmart	Eli Lilly	Microsoft	Guess	Tower Records	Gateway Learning	Petco	CartManager	BJ's Wholesale Club	ChoicePoint	CardSys. Solutions	DSW	Guidance Software	Life is Good	Goal Financial	ValueClick	Reed Elsevier	TJX
R1	AVOID any misrepresentation about the collection, use or disclosure of consumer information	●			●					●										
R2	AVOID any misrepresentation about the identity of the party collecting consumer information	●																		
R3	AVOID any misrepresentation about the identity of the sponsorship of any activity on its Web site.	●																		
R4	AVOID collecting personal information from any child without parental consent	●																		
R5	AVOID any misrepresentation about sharing consumer information with third parties		●																	
R6	AVOID disclosing, selling or offering for sale consumer information to any third party		●					●		●										
R7	AVOID misrepresentations about how it maintains and protects the privacy, confidentiality, or security of any personally identifiable information			●	●	●	●		●			●			●	●	●	●		
R8	AVOID misrepresentations about how it will notify consumers of changes to its privacy policy				●			●												
R9	AVOID misrepresentations about how parents may control what information their children can provide to third parties				●															
R10	AVOID misrepresentations about providing to any third party personal information about children under the age of thirteen							●												
R11	AVOID disclosing to any third party any personal information, without consumer consent							●												
R12	AVOID applying privacy policy changes to personal information collected about consumers before the date of the posting, without consumer consent							●												
	Settlement Year	**'99**	**'00**	**2002**		**'03**	**2004**		**2005**			**2006**				**2008**				