Economics of Cyber Security

Łoin, Michał
m.f.loin-1@student.tudelft.nl

Meijerink, Mart
m.m.j.meijerink@student.utwente.nl

Man, Ka-Wing
k.w.man@student.tudelft.nl

Tubbing, Rico
r.tubbing@student.tudelft.nl

October 9, 2017

1 Introduction

Security can not be perfect since companies try to make profit and thus do not invest all their money in security. Besides this, some threat events might have a very low impact or small probability of happening. Therefore, it would be wise to use some kind of risk assessment, so it is possible to determine where a company needs to invest. A common used metric to determine where you want to invest is Return On Security Investment (ROSI).

In this paper we will try to calculate ROSI for a certain actor. First, we define the security issue in section 2, then we will discuss actors who can influence the security issue by using a risk strategy in section 3. The return on security investment (ROSI) for one of the actors and strategies from section 3 will be determined in section 4. Finally, in section 5 we conclude this paper.

2 Security Issue

As we have covered in the previous assignment, the main problem owner in case of a DDoS attack is the Internet Service Provider (ISP). When analysing this type of adversary activity, numerous parties are involved. However, the ISP as the owner of the infrastructure is the most important one. Other parties are described in section 3.

In the previous assignment we have analysed multiple metrics, that help us describe the danger of DDoS attack for a particular organisation. Some of them were directly connected to the characteristics of an attack, such as *size*, *duration* or *number of packets*. When analysing them, it is easy to deduce several differences against this type of attack. As studies show [16], adversaries tend to test the capacity of a target organisation, by gradually increasing the size of the DDoS attack, and stopping when the job is accomplished - in most cases, that is when the service is down. Therefore, characteristics of a successful attack clearly show how much data any organisation's network can withstand. It is clear that attackers need to address more of their resources against companies, that perform better in DDoS security.

In order to protect themselves, the ISPs can follow different risk strategies to minimise the impact. The first one is risk acceptance. It is very frequently used strategy, since it does not involve as many necessary actions as the other ones. It should be pointed, that additional security does not provide additional income to the company. It only helps reducing the eventual losses in case of the attack. Since ISPs usually own infrastructure of a great size, the costs of the attack would be significant, what reduces the likelihood, and therefore the risk.

Another risk management strategy is risk transfer. The most common solution in terms of risk transfer is acquiring some sort of insurance. However, it is more complicated in the IT security domain. As commonly known, the main principle insurance is to distribute the cost of the incident over every party that obtained it. The solution works fine, unless all accidents happen in virtually the same time. In that case, the insurance provider cannot cover all losses without going bankrupt. Sadly, this is often the case in the field of cyber security. Different approach to risk transfer is collaboration with another ISP, that could take some of the packet load, leading to larger total bandwidth.

The final risk management strategy is risk reduction. It will be further evaluated in section 4.

3 Actors and Strategies

The identified security issue can be influenced by multiple actors, besides the ISPs and their users. These actors can be divided in four categories:

- Security providers
- Security consumers
- The security industry
- Attackers

Each actor can adopt a risk strategy to influence the number of DDoS attacks. Risk strategies can by divided in four categories: acceptance, reduction, transfer, and avoidance. Each actor should compare strategies to determine which strategy suits the best for the actor, since each actor has different incentives.

In this section we will discuss which actors could influence the number of DDoS attacks and with which strategies they can influence the problem. First, the risk strategies of manufacturers of IoT devices will be discussed in subsection 3.1. Then the strategies of the government will be discussed in subsection 3.2. The differences between the strategies for manufacturers and government will be compared in subsection 3.3 and in subsection 3.4 the evolution of those strategies will covered.

3.1 Manufacturer

Besides the ISPs, other 'security providers' like manufacturers could be identified. Manufacturers of IoT devices and (consumer) routers are most interesting to research, as these devices have the biggest impact on the security issue [4]. These security providers are able to implement certain security standards and patch known vulnerabilities. It is believed that developing and implementing standards plays a key role in securing IoT devices [8]. However, as the consumers of their products are usually unaware of DDoS attacks and neither are they the target, no incentives exist for the manufacturers to implement security in their devices. They do not receive any demand from their customers.

Neglecting the security of IoT devices can inflict reputation damage to a manufacturer of IoT devices [14]. To reduce the financial impact of such an event, manufacturers can adopt two types of risk strategies, risk reduction and risk transfer.

Security audits, standards, and so on can improve the security of an IoT device and thus reduce the risk of manufacturers. However, implementing all these types of security is expensive. Therefore, another strategy that can be adopted is transfer.

3.2 Government

It is estimated that in 2020 there are around 50 billion IoT devices that are connected to the Internet [5]. This would greatly increase the attack surface of attackers. Next to this, the government employs IoT devices to reduce costs of for example smart buildings [3].For these two reasons, it is inevitable that the government will intertwine with the security of IoT devices. A government can adopt two types of risk strategies: reduction of risk and transfer of risk.

Reduction can be accomplished by introducing legislation for manufacturers to adopt certain security standards for IoT devices. This way it is less trivial to exploit IoT devices and misuse them to perform DDoS attacks.

Additionally, actively searching for individuals or groups who perform DDoS attacks and increasing fines will decrease the number of DDoS attacks. This strategy will boost the risk of those who perform DDoS attacks, and will likely result in a drop of the number of attacks. However, this strategy might not be viable since DDoS-as-a-service has been a rising trend [13]. Therefore, identifying the source of a DDoS attack and fining the source is problematic due to the jurisdiction of law enforcement.

3.3 Differences in Strategy

This section describes the differences in strategy for the different identified actors. Due to different incentives for manufacturers as opposed to governments, differences exist in their risks, risk appetite, and therefore differences in their strategy to handle the security issue.

Whereas for the manufacturers the main reason to handle the risks the security issue imposes will be business driven, governments will view the security issue a threat to one of their nation's critical infrastructures. Also, governments are responsible for the security aspects of a nation and want to protect their citizens.

Governments will use the tools they already posses. This will lead to legislation which will enable law enforcement to take down the attackers or frustrate their business model. Manufacturers on the other hand are only able to improve the security measures in their devices. Or otherwise accept or transfer any consequences due to their devices being misused.

3.4 Evolution of Strategies

Legislation on cyber security is lacking behind, but slowly coming into place. As of August 2017, the United States introduced the '*IoT Cybersecurity Act*'. The goal of this act is to move the IoT device manufacturers to implement a basic minimum set of security measures in their IoT devices. The act tries to reach this objective by defining the basic security level for IoT devices sold to the federal government. The sheer buying power of the government is thus used in the hope to boost the overall level of security of all IoT devices being sold [9].

In the Netherlands the intelligence services are getting more possibilities to gather and store data with the '*Wet op de inlichtingen- en veiligheidsdiensten*' [10]. The law of 2002 gave the intelligence services the ability to intercept telephone data and wireless signals, however, cabled communication networks were not included. The new version of this legislation enables the services to also tap all

data from cabled communication networks. With these new abilities the intelligence services could gather information about botnets used for DDoS-as-a-service or investigate DDoS attacks which might pose a threat to the Dutch national network infrastructure.

4 Investment Calculation

A risk strategy we have picked is setting up DDoS mitigation services for the ISP's.

Since successful DDoS attacks causes downtime, we need to know what the monetary damage is, that is causes by the downtime. Several sources have different numbers:

- According to Phonemon Institute and Radware in 2012, the average downtime per minute costs companies $22.000, the average amount of downtime of 54 minutes and the average amount of attacks in the past 12 months was 3 times. [15] This results in a average loss of $3,5 million per company. 705 IT and IT security practitioners were surveyed. See Figure 4.

- According to Incapsula in 2014, the estimated cost of an DDoS attack is $40.000 per hour. 49% of DDoS attacks last between 6-24 hours. [7] They concluded that an average DDoS attack may cost about $500.000. 270 North American organizations has been surveyed with the companies' size ranging from as few as 250 employees to 10.000 or more. There is no number of average amount of attacks per company. See Figure 5.

- According to Neustar in 2014, the costs of a DDoS attack per hour in 2013 can be seen in Figure 6 [11].

- According to Arbor Networks in 2016, the costs of a DDoS attack per minute can be seen in Figure 7 [2].

- According to Neustar in 2017, their respondents have collectively experienced a **minimum** revenue risk disruption in excess of $2,2 billion during the previous 12, which is $2,6 million on average across 849 organizations. See Figure 8 [12].

It may be that the numbers are different because Incapsula surveyed only North American organisations, where Neustar also surveyed European and Asia-Pacific organisations. Also, different numbers could also be because it is measured in 2012, 2014 and 2017. But that is unlikely because the differences are too far apart (Phonemon has concluded an average loss of $3,5 million/3 = $1.17 million per DDoS attack, whereas Incapsula concluded a loss of $500.000). For further calculations, we use the the most recent report, which is the one in 2017 released by Neustar (unless indicated).

In Figure 9, the number of attacks can be seen in percentage of the respondents.

Incapsula provides DDoS protection services and guarantees an uptime of 99.999% [1]. Unfortunately, for pricing of their enterprise plan, companies need to contact them. this is why we made a rough estimation for what the enterprise plan might costs. For example, Dutch ISP Ziggo had 2.600 employees in 2013 had 3.076.000 internet users in 2015[6, 17]. Incapsula's second plan (after the enterprise version) business plan costs $299 per month is for small businesses. Small businesses that don't need lot of employees and do have many customers (like web hosting services) might have 30 employees and 15.000 customers. A rough estimation for the enterprise plan would be $299 * (3.076.000 / 15.000) = $61.314,93.

Using the expected annual costs for the DDoS protection services and the information in Figure 8 and Figure 9, we can calculate the annual expected loss (ALE) distribution.

If we assume that "So frequently, we lost count" means every day a DDoS attack, the average amount of DDoS attacks in a year is $1 * 0.11 + 3.5 * 0.35 + 8 * 0.20 + 12 * 0.11 + 52 * 0.06 + 365 * 0.01 \approx 11$ DDoS attacks per year.

Because the Neustar report does not report what the average amount of downtime is, we use the 54 minutes stated in the Phonemon Institue report in 2012.

Also, if we leave out "not sure", and assume that "greater than $1 million" means $2 million in Figure 8 we have these following numbers:

Peak hourly revenue loss	percentage *
$0 - $24.999	8,60%
$25.000 - $49.999	8,60%
$50.000 - $99.999	15,05%
$100.000 - $249.999	21,51%
$250.000 - $499.999	17,20%
$500.000 - $1.000.000	16,13%
$1.000.001 - $2.000.000	12,90%

Figure 1: Average peak hourly revenue loss according to Neustar (2017), without DDoS mitigation.

* = percentage is divided by 0,93 because "Not sure" is left out.

Multiplying it with the average 11 attacks per year and the average downtime of 54 minutes, we get these numbers.

If DDoS mitigation services is deployed by Incapsula, 99,999% of the losses are covered. This means that the costs are lowered by a factor of 1000.

In Figure 10 and Figure 11 you can find the probability distribution of the ALE estimation without mitigation and with mitigation respectively.

Peak annual revenue loss	percentage *
$0 - $247.499	8,60%
$247.500 - $494.999	8,60%
$495.000 - $989.999	15,05%
$990.000 - $2.474.999	21,51%
$2.475.000 - $4.949.999	17,20%
$4.950.000 - $9.990.000	16,13%
$9.900.001 - $19.800.000	12,90%

Figure 2: Average annual revenue loss, without DDoS mitigation.)

Peak annual revenue loss	percentage
$0 - $247	8,60%
$247 - $495	8,60%
$495 - $990	15,05%
$990 - $2.475	21,51%
$2.475 - $4.949	17,20%
$4.950 - $9.990	16,13%
$9.900 - $19.800	12,90%

Figure 3: Average annual revenue loss, with DDoS mitigation.)

5 Conslusion

As can be concluded from the probability distributions of the annual expected loss, it is better to reduce rather than to accept the the risk. Mainly because of the cost that is lowered by a factor of 1000. But how probable this estimation is can be argued with. Some assumptions, that might not be true, had to be made before this estimation could be made.

- Number of Ziggo employees was 2.600 in 2013. In 2017, this might not be the case as no other numbers were found. This also holds for all numbers that are given in old reports. This affects the estimated cost of the monthly subscription payments to the DDoS protection services of Incapsula.
- The cost estimation of the mitigation services for a ISP like ziggo is $61.314. Of course smaller companies have lower hourly revenue losses after a DDoS attack. However, in the estimation, the costs are the same for all companies. In real life this would be different because smaller companies have lower costs for mitigation services due to their size. It means that the smaller companies with lower revenue losses after an DDoS attack will have more benefit than we estimated (due to lower monthly costs) and the bigger companies with higher revenue losses after an DDoS attack will have less benefit than we estimated (due to higher monthly costs).
- Also, what is worth denoting is that the numbers of the table are peak revenue loss. This means all results are peak results, meaning the maximum possible loss, not the average or anything else.

References

[1] Incapsula ddos protection services enterprise plan. `https://www.incapsula.com/enterprise-plan.html`, 2017. Accessed: 7 October 2017.

[2] T. Bienkowski. Can you afford $500 per minute of internet downtime?1000? more? `https://www.arbornetworks.com/blog/insight/can-you-afford-500-per-minute-of-internet-downtime-1000-more/`, February 2016. Accessed: 1 October 2017.

[3] D. Castro, J. New, and A. McQuinn. How Is the Federal Government Using the Internet of Things? `http://www2.datainnovation.org/2016-federal-iot.pdf`, 2016.

[4] ENISA. Major DDoS Attacks Involving IoT Devices. `https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices`, November 2016. Accessed: 30 September 2017.

[5] P. Fraga-Lamas, T. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López. A review on internet of things for defense and public safety. *Sensors (Switzerland)*, 16(10), 2016.

[6] L. Global. Liberty global reports first quarter 2015 results. `http://www.libertyglobal.com/pdf/press-release/Liberty-Global-Earnings-Release-Q1-15-FINAL.pdf`, 2015. Accessed: 7 October 2017.

[7] Incapsula. Incapsula Survey : What DDoS Attacks Really Cost Businesses. `https://lp.incapsula.com/rs/incapsulainc/images/eBook-DDoSImpactSurvey.pdf`, November 2014. Accessed: 1 October 2017.

[8] S. L. Keoh, S. S. Kumar, and H. Tschofenig. Securing the Internet of Things: A Standardization Perspective. *IEEE Internet of Things Journal*, 1(3):265–275, June 2014.

[9] B. Krebs. Krebs on security. `https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/`, August 2017.

[10] Nederlandse Overheid. Wet op de inlichtingen- en veiligheidsdiensten 2017. http://wetten.overheid.nl/BWBR0039896/2017-09-01, 2017.

[11] Neustar. Neustar Annual DDoS Attacks and Impact Report. https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf, 2014. Accessed: 1 October 2017.

[12] Neustar. Worldwide DDoS Attacks & Cyber Insights Research Report. https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/neustar-2017-worldwide-ddos-attacks-cyber-insights-research-report.pdf, May 2017. Accessed: 1 October 2017.

[13] A. Noroozian, M. Korczyński, C. H. Gañan, D. Makita, K. Yoshioka, and M. van Eeten. *Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service*, pages 368–389. Springer International Publishing, 2016.

[14] Obermaier, Johannes, Hutle, and Martin. Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems. In *Proceedings of the 2Nd ACM International Workshop on IoT Privacy, Trust, and Security*, IoTPTS '16, pages 22–28, New York, NY, USA, 2016. ACM.

[15] Ponemon Institute. Cyber Security on the Offense: A Study of IT Security Experts. https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf, November 2012. Accessed: 1 October 2017.

[16] A. Wang, A. Mohaisen, W. Chang, and S. Chen. Delving into internet ddos attacks by botnets: characterization and analysis. In *Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP International Conference on*, pages 379–390. IEEE, 2015.

[17] Ziggo. Ziggo sociaal jaarverslag. https://www.ziggo.com/sociaal-jaarverslag/2013/facts-and-figures.php, 2013. Accessed: 7 October 2017.

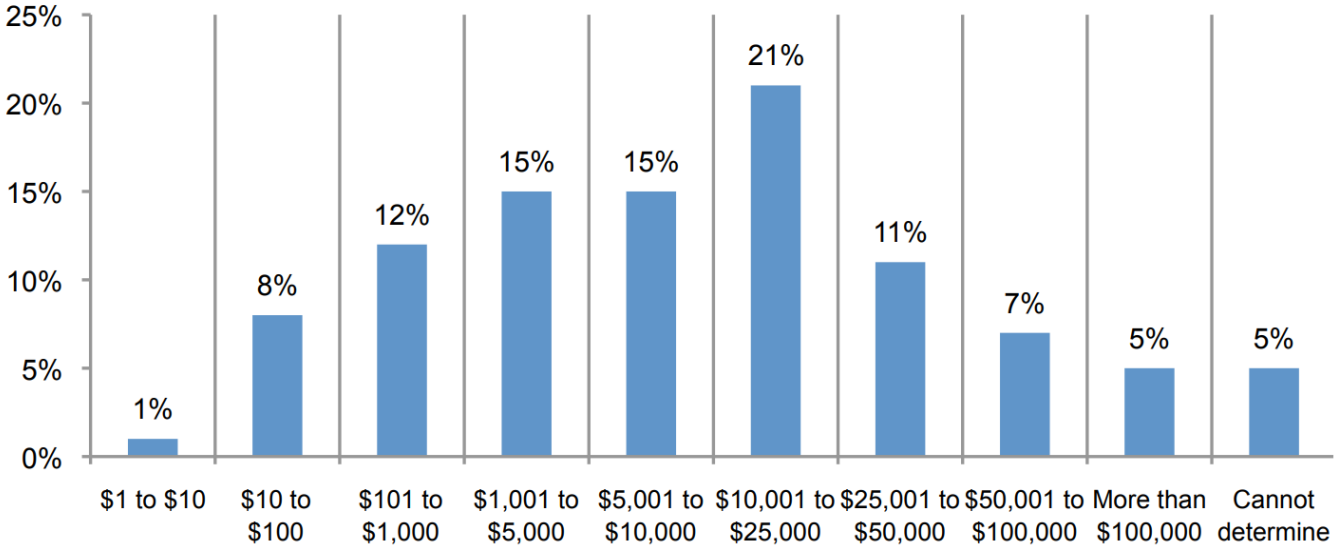

Figure 4: Cost per minute of downtime according to Phonemon Institute and Radware (2012).

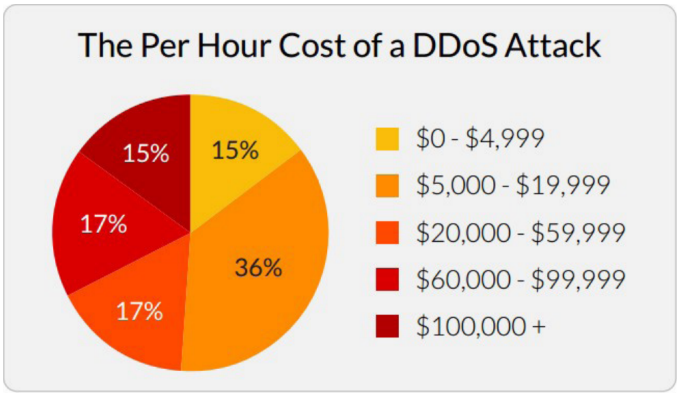

Figure 5: The per hour cost of a DDoS Attack according to Incapsula (2014).

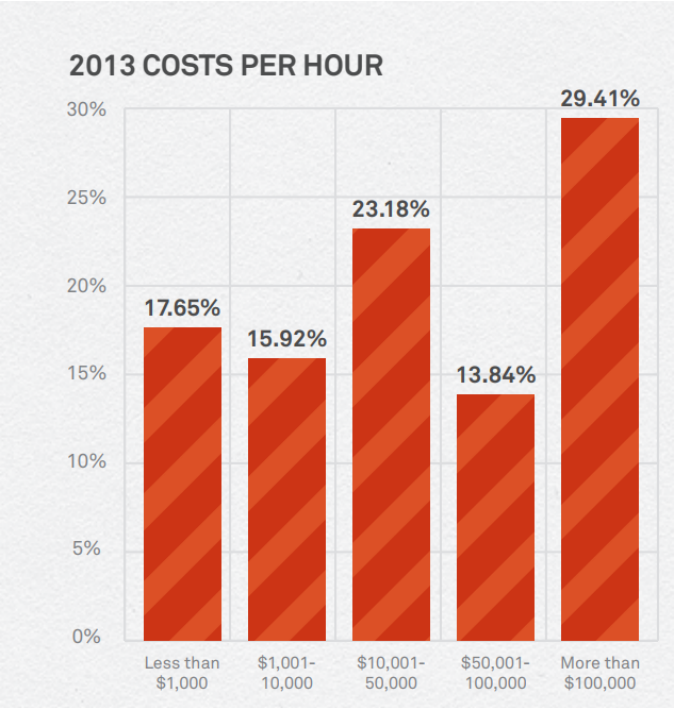

Figure 6: The per hour cost of a DDoS Attack in 2013 according to Neustar (2014).

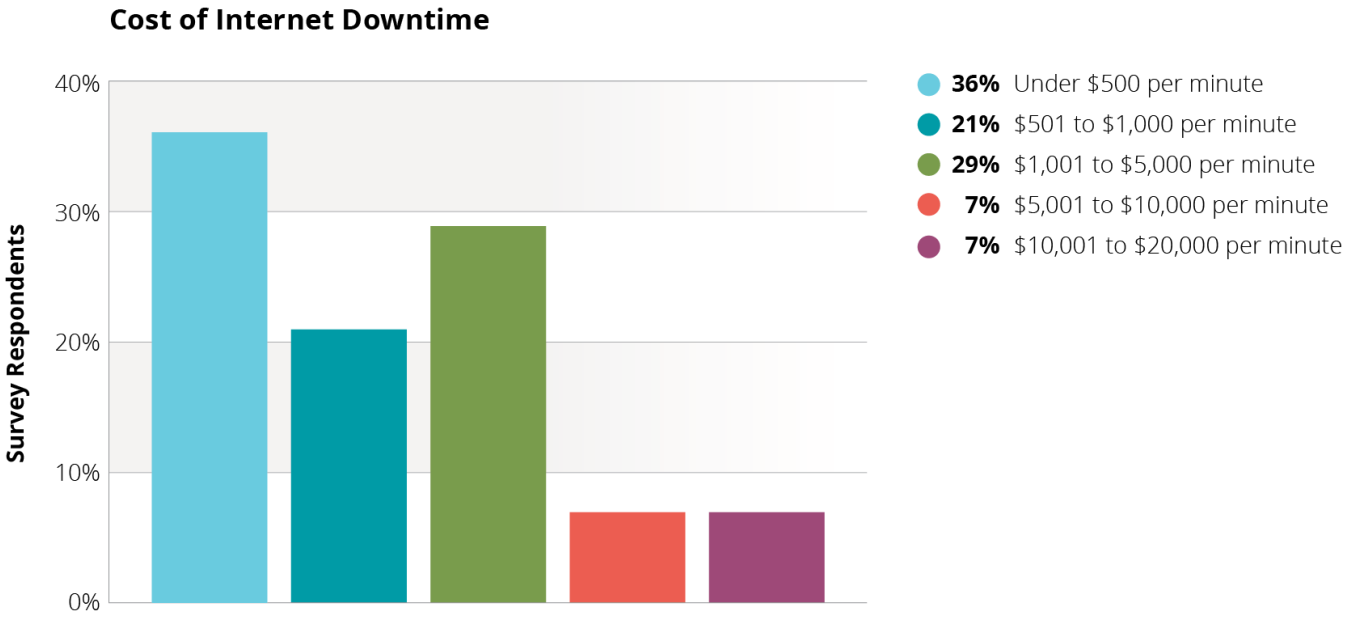

Figure 7: Cost of internet downtime per minute.

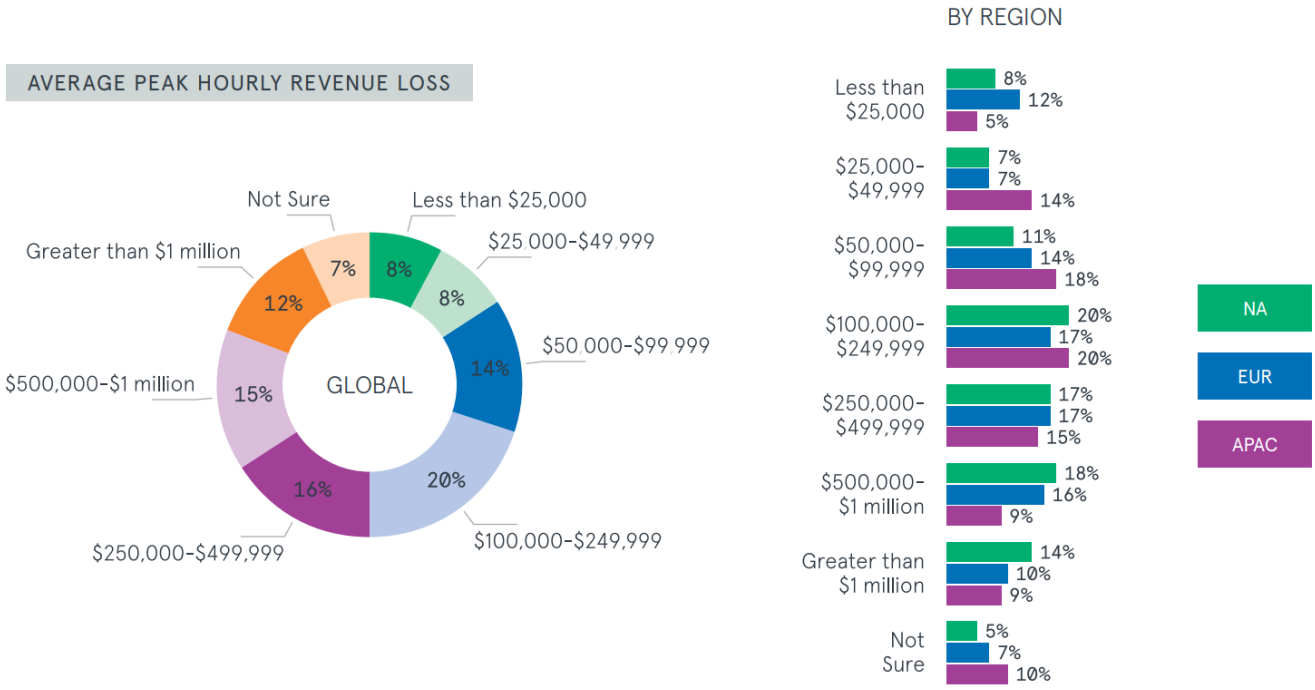

Figure 8: The average peak hourly revenue loss globally and regionally (North America, Europe and Asia-Pacific) according to Neustar (2017).

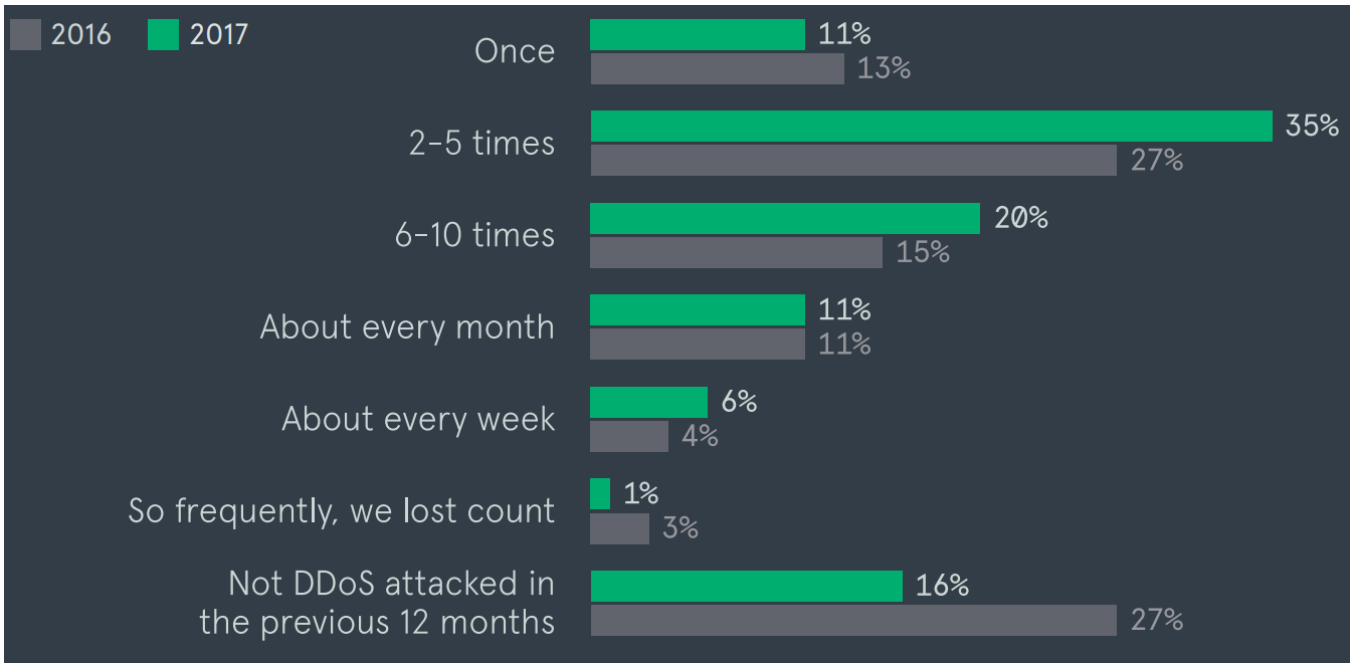

Figure 9: Ferquency DDoS attacks in the past 12 months in 2016 and 2017 according to Neustar (2017)

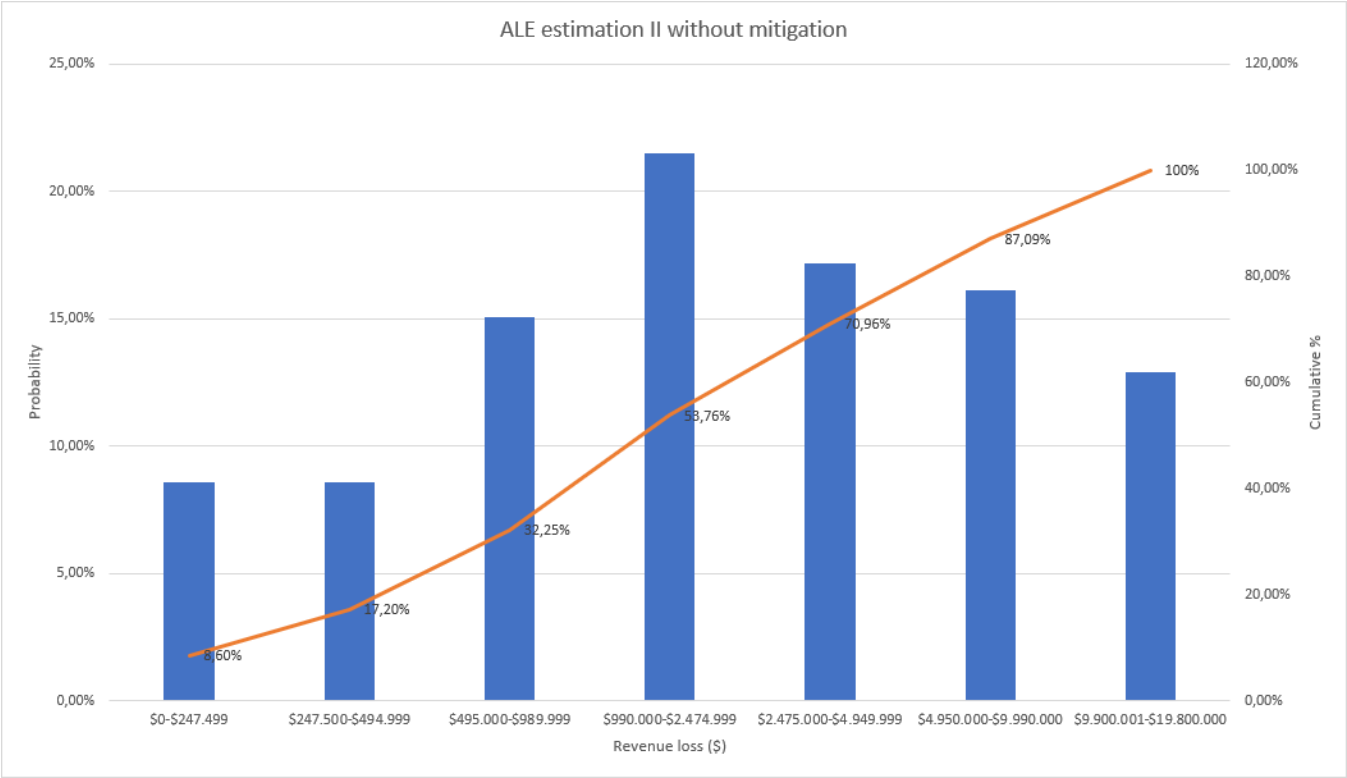

Figure 10: ALE estimation without mitigation probability distribution.

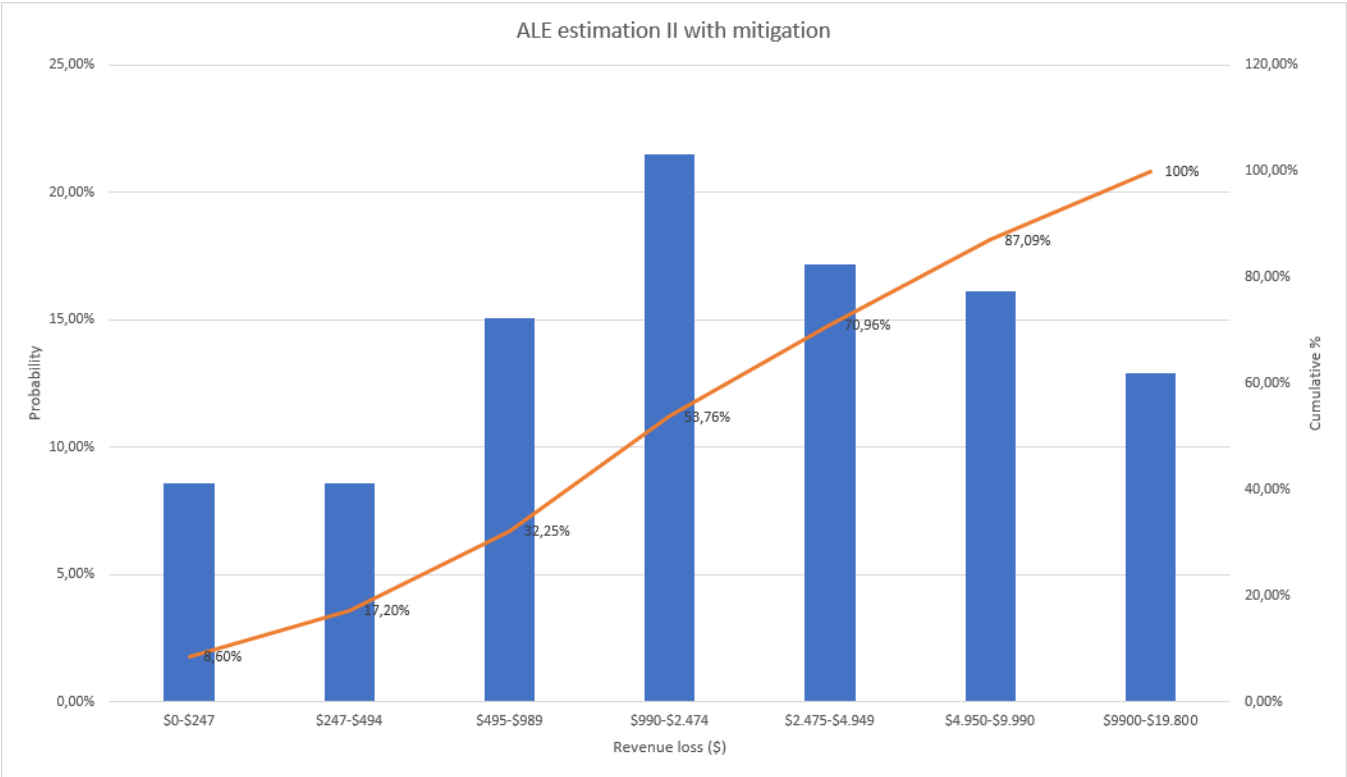

Figure 11: ALE estimation with mitigation probability distribution.