Delft University of Technology
Faculty of Technology, Policy and Management

WM0824TU – Economics of Cybersecurity
Individual Report

Prepared by
Jiang, Andrew Yi
Student ID Number: 4942795
User ID: ajiang
https://github.com/Andrewjiangyi/WM0824TU

15 November 2018

Table of Contents

List of Figures

List of Tables

Abstract

With the continuous expansion of e-commerce has followed organizations keen on employing security vulnerabilities to profit through criminal activities such as fraud and identity theft. Governments have attempted over the years to deploy cybersecurity policy, but to what effect? This study analyzes the effectiveness of governmental policy in ensuring domains operated within a given country are secure against the POODLE attack on SSLv3, by hypothesizing that the percentage of vulnerable domains per country and its decline over time are correlated with the same country's Global Cybersecurity Index (GCI). It was shown that there indeed exists a negative but weak correlation, indicating that countries with a higher GCI do have a lower percentage of vulnerable domains and a greater rate of decline in said percentage, but that existing cybersecurity policy is not directly targeting the issue. Research and development should be employed to come up with more effective policies and legislation.

Introduction

In today's society, global online retail and e-commerce has been increasingly rapidly [1], with $2.842 trillion USD in retail e-commerce sales worldwide in 2017 [2]. Such a large market is not only appealing for various businesses trying to increase their profits, but also appealing to criminal organizations who wish to inflict harm upon the businesses and individuals participating in online e-commerce for their own benefit, through the use of vulnerabilities within deployed systems in order to gain sensitive information, or to commit fraud. As the threat evolves, business strategies and governmental regulations must also evolve in parallel in order to combat the threat effectively.

This study is part of the *Economics of Cybersecurity* course at the Delft University of Technology. This study will explore security issues of domains using improper and outdated SSL encryption, with an emphasis on public domains that continue to use SSL version 3.0 (SSLv3) and is subject to the Padding Oracle on Downgraded Legacy Encryption (POODLE) attack. Previous studies have focused on the various actors and stakeholders present, along with the risk mitigation strategies that may be applied by each, and the externalities that occur because of their various actions. As there currently exists a lack of understanding regarding the effectiveness of cybersecurity policies and regulations in place, this study will aim to focus on the regulators and their policies and attempt to gain some of the understanding the industry has been lacking, through the use of the Global Cybersecurity Index (GCI). Some background will be given on both SSLv3 and GCI before proceeding in order to gain a better understanding of the issue at hand.

SSLv3 has two encryptions that both have known security issues, namely using the RC4 stream cipher (which have known biases), as well as the AES block cipher in CBC mode, which can be exploited with the POODLE attack, as outlined by Möller et al [3]. Though SSLv3 is used less often since the introduction of the TLS protocols, and can be disabled in the majority of cases with little damage, some legacy products may be dependent on SSLv3 and are unable to be upgraded. In such a case, TLS clients can downgrade the protocol to avoid interoperability bugs on the server-side. This downgrade can also be triggered by adversaries, when interfering with a handshake attempt between client and server [3]. If the attack is successful, the client and the server start communicating over a weakly-encrypted

connection, at which point an adversary can act as a ‘man-in-the-middle’, able to intercept and decrypt the data from the client and the server, thereby compromising the security of the client, allowing sensitive information regarding the client to be obtained and exploited in ways such as identity theft.

The International Telecommunication Union (ITU) produces a GCI report every year that aims to combine “25 indicators into one benchmark measure to monitor and compare the level of ITU Member States cybersecurity commitment with regard to the five pillars” as shown below in Figure 1 [4].

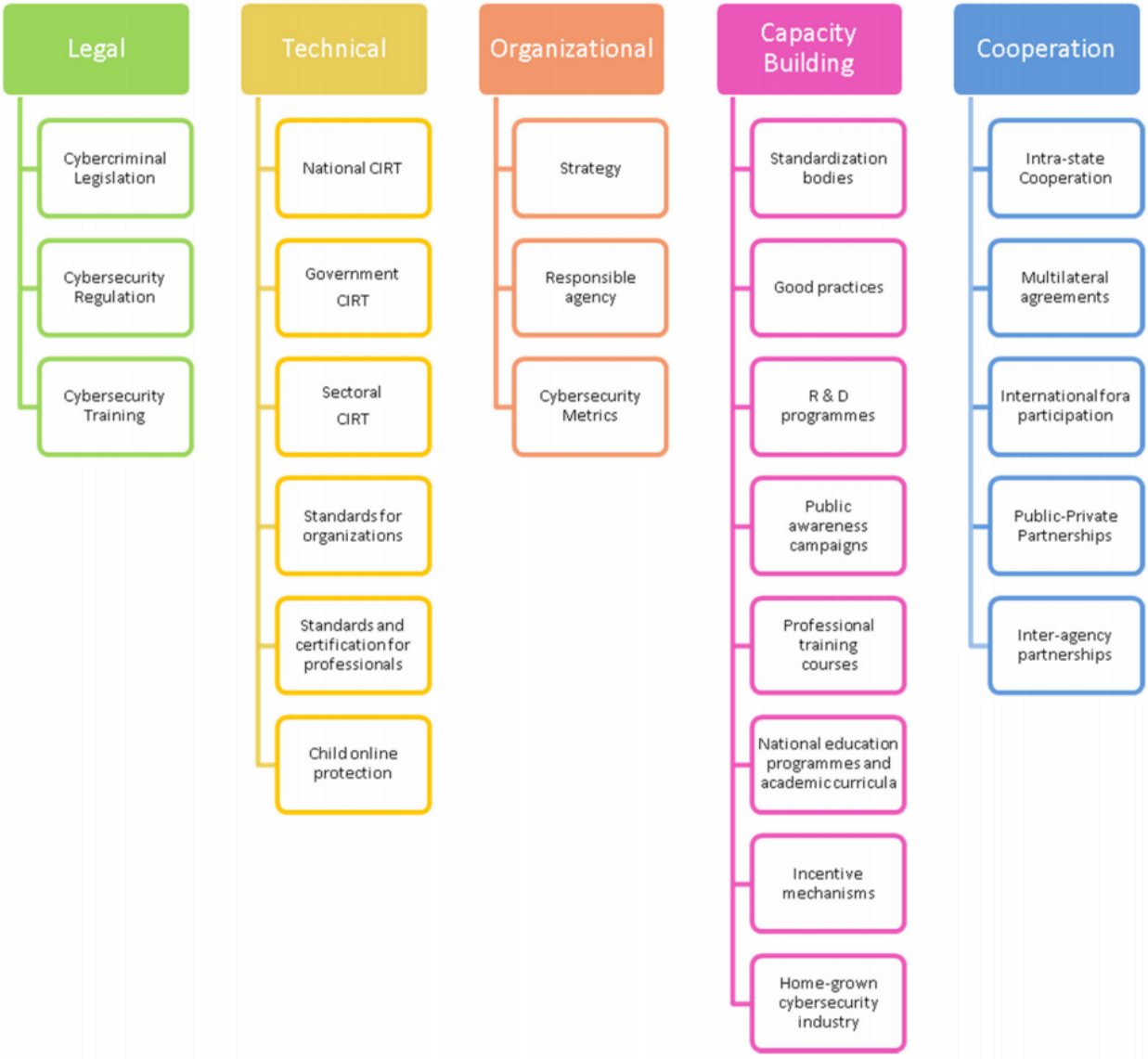

Figure 1: Global Cybersecurity Index (GCI) pillars and sub-pillars. [4].

The more sub-pillars fulfilled by any given country, the higher its GCI, and thereby the higher its cybersecurity level. This makes the GCI a nice metric that can be used while exploring whether regulations that have already put into place in countries around the world influence the security of the domains being operated from the country at hand, and on making recommendations regarding more modern measures and approaches that may be taken in order to enhance the cybersecurity landscape in general.

Literature Review

The connected world of today has brought about an enormous amount of convenience, but also an enormous amount of unintended consequences, in particular the rise of cybercrimes such as identity theft, phishing, and fraud. Over the past 30 years, the industry has attempted to come up with cybersecurity policies and various deterrents against adversaries, to varying degrees of success. This is caused of both a lack of understanding of the success of cybersecurity policies as they exist today, as well as a lack of proposed solutions that are able to address "operational tradeoffs, implementation costs, and consequent adversary adaptations across the full spectrum of vulnerabilities", Hughes and Cybenko argues [5].

One of the main issues with understanding the success of cybersecurity policies is the lack of reliable metrics: In Australia, the Australian Institute of Criminology commissioned a nation-wide survey in order to gather data regarding various aspects of cybersecurity incidents. Randomly sampled Australian businesses were asked to take part in the survey, of which only 29% responded, indicating the unwillingness of organizations to public discuss their security incidents. Perhaps more interesting is that out of all the survey respondents that were from the financial and insurance industry: 73% had indicated that they had experienced no incidents, and 10.4% had either declined to answer the question or indicated that they did not know the answer [6]. This high no-incident/no-response rate reported here does not appear to be congruent with how this is an industry that is often targeted as part of cyber attacks. Moore offers an explanation in that banks and businesses are incentivized to underreport incidents: Banks save significant amounts on branch operating costs thanks to the internet, and they do not want to scare customers away from online banking, even though there might be known security flaws with the mechanism currently employed. Similarly, businesses do not wish to have to cooperate with authorities through an investigation into various incidents, which would undoubtedly cause damage to their reputation and stock price [7].

With more of a focus on SSL incidents, a study done on the aftermath of the Heartbleed SSL vulnerability demonstrated that the rate of certificate revocations increased sharply in the weeks immediately following the disclosure of the Heartbleed vulnerability, but then dropped back closer to normal levels after roughly three weeks. Worse, 60% of domains that re-issued certificates in response to the Heartbleed vulnerability did not actually revoke their vulnerable certificates, meaning that systems will continue to trust those vulnerable certificates until they expire naturally, which would be two or more years for 20% of the certificates in question [8]. What is worrying is that these results are in line with previously observed timelines and patterns of other security vulnerability disclosures, indicating that perhaps the right market incentives and regulations are not in place for proper and thorough security practices to be implemented.

While the government is quite good at creating policy where cybersecurity becomes a matter of national security and creating contingencies for worst-case scenarios such as an attack on the national power grid, there is a lack of recognition for less drastic actions that should be taken to "align stakeholder incentives and correct market failures" in order to improve cybersecurity on a more day-to-day basis. Such everyday scenarios include online identity theft, cyber espionage, and participation in botnets of machines unbeknownst to their owners, and it is in these frequently occurring scenarios that the government has a duty to protect the interests of its citizens by stepping up with appropriate regulations. Moore also argues that it

is in these scenarios that the economics of information security have a far more profound impact, acting as guidance on the measures that should be taken [7].

So how should policy makers proceed in establishing guidelines and regulations that will be beneficial to cybersecurity and yield effective results? Various studies have suggested the use of quantitative metrics to derive risk estimates. As a relevant example, a specific vulnerability such as the POODLE attack on SSL can be quantified with the Common Vulnerability Scoring System (CVSS) [9], which take into account numerous factors such as attack complexity, privileges required, CIA (Confidentiality, Integrity, and Availability) requirements. Another discussed technique is QuERIES, which is a probabilistic analysis technique that include seven steps as shown in the figure below, where POMDP stands for "Partially Observable Markov Decision Process" [5].

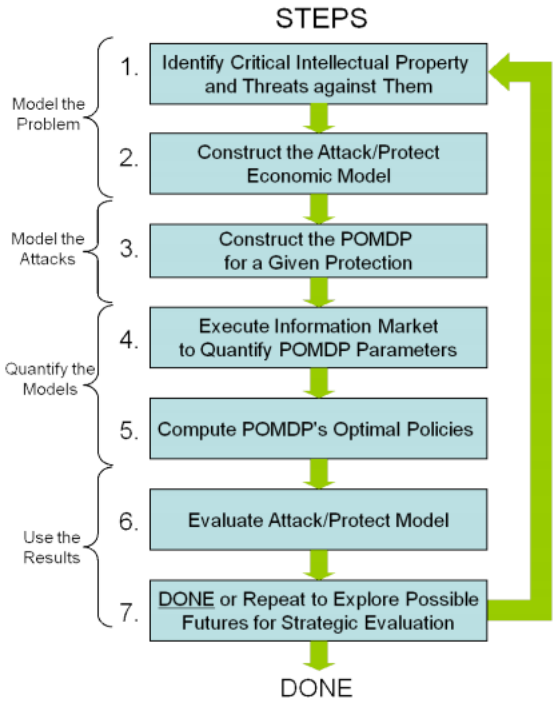

Figure 2. Graphical representation of the QuERIES technique [5].

Hughes and Cybenko then builds on this by proposing the "Three Tenets" threat model, a model which posits that three ingredients are "necessary and sufficient for successful attacks to occur" [5]:

- The existence of inherent system susceptibilities
- The threat's access to the susceptibility
- The threat's capability to exploit the susceptibility

Hughes and Cybenko then states that the measures necessary to mitigate these conditions are as follows:

- Focus on What Is Critical: Instructing the system designer to "consciously and methodically focus on including only those system functions that are essential to the

mission", and thereby reducing the number of potential attack vectors for an adversary to exploit.
- Move Key Assets Out-of-Band: Moving data used by mission-critical functions to a channel that is difficult for the adversary to potentially gain access to.
- Detect, React, Adapt: Deployment of dynamic sensing and response technologies that can be used to defend against and mitigate the tactics used by an adversary.

The discussion now becomes whether governments have the metrics they need on hand in order to motivate legislation regarding more effective cybersecurity policies. These policies in turn need to not only target the technical side of the issue through new, more refined cybersecurity proposals, such as the ones mentioned above, but also the industrial/economics side of the issue, which involves determining how to incentivize industry players into regular and transparent disclosure of security incidents, as well as the proper implementation of various cybersecurity proposals, for much of the problems in the field of security stems not from a poor security model, but rather a poor implementation of said model.

Research Question

Inspired by the research done by Zhang et al regarding how response to security vulnerabilities drop off sharply after approximately three weeks [8], the statements Moore made regarding how most governmental legislation regarding cybersecurity do not necessary target everyday scenarios [7], and the argument made by Hughes and Cybenko about the varying degrees of effectiveness of cybersecurity policies in place today [5], the research question is as follows:

"How are domains that use insecure SSL protocols in a given country correlate with the level of cybersecurity legislations of that country?"

Essentially, the aim is to determine whether stronger or weaker cybersecurity policies in a country have a correlation to the number of insecure domains within that country, and whether the same policies have any measurable impact in security vulnerability response rates long after the initial vulnerability disclosure. In order to properly research said question with the dataset on hand, the following hypotheses were made:

- Hypothesis 1: Countries with a higher Global Cybersecurity Index (GCI) have a smaller percentage of domains vulnerable to the POODLE attack
- Hypothesis 2: There exists a greater decline in percentage of domains vulnerable to the POODLE attack in countries with a higher Global Cybersecurity Index (GCI)

Statistics in support of both hypotheses will in turn be in support of the conclusion that countries with high levels of cybersecurity legislations have less domains that use insecure SSL protocols, and a higher rate of response to SSL vulnerabilities, even long after the initial disclosure of the vulnerability.

Methodology

The dataset on hand consists of many entries of connections to servers vulnerable to the POODLE attack. The servers are all from IP ranges belonging to various providers in the

Netherlands and are tested on average once a week. The total dataset consists of 28,357,106 records. The initial dataset can be found at [10].

The total number of domains per country has been sourced from [11]. Given the nature of the vulnerable servers data set, a currently vulnerable domain is defined as a domain that appears within the last week of the data set (From 2018-08-24 to 2018-08-31). The percentage of vulnerable domains per country is thereby defined as the number of currently vulnerable domains grouped by country, divided by the total number of domains of that country as a normalization measure. The decline of the percentage of vulnerable domains is defined as the number of currently vulnerable domains subtract the number of vulnerable domains that appear within the first week of the data set (From 2018-01-01 to 2018-01-08), grouped by country, and divided by the total number of domains of that country as a normalization measure.

The research method was inspired by the research done in [8], and a similar approach was taken by analyzing the subject common name field of the certificate entries in the dataset and the certificate entries were filtered based on [12] to ensure that only entries with valid Top-Level Domain endings along with a valid subject country remained. The entries were then grouped by subject country and normalized based on known statistics regarding the number of domains registered to each country around the global, creating the percentage of domains vulnerable to the POODLE attack within each country. This will be compared to the Global Cybersecurity Index (GCI) of each country from [4] in order to determine whether a correlation exists.

As the data variables subject to analysis here are both continuous, one may immediately think of using Pearson's correlation coefficient to determine whether such a correlation exists: Pearson's correlation coefficient is defined as follows:

$$\rho_{X,Y} = \frac{\sum(X_i\text{-}\overline{X})(Y_i\text{-}\overline{Y})}{\sqrt{\sum(X_i\text{-}\overline{X})^2 \sum(Y_i\text{-}\overline{Y})^2}}; -1 \leq \rho_{X,Y} \leq 1$$

Where a correlation (ρ) of 1 means that the variables are perfectly, positively, and linearly correlated, and vice versa, a correlation of -1 means that the variables are perfectly, negatively, and linearly correlated. A correlation of 0 means that there is no linear correlation. Values in between may be interpreted as having varying degrees of strength with regards to the linear correlation.

Before applying Pearson's correlation coefficient, one must ensure that the data is bivariate normally distributed before being able to proceed with the test. This will be done by determining whether each variable is indeed normally distributed through the Shapiro-Wilk normality test (in which the p-value must be greater than 0.05 for the data to be of a normal distribution) and a visual Q-Q plot inspection (in which an overwhelming majority of points must lie on the line). This holds since if both variables are individually normally distributed, they must be bivariate normally distributed.

In the event that the normality condition does not hold, Spearman's Correlation Coefficient is to be employed instead, which is defined as follows:

$$\rho_{\mathrm{rank}_X,\mathrm{rank}_Y} = \frac{\mathrm{cov}(\mathrm{rank}_X, \mathrm{rank}_Y)}{\sigma_{\mathrm{rank}_X}\sigma_{\mathrm{rank}_Y}}; \ -1 \leq \rho_{\mathrm{rank}_X,\mathrm{rank}_Y} \leq 1$$

Where a correlation (ρ) of 1 means that the variables are perfectly and positively correlated, and vice versa, a correlation of -1 means that the variables are perfectly and negatively correlated. A correlation of 0 means that there is no correlation. Note that this is very similar to Pearson's correlation, except that there is no normality requirement, and there is no linear correlation requirement, as Spearman's Correlation Coefficient operates on ranks rather than raw scores, and that it tests for monotonicity rather than linearity.

If the data is indeed normally distributed, then the Pearson Correlation Coefficient is to be calculated; otherwise, Spearman's Rank Correlation is to be calculated to determine whether a correlation exists.

Research

The result of the data filtering and aggregation by country process may be found in Appendix A. Firstly, the normality of the GCI data set was determined, the Shapiro-Wilk test results may be found in Table 1 below, and the corresponding Q-Q plot in Figure 3.

Table 1. Shapiro-Wilk Normality Test Results for the GCI data set.

Mean	0.493428571429
Standard Deviation	0.236865356857
Test Statistic	0.964513301849
p-value	0.00653609540313

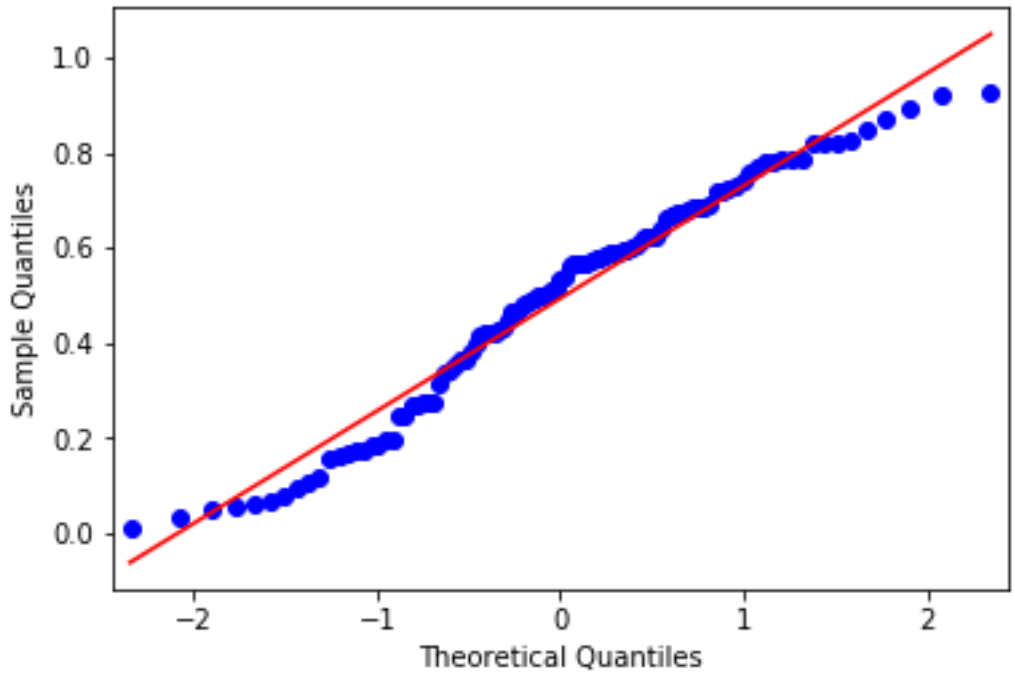

Figure 3. Q-Q plot of the GCI data set.

From inspection of the Q-Q plot and a p-value of 0.00653609540313, the GCI data does not exhibit a normal distribution. This is logical, given that the goal of the GCI report is to push all countries towards a higher GCI, which means that the GCI data will be continuously skewed to the right over time.

Hypothesis 1:

The normality of the percentage of currently vulnerable servers per country was determined, for which the Shapiro-Wilk test results may be found in Table 2 and the corresponding Q-Q plot in Figure 4.

Table 2. Shapiro-Wilk Normality Test Results for the percentage of currently vulnerable domains per country.

Mean	0.000157851960873
Standard Deviation	0.000359606775333
Test Statistic	0.330132365227
p-value	9.70157101222e-20

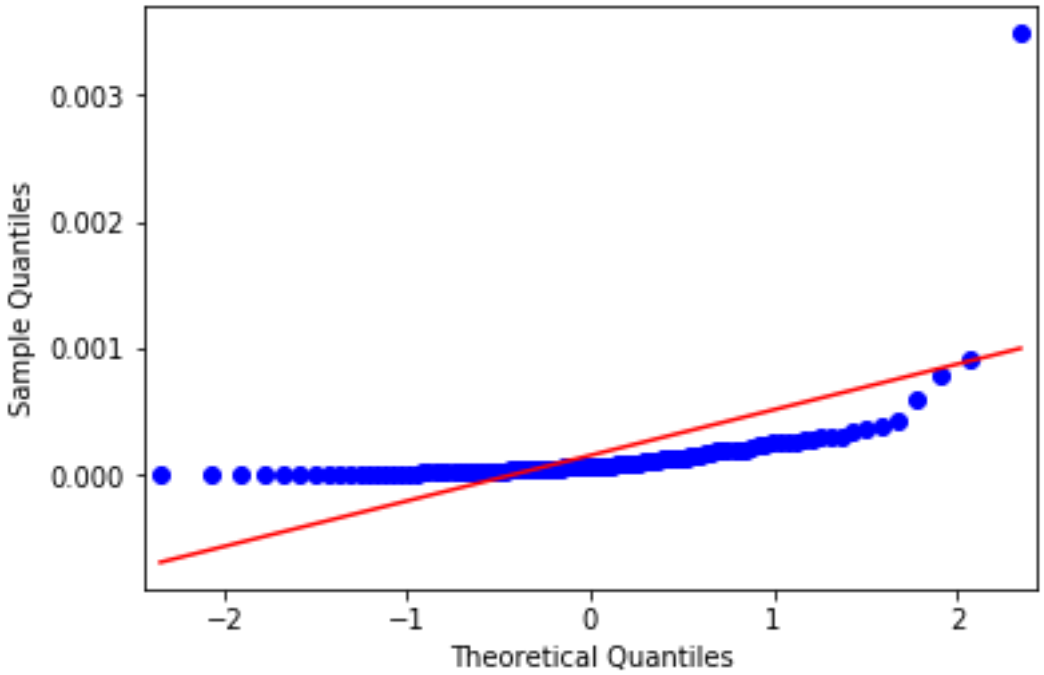

Figure 4. Q-Q plot for the percentage of currently vulnerable domains per country data.

As it can be seen from the Q-Q plot and from the astronomically small p-value, the data does not exhibit a normal distribution. Given that the sample size for each of these data sets is greater than 100, this does not seem to stem from a small sample issue, and therefore, it is quite likely that the data sets simply do not conform to a normal distribution. All of this points to the inability to perform a parametric analysis with Pearson's correlation coefficient, and that a non-parametric analysis through Spearman's rank correlation should be performed, with a null hypothesis that the percentage of currently vulnerable servers per country and the GCI value of that country are uncorrelated. This yields the results shown in Table 3.

Table 3. Spearman's rank correlation results for the percentage of currently vulnerable domains per country.

Spearman Correlation Coefficient (ρ)	-0.199776586176
p-value	0.0410285003474

With a p-value of 0.04 < alpha = 0.05, the null hypothesis is rejected, meaning that there exists a statistically significant correlation between the percentage of currently vulnerable servers of a country and the GCI value of said country. However, with a ρ of -0.199776586176, this means that the two are only weakly and negatively correlated. This result is therefore in support of the hypothesis that countries higher on the GCI have a smaller percentage of domains vulnerable to the POODLE attack in general, but at the same time supports the idea that the ties between the two are weak, and that there are potentially external factors that can have much stronger influence.

Hypothesis 2:

The normality of the decline in percentage of vulnerable servers per country was determined, for which the Shapiro-Wilk test results may be found in Table 4 and the corresponding Q-Q plot in Figure 4.

Table 4. Shapiro-Wilk Normality Test results for the decline in percentage of vulnerable servers per country.

Mean	-1.7827833253e-05
Standard Deviation	7.12634620028e-05
Test Statistic	0.49278652668
p-value	2.27249278279e-17

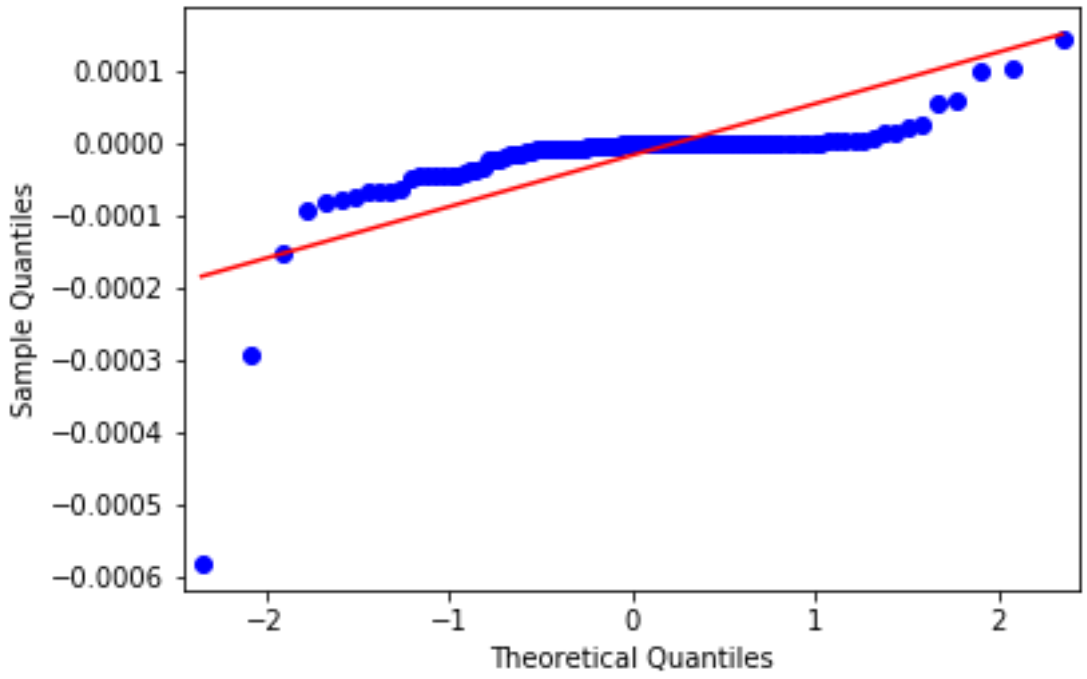

Figure 5. Q-Q plot for the decline in percentage of vulnerable servers per country.

As observed from the Q-Q plot, along with the extremely miniscule p-value from the Shapiro-Wilk test, the data once again does not exhibit a normal distribution. Given that the sample size for each of these data sets is again greater than 100, it is therefore quite likely that the data set also does not conform to a normal distribution. Once again, this points to the inability to perform a parametric analysis with Pearson's correlation coefficient, and that a non-parametric analysis through Spearman's rank correlation should be performed, which yield the results shown in Table 5.

Table 5. Spearman's rank correlation results for the percentage of currently vulnerable domains per country.

Spearman Correlation Coefficient (ρ)	-0.246783183825
p-value	0.0111524200344

With a p-value of 0.0111524200344 < alpha = 0.05, the null hypothesis is rejected, meaning that there exists a statistically significant correlation between the decline in percentage of vulnerable servers of a country and the GCI value of said country. However, with a ρ value of -0.246783183825, this means that the two are once again only weakly and negatively correlated, albeit the correlation is slightly stronger than in hypothesis 1. This result is therefore in support of the hypothesis that there indeed exists a greater decline in the percentage of domains vulnerable to the POODLE attack in countries higher on the GCI value, but at the same time, the support from the results are weak, and that there are once again potentially external factors that can have much stronger influence.

Limitations

Unfortunately, the data set of servers vulnerable to the POODLE attack is only available for a period of 8 months, from January 2018 to August 2018. This data set is also constructed by IP range scans, with Dutch IP ranges being the primary target. Both these factors limit the effectiveness of the study, as the data set represents only a subset of all servers vulnerable around the world, and for a relatively short period of time, and long after the initial disclosure of the vulnerability, which limits its power in supporting the hypotheses, particularly hypothesis 2, as the most valuable period for which to have data would be three weeks after the initial disclosure, the point at which Zhang et al stated that vulnerability response levels off [8]. It is recommended for future research to obtain more vulnerable server data, for greater and more relevant timeframes, in order to get a clearer and better picture of the vulnerability percentages and rates for various countries.

This study was also restricted to countries that appear both in the GCI data set and the vulnerable servers data set; while there were more countries in the latter, they could not be used since there would be no entry in the GCI data set to compare them against. The latter also contained a large amount of server entries with an invalid or empty subject country field in the SSL certificates, reducing the number of usable vulnerable server entries for the purpose of this study, and thereby reducing the sample size. It is recommended for future research to also find other independent metrics that may be used as indicators of a country's cybersecurity level, and to utilize them as benchmarks to see if different outcomes are discovered.

Lastly, there were mainly two limitations in the methods used in this analysis: One is that the Spearman's Rank Correlation analysis is by nature non-parametric, and therefore has weaker power than parametric analysis methods. The other is that this method of analysis reveals nothing regarding causality; that is, while it was determined that a certain level of correlation exists between the percentage of vulnerable servers per country and said country's GCI value, it was assumed that the latter caused the former, rather than having that be proven by statistical analysis. In other words, the analysis does not speak to whether the former caused the latter, or vice versa. The same applies to the correlation between the decline in percentage of vulnerable servers per country and said country's GCI value. It is recommended for future research to discover exactly what kind of distributions the percentage of currently vulnerable servers per country and the decline in percentage of vulnerable servers per country follow, so that more powerful statistical analysis methods may be applied in order to have a more accurate support level for the hypotheses at hand.

Conclusion

As online retail and e-commerce grows, so will the cybercrimes that aim to take advantage of the participating businesses and customers. Therefore, it is imperative to have a good understanding of the issues that plague the industry today, as well as the effectiveness of existing, already deployed strategies, especially if new government regulations and interventions are to be made in order to correct for market failures. The data set of domains vulnerable to the POODLE attack offers a glimpse into the world of SSL vulnerabilities that an adversary may exploit, and the Global Cybersecurity Index (GCI) offers a nice metric in which one may relatively judge the cybersecurity efforts of various countries. This leads to the main research question of to which degree are the domains running insecure SSL protocols within a country correlated to the level of cybersecurity laws and regulations of that same country, and in order to answer this question, two hypotheses were created in order to guide the research and data analysis:

- Hypothesis 1: Countries with a higher GCI have a smaller percentage of domains vulnerable to the POODLE attack
- Hypothesis 2: There exists a greater decline in percentage of domains vulnerable to the POODLE attack in countries with a higher GCI

Based on the results in the Research section, there is indeed a negative but weak correlation between the percentage of vulnerable domains and the GCI of a given country, as well as between the decline in percentage of vulnerable domains and the GCI of a given country. This means that both hypotheses are supported, which in turn lends support to the conclusion that higher levels of cybersecurity legislation do have an impact on reducing the number of domains that continue to use insecure SSL protocols.

However, because of the weakness of the correlation, this result is in support of Moore's argument that governmental intervention today is indeed not particularly effective for everyday scenarios that consumers face, as well as the argument of Cybenko and Hughes that policies in place today are not capable of facing adversarial threats across a full spectrum of vulnerabilities. All of this means that indeed, further research and development is required to determine a modern, full-spectrum solution that will be effective against the cyber threats faced by consumers everyday, and that regulatory bodies must put together the market

incentives and regulations to ensure that the solution will be implemented properly, for the sake of the affected nation’s economy and its citizens.

References

[1] Ecommerce Europe, "Release Global Ecommerce Report," 5 October 2017. [Online]. Available: https://www.ecommerce-europe.eu/press-item/release-global-ecommerce-report/. [Accessed 15 November 2018].

[2] Statista, "Retail e-commerce sales worldwide from 2014 to 2021 (in billion U.S. dollars)," March 2018. [Online]. Available: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/. [Accessed 15 November 2018].

[3] B. Möller, T. Duong and K. Kotowicz, "This POODLE Bites: Exploiting The SSL 3.0 Fallback," September 2014. [Online]. Available: https://www.openssl.org/~bodo/ssl-poodle.pdf. [Accessed 15 November 2018].

[4] International Telecommunication Union, "Global Cybersecurity Index 2017," 2017.

[5] J. Hughes and G. Cybenko, "Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity".

[6] K.-K. R. Choo, "Cyber threat landscape faced by financial and insurance industry".

[7] T. Moore, "The economics of cybersecurity: Principles and policy options," *International Journal of Critical Infrastructure Protection,* vol. 3, no. 3-4 , pp. 103-117, 2010.

[8] L. Zhang, D. Choffnes, T. Dumitras, D. Levin, A. Mislove, A. Schulman and C. Wilson, "Analysis of SSL Certificate Reissues and Revocations in the Wake of Heartbleed," *Communications of the ACM,* vol. 61, no. 3, pp. 109-116, 2018.

[9] L. Allodi and F. Massacci, "Security Events and Vulnerability Data for Cybersecurity Risk Estimation," *Risk Analysis - Special Issue: Advances in Risk Analysis with Big Data,* vol. 37, no. 8, pp. 1606-1627, 2017.

[10] "poodlessl.csv.gz," [Online]. Available: https://surfdrive.surf.nl/files/index.php/s/3l3byoxrUJM8mKd. [Accessed 6 September 2018].

[11] "Domain registrations, by country," Domain Name Stat, [Online]. Available: https://domainnamestat.com/statistics/country/others. [Accessed 15 October 2018].

[12] Internet Assigned Numbers Authority, "TLDs Alpha By Domain," 8 Nov 2018. [Online]. Available: http://data.iana.org/TLD/tlds-alpha-by-domain.txt. [Accessed 8 Nov 2018].

Appendix A

Table 6. Filtered domain data from the data set of servers vulnerable to the POODLE attack, grouped by country.

Country	Vulnerable domain count at the beginning of dataset	Vulnerable domain count at the end of dataset	Total domain count	Vulnerable domain percentage at the beginning of dataset	Vulnerable domain percentage at the end of dataset	GCI	Decline in percentage of vulnerable domains
AD	1	1	17596	0.000057	0.000057	0.057	0.00E+00
AE	28	25	363277	0.000077	0.000069	0.566	-8.26E-06
AF	1	1	67178	0.000015	0.000015	0.245	0.00E+00
AM	3	1	23782	0.000126	0.000042	0.196	-8.41E-05
AO	1	1	6320	0.000158	0.000158	0.078	0.00E+00
AR	5	9	263023	0.000019	0.000034	0.482	1.52E-05
AT	36	32	1312974	0.000027	0.000024	0.639	-3.05E-06
AU	107	78	1971599	0.000054	0.00004	0.824	-1.47E-05
AZ	1	1	19373	0.000052	0.000052	0.559	0.00E+00
BA	1	1	23639	0.000042	0.000042	0.116	0.00E+00
BE	214	208	679946	0.000315	0.000306	0.671	-8.82E-06
BG	12	13	762493	0.000016	0.000017	0.579	1.31E-06
BH	5	6	17527	0.000285	0.000342	0.467	5.71E-05
BR	17	8	3142883	0.000005	0.000003	0.593	-2.86E-06
BY	6	6	30356	0.000198	0.000198	0.592	0.00E+00
BZ	1	2	51103	0.00002	0.000039	0.182	1.96E-05
CA	116	78	10091306	0.000011	0.000008	0.818	-3.77E-06
CH	147	106	902136	0.000163	0.000117	0.727	-4.54E-05
CI	2	4	20376	0.000098	0.000196	0.416	9.82E-05
CL	4	3	89239	0.000045	0.000034	0.367	-1.12E-05
CN	164	124	27839624	0.000006	0.000004	0.624	-1.44E-06
CO	1	2	357536	0.000003	0.000006	0.569	2.80E-06
CR	2	2	85555	0.000023	0.000023	0.336	0.00E+00
CV	1	1	3766	0.000266	0.000266	0.058	0.00E+00
CY	25	18	198101	0.000126	0.000091	0.487	-3.53E-05
CZ	49	40	1173642	0.000042	0.000034	0.609	-7.67E-06
DE	337	271	6460161	0.000052	0.000042	0.679	-1.02E-05
DK	95	90	1185236	0.00008	0.000076	0.617	-4.22E-06
DM	2	1	3419	0.000585	0.000292	0.01	-2.92E-04
DO	1	1	52957	0.000019	0.000019	0.162	0.00E+00
DZ	1	1	27539	0.000036	0.000036	0.432	0.00E+00
EC	1	1	77663	0.000013	0.000013	0.466	0.00E+00
EE	24	22	114508	0.00021	0.000192	0.846	-1.75E-05

EG	16	10	131213	0.000122	0.000076	0.772	-4.57E-05
ES	197	178	2874154	0.000069	0.000062	0.718	-6.61E-06
FI	83	71	492535	0.000169	0.000144	0.741	-2.44E-05
FR	269	229	6567038	0.000041	0.000035	0.819	-6.09E-06
GB	679	567	12659295	0.000054	0.000045	0.783	-8.85E-06
GE	3	3	28845	0.000104	0.000104	0.819	0.00E+00
GR	53	43	197309	0.000269	0.000218	0.475	-5.07E-05
HN	1	1	13640	0.000073	0.000073	0.048	0.00E+00
HR	18	13	73139	0.000246	0.000178	0.59	-6.84E-05
HU	35	25	126979	0.000276	0.000197	0.534	-7.88E-05
ID	11	7	850447	0.000013	0.000008	0.424	-4.70E-06
IE	42	33	365793	0.000115	0.00009	0.675	-2.46E-05
IL	64	45	404541	0.000158	0.000111	0.691	-4.70E-05
IN	51	44	3730226	0.000014	0.000012	0.683	-1.88E-06
IR	14	18	742938	0.000019	0.000024	0.494	5.38E-06
IS	2	3	19011	0.000105	0.000158	0.384	5.26E-05
IT	237	215	2861561	0.000083	0.000075	0.626	-7.69E-06
JO	3	3	46202	0.000065	0.000065	0.277	0.00E+00
JP	156	114	5874216	0.000027	0.000019	0.786	-7.15E-06
KE	9	7	96560	0.000093	0.000072	0.574	-2.07E-05
KG	2	2	7676	0.000261	0.000261	0.27	0.00E+00
KR	34	36	1299436	0.000026	0.000028	0.782	1.54E-06
KW	18	15	39374	0.000457	0.000381	0.104	-7.62E-05
KZ	1	4	115402	0.000009	0.000035	0.352	2.60E-05
LB	3	3	73334	0.000041	0.000041	0.172	0.00E+00
LI	2	4	14088	0.000142	0.000284	0.194	1.42E-04
LK	2	2	46546	0.000043	0.000043	0.419	0.00E+00
LT	3	3	43331	0.000069	0.000069	0.504	0.00E+00
LU	13	10	168038	0.000077	0.00006	0.602	-1.79E-05
LV	18	18	57919	0.000311	0.000311	0.688	0.00E+00
MA	5	5	86146	0.000058	0.000058	0.541	0.00E+00
MD	3	3	14518	0.000207	0.000207	0.418	0.00E+00
ME	1	1	13209	0.000076	0.000076	0.422	0.00E+00
MK	3	2	15261	0.000197	0.000131	0.517	-6.55E-05
MT	19	15	58849	0.000323	0.000255	0.399	-6.80E-05
MX	6	7	1024420	0.000006	0.000007	0.66	9.76E-07
MY	6	4	482798	0.000012	0.000008	0.893	-4.14E-06
NA	3	2	24377	0.000123	0.000082	0.066	-4.10E-05
NE	7	6	1719	0.004072	0.00349	0.17	-5.82E-04
NG	11	10	226828	0.000048	0.000044	0.569	-4.41E-06
NL	11584	9249	15285581	0.000758	0.000605	0.76	-1.53E-04
NO	98	89	888645	0.00011	0.0001	0.786	-1.01E-05
NP	1	1	33736	0.00003	0.00003	0.275	0.00E+00

NZ	7	5	655962	0.000011	0.000008	0.718	-3.05E-06
OM	2	2	22391	0.000089	0.000089	0.871	0.00E+00
PH	8	5	277244	0.000029	0.000018	0.594	-1.08E-05
PK	2	2	229098	0.000009	0.000009	0.447	0.00E+00
PL	101	84	457819	0.000221	0.000183	0.622	-3.71E-05
PT	51	31	213710	0.000239	0.000145	0.508	-9.36E-05
QA	6	9	29121	0.000206	0.000309	0.676	1.03E-04
RO	35	23	178024	0.000197	0.000129	0.585	-6.74E-05
RS	12	9	66564	0.00018	0.000135	0.311	-4.51E-05
RU	234	169	1384633	0.000169	0.000122	0.788	-4.69E-05
SA	15	17	133337	0.000112	0.000127	0.569	1.50E-05
SB	1	1	1097	0.000912	0.000912	0.095	0.00E+00
SC	4	4	128454	0.000031	0.000031	0.184	0.00E+00
SD	1	1	2328	0.00043	0.00043	0.271	0.00E+00
SE	227	229	626426	0.000362	0.000366	0.733	3.19E-06
SG	20	14	801761	0.000025	0.000017	0.925	-7.48E-06
SI	11	11	47092	0.000234	0.000234	0.343	0.00E+00
SK	15	12	79573	0.000189	0.000151	0.362	-3.77E-05
SM	1	1	4789	0.000209	0.000209	0.174	0.00E+00
SO	0	1	3718	0	0.000269	0.034	0.00E+00
SR	3	3	3749	0.0008	0.0008	0.155	0.00E+00
TH	132	111	447659	0.000295	0.000248	0.684	-4.69E-05
TN	3	3	35581	0.000084	0.000084	0.591	0.00E+00
TR	69	58	2105520	0.000033	0.000028	0.581	-5.22E-06
UA	55	45	427020	0.000129	0.000105	0.501	-2.34E-05
US	2523	2029	71000898	0.000036	0.000029	0.919	-6.96E-06
UZ	2	2	26106	0.000077	0.000077	0.277	0.00E+00
VN	4	4	743445	0.000005	0.000005	0.245	0.00E+00
ZA	48	41	867599	0.000055	0.000047	0.502	-8.07E-06