Internet Hosting Provider Security Investments in server vulnerability to POODLE attacks

Delft University of Technology
WM0824TU Economics of Cybersecurity - Assignment Block 3

Group 16:
Marco Boom: 4393031
Maartje Flipsen: 4206444
Andrew Jiang: 4942795
Bryan van Wijk: 4363329

Monday October 8th 2018

Attachments: https://github.com/bryanvanwijk/TUD_WM0824

1 Security issue

The security issue explained is that of vulnerable servers as a consequence of SSL certification, in particular the SSL 3.0 version (SSLv3). Basically, an insecure server is vulnerable to POODLE attacks. In such an attack, an adversary exploits the vulnerability in the SSLv3 certification during the handshake protocol between client and server. He then acts as man-in-the-middle and is able to look into and interfere with the data traffic that uses the insecure channel.

The data set demonstrates that there are a large number of servers that remain vulnerable, even though the SSLv3 has long been replaced by more recent TLS versions (Holmes, 2015). In order to closely analyze how the vulnerable server entries in the data set relate to each internet hosting provider (IHP), a count of distinct IP addresses from the last week of the data set was selected, and grouped by the Autonomous System Number (ASN) they belonged to. This was done since it is assumed that any entry in the last week of the data set is still vulnerable, and that each IHP is assumed to run one ASN. This data was then normalized by querying WHOIS databases for all the IP ranges belonging to a given ASN, and aggregating the ranges to get the number of IPs. The result is shown in Figure 1. Note that there are 776 other ASNs that had a vulnerable percentage of lower than 5% that were filtered out for the sake of readability, making for a total of 791 ASNs.

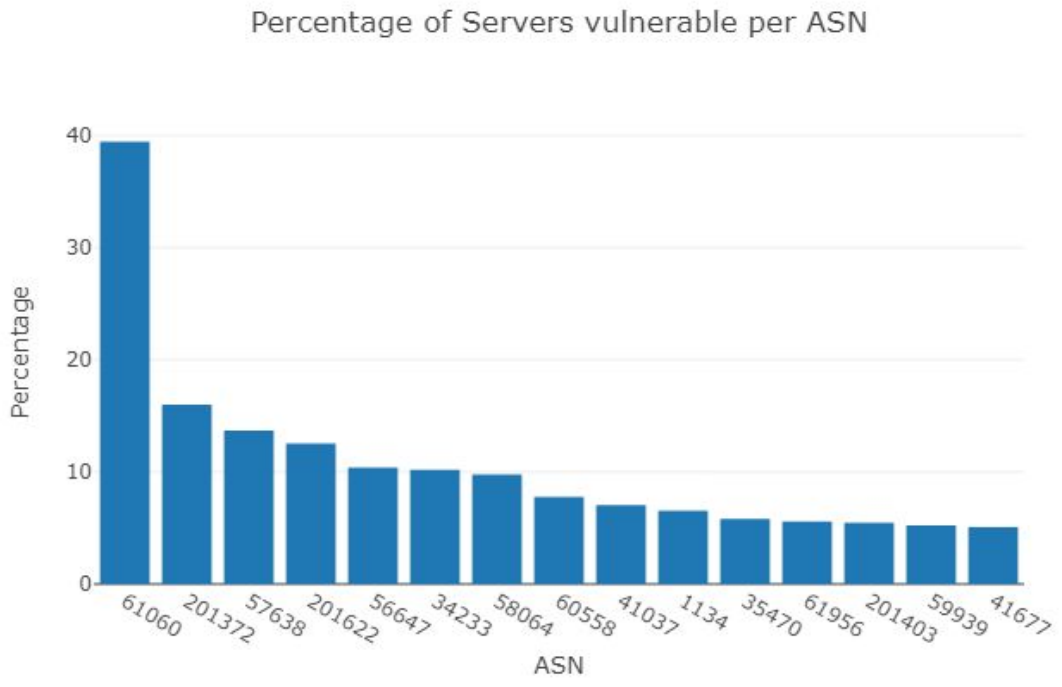

Figure 1: Percentage of servers vulnerable per ASN, for ASNs with vulnerability percentages >5%.

The large difference between each of the ASNs can potentially be explained by the different security policies in place by the IHPs handling them. For example, the IHP running ASN 61060, also known as XRCSERVICES, NL, may have lax security policies regarding protocols, hence such a high percentage rate. Another potential reason could be that they are specifically catering to customers who require older protocols for their legacy systems, and so, insecure protocols such as SSLv3 cannot be disabled.

2 Actors

2.1 Problem owner: Internet Hosting Provider (IHP)

The problem owner for this security issue is the organization that provides web servers to individuals and organizations: the Internet Hosting Provider (IHP).

In relation to the POODLE vulnerability, we assume the goal of the problem owner is to have secure servers. A fault tree analysis is used to understand which event leads to insecure servers. This is used as a starting point to identify possible strategies by the Internet Hosting Service. Figure 2 shows the developed fault tree. Here, the undesired event is the server being vulnerable to POODLE attacks, i.e. a web server being insecure. There are two ways a server can become insecure: either insecure protocols are used (e.g. SSLv3), or insecure server software is used. Considering the use of insecure protocols, three component failures lead to this: either server configuration is outdated, a new vulnerability is discovered, or fallback to insecure protocols is possible. Similarly, the use of an insecure server software can occur because of insecure acquired server software or outdated server software.

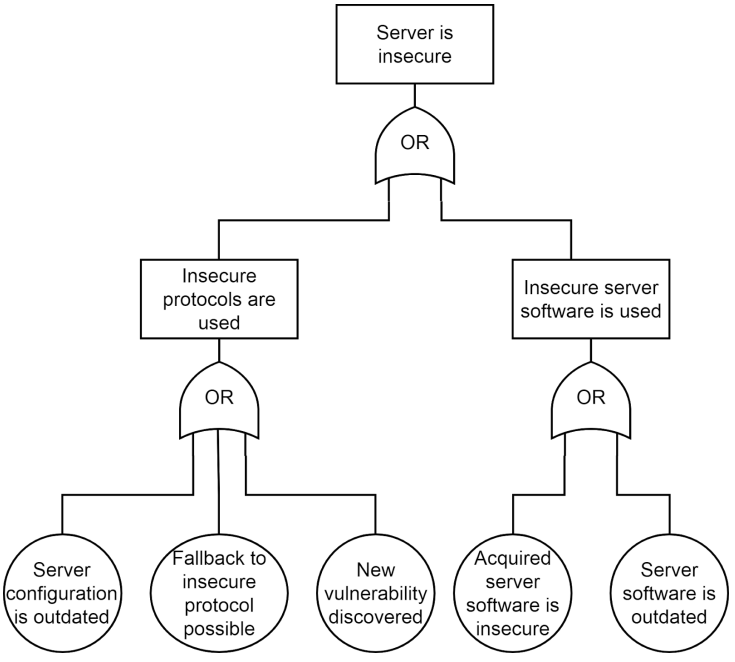

Figure 2: Fault tree analysis for insecure servers.

2.2 Problem owner strategies

We assume that the goal of the problem owner is to have secure servers. Figure 2 informs us on the components relevant to the event of a server being insecure. Failures by these components pose risks to the IHP. Instruments to deal with these risks can be divided into risk *avoidance*, risk *transfer*, risk *acceptance* and risk *mitigation.*

Risk avoidance strategies eliminate the risk completely. The most rigid strategy for this would be for an IHP to change their business model: you can't have vulnerable web servers if you don't deal in servers in the first place. A more realistic strategy would be for the IHP to avoid the risk by absorbing the responsibility to update the server configuration themselves, by disabling configuration updates of the servers by customers. This way, the IHP can be certain that necessary configuration updates to secure protocols are made directly. Those servers that cannot be updated should be dropped, as they pose continuous risk for which there is no patch.

Figure 3: strategies of the problem owner (IHP).

Alternatively, to risk avoidance, risk can be transferred. This can be to an insurance company or to the customer. In the first case, any or a part of the losses incurred by the IHP as a consequence of a security incident will be reimbursed by the insurance company. In the second case, the IHP is not liable anymore for the risks. Instead, the customer carries the risks. This risk transfer requires formalization in the forms of terms or clauses in the contract between the IHP and the customer.

Another formalization to deal with risk is the documentation of which risks are intentionally accepted by the IHP. Risk acceptance requires documentation before an incident occurs, since this justifies the lack of what appears at first glance due diligence by IHP to share- and stakeholders.

Most importantly, the risk can be mitigated. In the case where customers are responsible for the configuration of the server, the IHP could stimulate the updates. A system should be in place that detects the use of SSLv3 by servers. The customers utilising these web servers

should then be given a notice by the IHP to update the server configuration. Additionally, enforcement of the configuration updates is necessary. For example, within a certain time period after receiving the notice, customers should have updated their servers' configurations, or the IHP is entitled to suspend any services until the update is completed. Without enforcement, there would be no consequence to the customers and the risks are not mitigated when customers ignore notices.

2.3 Other actors

As mentioned before, in the security issue of vulnerable servers, customers and adversaries are involved. customers can either be individuals or organizations, the same applies to adversaries. However, because the goals and means of the individuals and organizations are expected to overlap significantly, they are taken as one actor.
Besides customers and adversaries, the actor network surrounding the security issue involves security providers and regulators. Security providers are companies that design and sell server software. Regulators consist of governments or internationally acclaimed NGOs that develop standards for voluntary compliance groups.

2.4 Other actors' strategies

The regulators can play a large role in legislation, litigation and standardization. With regards to the server vulnerability, regulators can design and implement regulations that stimulate security measures by the problem owner, like the enforcement of configuration updates. As well, the regulators can influence which risks can be transferred, or which risks are illegal to be accepted by the IHP. For regulators, the strategy has shifted to have more applicable laws and regulations in various areas regarding data protection and security (See the NIS Directive and GDPR in Europe). This reduces the risk of losses for consumers and corporations when an incident occurs, albeit at an increased cost to organizations, which need to implement measures to be compliant with these laws/regulations.

Depending on the contracts between IHPs and their customers, customers can update server configurations to use secure protocols. As well, they can undertake risk avoidance measures like avoiding the use of an insecure handshake protocol. Additionally, they can ask for support from the IHP, and should the IHP refuse to assist in helping to secure the servers provided to them, they can (like in the case of the Google Chrome privacy settings) do naming and shaming, causing the IHP to lose future customers.

For customers of IHPs, security awareness has risen due to data breaches where personal information was compromised (e.g., Equifax); no organization would willingly expose themselves to such bad press, and as such, the strategy for customers of IHPs has been to demand higher levels of security and better practices throughout their own organizations, as well as partner organizations, and to be more risk averse. This also reduces the risk of losses when an incident occurs.

Security providers have similar goals to the customers of the problem owners, since their revenue model is based on the security they can deliver to their security consumer (which

are the IHPs). Security providers deliver the server software, along with updates for it, and thereby influence how secure server software is. The speed with which the security provider responds to vulnerabilities, can also be relevant to the security of the server. For security providers, the strategy has shifted to changing default configurations in products that security consumers use so that by default, they will be more secure (Beck, 2014; Prince, 2014). This reduces risks for the customers, since it is less likely for them to make an error in the configuration that will cause a security issue in the future if the default configuration for their products is already secure.

Adversaries are actors that would want to enforce strategies that increase the risks for the customers of the problem owner. So, their interests are opposite of the other actors at play. The adversaries in the case of vulnerable servers to POODLE could impose strategies that make investing in security by the server owner seem unattractive. For example, adversaries could create a botnet posing as clients to organizations running outdated configurations on servers provided by IHPs, requesting the support for SSLv3 by a server. For the organization receiving these requests, this could lead them to believe that such a large amount of support requests for SSLv3 would make it unattractive to stop supporting SSLv3 by e.g. disabling fallbacks. This could lead to customers demanding support for SSLv3 at the IHPs and IHPs discontinuing with applying measurements for mitigating the POODLE vulnerability.

For adversaries, the migration of the majority of internet users to modern, up-to-date, and secure browsers also means that organizations that run various services are able to also take mitigation measures against POODLE with minimal impact to their customers, and attacks through POODLE have become much less exploitable. Therefore, the adversaries must change their attack vector in order to continue to succeed. This could mean exploiting newer vulnerabilities, or some sort of phishing attempt. As such, it has reduced the risk of the POODLE attack specifically, but may have increased the risk of incidents regarding other security vulnerabilities in the future.

3 Return on Security Investment (ROSI)

Because IHPs are constrained by resources and time, they opt to put the most effective strategy in place. For this, strategies need to be compared. One metric to do so is comparing in terms of money, using the Return on Security Investment (ROSI) (Sonnenreich, Albanese, & Stout, 2006). The ROSI aims to answer thich strategy provides the most value for money. The ROSI for a certain solution is calculated by determining the remainder of the amount of risk exposure mitigated by the solution and the cost of the solution. To say something on the result in comparison to the investment, the remainder is divided by the solution cost, resulting in the following equation:

$$ROSI = \frac{(Risk\ exposure * \%Risk\ mitigated) - Solution\ Cost}{Solution\ Cost}$$

Thus, the higher the return on investment, the better the strategy. The challenge for ROSI lies in an accurate estimation of the properties risk exposure, risk mitigation and solution cost (Sonnenreich et al., 2006).

To begin, risk exposure can be calculated by multiplying the estimated costs of an, in the case of POODLE vulnerability, insecure server with the estimated occurrence per year. It can be difficult to determine financial realistic cost factors, as the cost is usually dependent on business factors (cost of replacement, insurance, tax implications, etcetera). Therefore, one should strive to seek cost factors that can be measured independently from the problem owner context. For example, loss of intellectual property and loss of productivity (Sonnenreich et al., 2006). Other forms of loss are replacement costs, fines and judgements, competitive advantage and reputation loss (Jones, 2005).

Next, the percentage of mitigated risk by the solution should be estimated. Since it is difficult to quantify security, often is spoken mitigated risk in the concept of *prevented loss*. A hundred percent (100%) loss is prevented if the solution functions perfectly. Yet, this is most often not the case, because a trade-off is made in the functioning of the solution and the investment made, i.e. money spent on the solution or that no solution is capable of mitigating the risk perfectly. To be conservative, one could estimate a well-functioning solution to mitigate 85% of risk. Of course, this is a simplistic view, so multiple scenarios could be investigated where this percentage differs. For example, one could argue that the percentage of risk mitigated will decrease over time, as new risks are created. Similarly, the surrounding controls in place or additional solutions can have an influence on the percentage mitigated risk: complementing security solutions can profit from positive network effects (Sonnenreich et al., 2006).

Finally, the solution cost needs to be quantified. This cost consist of internal costs as a consequence of the implementation of the solution, as well as the affected productivity. For example, a two-step verification for authorized access will cost end-users time, this time can be perceived as lost productivity. Conversely, the productivity can also be increased due to the solution, as it may have solved other issues hampering productivity (Sonnenreich et al., 2006).

3.1 Updating to secure protocols by Leaseweb N.L.

We calculate the ROSI for the first strategy of the IHP described earlier, which is enforcing configuration updates to disable SSL usage. To use secure protocols, the IHPs should enforce upon its customers a requirement for an updated server configuration to completely disable insecure protocols, or prevent fallbacks (a.k.a. downgrades) to insecure protocols. As well, clients should be aided through this migration process as best as possible, and should migration not be possible, relationships with those customers should be terminated.

The calculation is made for one IHP chosen from our dataset, which is Leaseweb N.L. It is assumed that the same goals and means apply as discussed in the first section. Leaseweb is one of the organizations with a relative large number of servers in its organization, and as such, analyzing such an organization makes the calculations more interesting. Before

calculating the ROSI, estimations have to be provided for risk exposure, mitigation and the solution costs. As ROSI does not take time into account, the calculation is based on estimates for the first year after a security incident. For each estimation, a reflection is provided to discuss assumptions and restrictions of the method.

3.1.1 Risk exposure

The exposure to risk is the estimated cost of an insecure server multiplied by the estimated annual occurrence of a server being insecure. When exploring the costs and their occurrence, a scenario is considered where a breach has occurred and customers are fully aware of the security issues at Leaseweb. Several types of cost factors can be distinguished: reputation loss and the costs of litigation and fines as a consequence of the breach (Jones, 2005).

Firstly, the reputation costs which are estimated to be $200000, based on the average costs of cyber incidents found by Romanosky (2016). This is a rough estimate as it will depend on the media attention and other factors in the future, and will likely decrease over time. As well, because of the size and market share of the company, it is likely for these costs to be much higher. Opposingly, the time it takes to detect the incident, the way the IHP responds to it, the timing of the incident, and due diligence all affect the costs incurred (Jones, 2005).

Secondly, insecure servers can result in legal or regulatory costs. Depending on the sensitivity of the compromised information between end-user and server, the customers of Leaseweb might have complaints or lawsuits filed against them by their respective clientele. Leaseweb, therefore, might need to take up the responsibility of dealing with forwarding said filings to the appropriate customers, as well as acting as an intermediary, all of which amount to additional costs to the company's legal department, which could be $312000.

The estimated costs resulting from risk exposure will therefore be $200K + $312K = $512K per expected incident (see Table 1).

Table 1: Estimated risk exposure costs.

Cost factor	**Costs ($)**
Reputation cost	200,000
Legal costs overhead	312,000
Total costs for 1 incident	512,000

From the dataset we can derive the percentage of vulnerable servers Leaseweb owns in the Netherlands in the past weeks. Based on these measurements, the percentage of vulnerable servers in the future can be predicted assuming this percentage will be normally distributed. A normal distribution with $\mu = 5.2$ and $\sigma = 0.27$ does optimally fit the data. This percentage of

vulnerable servers can be mapped to the expected impact to make a prediction of the risk exposure impact. For sake of simplicity, we assume the expected number of incidents to be 100 per year which are equally spread over all servers vulnerable for the poodle attack in the Netherlands. This means that it is expected that when you have as a company 1% of all these vulnerable servers there will be 1 incident. Assuming this will linearly scale, in the case of 5% of the vulnerable servers there will be 5 incidents. The risk exposure will be normally distributed with μ = 5.2 * $512,000 = $2662400 and σ = 0.27 * $512,000 = $138240, as plotted in Figure 4. From this plot we derive the expected risk exposure to be between $2377426 and $2940366 with a 95.45% probability. The blue axis indicates the probability the impact is within a range of $50000 so, for example, the probability the impact is between $2600000 and $2650000 is 13.7%.

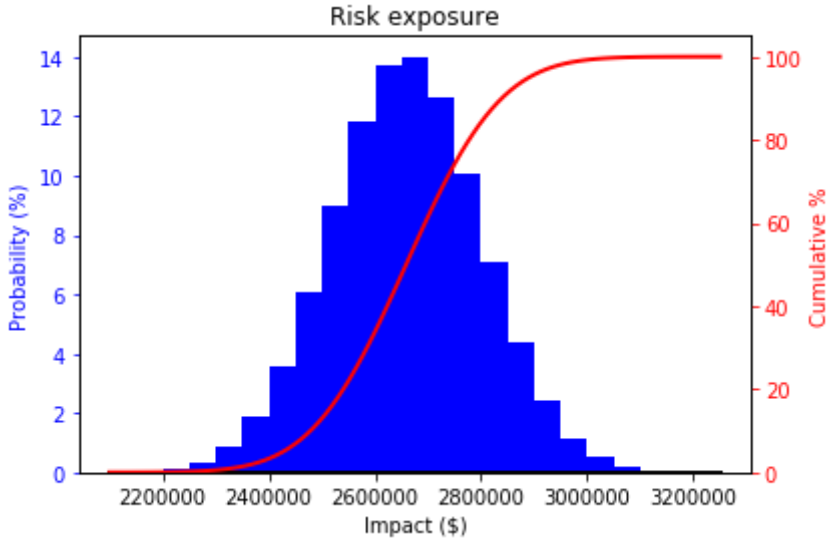

Figure 4: Risk exposure for Leaseweb without risk strategy.

3.1.2 Risk mitigation

The ‘security’ that enforcing to update the protocols will produce is difficult to measure. However, Sonnenreich et al. (2006) suggest a conservative valuation of a well-functioning solution should could mitigate 85% of the risk. Returning to the fault tree in Figure 2, the strategy of updating servers will secure the server directly. Therefore, one can assume the risk mitigation percentage to be high. Since the ROSI is only calculated for the first year after the servers were found insecure, a time-dependent decrease of risk mitigation percentage is out of scope. The solution that is being proposed ensures that servers will not be vulnerable at all to future POODLE attacks, and as such, the risk mitigated is 100% for the given scenario. However, the real-world effectiveness of the mitigation is dependent on how good the detection of SSLv3 works and how fast the customers update their servers. Therefore, in the upcoming calculations a mitigation of 85% is assumed.

3.1.3 Solution costs

With the chosen strategy, there are a few solution costs that would be incurred. These costs entail implementation and maintenance costs, but also lost revenues due to lost customers.

Firstly, losing customers because they should be able to support SSLv3 and are not able to support a newer protocol. Leaseweb has 7417 vulnerable servers before the risk strategy is applied. Shutting down these servers will cost $800 per year per server, because new customers for these servers will have to be found. Approximately 30% of these servers will need to be shut down which means a loss of 7417 * 0.3 * $800 = 1,780,080. There would likely also be additional customer support costs associated with this endeavour. This could be for training existing customer service agents to know how to address customers calling about this issue, or for creating a new support line specifically for this issue. Based on the prices for call center services from WorldWide Call Center (n.d.), we can make an upper-bound estimate of roughly $60USD/hour, at a rate of 10 hours a day. This yields a cost of $60 * 10 * 365 = $219,000/year.

Secondly, actually detecting if the customers are still using SSLv3 on the servers will at least require the man hours to setup a system which could automatically do this. As an upper-bound, let us estimate the amount of work to be roughly 8 weeks by a 4 man team; this yields 1280 hours on the project. At a rate of $50 salary per hour, this leads to a one-time expenditure of 1280 * $50 = $64000. Plus the cost of future maintenance, which we estimate to be $20000 per year.

The total cost for this risk strategy is a fixed $64,000 upfront, with a yearly recurring cost of $1,780,080 + $219,000 + $20,000 = $2,019,080/year (see Table 2).

Table 2: Estimated solution costs.

Cost factor	**Costs**	**Units**
Implement solution	64,000	$
Customer loss	1,780,080	$/year
Customer support costs (upper-bound)	219,000	$/year
Software & maintenance costs	20,000	$/year
Total fixed costs	64,000	$
Total recurring costs	2,019,080	$/year
Total costs for 1 year	2,083,080	$

3.2 ROSI calculation

$$ROSI = \frac{Risk\ Exposure * \%Risk\ Mitigated - Solution\ Cost}{Solution\ Cost}$$

Based on a risk mitigation of 85% the risk exposure should at least be higher than $\frac{Solution\ Cost}{0.85} = \frac{\$2{,}083{,}080}{0.85} = \$2,450,682$ to have a positive ROSI. From figure 4 we can derive a probability of 93% to have a risk exposure greater than $\$2,450,682$. This means the risk strategy to enforce customers to update their server configuration is a cost-effective strategy with 93% probability. However, given the rough estimation of the risk exposure costs and solution costs, as well as the fact that this return is for the first year after a security incident, this is a rough estimation.

4 Conclusion

There are still many servers vulnerable, even though the SSLv3 has long been replaced by more recent TLS versions. The problem owner for this security issue is the organization responsible for the server, i.e. the IHPs. From the perspective of the IHP, possible strategies were investigated. The most relevant strategy is to enforce rules and restrictions upon the IHP's clients to prevent fallback to less secure protocols and to force an update to the security protocols used. Another strategy is a preventive strategy focused on the mitigation of risks from the IHP to its clients by disclosing in the user agreement that the IHP takes no security responsibilities should the client choose to continue using insecure protocols.

There are different actors involved in this security issue, for example, the regulators, they can play a large role in legislation, litigation and standardization. Other actors are the customers that can undertake risk aversion measures like avoiding a handshake with an insecure protocol by disabling said protocol on the servers they acquire from the IHP. With the risen security awareness among the public, the IHP's customers should step up to the task, as the public demands higher levels of security from them. Adversaries are actors that would want to enforce strategies that increase the risks for the problem owner, and for the problem owner's customers. So, their interests are opposite of the other actors at play.

The ROSI calculation focused on the strategy of enforcing to use secure protocols, in which the server owner should either update the server configuration or prevent its customers from falling back to insecure protocols. From the calculated ROSI can be concluded that this strategy is a cost-effective strategy with a 93% probability, despite the variability in risk exposure.

5 References

Beck, B. (2014). LibreSSL 2.1.1. Released. Retrieved September 28, 2018, from https://marc.info/?l=openbsd-announce&m=141347213320729&w=2

Holmes, D. (2015). How much is my traffic is still SSLv3? Retrieved September 28, 2018, from https://devcentral.f5.com/articles/how-much-of-my-traffic-is-still-sslv3

Jones, J. A. (2005). An Introduction to Factor Analysis of Information Risk. *Risk Management Insight*, *1*(614). https://doi.org/10.1037/h0038787

Louis, T. (2011). How Much Is A User Valued At? Retrieved September 30, 2018, from https://www.businessinsider.com/how-much-is-a-user-worth-2011-7?international=true&r=US&IR=T

Prince, M. (2014). SSLv3 Support Disabled By Default Due to POODLE Vulnerability. Retrieved September 28, 2018, from https://blog.cloudflare.com/sslv3-support-disabled-by-default-due-to-vulnerability/

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

SimilarWeb. (2018). Playstation.net August 2018 Overview. Retrieved September 30, 2018, from https://www.similarweb.com/website/playstation.net

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return On Security Investment (ROSI) - A Practical Quantitative Model. *Journal of Research and …*, *38*(1), 45–56. https://doi.org/10.1145/581271.581274

WorldWide Call Center. (n.d.). Outsourcing Costs | Call Center Pricing. Retrieved September 30, 2018, from https://www.worldwidecallcenters.com/call-center-pricing/