# Progressing toward a ‘Reasonable Security’ Wizard

Whitepaper, April 2017

Craig Erickson, CISSP CISA

## Introduction

I recently joined SIRA, the Society of Information Risk Analysts, as a proponent of “Data-Driven Security” championed by Jay Jacobs and Bob Rudis, co-authors of a book by that title. This whitepaper is based on SIRA members’ suggestions for composing either a prescriptive, technical definition of ‘reasonable security’, or dynamically through a wizard-style tool, which could be used to evaluate the legal defensibility of an organization’s information security practices, and to provide actionable recommendations.

This whitepaper also builds upon a previous work by Travis D. Breaux, (Institute for Software Research at Carnegie Mellon University) in September 2010 entitled: Legally “Reasonable” Security Requirements: A 10-year FTC Retrospective. This work is also referred to in my paper as the “FTC Study” and excerpts are in italics for clarity.

My original goal was to prove that through the use of text-mining techniques and machine learning algorithms, we could dynamically refine which factors are most critical in predicting whether a set of security practices are legally defensible in the eyes of the Federal Trade Commission. At the time of this writing, my revised goal is publishing the actual methodology and project artifacts I used and produced, so that others can reproduce and improve upon these methods.

Predicting how “evolving legal standards” pertaining to information security and privacy will be litigated, can be problematic for mitigating future risks. This paper proposes methods of finding answers to questions posed by SIRA members, such as:

*[All questions liberally paraphrased by the author]*

Adam Shostak: What makes this or that set of security controls, ‘reasonable’?

Pete Lindstrom: How best to identify the event set or population? By organization? By asset?

Russ Thomas: What are the contextual questions a "wizard-style" web application asks, as input for generating an evidence-based list of “reasonable security practices"?

Daniel Arista: What are the dynamics explaining why a particular security practice is reasonable in one set of circumstances, but unreasonable in another, when the same reasonableness standard is applied? Is it up to the decision maker? Does it depend on the circumstances in which the decision was made?

Ben Tomhave: Can we define "reasonable" based on cases decided in court?

Daniel Arista: When assessing 'reasonableness', what should a risk manager have been expected to do in that particular context, and are those expectations ‘reasonable’? Should a risk manager be expected to know to what to do, and how to do it?

John T. Hoffoss: What are the security standards we set (security / compliance profession) that the courts look to when they try to determine what's reasonable? Are there general requirements to take based on your business? Are there more granular requirements that need to be applied to certain systems, scopes, lines of business etc. based on their nature?

## Methodology

Jeff Lowder, is a prominent SIRA member who researched the feasibility of tracking all U.S. Federal Trade Commission (FTC) enforcement actions relevant to determining whether an organization had failed to implement "reasonable security". I credit Jeff for inspiring me to explore this approach in greater depth.

Rather than focus on a predetermined final product or targeted audience, my work used guiding principles in the form of constraints, such as:

* Data-driven vs. expert opinion
* Nuanced guidance tailored for each specific case vs. static prescriptive checklists
* Open source toolset vs. conclusions based on unknown work products and methods
* Methods must be reproducible and adaptable as datasets change

Generally, I seek to find the best methods for mining and analyzing this data set to produce maximum capability and benefits.

Iteration #1, Experiment #1

## FTC case selected as baseline data model for supervised text-mining

Our first goal is to find definitions and characteristics of reasonable security from one document in one FTC case, and attempt applying it to other documents in other FTC cases.

Q. Which case should I select, and why?

Q. Which document should I select, and why?

In response to a question from Pete Lindstrom: “How best to identify the event set or population? By organization? By asset?” Craig Erickson writes: “Initially, I want to select the most relevant, interesting data from the entire set of documents from all cases in the FTC repository. Ultimately, this selection process would be automated, but for now, I just pick one at random because it looks interesting.”

## Cases and Proceedings

All FTC cases & proceedings can be filtered by name and date, but some older actions may not be filtered by other attributes (industry, topic, enforcement type, etc.).Filters include:

Mission = Competition or Consumer Protection Type of Action = Administrative or Federal

|  |  |  |
| --- | --- | --- |
| **Case Title** | **FTC Matter / File No.** | **Updated** |
| LabMD, Inc. v. Federal Trade Commision (Federal) | 102 3099 | February 9, 2017 |
| LabMD, Inc., In the Matter of (Administrative) | 102 3099 | September 20, 2017 |

<https://www.ftc.gov/enforcement/cases-proceedings>

Out of a total of 2733 FTC cases, 1055 cases include both Administration and Federal actions for cases tagged as ‘Consumer Protection’ exclusively.

Classifications of cases are organized on the FTC website as tags for filtering searches. These tags are not used for selecting cases in this study because they are not embedded in the metadata or body of the documents.

Each FTC case listed links to an html page which includes this metadata:

# LabMD, Inc., In the Matter of

Tags: [Health Care](https://www.ftc.gov/industry/health-care) [Consumer Protection](https://www.ftc.gov/mission/consumer-protection) [Privacy and Security](https://www.ftc.gov/consumer-protection/privacy-and-security) [Data Security](https://www.ftc.gov/consumer-protection/data-security)

Last Updated: September 29, 2016

In the Matter of LabMD, Inc., a corporation

FTC Matter/File Number: 102 3099

Docket Number: 9357

Related Case: [LabMD, Inc. v. Federal Trade Commission](https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-v-federal-trade-commission)

**Case Summary**

The Federal Trade Commission filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers’ personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers. The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves. The case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers’ personal data.

**Case Timeline**

### September 29, 2016

application/pdf icon[Commission Order Granting Motion To Withdraw As Counsel of Record (12.7 KB)](https://www.ftc.gov/system/files/documents/cases/160929labmdwithdraworder.pdf)

application/pdf icon[Commission Order Denying Respondent LabMD, Inc.'s Application For Stay of Final Order Pending Review By A United States Court of Appeals (69.66 KB)](https://www.ftc.gov/system/files/documents/cases/160929labmdorder.pdf)

### September 21, 2016

application/pdf icon[Respondent LabMD, Inc.'s Opposition to Complaint Counsel's Motion for Leave to File Surreply (4.19 MB)](https://www.ftc.gov/system/files/documents/cases/160921labmdoppsurreply.pdf)

[ LabMD timeline includes a total of 317 documents within 222 date records spanning a date range of September 29, 2016 to August 29, 2013]

PRESS RELEASE: [FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy](https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers)

[Most press release documents are in html formats.]

I selected LabMD after browsing the case summaries, just looking for what I thought might be interesting and relevant to “the average business” – my fuzzy profile of a probable intended audience for a ‘Reasonable Security’ Wizard. The case scenario seemed to be fairly straightforward and typical. At the time, I was unaware of the (Federal) case, and selected by default, the case from the (Administrative) mission type.

I chose one FTC Opinion document from the case of LabMD, after reviewing some of the documents which had substantial titles, relatively recent modified dates, and larger-than-average file sizes.

160729labmd-opinion.pdf 8/1/2016 12:46:51 PM 254.31 KB

Using this document, I manually analyzed it for words and phrases that represented 5 inputs to a supervised, evidence-based data model:

1) definitions of "reasonable" and "unreasonable" security practices, and also, in FTC jargon, "unfair" and "unjust", in order to answer:

Q. What is the definition of "reasonable security"?

2) characteristic attributes of reasonable/unreasonable practices, in order to answer:

Q. What qualifiers are used to evaluate and classify something as "reasonable" or "unreasonable"?

3) security controls identified in case matters, in order to answer:

Q. Which measures and controls are identified as absent, deficient, expected, or recommended?

4) resources and/or assets which require security controls, in order to answer:

Q. What are we protecting that requires "reasonable security"?

5) what the harms, consequences, or impacts are from failing to provide "reasonable security".

Q. Can we normalize threats, vulnerabilities, and injuries in a CVE/CWE/CSVV-compatible format? And can these be used as classifiers for matching our audience with appropriate cases?

\analysis\LabMD-Opinion-ReasonableSecurity.docx

One challenge, involved identifying single terms which represent harms. I left this out for the first iteration, and returned to it during a second iteration, using only the press release document in html format.

\analysis\LabMD-PressRelease.docx

I also had to keep in mind, what is the intended purpose of this exercise? We don’t want to miss important data outputs because it wasn’t considered and collected properly at the beginning of this experiment. Based on SIRA member comments about objectives and usability, I also created some desirable outputs:

6) the Top [20] Questions the defendant/respondent should have answered and acting upon in order to avoid the FTC ruling.

Q. Could we link the questions to controls, and could we recommend "reasonable parameters" for these controls?

7) what the report format should contain, for each vertical industry, according to factors that would be considered by the FTC.

Q. Can we generate a one or two-page report for each case we mine from the FTC regarding cybersecurity?

8) what other deliverables or outputs could be produced from such analyses, for instance:

Q. Could we also document defense arguments invoked and the actual outcome, to help a user determine whether "this doesn't apply to us because we're special"?

## Input-Output Considerations

Who is the consumer of such a wizard, and why would they be interested? After all, there is no shortage of best practice standards and measures for mitigating risks. Let's assume for now, that our audience is someone who is inclined to think that, for some reason, the prevailing wisdom regarding information security does not apply to them. Yet, they are concerned enough about getting sued or fined, and are looking for the "bare minimum" effort required to avoid this unwanted outcome. Who would this be?

LabMD represents the small, unsophisticated organization with limited resources and technical expertise, aspiring only to meet the lowest standards for “reasonable security”. Using LabMD as the one case used to supervise my data model made sense to me: it is simple and straightforward to infer linkage between “reasonableness”, assets, risks, controls, and harms.

While other cases range from small security vendors to giants like Microsoft and Google, it made sense to compose a supervised model from cases in the lower-capability tier. It may turn out that, like in the case of LabMD, even the most sophisticated organizations share the same tendency: thinking “this does not apply because we’re special”. Another factor I added to my selection criteria, after-the-fact, was the “level of aggression in fighting the FTC case”. After reading this case, it occurred to me that that an organization which is “too passive” might reveal nothing useful if it intends to accept the consequences of non-compliance with an FTC Order. This point is relevant to forming case selection criteria according to who our intended audience might be and what value they might obtain through our ‘Wizard’.

The inputs 1-5 listed above (1-definitions of "reasonable" and "unreasonable"; 2-characteristic attributes of reasonable/unreasonable practices; 3-security controls identified; 4-resources and/or assets which require security controls; 5-harms, consequences, or impacts) are used to compose a baseline data dictionary, which is used to find similar terms in this and other case documents. This baseline data dictionary is also referred to as my initial “supervised data model” throughout the remainder of this whitepaper.

Iteration #1, Experiment #2

## FTC cases selected for unsupervised text-mining

Can we use our supervised data model from LabMD to identify relevant documents and terms in other FTC cases, to produce an enriched understanding of how “reasonable security” is determined?

The following table displays each case selected for unsupervised analysis:

|  |  |
| --- | --- |
| **Metadata Attribute** | **Metadata Value** |
| Case Title | LabMD, Inc. |
| Tags | Consumer Protection; Data Security; Privacy and Security; Health Care |
| Date Range | September 29, 2016 to August 29, 2013 |
| Document Count | 317 |
|  |  |
| Case Title | Wyndham Worldwide Corporation |
| Date Range | June 26, 2012 to December 11, 2015 |
| Tags | Consumer Protection; Data Security; Privacy and Security |
| Document Count | 14 |
|  |  |
| Case Title | Ashley Madison |
| Date Range | December 14, 2016 to December 14, 2016 |
| Tags | Consumer Protection; Data Security; Privacy and Security; Consumer Privacy |
| Document Count | 4 |
|  |  |
| Case Title | Guidance Software, Inc. |
| Date Range | November 16, 2006 to April 3, 2007 |
| Tags | Consumer Protection; Data Security; Privacy and Security |
| Document Count | 10 |
|  |  |
| Case Title | True Ultimate Standards Everywhere, Inc. (TRUSTe) |
| Date Range | November 17, 2014 to March 18, 2015 |
| Tags | Consumer Protection |
| Document Count | 11 |
|  |  |
| Case Title | Fandango, LLC |
| Date Range | March 28, 2014 to August 19, 2014 |
| Tags | Consumer Protection; Privacy and Security; Data Security; Tech |
| Document Count | 8 |
|  |  |
| Case Title | LifeLock, Inc. |
| Date Range | March 9, 2010 to January 5, 2016 |
| Tags | Consumer Protection; Privacy and Security; Data Security |
| Document Count | 15 |
|  |  |
| Case Title | D-Link |
| Date Range | January 5, 2017 to January 5, 2017 |
| Tags | Consumer Protection; Privacy and Security; Data Security; Tech |
| Document Count | 2 |
|  |  |
| Case Title | IOActive, Inc. |
| Date Range | August 17, 2015 to October 9, 2015 |
| Tags | Consumer Protection; Privacy and Security; Privacy Shield; U.S.-EU Safe Harbor Framework |
| Document Count | 7 |
|  |  |

Tags included in this set can also be queried for total count among all FTC cases:

|  |  |
| --- | --- |
| **Tag** | **Count** |
| Consumer Protection | 1055 |
| Data Security | 636 |
| Privacy and Security | 215 |
| Privacy Shield | 224 |
| U.S.-EU Safe Harbor Framework | 49 |
| Tech | 33 |
| Consumer Privacy | 1350 |
| Health Care | 216 |

The document selection process is also intended to be dynamically determined by rules applied to content analysis, iterated over time. Documents represent a variety of legal instruments such as Orders, Opinions, Letters, Press Releases, etc., as well as less-relevant administrative procedures. For now, I included all pdf documents for each case, with one exception: out of 317 documents in the case of LabMD, I hand-picked only 14 of the most relevant ones for inclusion.

After selecting the appropriate documents relevant to each FTC case, I use the tm package in R to load them all into a corpus, and perform typical pre-processing tasks such as:

a) removing punctuation, which also preserves hyphenated words

b) removing numbers,

c) converting to lowercase.

Other pre-processing operations such as:

e) removing common "stopwords",

f) deleting terms with special characters, and

g) removing terms without standard dictionary entries

are optionally performed on selected operations rather than the raw corpus.

Each of these preprocessing steps should have some rules and guidelines, due to the effects of altering the raw data used in producing analytic outputs which could result in a loss of context or raw data. For instance, if we rely on methods employing single term frequency, the effect of removing common terms such as “and” and “the” might be appropriate, whereas terms such as “their” or “its” implying possession might be contextually significant. Similarly, numbers and dates are also constructs important for measuring severity of impact which could be lost.

In this experiment, I documented which terms were marked for removal as “having almost no value”, and stopwords, which have “little value” due to common usage such as ‘ftc’, or common terms which don’t significantly affect contextual meaning.

It is intended that similar text-mining and machine-learning techniques would be applied to these pre-processing steps in future experiments as well.

wyndham <- VCorpus(DirSource("wyndham"), readerControl = list(reader = readPlain,

language = "en", load = TRUE) )

cleanWyndham <- tm\_map(wyndham, content\_transformer(removeNumbers))

cleanWyndham <- tm\_map(cleanWyndham, content\_transformer(removePunctuation))

cleanWyndham <- tm\_map(cleanWyndham, content\_transformer(tolower))

dtm <- DocumentTermMatrix(cleanWyndham)

> inspect(dtm)

<<DocumentTermMatrix (documents: 11, terms: 6369)>>

Non-/sparse entries: 14033/56026

Sparsity : 80%

Maximal term length: 109

Weighting : term frequency (tf)

Sample :

Terms

Docs for ftc hotels not security that this wyndham

120626wyndamhotelscmpt.txt 52 23 95 21 29 36 60 43

120809wyndhamcmpt.txt 36 24 118 16 30 37 42 42

140407wyndhamopinion.txt 69 183 210 111 42 324 76 19

141105wyndham\_3cir\_ftcbrief.txt 91 162 4 118 51 335 42 141

150327wyndhamsuppbrief.txt 37 74 1 24 12 78 33 6

150824wyndhamopinion.txt 84 110 15 115 18 214 48 116

151209wyndhamappendix-a-stip.txt 80 0 0 20 54 42 4 0

151209wyndhamappendix-b-stip.txt 54 0 0 41 65 83 43 0

151209wyndhamstipulated.txt 36 6 58 14 19 55 53 35

151211wyndhamstip.txt 41 6 65 14 19 55 53 51

DocumentTermMatrix before the removal of stopwords, potential use for document selection per case:

> dtm

<<DocumentTermMatrix (documents: 11, terms: 10790)>>

Non-/sparse entries: 19838/98852

Sparsity : 83%

Maximal term length: 197

Weighting : term frequency (tf)

# terms occurring at least 150 times…

> findFreqTerms(dtm, 150)

[1] "all" "any" "are" "assessment" "business"

[6] "commission" "consumers" "court" "data" "document"

[11] "dss" "filed" "for" "from" "has"

[16] "have" "hotel" "hotels" "information" "its"

[21] "management" "may" "not" "page" "pci"

[26] "practices" "resorts" "risk" "section" "security"

[31] "such" "that" "the" "their" "this"

[36] "u.s." "under" "which" "with" "wyndham"

> inspect(DocumentTermMatrix(cleanWyndham, list(dictionary = c("reasonable", "security", "risk", "harm", "data", "environment"))))

<<DocumentTermMatrix (documents: 11, terms: 6)>>

Non-/sparse entries: 49/17

Sparsity : 26%

Maximal term length: 11

Weighting : term frequency (tf)

Sample :

Terms

Docs data environment harm reasonable risk security

120626wyndamhotelscmpt.txt 1 0 1 1 1 1

120809wyndhamcmpt.txt 1 0 1 1 1 1

140407wyndhamopinion.txt 1 0 1 1 1 1

141105wyndham\_3cir\_ftcbrief.txt 1 0 1 1 1 1

150327wyndhamsuppbrief.txt 1 1 1 1 0 1

150824wyndhamopinion.txt 1 0 1 1 0 1

151209wyndhamappendix-a-stip.txt 1 1 0 1 1 1

151209wyndhamappendix-b-stip.txt 1 1 1 0 1 1

151209wyndhamstipulated.txt 1 1 0 1 1 1

151211wyndhamstip.txt 1 1 0 1 1 1

## Unsupervised correlation of core input factors

How can we best derive requirements, definitions, findings, etc. from the FTC case repository, relying on the least amount of “expert opinion”?

For each core input, find highly correlated terms:

1) reasonable; 2) security; 3) risk; 4) harm; 5) data; 6) environment [or] systems [or] protect

# write csv output of terms => 94% correlation with core input…

tdm <- TermDocumentMatrix(cleanWyndham)

a1 <- findAssocs(tdm, "reasonable", 0.94)

write.csv(a1, file = "clean.csv")

Each correlation percentage was manually chosen; using a trial-and-error approach for each core input intended to produce a reasonable volume of the most relevant terms.

These correlated terms represent term candidates we should add to our data dictionary, to further refine our data model for “evidence-based reasonable security factors”:

|  |  |
| --- | --- |
|  | reasonable |
| Funds | 0.99 |
| mitigating | 0.98 |
| Suffered | 0.98 |
| Identity | 0.97 |
| Liable | 0.97 |
| substantial | 0.97 |

…

This approach, repeating this exercise for each core input factor per FTC case, and aggregated across a corpora for the entire dataset of FTC cases, is intended to discover the most valuable candidates for a data dictionary of single terms. This technique also applies to refining and enriching the stopword list.

Single term frequency and correlation techniques are probably inferior to using multiple word phrases for the following reasons:

1) overlaps of terms identified in multiple core factor classifications;

2) excessive duplication of terms used in document content headings, footnotes, exhibits, etc. bias the term frequency;

3) wordclouds and other graphs do not produce any obvious story or theme representative of the case(s) weighted by term frequency alone.

Future experiments should utilize “common phrases” in a data dictionary, so the efficacy of each approach can be better evaluated.

As an example, identifying harms can be challenging without using qualifiers such as:

“failed to”; “liable for”; “charges against”; “were unreasonable”; “constitute an unfair act or practice”; “finds that”; “neglected to”; “lacking even”, “causes or is likely to cause”; etc.

Second, determining the severity of harm, requires “parameter phrases” such as:

“between 2001 and 2014”; “for over 750,000 patients”; “millions of”

To overcome some of these challenges, I tried an approach used in the FTC Study which relied exclusively on FTC press release documents in html format, and used my supervised method to manually select and classify key terms and phrases relative to the concept of harm:

Who What Verb Outcome *Qualifier*

[This was not pursued further at this time – I believe the press releases should be exclusively loaded into a corpus because they provide the best summary – possibly superior to processing all other documents.]

## Construct Validity Methodology

Q. How does the supervised list of core input terms appear in the unsupervised lists?

A. The supervised list of core terms extracted only from the Opinion for LabMD are labeled “WatchWords”. These are compared with the unsupervised list of terms generated for all documents within the LabMD corpus. Matches are identified and marked, with the remaining terms classified as “NOT HIT”.

I also manually selected terms in the supervised model which I thought were of high value, but were not hit in the unsupervised model. These terms are on my ‘watchlist’ to see if they appear in the analysis aggregated in the overall ftcCorpus.

Q. Which terms appear most frequently in each class (reasonable, harm, etc), within the supervised model, and within the unsupervised model, and across both models?

Q. What is the effect of using preprocessing steps such as stopwords, removing punctuations, numbers, special characters, and stemwords?

Q. How can we use other weighted measures to value each term, aside from term frequency?

The final product of these experiments and iterations results in a wordcloud of the most “interesting terms” representing the entire FTC Corpus:

|  |  |  |  |
| --- | --- | --- | --- |
| **FtcCorpus Wordcloud** | |  | |
| **Term** | **Weight** | **Term** | **Weight** | |
|  |  |  |  | |
| practices | 9 | allows | 1 | |
| apply | 7 | credit | 1 | |
| result | 7 | customer | 1 | |
| provide | 6 | appropriate | 1 | |
| security | 6 | authorized | 1 | |
| card | 6 | reviews | 1 | |
| controls | 5 | reports | 1 | |
| harms | 4 | failures | 1 | |
| data | 4 | activities | 1 | |
| take | 3 | activities | 1 | |
| information | 2 | achieve | 1 | |
| risk | 2 | alert | 1 | |
| access | 1 | adequately | 1 | |
| financial | 1 | personal | 1 | |
| disclosure | 1 |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

## Similarities and Differences in Approaches Used in the FTC Study

The “FTC Study” refers to a previous work by Travis D. Breaux, (Institute for Software Research at Carnegie Mellon University) in September 2010 entitled: Legally “Reasonable” Security Requirements: A 10-year FTC Retrospective.

The FTC Study’s primary goal is similar: to discover and measure the meaning and evolution of “reasonable” security.

One obvious difference is that the FTC Study examined 19 cases over a 10-year period, while the approach used here examines 9 cases still active over the past 3 years. The reason for selecting the most recent cases is due to evolving trends the FTC Study reported on: factors such as additional mandates, improved sophistication and access to mitigating technologies bias the results, which were relevant to the FTC Study’s secondary goal of reporting trends on how “reasonable security” has evolved over time. Our goal is to discover how we can build a tool that predicts how “reasonable security” evolves in the future, based on past evidence. Additionally, some of the larger cases are too complex for predictive analysis purposes.

The FTC Study first examines what constitutes unreasonable security by itemizing vulnerabilities identified by the FTC in these regulatory enforcement actions. These vulnerabilities also represent a data dictionary, from which mitigating security requirements can be deduced (generally from FTC-imposed remedies). Exactly how the researchers identified “vulnerabilities” was not explained in the FTC study, but I found this to be too specific and complex to be useful in my approach, which also, does not seek to enumerate specific security requirements for cases taken individually or as a whole.

Instead of considering what constitutes “reasonable security” under the FTC in terms of specific security requirements, or how this definition of reasonable security aligns with existing security standards, my approach focuses on which factors are most critical in determining reasonable security. These factors include multiple, complex, environmental, and time-dependent factors which are variables for consideration.

The FTC Study endeavors to discover:

*• 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.*

Whereas this proposal for a building a “Reasonable Security Wizard” endeavors to discover factors used in the calculation of mitigating the risks of litigation for *not providing* reasonable security. Consider Daniel Arista’s questions:

“When assessing 'reasonableness', what should a risk manager have been expected to do in that particular context, and are those expectations ‘reasonable’? Should a risk manager be expected to know to what to do, and how to do it? What are the dynamics explaining why a particular security practice is reasonable in one set of circumstances, but unreasonable in another, when the same reasonableness standard is applied? Is it up to the decision maker? Does it depend on the circumstances in which the decision was made?”

In the case of LabMD, the Commisioner wrote in her opinion, “in spite of the fact that LabMD had *multiple* IT staff members…”, and upon further reading we discover that the grand total of IT staff = 2. Such nuance presents challenges in text-mining operations.

Both approaches 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.

## Classifications Used in the FTC Study

Each FTC case is classified by one of the following types:

illegal disclosure (ID), illegal collection (IC) or data breach (DB)

The FTC Study does not explain how FTC cases were classified in these types.

Reference materials acquired for the FTC 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. I found other documents such as the opinion, and legal defenses were also valuable and thus included in experiments I conducted.

Both approaches employ similar analysis procedures which provide the analyst a means to identify, classify and extract statements and phrases that represent instances of the above units of analysis. The FTC Study focuses on “legal vulnerabilities” sorted by security category (below), contrasts with my focus on “risk factors of legal vulnerabilities” of any and all FTC cases with no artificial categorization.

Security categories used for sorting legal security vulnerabilities in the FTC Study:

Access, Monitoring, Retention, Consent, Notification, Training, Encryption, Patching, Verification

*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.*

*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.*

- In the Matter of Guidance Software, Inc. (2007)

respondent *engaged in a number of practices* that, *taken together*,

*failed to* provide reasonable and appropriate security *for* sensitive personal information

stored *on* its corporate network.

*SR18: Require encrypted information during storage.*

*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.*

My study does not attempt to derive security requirements – based on comments from SIRA members, generating yet another checklist or recommending one security framework over another is just another exercise in using ‘expert opinion’ to jump to false conclusions. Our goal is to better understand the factors used by judges and regulators in determining “reasonable security” so we could build a better model for making risk decisions.

Deriving actionable *security requirements* from *legal vulnerabilities* identified in the FTC Study is not possible without the construct of “security categories”:

*Each vulnerability is mapped to a mitigating security requirement, and for the 110 vulnerabilities identified, 39 unique mitigating security requirements were derived.*

*The following table, 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. 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%).*

**FTC Study Table: Distribution of Legal Vulnerabilities by Security Category and Settlement Year**

**Security Settlement Years from 1999 to 2008 Totals**

**Category ʻ99 ʻ00 ʻ02 ʻ03 ʻ04 ʻ05 ʻ06 '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

*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).*

The table above is presented to illustrate how “security categories” are used in the FTC Study. According to this table, *access* represents the greatest legal vulnerability, and whatever security requirements can be derived from these would be among the highest priority for our intended audience.

*3.3.3 Identify legal remedies*

*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.*

*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.*

*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.”*

*Complex factors affect the order of magnitude for an exploited vulnerability in terms of number of affected consumers.*

*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.*

I question the value of ranking vulnerabilities by severity, as being more hypothetical and less relevant for our purposes. However, considering who can get hurt and how badly, seems not only more relevant but also more actionable: “saving lives” is less influential than “saving Johnny’s life”.

In contrast to the FTC Study, my approach identified “security controls” rather than “legal vulnerabilities”. I found it too difficult to otherwise identify whether the terms represent vulnerabilities or remedies:

1c. Identify security controls which are absent, deficient, expected, or recommended.

intrusion detection system – 4 file integrity monitoring – 5 firewalls - 3

data security training -2 strong passwords – 1

These terms representing security controls were manually identified from the supervised model. Using unsupervised, text-mining techniques such as term frequency fails to discover these controls. Likewise, it is also challenging to identify assets without the use of a dictionary of known controls or assets.

## How the FTC Study Derives Actionable Security Requirements

*Whereas the steps in the analysis procedure described [previously] 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.*

The FTC Study also includes this as a possible weakness of the study, regarding Construct Validity:

*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.*

**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

The table above illustrates to me the inadequacy of these relatively vague security requirements, which appear to be derived more from remedies, obligations, and refrainments ordered by judicial or enforcement agencies:

*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.*

Our approach includes another facet, “assets and/or resources” in need of protection from attackers, which is most closely represented as “remedial obligations” implemented as “safeguards rules” in the FTC Study’s approach:

**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 safeguardsʼ 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) |

Notice the absence of ‘risk’ in the table above.

## Did the FTC Study Achieve Its Primary Goals?

*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.*

First, if “*resulting security requirements provide a partial definition of reasonable security”*, then the term ‘reasonable’ should not be repeatedly used in security requirements and other products such as the Remedial Obligation Description above. I would not expect these requirements to be of any practical use to software developers and testers.

Second, stating “*vulnerabilities they mitigate provide insight into the broader security context”* by showing *“actual violations of law”* , only obscures the definition rather than produce a “*current picture of both legal and security risks”*, in my opinion. The statement implies that security standards only provide general guidance on improving security, while legal vulnerabilities are more specific? If true, then why use any security standards if there are specific legal vulnerabilities one could mitigate through proposed security requirements?

According to the authors of the FTC Study:

*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.*

In response to a question from John T. Hoffoss: What are the security standards we set (security / compliance profession) that the courts look to when they try to determine what's reasonable? Are there general requirements to take based on your business? Are there more granular requirements that need to be applied to certain systems, scopes, lines of business etc. based on their nature?

Craig Erickson writes: I did find references to SANS Institute and other frameworks, including pdf-0154\_data-breach-response-guide-for-business.pdf, the FTC’s own guidance. I also found references to free security tools, training, and other resources but suspect that ‘expert witnesses’ are most commonly used based upon term frequency.

## Future Work Remaining

This whitepaper presents a methodology and open source project for this future work.

After soliciting feedback and engaging with other contributors, I would be inclined to add stemming and stopword pre-processing techniques, and apply these steps to the largest subset of FTC cases in one corpus.

I would also experiment with processing only the press releases for each case.

With regards to specific assets and controls, I don’t see much value there. The reason for identifying them in the first place was the idea of producing a Wizard or dynamically-generated checklist.

From what I see, “reasonable security” is entirely dependent on monitoring and managing risk. Does a checklist function as a risk register? Do plugged-in security appliances mitigate risks? How do ‘actual violations of law’ guide anyone else’s security requirements or legal vulnerabilities? Just look at the most common remedy ordered by the FTC: “establish and maintain a comprehensive security program”. We know that risk management is the most significant component of any such program, and we also know that it’s the most neglected.

Going forward, I’m intrigued by analyzing defensive arguments. Earlier in this paper, I made some assumptions about who our audience might be, and what they would find of value. Managing risk is probably not their cup of tea, but shooting down common excuses for ignoring the risks of harm to real people might move the needle toward a greater appreciation of risk management.

6. Identify the Top 20 Questions the defendant should have addressed to avoid its FTC ruling.

Q. Are we able to link these questions to controls, and could we recommend "reasonable parameters" relevant to each case for these controls?

I made only a meager attempt to do this (in the worksheet output), mostly because I feel it’s more important to better identify harms. However, the FTC Study claims:

*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.*

Whether or not this is satisfactory for our SIRA members is another topic, but I researched most of the references cited in the FTC Study pertaining to “recommended resources to help businesses” and the most specific guidance I found was Hanson:

*COMMON FACTORS CITED BY THE FTC COMPLAINTS FOR BUSINESSES THAT FAIL TO EMPLOY REASONABLE SECURITY MEASURES UNDER SECTION 5*

*When the FTC has brought Section 5 claims against businesses for failure to employ reasonable security measures, the FTC has noted a number of practices that, “taken together,” failed to provide reasonable and appropriate security for personal information. Such business practices can include:*

* *Not adequately assessing the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks.*
* *Not implementing simple, low-cost, and readily available defenses to such attacks.*
* *Failing to use strong passwords to prevent a hacker.*
* *Storing the information in unencrypted files that could be accessed easily by using a commonly known user ID and password.*
* *Failing to employ sufficient measures to detect unauthorized access.*
* *Not encrypting the information while in transit or when stored on the in-store computer networks.*
* *Using a commonly known default user id and password to protect consumer information.*

*The FTC has typically cited five or more of these and other factors when delineating the reasons a particular business failed to employ reasonable and appropriate security measures to protect personal information.*

I also cite Hanson’s work as an indication of insufficient guidance, which also begs the question, “Are we concerned about the risk of being prosecuted or the severity of penalties?”

*THE CHOICEPOINT SETTLEMENT CONTAINS HARSHER PENALTIES BECAUSE IT INVOLVED MORE SENSITIVE INFORMATION AND ALLEGED FCRA VIOLATIONS*

7. Identify what the report format should contain, for each vertical industry, according to factors that would be considered by the FTC.

Q. Can we generate a one or two-page report for each case we mine from the FTC regarding cybersecurity?

8) what other deliverables or outputs could be produced from such analyses, for instance:

Q. Could we also document defense arguments invoked and the actual outcome, to help a user determine whether "this doesn't apply to us because we're special"?

*Legal compliance is defined as an organization’s ability to maintain “a defensible position in a court of law” [BAK06].*

In the case of LabMD, the arguments made in defense could be characterized as, "willful disregard to protect the interests of consumers" coupled with "inconvenience and punitive costs incurred".

For example, LabMD’s CEO complained that (paraphrasing here) since he would have to personally mail out breach notices himself because most of his staff left, the Commissioner’s ruling was excessive. (i.e. unreasonable, unfair, unjust). Is it possible that LabMD's ‘hostile attitude’ toward security and government interference was as significant a factor as any failure of administrative or technical controls?

Q. What comparisons can be made against other instances, such as: cases which were dismissed or NOT decided against respondents/defendants? Even the FTC Study acknowledged this lack of a control population:

*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.*

Ideally, any useful methodology should also apply to other enforcement agencies, case study repositories, and other venues such as private lawsuits. In September 2008, J.B. Hanson authored “Liability for consumer information security breaches: deconstructing FTC complaints against businesses victimized by consumer information security breaches,” published by Shilder J. L. Com. & Tech.

*PRIVATE LAWSUITS AGAINST BUSINESSES FOR FAILING TO PROVIDE ADEQUATE SECURITY HAVE BEEN LARGELY UNSUCCESSFUL*

*Private lawsuits attempting to hold businesses liable for the injuries to consumers resulting from security breaches have been generally unsuccessful. While several commentators have argued for common law theories of liability for security breaches, courts have been reluctant to impose such liability. For example, BJ’s Wholesale Club, Inc. (BJ’s) and Cardsystems Solutions, Inc. (Cardsystems) had security breaches that led to both FTC complaints and private actions against the businesses. While the FTC complaints led to settlement agreements with significant penalties or concessions by the businesses, four private actions related to those breaches have been dismissed.*

*It should be noted that while businesses that fail to implement appropriate security precautions have generally not been held liable in private lawsuits, the law is developing and there have been some successes in private lawsuits. Lawsuits against TJX have ended in large multi-million dollar settlements. At least 19 private lawsuits were filed against TJX as a result of the security breach.*

A good example of a private lawsuit (not?) pursued by the FTC, which could be used for comparative analysis, might be the case of Affinity vs. Trustwave.

## Techniques for Unsupervised Text-Mining Analyses

The methodology outlined in this whitepaper has to this point, been primarily devoted to a supervised model requiring “expert opinion” to determine relevant content from one FTC case. However, the ultimate goal is to build a machine learning algorithm which could be applied to additional cases, and further refine data dictionaries identifying 1) definitions of reasonable security, 2) characteristic attributes of reasonable security, 3) security controls, 4) assets and/or resources, and 5) harms.

Without actually proving the efficacy of these techniques, I experimented with them by:

1. Loading all documents from each of the 9 FTC cases selected into a corpus, using the tm package in R;

2. Finding the most frequent terms in the corpus;

3. Finding the most highly correlated words for the key terms produced by the supervised model;

4. Aggregating the most common terms identified in steps 2) and 3);

5. Comparing the aggregated results in step 4) with the data dictionaries produced under my supervised model, and selecting additional term candidates or deselecting existing terms for the purpose of refining our data model.

A step-by-step cookbook can be found in the cover sheet of the ReasonableSecurityMethodology.xlsx workbook in the GitHub Project Folder.

## Conclusion

In response to a question from Ben Tomhave: “Can we define "reasonable" based on cases decided in court?” Craig Erickson writes: “Not yet, and perhaps, not ever. I haven’t explored the legal construct of “reasonableness”, and although I’m not an attorney, I’m sure there are many papers on this topic outside of a security context that would shed more light.”

Determining what is “reasonable security”, seems to depend more on:

* What is declared unreasonable
* What action or lack of actions cause “substantial harm”
* The “likelihood or magnitude” of actual or potential harm (severity)
* Whether or not a respondent/defendant had access to relatively low-cost tools and resources to mitigate identified vulnerabilities.
* Whenever a vulnerability or harm to consumers was known or should have been known and nothing was done to mitigate it.
* Managing overall risk vs. specific security controls

The project files containing analysis, scripts, source documents, and reference documents are freely available on GitHub. Please send me an email at [craigergrc@gmail.com](mailto:craigergrc@gmail.com) and I will send you the link.

Craig Erickson, CISSP CISA