risks

Article

Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk

Albina Orlando

Istituto per le Applicazioni del Calcolo "Mauro Picone", Consiglio Nazionale delle Ricerche (CNR),
Via Pietro Castellino 111, 80131 Naples, Italy; a.orlando@na.iac.cnr.it

Abstract: The aim of this paper is to deepen the application of value at risk in the cyber domain, with particular attention to its potential role in security investment valuation. Cyber risk is a fundamental component of the overall risk faced by any organization. In order to plan the size of security investments and to estimate the consequent risk reduction, managers strongly need to quantify it. Accordingly, they can decide about the possibility of sharing residual risk with a third party, such as an insurance company. Recently, cyber risk management techniques are including some risk quantile-based measures that are widely employed in the financial domain. They refer to value at risk that, in the cyber context, takes the name of cyber value at risk (Cy-VaR). In this paper, the main features and challenging issues of Cy-VaR are examined. The possible use of this risk measure in supporting investment decisions in cyber context is discussed, and new risk-based security metrics are proposed. Some simple examples are given to show their potential.

Keywords: cyber risk management; value at risk; cyber value at risk; security investments

check for updates

Citation: Orlando, Albina. 2021. Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. *Risks* 9: 184. https://doi.org/10.3390/risks9100184

Academic Editors: Tomas Kliestik, Michel Dacorogna and Marie Kratz

Received: 1 April 2021
Accepted: 8 October 2021
Published: 18 October 2021

1. Introduction

Companies worldwide face several challenges in managing the impact of increasing interconnectivity on their business. Indeed, cyber risk is a fundamental component of the overall risk addressed by the organizations, and its significance is expected to increase. According to Allianz Global Corporate & Specialty (2021) (AGCS) "cyber crime now costs the global economy over $1*trn*—more than one per cent of global GDP—up 50% from two years ago. Meanwhile, the threat of business interruption, whether from ransomware attacks, technical failure or via the supply chain, more severe consequences from data breaches and risks emerging from the acceleration of digitalization post-Covid-19 loom large". In this report by AGCS, cyber risk trends are analyzed, highlighting some key points: cyber claims are growing in number and complexity, external attack causes more expensive losses, and internal accidents occur more frequently. AGCS points out that both the consequences from more robust regulation and the potential of litigation if things should go wrong, are increasing too. Pandemic outbreak, business interruption, and cyber risk are strongly interlinked and Joachim Müller, CEO of AGCS, tells us: "the coronavirus pandemic is a reminder that risk management and business continuity management need to further evolve in order to help businesses prepare for, and survive, extreme events" ... "we also have to ready ourselves for more frequent extreme scenarios".

Extreme scenarios refer to the worst events that can hit a business. In the cyber risk domain, they can have a very high financial impact, and this is the reason why the scientific community is giving more and more attention to this issue. Risk officers are strongly concerned about the possibility of an extremely bad result, and quantile-based risk measures, such as value at risk (VaR), employed in the assessment of the amount of money needed to front such events. VaR was formally introduced by JP Morgan in 1995; it is the risk measure which tells us, at a given confidence level, the foreseen worst-case loss over a specific period of time. The potential utility of this risk measure in cyber domain has been recently discovered. Based on the principles of VaR, and in the interest of helping organizations facing cyber security issues, the World Economic Forum's Partnering for Cyber Resilience initiative (WEF 2012) introduced a model to measure and quantify the impact of cyber threats on business and the exposure to them. This model, which is known as cyber value-at-risk (Cy-VaR), offers a starting point to quantify risk, and tries to bring more discipline into that area, even if it needs further improvements and testing in the field (Buith and Spataru 2015). The factor analysis of information risk (FAIR) is a Cy-VaR method chosen as the "international standard information risk management model" by the Open Group, which is a consortium consisting of more than 500 member organizations comprising HP, IBM, Oracle (Jones and Tivman 2018). FAIR is defined as "a standard Value-at-Risk model for information and operational risk that helps information risk, cybersecurity and business executives measure, manage and communicate on information risk in a language that business understands, dollars and cents" (FAIR Insitute). A Cy-VaR harm propagation model is discussed by University of Oxford and AXIS (2020), introducing threat into the model by virtue of harm trees. They establish some intuitive conditions concerning the harm propagation factors which impact on Cy-VaR: increase in volume of threat and potential attack vectors, in threat likelihood, in value and interdependence of assets, increases Cy-VaR. On the other hand, increase in risk control effectiveness decreases it. They suggest to use these conditions to test the successful implementation of the mathematical model for Cy-VaR. A very interesting contribution is given in Radanliev et al. (2020b), which surveys deep learning algorithms, IoT cyber security, and risk model. The aim is to build a dynamic and self-adapting system to predict cyber risk. Their approach is supported with artificial intelligence and machine learning, and real-time intelligence in edge computing. In this contribution, it is stressed that the AI/ML are fundamental to move beyond the drawbacks of Cy-VaR models that mainly apply Bayesian and frequentist methods.

The aim of this paper is to deepen the role of Cy-VaR in quantifying cyber risk. The main contribution is to highlight further possible employment of this quantile-based risk measure in the cyber security domain. In particular, the potential use of this risk measure in supporting investment decisions is discussed, and new risk metrics are proposed which are based on Cy-VaR. Our idea moves from the consideration that an effective risk management process must consider the extreme cases in which a cyber incident is severe enough to cause massive losses. Therefore, tools and metrics supporting investment decisions should not only rely on traditional expected value, but should focus on the unexpected losses too, taking into account unwanted tail events. In cyber security literature, great work has been done to adapt the fundamentals and metrics of investment theory to security investment (Böhme and Nowey 2008; Böhme 2010; SooHoo 2002; Su 2006). Most popular is the notion of return on security investment(ROSI), drawing from the classical return on investments (ROI). Another metric employed in investment theory to evaluate investments is the net present value (NPV), and, in information technology framework, a more sophisticated NPV calculation is proposed (Locher 2005).

In line with the practice of the existing literature to employ metrics from banking and financial area in cyber domain, our paper contributes by proposing a risk-adjusted version of the aforementioned main security metrics. Moreover, we consider the potential of the risk-adjusted performance measures (RAPMs), which are commonly used by banks and insurance companies. Risk-adjusted return measures arise from a very common need in the financial world: having to make a choice between multiple products, selecting those that seem most attractive to a potential investor in terms of both return and risk; RAPM measures operate according to this logic (Matten 2000). In particular, we refer to the risk-adjusted return on capital (RAROC), which is a modified return on investment figure that takes risk into account by means of VaR. We propose to adapt this risk measure to security investment valuation, by including Cy-VaR in its formulation. Some simple examples are given to show the potential of the proposed metrics.

The paper is organized as follows: Section 2 deals with the concept of cyber risk management, Section 3 concerns the definition of Cy-VaR and its main features. Section 4 deals with the critical issues in Cy-VaR estimation and Section 5 proposes investment security metrics based on Cy-VaR estimation. Section 6 concludes.

2. Cyber Risk Management

Risk management enables a system to cope with the effects of uncertainty on business activity. According to the international standards (ISO 2018), the goal of risk management is creating and protecting value. To this aim, it enhances the performance of the organization, encouraging innovation, and supporting the attainment of the objectives set (Luburic 2019). In order to make risk management process effective and efficient, some fundamental principles must be taken into account. Risk management tasks must be proportional to the level of risk that an organization copes with, in line with the other activities in the organization, and they have to be comprehensive and embedded within the organization. Finally, they must be proactive and reactive to upcoming and mutating risks.

Among the risks faced in business activity, operational risks are those stemming from external occurrences or bad and unfruitful internal systems, people, and processes. Cyber risks belong to the category of operational risks, even if they show peculiar characteristics. In this regard, it is well known that the environment of cyber risks is constantly evolving, because of new technologies and the rapid development of computer information systems. Attack techniques change continuously and can be performed in a easy and cheap fashion. In the Allianz Risk Barometer 2020 (Allianz Global Corporate & Specialty 2020), more than 2700 risk management experts from 102 countries and territories tell us that cyber incidents are considered the most important business risk. Cyber risks keep evolving and businesses tackle an increasing number of new challenges, which include bigger and more expensive data breaches, a rise in business email compromise (spoofing) incidents ransomware, as well as the possibility of litigation after an event. As a consequence, many companies are aware that cyber risk is a key component of enterprise risk management (ERM), and their main goal is to strengthen cyber resilience; that is, the "ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery” (WEF 2012).

Security risk management involves identifying, assessing, and treating risks connected to integrity, availability and confidentiality of an organization’s assets, being fully aware that a residual risk must be accepted. Indeed, the adoption of the best cyber security procedures and the setup of different countermeasures do not ensure avoiding cyber incidents, regardless of their remarkable cost (Martinelli et al. 2018). Accepting residual risk is part of being cyber-secure together with trying to manage it with the purpose of being resilient.

According to Stonebumer et al. (2002), once risks have been identified and assessed, the right minimization strategy has to be chosen. The alternatives to minimize risk include risk mitigation, transferring, avoidance, and acceptance. Mitigating risk relates to efforts which aim at reducing it (i.e., reduce the likelihood of a risky event to happen, its impact or both). Risk transfer means burden-sharing of prospective losses with another party: insurance is a possible option to transfer risk. Risk avoidance involves the decision to avoid a risky event (e.g.withdraw from a risky part of business), and risk acceptance is a way to accept risk as a cost of doing business.This decision makes sense when the cost of investment or insuring against it should exceed the total losses over time.

As is well known, risk is the possibility of suffering harm or loss (Alberts and Dorofee 2001). It is connected to the possibility of an incident, depending on future threats and vulnerabilities. Cyber threats may provoke undesired results, coming from a harm to a system or organization. They can be external or internal, and may be caused by individuals or organizations. Cyber vulnerabilities are existing flaws or weaknesses, which can be exploited and result in an incident. Losses are the consequences of incidents and are called "impact". They may be tangible (e.g., financial penalties or loss of revenue) or intangible (loss of reputation), according to the hit assets.

Thus, risk can be defined as a mix of a threat, a vulnerability and an impact. Managers need to make informed decisions about their business risk tolerance and, as a consequence, they have to plan cyber security investments and other mitigation or transfer strategies. They need to estimate the likelihood of experiencing a damaging incident. Moreover, they have to measure the effectiveness of risk mitigation actions, estimating any risk reduction resulting from some investment expenditure.

3. The Role of Cyber Value at Risk

Consistently with the aforementioned issues, in recent years, VaR has started to be implemented in a cyber security context, and many efforts have been made to adapt this risk measure to the methods specially developed to assess cyber risk. These new models, referred to as Cy-VaR, offer "top management with a single risk number and a statistical probability to understand the overall cyber security risk of an enterprise" (Beckstrom 2014). Cy-VaR has two main objectives: to "help risk and [information security] professionals articulate cyber risk in financial terms" and to "enable business executives to make cost-effective decisions and achieve a balance between protecting the organization and running the business" (Freund and Jones 2014).

Cy-VaR is based on the concept of VaR that is a risk measure proposed by JP Morgan in 1995 as the "predicted worst-case loss at a specific confidence level". VaR is considered a main risk measure. It is very popular because it is intuitive and its numerical values are easier to interpret, compared to other risk measures. Moreover, it is stated by regulators in the Basel II and Basel III accords (Gilli et al. 2019).

The VaR "at a fixed confidence level $\alpha \in [0, 1]$, is defined as the smallest number l such that the probability that the loss L exceeds l is not greater than $(1 - \alpha)$" (McNeil et al. 2015):

$$VaR_{\alpha}(L) = \inf[l \in R | P(L > l) \leq 1 - \alpha]. \tag{1}$$

$VaR_{\alpha}(L)$ is the α-quantile q_{α} of the distribution function of the losses L. In financial and actuarial context, traditional values for α are $\alpha = 0.95$, $\alpha = 0.99$ and $\alpha = 0.995$.

Several organizations are used to estimate VaR as a component of their corporate risk assessment, while few organizations employ VaR for cyber risks, so far. In the past, those risks were managed simply by avoiding attacks or promptly retrieving. Nevertheless, technical reviews of security controls cannot help to quantify the economic impact of cyber attacks. Managers need to quantify cyber risks, to plan the size of security investments and estimate the consequent risk reduction. Moreover, they need to decide about the possibility of sharing residual risk with a third party, such as an insurance company. The rationale of value at risk models applied to cyber domain helps to address those issues.

Indeed, Cy-VaR allows one to explore the consequences of additional threats and compare how different security control configurations can help to limit residual risk as threat increases.

The loss distribution approach is the best-known approach to operational risk measurement and regulatory capital calculation (Locher 2005). In the actuarial field, it is a very popular statistical approach, and it relies on the concept that losses can occur randomly in frequency and severity in accordance with characteristic distributions. In particular, the frequency and the severity of losses are each independently assumed to follow a statistical distribution, with parameters estimated directly from the data. Let us consider the total amount L of all losses arising in a given time period; that is, the aggregate losses. Hence (Carfora and Orlando 2019),

$$L = \sum_{j=1}^{N} X_j, \qquad N = 0, 1, 2, ... \tag{2}$$

where $X_j(J = 1, \ldots, N)$ are the single loss amounts. $L = 0$ when $N = 0$. Both the number N of individual events; that is, the frequency of the attacks, in the considered time period and the related individual loss amounts $X_1, \ldots, X_N$ which represent the severity of damage for each attack, are random variables. In order to obtain the compound distribution of L, the frequency and the severity of these losses are modeled separately.

The random sum L in (2) has distribution function (Panjer 2006):

$$F_L(x) = \sum_{n=0}^{\infty} p_n F_X^{*n}(x) \tag{3}$$

The common distribution of the two random variables X_j and $p_n = Pr(N = n)$ is $F_X(x)$. $F_X^{*n}(x)$ represents the n-fold convolution of the cdf of X.

A closed form for such a distribution is not always achievable. As a consequence, it is necessary to rest on simulation techniques to estimate its quantiles, the corresponding VaR measure and the unexpected loss, given by the losses in between the expected loss and the value at risk.

Looking at literature on cyber security, with regard to frequency, it is generally modeled by either a Poisson or a negative binomial distribution (Eling and Loperfido 2017). (Bentley et al. 2020) suggest that a suitable way to model the effect of mitigation on the frequency of attacks, is to resort to a Poisson process.

As severity is concerned, log-normal and skew-normal models are frequently being used in the actuarial literature. Models from extreme value theory (ETV) are popular too, because the data from operational risk are severely tailed. The peaks-over-threshold method (POT) is the most common EVT approach, because it is more efficient compared to other methods (Strupczewski 2019). This approach allows the modelling of losses above a threshold (e.g., the 90% quantile) by a generalized Pareto distribution (GPD), and losses below the threshold with another common loss distribution. Applications of these models in the cyber risk domain are proposed by Eling and Loperfido (2017). It is pointed out that different kinds of cyber incidents often show a different statistical nature, requiring separate modeling (Carfora et al. 2019).

Another issue concerns the dependability structure of losses, requiring a model able to deal with various, but dependent, classes of damages (Bentley et al. 2020). In order to model dependency structure, copulas are commonly used (Bentley et al. 2020; Eling and Jung 2018). Recent actuarial studies focus on modelling the dependence between the claim frequency and the average severity (Alemany et al. 2021).

4. Critical Issues in Cyber Value at Risk Estimation

In order to obtain a reliable estimate of Cy-VaR, an account must be taken of vulnerability, assets, and the profile of potential attackers (see Figure 1). According to the European Union Agency for Cyber Security (ENISA), a vulnerability relates to the occurrence of a flaw, design, or implementation error that can induce an unexpected event affecting the security of the information system. The undesirable event can be certain or uncertain, and it can be due to a single or a series of occurrences. Users can be a significant source of vulnerabilities; indeed, whether intentionally or not, many employees are often the weak link of a successful cyberattack (e.g., accidental publication of confidential information, non-custody of laptop computers containing highly sensitive information). Moreover, the vulnerability assessment of an organization depends on its previous ability to front successful attacks and on the maturity level of its security system (Buith and Spataru 2015). The shortage of standard maturity settings across industries reduces cyber value-at-risk performance. Indeed, the consequence could be a subjective rather than objective quantification of threat exposure. Rabii et al. (2020) research proposes several experience reports and some case studies on information security maturity ranking, offering a comprehensive review and summary of this rising field.

Another basic element of Cy-VaR models is the identification of tangible and intangible assets under threat. In particular, intangible assets (i.e., human-capital, reputation, knowledge, expertise, etc.), which contribute up to 80% of an organisation's value, are now recognised as essential to the rendering of companies and nations (Dambra and Frumento 2019). After identification, assets must be evaluated, and this task, with regard to intangible assets, can be quite difficult. The final step is asset classification into discrete categories that facilitate the definition of the overall security risk (Bonjac and Jerman-Blazic 2008). We observe that estimating the economic and financial consequences of a cyber incident is hard because of the distinctive nature of information assets.

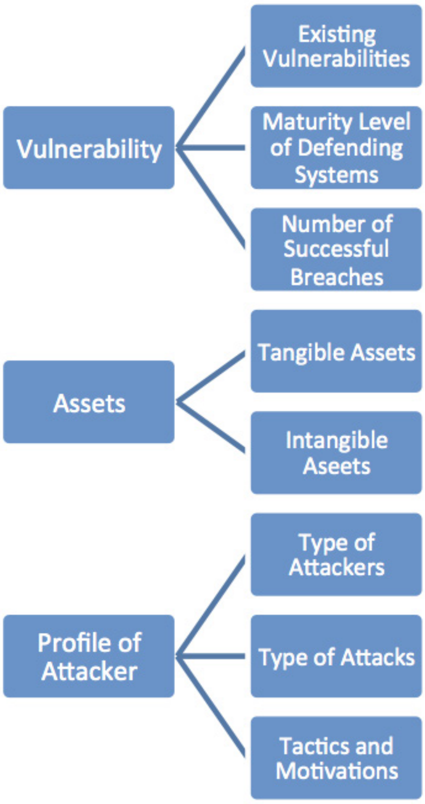

Figure 1. Cyber Value at Risk Components. Source: World Economic Forum, "Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats".

The third element is the profile of the potential attackers, that is, the type of attackers, their motivations, and the kind of attack they are prone to perpetrate. With regard to the type of attackers, we can distinguish four types: cyber criminals, hacktivists, state-sponsored attackers, and insider threats. A more detailed classification is given in Bruijne et al. (2017). Cyber criminals commit cyber crime aiming at generating profits by stealing confidential company information or personal data. Nowadays, they represent the most leading and most proactive kind of attacker. Hacktivists are individuals or groups of hackers who act on religious belief or social and political ideology. State-sponsored attackers have particular goals which comply with the main interests of their home country. Finally, insider threats come from both full-time and temporary workers, but also from customers and contractors. The threats can be motivated by malicious, accidental or negligent behavior. In its 2019 report, the World Economic Forum (WEF) listed the most common cyber attacks. that can be faced by an individual or an organization. Among the others, we find the brute-force attack by which the criminals use the trial and error approach to guess the passwords successfully, the credential stuffing used to stolen credentials to access to a user's account. One of the most prevalent kind of cyber attacks is phishing, which consists of sending emails from a trust-seeming source to gain personal information. Finally, we mention malware, which is a malicious software downloaded in a system without any visible signs.

The fundamental goal of handling cyber attacks efficiently, strongly depends on the probability estimation of a successful attack. Indeed, the rate of occurrence is really hard to assess, because attackers are adaptable and the changes in their strategies are unpredictable. Al-Mohannadi et al. (2016) offer an analysis of various kinds of available attack modelling techniques to learn about the weakness of the network, and the attitude and objectives of the adversary.

Regarding the estimation of the probability of a successful attack, it is not an easy task, either. The reason is that there is a lack of historical data on the frequency and severity of attacks. One reason could be found in information sharing barriers, due to the fact that companies do not want to disclose cyber incidents that they have been exposed to, since this could cause huge secondary damage. Reporting requirements have been introduced since 2002 in many US states. The situation is moving in Europe too, due to GDPR (General Data Protection Regulation), introduced in May 2018. The GDPR involves stricter rules, such as the requirement to notify the regulator and data owner of a data breach. High penalties are introduced for companies who do not comply: they could be fined as much as 4% of global incomes (Carfora et al. 2019).

In estimating Cy-VaR, we cannot ignore that the security level of one system may depend on the security of others. As a consequence, an attacker could potentially exploit a system through a channel that the organization shares with a partner with a much weaker security level.

Moreover, in order to estimate risk exposure using Cy-VaR, it is essential to take into account the dependencies among the three components (vulnerability, assets, and attacker profile). For example, the vulnerability of a system mainly depends on the relevance of its assets to eventual attackers and the common behaviour in the attacker community. Thus, the risk of undergoing a cyber attack is closely linked to the company's assets and the attacker profile.

An interesting approach is offered in Radanliev et al. (2020a), where prospective and concrete evidence in the use of artificial intelligence (AI) in cyber risk analytics is deepened, and new cyber risk architectures are proposed. The aim is to improve resilience and cyber risk understanding. The research concerns the identification of AI role in connected devices (e.g., Internet of Things devices).

An other approach to face the lack of reliable data, concerns the expert judgment methods. A recent contribution is given in Krisper et al. (2020), which shows a case of using the judgment of experts to evaluate the risk of a cyber-security incident.

5. Cyber Value at Risk in the Valuation of Information Security Investments

A hard task for companies is to determine how much resources to invest in the various business projects. The difficulty is particularly great if the projects in question, instead of generating an immediate economic return, have, as their main objective, the prevention of future losses. Investments in cyber security have just this feature. Every euro invested to make your business networks and devices safer does not translate into an immediate gain for companies, and without suitable security investment metrics, it is difficult for management to make any investment decisions. Of course, a significant reduction in cyber risk can be an ambitious goal, which faces spending and budget limits. Consequently, it is necessary to identify an "optimal" level of risk exposure below which the cost of investment would exceed the benefits of risk reduction. The traditional trade-off between risk and return typical of financial investments, gives way to a trade-off between risk and lower costs. As is well known, risk exposure can be defined as the product of expected likelihood vs. expected severity of an unpleasant event. The aim of investing in IT security is either to lower the probability of incidents or to reduce the potential loss coming from the undesirable event, or both. Gordon and Loeb (2002) show that those parameters are critical factors in budgeting for information security. So, the important thing is to assess the impact of a certain security measure on those parameters. Many contributions in literature propose to adapt the metrics of investment theory to security investment valuation (Böhme and Nowey 2008; Böhme 2010; SooHoo 2002; Su 2006). Most popular is the notion of return on security investment (ROSI), drawing from the classical return on investments (ROI). ROI is a performance measure that assesses the effectiveness of an investment or compares the result of different investments. It measures the income or loss that comes from investing a certain amount of money. ROI is a percentage or ratio, and it is calculated by dividing the benefit (return) of an investment by its cost. As an adaptation of ROI to security investment valuation, ROSI is defined as follows (Enisa 2012):

$$ROSI = \frac{\Delta L - I_0}{I_0} \tag{4}$$

where ΔL is the loss reduction deriving from the investment with initial cost I_0 and represents the benefit due to the investment. Indeed, Equation (2) can be rewritten in terms of expected aggregate loss $E[L]$ as follows:

$$ROSI = \frac{\Delta E[L] - I_0}{I_0} \tag{5}$$

with $\Delta E[L] = E[L_t] - mE[L]$. Loss reduction $\Delta E[L]$ is measured in terms of the expected aggregate loss $E[L]$ over a certain period, as L is defined in Equation (1). $mE[L]$ is the mitigated loss expectancy, as a result of the investment in security. An investment is considered profitable if the risk mitigation effect is greater than the expected costs. In many contributions on cyber security, expected loss is often referred to as annual loss expectancy (ALE), which is given by the product of the single loss expectancy (SLE) multiplied by the annual rate of occurrence (ARO). Referring to a single unwanted event, SLE is the expected loss due to a risk occurrence. ARO is a measure of the probability that a risk occurs, being equivalent to the number of occurrences of that type of event in the reference period. An efficient investment lowers the ALE and the loss reduction is quantified by the difference of the ALE without investment versus the mitigated ALE.

In line with the tendency to borrow investment valuation metrics from the financial world, a more sophisticated net present value (NPV) calculation is proposed by Locher (2005). As is well known, NPV is given by the present value of the difference of the future inflows versus outflows, where the discounting rate is the opportunity cost of capital. This discounting rate is exogenous, being a measure obtained from the environment of the investment. The modified NPV is:

$$NPV_0 = -I_0 + \sum_{t=1}^{T} \frac{\Delta E[L_t] + \Delta C_t * i_{ROE,t}}{(1+i)^t} \tag{6}$$

where I_0 is the initial investment, $\Delta E[L_t]$ measures the reduction of the annual expected loss as benefit of the investment, and ΔC_t incorporates the reduction of capital charge as a positive effect of investing in security, with $i_{ROE,t}$ being the targeted return on equity set by the organization. The discounting rate i is the risk-free rate. This approach is suitable for multi-period investments and takes into account time preference.

Limitations and challenges of these metrics are deepened by the existing literature (Böhme and Nowey 2008; Enisa 2012). It can be hard to determine the costs of IT security. The reason lies in the necessity to estimate both direct costs (e.g., installation, maintenance, training) and indirect costs (e.g., through changes in employee motivation or changed workflows). Another critical issue is the estimation of mitigation effects of investments in security. Bentley et al. (2020) propose an interesting model for mitigation that targets frequency and severity separately.

As discussed in the previous sections, an effective cyber risk management process must consider that some extreme cases may cause huge losses. Observations that initially seem to be outliers could not actually be incoherent with the rest of the data if they belong to a long-tailed distribution. Therefore, tools and metrics supporting investment decisions, should rely on the unexpected losses too, taking into account unwanted tail events. This approach could help taking suitable investment decisions based on personal risk preferences instead of choosing solutions that look only at the expected loss reduction. With this in mind, this contribution aims to reflect that Cy-VaR could provide additional information in the security investment decision process.

To this aim, we propose a risk-adjusted ROSI (RaROSI), which takes into account worst cases. The idea is to consider the difference between the expected loss without mitigation effect of the investment $E[L]$ and the worst case loss, at a given confidence level α, mitigated by the investment:

$$RaROSI_{\alpha} = \frac{\Delta U[L] - I_0}{I_0} \tag{7}$$

where $\Delta U[L] = E[L] - mCyVaR(\alpha)$ with $mCyVaR(\alpha)$, being the mitigated value of the expected worst case loss at the given confidence level α. This parameter reflects the degree of risk aversion of the decision maker; as the confidence level increases, the Cy-VaR increases too. RaROSI can complement and enrich the information given by ROSI, including a measure of cyber risk expressed by Cy-VaR.

As the NPV (Equation (6)) formula is concerned, we can observe that in the financial context, VaR is also referred to as capital at risk (CaR); that is, the amount of capital set to face any unexpected losses. In this perspective, we think that the reduction of capital charge ΔC_t in (6) could be measured in terms of Cy-VaR.

Other risk metrics of financial and banking domain could be used in the cyber area. In particular, we refer to risk-adjusted performance measures (RAPMs). RAPMs is a risk-return ratio and can be estimated ex ante by considering expected earnings and current risk value. It can also be verified ex post, as a quotient between the profit actually achieved and the VaR actually recorded over a certain period.

Among these risk measures, we find the risk-adjusted return on capital (RAROC) which was first applied in the early 1990s at the Bank of America (Zaik et al. 1996). RAROC is a modified ROI figure, that takes elements of risk into account. It allows one to adjust the ROI numerator and denominator based on risk (Resti and Sironi 2012):

$$RAROC = \frac{E(u) + i * VaR(\alpha)}{VaR(\alpha)} \tag{8}$$

with $E[u]$ indicating the expected profit. At the numerator of (8), we have the sum of the expected profit and the profit derived from the investment at the risk-free rate of the allocated capital (VaR) in case of unexpected losses.

Applying this risk measure to cyber security investments, we could write:

$$CyRAROC = \frac{\Delta E[L] - I_0 + i * CyVaR(\alpha)}{CyVaR(\alpha)} \tag{9}$$

with $E(u) = \Delta E[L] - I_0$, as defined in ROSI formula. Therefore, the expected profit is measured in terms of the expected loss reduction $\Delta E[L]$ net of the investment cost I_0.

In what follows, we propose two very simple examples to show the potential of the aforementioned risk metrics.

Example 1. *The company Hassisto s.r.l. has been hit by increasing security breaches in recent years, and decided to invest money in a security solution. Based on past successful cyber attacks, an expected annual loss in data, fine and productivity of 200,000 $ are estimated. Moreover, 350,000 $ is the estimated maximum expected loss, with a confidence level of 5%. The cost of the security solution is 74,000 $ per year. The expected mitigation effect of the investment is an annual loss reduction to its 90%.*

Example 2. *AlfaOmega s.p.a. is considering investing in a security solution. The expected annual loss of data and productivity is 400,000$. The estimated worst case loss at a 5% confidence level is* *about 950,000 \$. The cost of the security solution is of 60,000 \$ per year, and it is expected to block 50% of the attacks*

Table 1 shows the results. Basing on Equations (5), (7) and (9), ROSI, RaROSI and CyRAROC are computed. We can observe that the estimated ROSI for Hassisto s.r.l. is 143%. The investment that, in this example, is of 74,000 \$ per year, would save Hassisto s.r.l. an estimated 106,000 \$ per year, given by the difference between the expected loss reduction $\Delta E[L]$ and the investment cost I_0. As a consequence, the saving produced by the investment would give a 143% payback on the security investment. Nevertheless, considering the worst case loss with a 5% confidence level, RaROSI is 122.9%, lower than ROSI. Indeed, in this case, the company saves an estimated 91,000 \$, given by the difference $\Delta U[L] - I_0$, the denominator of Equation (7). This lower value is due to the fact that the mitigation effect of the investment is computed as a percentage of CyVAR, being $\Delta U[L] = E[L] - mCyVaR(\alpha)$. CyRAROC is 45.28%, setting $i = 15\%$ in Equation (9).

The second example, relative to AlfaOmega s.p.a., shows an estimated ROSI of 233% that is very high. In this case, the investment of 60,000 \$ per year, would save AlfaOmega s.p.a. an estimated 140,000 \$ per year. Therefore, the estimated risk-adjusted ROSI is negative (-225%) and tells us that, with a 5% confidence level, AlfaOmega could lose 125,000 \$ in one year suffering a very high negative payback of -225%. The CyRAROC is 29.7%, very low compared to the one obtained by Hassisto s.r.l.

Even if, in the two examples, ROSI gives very good results, RaROSI is lower in both cases. Indeed, it takes into account the risk that a tail event occurs. Actually, its value strongly depends on the chosen confidence level α, reflecting the risk aversion degree of the decision maker.

In the second example, we observe that, even if ROSI is very high with respect to Example 1, its risk-adjusted value (RaROSI) is deeply negative, with CyVaR being very high compared to expected loss $E[L]$. More information is given by CyRAROC, which can help the decision maker to compare different investments. Based on the given examples, the investment by Hassisto s.r.l. is better than the one by AlfaOmega s.p.a. both with regard to RaROSI and CyRAROC, even showing a very high ROSI percentage. These results show that Cy-VaR offers additional information supporting investment decisions. Indeed, the risk metrics including worst case losses, should be taken into account in an effective investment choice.

Table 1. Security investment metric results for Hassisto s.r.l. and AlfaOmega s.p.a. $i = 0.15$.

	Hassisto s.r.l.	**AlfaOmega s.p.a.**
Investment cost	−74,000	−60,000
$\Delta E[L]$	180,000	200,000
$\Delta U[L]$	165,000	−75,000
ROSI	143%	233%
RaROSI	122.9%	−225%
CyRAROC	45.28%	29.7%

6. Concluding Remarks

Cy-VaR assesses the unexpected loss at a specified confidence level over a given period of time. It helps to address important issues like the quantification of losses due to cyber incidents over a given period of time, and how much an organization could reduce its risk by investing more in security. Although going deep into these issues is neither easy nor certain, Cy-VaR can be an effective tool for the risk estimation process and discussion. Traditional cyber security emphasizes the type of attacker and the methods used in the attacks. Instead, Cy-VaR considers the three primary components of cyber risk: its vulnerability, its assets, and the profile of the potential attackers. A suitable Cy-VaR model should address threat type executing the attack scenario, the type of attacks, and the vulnerability of the system taking into account its maturity level. Reaching these objectives is still challenging.

Precise estimates of Cy-VaR require exact information about every computer vulnerability at every level within an organization; reliable assessment of assets and business activities; and the expertise to foresee the behaviours of clients, hackers and employees. Bearing in mind that the flawless information does not exist, appropriate risk assessment and estimation are all the more important and Cy-VaR offers a reasonable approach and a goal to move towards.

In this paper, we follow the approach of adapting tools and metrics from investment theory to cyber security framework, featuring several contributions in the literature. In particular, basing on the Cy-VaR main feature, we highlight its role in giving support to security investment decisions, observing that it can improve the commonly used investment risk metrics. Our research is still preliminary and offers simple examples to show the basic idea, but it could provide insights for cyber risk management. In future research, it could be interesting to assess the proposed metrics modelling aggregated loss distribution, by taking into the dependence between actual cyber losses. Furthermore, empirical results would improve future investigations.

Funding: This work has been partially supported by the EU project CyberSure 734815.

Acknowledgments: The author thanks the anonymous referees for their valuable suggestions and critical reading of the manuscript. The author thanks Mariarosaria Aletta for bibliographic support.

Conflicts of Interest: The author declares no conflict of interest.

References

Alberts, Christopher J., and Audrey J. Dorofee. 2001. *OCTAVE Criteria*. Technical Report CMU/SEI-2001-TR-016. Pittsburg: Carnegie Mellon Software Engineering Institute.

Alemany, Ramon, Catalina Bolancé, Roberto Rodrigo, and Raluca Vernic. 2021. Bivariate Mixed Poisson and Normal Generalised Linear Models with Sarmanov Dependence—An Application to Model Claim Frequency and Optimal Transformed Average Severity. *Mathematics 9*: 73. [CrossRef]

Allianz Global Corporate & Specialty. 2020. Allianz Risk Barometer 2020: Top Business Risks for 2020. Report. Available online: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (accessed on 9 January 2021).

Allianz Global Corporate & Specialty. 2021. Allianz Risk Barometer 2021: Top Business Risks for 2021. Report. Available online: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (accessed on 10 February 2021).

Al-Mohannadi, Hamad, Qublai Khan Ali Mirza, Anitta Patience Namanya, Irfan Awan, Andrea J. Cullen, and Jules Pagna Diss. 2016. Cyber-Attack Modeling Analysis Techniques: An Overview. Paper presented at 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, August 22–24. pp. 69–76. [CrossRef]

Beckstrom, Rod. 2014. CyberVaR: Quantifying the Risk of Loss from Cyber Attacks. Available online: http:www.beckstrom.com/uncategorized/cybervar-quantifying-risk-loss-cyber-attacks (accessed on 16 November 2020).

Bentley, Mark, Alec Stephenson, Peter Toscas, and Zili Zhu. 2020. A multivariate model to quantify and mitigate cybersecurity risk. *Risks* 8: 61. [CrossRef]

Böhme, Rainer, and Thomas Nowey. 2008. Economic Security Metrics. In *Dependability Metrics. Lecture Notes in Computer Science*. Edited by Irene Eusgeld, Felix Freiling and Ralph H. Reussner. Berlin and Heidelberg: Springer, vol. 4909.

Böhme, Rainer. 2010. Security Metrics and Security Investment Models. In *Advances in Information and Computer Security*. Edited by Isao Echizen, Noboru Kunihiro and Ryoichi Sasaki. IWSEC 2010. Lecture Notes in Computer Science. Berlin and Heidelberg: Springer, vol. 6434.

Bonjac, Rok, and Borka Jerman-Blazic. 2008. An economic modelling approach to information security risk management. *International Journal of Information Management* 28: 413–22.

Buith, Jaques, and Dana Spataru. 2015. The benefits, limits of Cyber- Value-at-Risk. *The Wall Street Journal—Business*. Available online: deloitte.wsj.com/cio/2015/05/04/the-benefits-limits-of-cyber-value-at-risk/ (accessed on 20 November 2020).

Bruijne, Mark d., Michel van Eeten, Carlos Hernandez Ganan, and Wolter Pieters. 2017. *Towards a New Cyber Threat Actor Typology. A Hybrid Method for the NCSC Cyber Security Assessment*. WODC Rapport 2740. Delft: Delft University of Technology.

Carfora, Maria Francesca, Fabio Martinelli, Francesco Mercaldo, and Albina Orlando. 2019. Cyber Risk management: An actuarial point of view. *Journal of Operational Risk* 14: 77–103.

Carfora, Maria Francesca, and Albina Orlando. 2019. Quantile-based risk measures in cyber security. Paper present at the International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, June 3–4. pp. 1–4.

Dambra, Carlo, and Enrico Frumento. 2019. The role of intangible assets in the modern cyber threat landscape: The HERMENEUT Project. *European Cybersecurity Journal* 5: 56–65.

Eling, Martin, and Kwangmin Jung. 2018. Copula approaches for modeling cross sectional dependence of data breach losses. *Insurance: Mathematics and Economics* 82: 167–180. [CrossRef]

Eling, Martin, and Nicola Loperfido. 2017. Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: Mathematics and Economics* 75: 126–36. [CrossRef]

European Network and Information Security Agency. 2012. Introduction to Return Security Investment. Report. Available online: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment (accessed on 15 September 2020).

Freund, Jack, and Jack Jones. 2014. *Measuring and Managing Information Risk: A FAIR Approach*. Oxford: Butterworth-Heinemann Publisher, ISBN 10:0124202314.

ISO. 2018. *International Organization for Standardization ISO 31000: Risk Management—Guidelines*. Geneva: International Organization for Standardization.

Gilli, Manfred, Dietmar Maringer, and Enrico Schumann. 2019. Financial simulation at work: Some case studies. In *Numerical Methods and Optimization in Finance*, 2nd ed. Cambridge, MA: Academic Press, ISBN 9780128150658.

Gordon, Lawrence A., and Martin P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* 5: 438–57. [CrossRef]

Jones, Nathan, and Brian Tivman. 2018. Cyber Risk Metric Survey, Assessment, and Information Plan. HSSEDI. Case Number 18-1246/DHS Reference 16-J-00184-05. Available online: https://www.mitre.org/sites/default/files/publications/pr_18-1246-ngci-cyber-risk-metrics-survey-assessment-and-implementation-plan.pdf (accessed on 9 January 2021).

Krisper, Michael, Jurgen Dobaj, and Georg Macher. 2020. Assessing Risk Estimations for Cyber-Security Using Expert Judgment. In *Systems, Software and Services Process Improvement*. Edited by Murat Yilmaz, Jorg Niemann, Paul Clarke and Richard Messnarz. EuroSPI 2020. Communications in Computer and Information Science. Cham: Springer, vol. 1251.

Locher, Christian. 2005. Methodologies for Evaluating Information Security Investments—What Basel II Can Charge in the Financial Industry. ECIS 2005 Proceedings. vol. 122. Available online: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1136&context=ecis2005 (accessed on 20 June 2020).

Luburic, Radoica. 2019. A model of crisis prevention (based on managing change, quality management and risk management). *Journal of Central Banking Theory and Practice* 8: 33–49. [CrossRef]

Martinelli, Fabio, Albina Orlando, Ganbayar Uuganbayar, and A. Yautsiukhin. 2018. Preventing the Drop in Security Investments for Non-competitive Cyber-Insurance Market. In *Risks and Security of Internet and Systems*. Edited by Nora Cuppens, Frederic Cuppens, Jean- Louis Lanet, Axel Legay and Joaquin Garcia-Alfaro. CRiSIS 2017. Lecture Notes in Computer Science. Cham: Springer, vol. 10694. [CrossRef]

Matten, Chris. 2000. *Managing Bank Capital. Capital Allocation and Performance Measurement*. Chichester: Wiley.

McNeil, Alexander J., Rudiger Frey, and Paul Embrechts. 2015. *Quantitative Risk Management: Concepts, Techniques and Tools*. Revised Edition. Princeton: Princeton University Press.

Stonebumer, Gar, Alice Goguen, and Alexis Feringa. 2002. Risk Management Guide for Information Technology Systems. NIST Special Pubblication 800-30. Available online: https://doi.org/10.6028/nist.sp.800-30 (accessed on 15 October 2021).

Panjer, Harry H. 2006. *Operational Risk Modelling Analytics*. Wiley Series in Probability and Statistics. Hoboken: Wiley.

Rabii, Anass, Saliha Assoul, Khadija Ouazzani Touhami, and Ounsa Roudies. 2020. Information and cyber security maturity models: A systematic literature review. *Information and Computer Security* 28: 627–644. [CrossRef]

Radanliev, Petar, David De Roure, Rob Walton, Max Van Kleek, Rafael Mantilla Montalvo, Omar Santos, Peter Burnap, and Eirini Anthi. 2020a. Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. *SN Applied Science* 2: 1773. [CrossRef]

Radanliev, Petar, David De Roure, Rob Walton, Max Van Kleek, Rafael Mantilla Montalvo, Omar Santos, Peter Burnap, and Eirini Anthi. 2020b. Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments—Cyber risk in the colonisation of Mars. *Safety in Extreme Environments* 2: 219–30. [CrossRef]

Resti, Andrea, and Andrea Sironi. 2012. *Risk Management and Shareholders' Value in Banling: From Risk Measurement Models to Capital Allocation Policies*. Wiley Finance. Hoboken: John Wiley & Sons Ltd., ISBN 9780470029789.

Soo Hoo, Kevin J. 2002. How much is enough? A risk management approach to computer security. In *Workshop on Economics and Information Security (WEIS)*. Berkley: University of California.

Strupczewsli, Grzegorz. 2019. What is the worst scenario? Modeling extreme cyber losses. In *Multiple Perspectives in Risk and Risk Management*. Edited by Philip Lindsey, Philip Shrives and Monika Wieczorek-Kosmala. Springer Proceedings in Business and Economics. Cham: Springer,

Su, Xiaomeng. 2006. *An Overview of Economic Approaches to Information Security Management*. Technical Report TRCTIT0630. Twente: University of Twente.

University of Oxford and AXIS. 2020. *Calculating Residual Cyber Risk*. White Paper. Oxford: University of Oxford, Department of Computer Science.

WEF. 2012. Risk and Responsibility in a Hyperconnected World—Principles and Guidelines. Available online: www3.weforum.org/docs/WEF_IT_PartneringCyberResiliance_Guidelines_2012.pdf (accessed on 10 February 2021).

Zaik, Edward, John Walter, Gabriela Retting, and Christopher James. 1996. RAROC at Bank of America: From theory to practice. *Journal of Applied Corporate Finance* 9: 83–93 [CrossRef]