Data Science in Finance and Economics

https://www.aimspress.com/journal/dsfe

DSFE, 4(4): 601–614.
DOI:10.3934/DSFE.2024025
Received: 06 August 2024
Revised: 12 November 2024
Accepted: 01 December 2024
Published: 17 December 2024

Research article

Application of the Gordon Loeb model to security investment metrics: a proposal

Maria Francesca Carfora* **and Albina Orlando***

Istituto per le Applicazioni del Calcolo "Mauro Picone" - Consiglio Nazionale delle Ricerche, Italy

* **Correspondence:** Email: f.carfora@iac.cnr.it; a.orlando@iac.cnr.it.

Abstract: Cyber risk is a significant concern for all types of businesses. The consequences of a cyber attack can be quite severe. Investing in security to mitigate the impact of such risks is a crucial task, both in terms of the frequency and the severity of cyber incidents. In this paper, we propose a practical application of the Gordon and Loeb model, thereby suggesting a methodology to estimate risk exposure and reconsidering some investment evaluation metrics. Our findings strongly support the claim that maximizing the expected net benefit of an investment solely at the optimal level is not sufficient for sound decision-making. On the contrary, incorporating metrics that evaluate the benefit in relation to risk and consider worst-case scenarios offers deeper insights.

Keywords: cyber risk; security economics; security investments; risk exposure; Gordon-Loeb model

JEL Codes: M15, D81, C60, C80

1. Introduction

The global cybersecurity market is expected to expand from USD 193.73 billion in 2024 to USD 562.72 billion by 2032, with a compound annual growth rate (CAGR) of 14.3% over this period (Fortune Business Insights, 2023). This growth is driven by increasing cyber threats, the expansion of digital infrastructure, and the rising awareness of the need for robust security measures across all industries. Recent regulatory actions have confirmed the central importance of digital technology, thus emphasizing the need to both foster innovation and carefully assess potential risks. Notably, Regulation (EU) 2022/25541, which was adopted on December 14, 2022, plays a key role in this context. It is known as the Digital Operational Resilience Act (DORA) (European Commission, 2024) and aims to ensure that financial sector operators can effectively handle cyberattacks and operational disruptions. It introduces measures for governance, cybersecurity, Information and Communications Technology (ICT) risk management, and incident reporting. The regulation, which came into force on January 16, 2023, will be applied starting on January 17, 2025, thus impacting around 22,000 companies in the financial services sector. While focused on financial entities, DORA's provisions may also serve as a useful benchmark for non-financial companies in terms of digital resilience, as financial sector regulations often set best practices for other industries. In this scenario, effective risk management requires informed decisions on risk tolerance, cybersecurity investments, and mitigation strategies, along with evaluating their effectiveness. Investing in cybersecurity and conducting thorough risk assessments are crucial to protect assets, to ensure compliance, and to maintain business continuity as they help organizations to mitigate risks and safeguard against cyber attacks. Allocating resources to enhance the security level is a strategic decision and is driven by experienced cyber attacks and by the need to tailor their investments based on the types of threats that pose the most significant financial risk (Javadnejad et al., 2024). An interesting contribution is given by Fernandez De Arroyabe et al. (2023), who explored how cyber-capabilities and cyber-attacks drive investments in cybersecurity systems. The goal of investing in Information Technology (IT) security is to lower the probability of cyber incident, to reduce the resulting potential losses, or to achieve both. Mitigating risk exposure can be an ambitious objective, and is often constrained by budget limitations. Therefore, it is crucial to identify an "optimal" level of acceptable risk, below which the cost of further investments would outweigh the benefits of an additional risk reduction. Nevertheless, determining the appropriate level of resources to allocate to such investments is not an easy task because, unlike traditional investments, security investments are aimed at preventing future losses rather than generating immediate economic returns. Indeed, every euro spent on enhancing the safety of business networks and devices does not result in an immediate profit for the company. This situation shifts the traditional trade-off between risk and return that are typical of financial investments to a trade-off between risk and cost savings. Moreover, the cost assessment can be challenging due to the necessity of taking both direct expenses (such as installation and maintenance) and indirect costs (such as changes in employee motivation or workflow) into account (Böhme, 2010).

Several contributions in the literature have studied this topic in different contexts. In Fedele and Roner (2022), a taxonomy of existing scientific papers was presented and organized within a common reference framework. Additionally, a model was developed to integrate these contributions and to analyze their key findings. Studies that have focused on the investment challenges faced by individual firms are distinguished from those that examined interdependent firms. Among the former, a milestone is the Gordon & Loeb model (hereinafter G&L model), which was proposed in their foundational paper on the economics of information security investments (Gordon and Loeb, 2002).

This model is instrumental in determining the optimal level of cybersecurity investments by balancing the costs of security measures against the potential losses from security breaches. The model typically suggests that it is not optimal to invest more than 37% of the expected loss. Several studies have expanded on or applied the G&L model in various contexts (Skeoch, 2022; Feng et al., 2022; Gordon et al., 2021, among the others) . Even remaining a cornerstone in the field of cybersecurity economics, several contributions have underlined some criticism such as its simplistic assumptions and static nature together with the lack of consideration for the interdependence of security risks (Böhme and Schwartz, 2020; Shetty et al., 2018). Nevertheless, the key advantage of this model is a balanced approach that combines rigor with simplicity, thus offering initial quantitative inputs adaptable to real-world experience. Regarding the valuation of security investments, many contributions in literature have proposed to adapt the metrics of investment theory to security investment valuations. Actually, the most used one, the Return on security investments (ROSI), is an adaptation of the Return on investments (ROI) (Böhme and Nowey, 2008; Böhme, 2010; Sonnenreich et al., 2006). Another metric was proposed in

Orlando (2021), which adapted the Risk adjusted return on capital (RAROC) to the security investments context. However, an effective cyber risk management process must also consider that some extreme cases may cause huge losses, thus avoiding investment underestimation. With this in mind, Orlando (2021) proposed some risk adjusted metrics based on a measure of the extreme losses, namely the Value at Risk (VaR). It is a risk measure that comes from the financial field and was adapted to cybersecurity domain; it is often referred to as the Cyber-Value at risk (World Economic Forum, 2012). In this framework, we propose a methodology to estimate a business organization's risk exposure and expand the evaluation of security investment effectiveness by incorporating the aforementioned metrics in the G&L framework. In line with Gordon et al. (2016, 2020) and aware that this is a field where theoretical economic models of security investments could offer valuable insights, we test the potential practical applications of the G&L model. The paper is organized as follows: in Section 2 we recall the main features of the G&L model and, in light of its main findings, propose a revision of the main valuation metrics, as well as describe the methodology to estimate the risk exposure in the context of a specific application example; in Section 3, we apply the proposed methodology and show the results; and Section 4 concludes the paper by discussing advantages and limitations of this approach and suggests further developments.

2. Materials and methods

2.1. The Gordon-Loeb model

In their seminal paper (Gordon and Loeb, 2002), Gordon and Loeb proposed an approach to derive the required optimal level of security investments for an organization. Referring to the potential economic impact of a cyber incident *L*, they started from the assumption that an invested amount of money, denoted by *z*, reduces the probability *v* that a breach will occur (vulnerability). The G&L defines the security breach probability function *p(v,z)*, which takes the productivity of different values of *z* into account, thus providing a revised measure of the probability *v* consequent to the investment. The model assumes that the probability *p(v,z)* is twice continuously differentiable and strictly convex, thus ensuring that the benefits from increasing security investments related to a specific information set grow at decreasing rates.

One of the proposed security breach functions is as follows:

$$p(v, z) = \frac{v}{(\alpha z + 1)^{\beta}} \tag{1}$$

where $\alpha > 0$ and $\beta \geq 1$ are the parameters of the amount z productivity in raising the firm's security level (regarding parameters calibration, see Naldi and Flamini, 2017). Then, the expected net benefit deriving from investing an amount z, ENBIS in Gordon and Loeb (2002), is defined as follows:

$$ENBIS(z) = E[L] - E_z[L] - z. \tag{2}$$

where $E[L] = vL$ is the expected loss before the investment and $E_z[L] = p(z, v)L$ is the reduced expected loss after the investment z. Based on formula (1), it follows that

$$E_z[L] = \frac{E[L]}{(\alpha z + 1)^{\beta}}. \tag{3}$$

ENBIS represents the balance between costs and benefits of investing in security, and it must be strictly positive for a rational individual who is investing in security measures. Given that the probability function of a security breach is strictly convex in relation to z, ENBIS, in turn, is strictly concave in z, thus implying the existence of an interior optimal level of an investment greater than zero. Letting z^* denote this optimal level yields the following (Gordon and Loeb, 2002):

$$z^* = \frac{(E[L]\alpha\beta)^{\frac{1}{\beta+1}} - 1}{\alpha}. \tag{4}$$

At the optimal investment level z^*, the expected marginal benefits equal the marginal cost of the investment. Gordon and Loeb demonstrated that this sum of money would never exceed 37% of the expected loss E[L]. Contrary to fundamental risk assessment principles, they asserted that a more valuable asset does not necessarily require a higher investment for its protection; there comes a point where it is not advantageous for a company to continue increasing its expenditure on information security (European Union Agency for Cybersecurity (ENISA), 2012).

2.2. Security investment metrics

A well-known metric to assess the value of security investments is ROSI. ROSI is a financial metric that helps organizations assessing the value of their security expenditures by comparing the expenses incurred with the financial gains achieved through the prevention of potential security incidents. It is an adaptation of the ROI broadly used in the financial and economic domain. It is defined as follows (European Union Agency for Cybersecurity (ENISA), 2012):

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

where E[L] is the expected aggregate loss and $\Delta E[L]$=$E[L_t]$-$mE[L]$ is the loss reduction over a certain period measured by the difference between the expected aggregate loss $E[L]$ and the term $mE[L]$, which is the mitigated loss expectancy due to the investment in security z.

Several contributions in the existing literature have pointed out the main challenges in estimating ROSI (Sonnenreich et al., 2006; Böhme and Nowey, 2008, (among the others). Indeed, it can be challenging to assess the expenses associated with IT security. This difficulty stems from the need to account for both direct and indirect costs. Another significant concern is the evaluation of the mitigating impact of security investments.

Despite these challenges, ROSI remains a useful metric in a real-world scenario. Nevertheless, this is a field where theoretical economic models of security investments could offer valuable insights by supplying initial quantitative data, which can later be refined through real-world experiences. As observed in Skeoch (2022), ROI is quite similar to ENBIS (Eq. 2), though it is expressed as a percentage rather than in monetary terms. Starting from this consideration, we propose an application of the G&L model to assess the ROSI metric. Based on Equation 2 , we can rewrite Equation 5 as follows:

$$ROSI = \frac{E[L] - E_z[L] - z}{z}. \tag{6}$$

This approach allows us to have a rough estimation of the ROSI numerator by assessing the expected loss reduction consequent to the investment of the amount z. Moreover, the expected ROSI obtained by investing the optimal amount of the investment z^* can be assessed and compared to alternative invested amounts of money.

In this context, worst-case scenarios cannot be neglected, that is, the possibility of events with a low probability of occurrence but a high negative impact must be considered. To this aim, Orlando (2021) introduced a risk adjusted ROSI measure, RaROSI, which took the worst cases into account. The idea is to consider the difference between the expected loss without a mitigation effect of the investment $E[L]$ and the worst case loss at a given confidence level α mitigated by the investment.

RaROSI is based on the Value at Risk (VaR), which was formally introduced by JP Morgan in 1995 (Morgan and Reuters, 1996), thereby defining it as the "predicted worst-case loss at a specific confidence level", ϵ:

$$VaR(\epsilon) = F_L^{-1}(1 - \epsilon) \tag{7}$$

where F is the distribution function of the loss L and $\epsilon \in (0, 1)$ is the confidence level. Indeed, it is the quantile of order $(1 - \epsilon)$ of the loss distribution. The potential utility of this risk measure in the cyber domain, where it is referred to as the Cyber-Value-at Risk (World Economic Forum, 2012), has been broadly recognized.

Based on Equations 2 and 5, RaROSI can be rewritten as follows:

$$RaROSI(\epsilon) = \frac{E[L] - VaR_z(\epsilon) - z}{z} \tag{8}$$

where $VaR_z(\epsilon)$ measures the extreme expected loss mitigated by the investment z at a confidence level α. RaROSI supports investment decisions by accounting for unexpected losses considering rare but impactful tail events. In the G&L model, the optimal investment z^* (Eq. 4), as well as a generic investment z in a real world scenario, depends on the expected loss. Accordingly, if an extreme event occurs, then z could be insufficient to adequately reduce the worst case loss. Based on these considerations, it follows that RaROSI can potentially support the security investment decisions, thereby improving the commonly used investment risk metrics.

Other indicators used in the financial sector can enrich the analysis for evaluating investments in security (Orlando, 2021). Among these, the so-called risk-adjusted return on capital (RAROC) was first applied in the early 1990s at the Bank of America (Zaik et al., 1996). It is a financial metric that assesses the profitability of an investment by taking the risk involved into account. It is calculated by dividing the expected return of the investment by the economic capital required to sustain the investment's risk (Resti and Sironi, 2012) and is expressed as a percentage. Higher RAROC percentages indicate greater returns in relation to the risk exposure. By adapting this indicator to the context of our analysis, we can write the following:

$$RAROC(\epsilon) = \frac{\Delta E[L] - z + i * C}{C} \tag{9}$$

where $\Delta E[L] - z = ENBIS$, $C = x\% VaR(\epsilon)$ is the reserve capital in case of unexpected losses expressed as a percentage $x\%$ of the Value at Risk, and i is the risk-free rate. Therefore, RAROC is the ratio between ENBIS plus the investment gains of the allocated capital C and the capital itself. RAROC allows us to assess if investments are generating adequate returns given a firm's risk profile. Therefore, it can be a key tool to quantify risk and optimize capital usage. A crucial step to compute the described indicators is the estimation of the probability distribution of losses, which is necessary to assess both the expected value, $E[L]$, and the Value at Risk, $VaR(\epsilon)$. To this aim, we need to model both the frequency with which a negative cyber event occurs and its severity. Indeed, the frequency allows to estimate the likelihood of a cyber incident, while severity gives a measurement of its impact. In what follows, we refer to a publicly available dataset, the Privacy Rights Clearinghouse (hereinafter, PRC data). We chose this dataset on the grounds that data breaches, together with ransomware attacks, are the main cause of cyber incidents and the most concerning cyber risk exposure for companies (Allianz Global Corporate & Specialty, 2022).

2.3. Data description

PRC, a nonprofit organization focused on data privacy rights and issues, maintains a dataset of cyber incidents, called Chronology of Data Breaches in the US (Privacy Rights Clearinghouse, 2018). Data are sourced from official breaches reports, (e.g., State Attorneys General, U.S. Department of Health and Human Services) and all the events are confirmed by major media sources. Information on data breaches occurred in the US from January 2005 to December 2019 includes a description of the type of breach and the breached entity, and the number of breached records, when available. Specifically, organizations are classified as follows: business-financial and insurance services (BSF); business-retail/merchant including online retail (BSR); business-other (BSO); educational institutions (EDU); government and military (GOV); healthcare, medical providers and medical insurance services (MED); and nonprofit organizations (NGO). Information exposures (breaches) are reported as CARD (Debit and Credit Cards Frauds excluding Hacking), HACK (data loss due to hacking or malware infection), INSD (data loss due to insiders, such as employees, contractors or customers), PHYS (physical data loss, such as lost, stolen or discarded documents), PORT (data loss due to lost, discarded or stolen portable devices such as laptops, smartphones, memory sticks, hard drives, etc.), STAT (stationary computers or servers data loss), DISC (unintended disclosure of data not involving hacking, intentional breach or physical loss, such as sensitive information posted publicly, mishandled or sent to the wrong party via online publishing, emails, faxes,..), and UNKN (unknown cause, not enough information). For a detailed description of this dataset, see Carfora and Orlando (2022b).

These data represent the more complete publicly available resources on cyber breaches; however, they suffer from two main limitations. First, the number of incidents is underestimated, since the dataset only relies on publicly acknowledged breaches. Second, they do not have information on the financial losses derived from the breaches. The severity of each event is just measured by the number of affected records, from which the financial impact of the breach can be approximately retrieved through empirical regression formulas (Jacobs, 2014; Farkas et al., 2021). In agreement with other studies (Sun et al., 2021), we assume that more recent data could better represent the current cyber threat situation. Indeed, in the last few years, cyberspace safety has been widely recognized as a fundamental issue and several interventions have confirmed the growing concern of both public institutions and private companies regarding cyber risks. As a consequence, more recent incidents are regularly and more accurately documented. This is the reason for restricting our analysis to the breaches reported starting from January 2010. Moreover, we considered only breaches with complete information on the severity and the cause. Table 1 reports the number of breached records in the considered time interval for the different typologies of organizations and causes.

Table 1. Number of breached records reported in the PRC Chronology from January 2010 to December 2019 for the different organization types and breach causes.

	BSF	**BSO**	**BSR**	**EDU**	**GOV**	**MED**	**NGO**	**UNKN**
#N/A	0	0	0	0	0	3079889	0	0
CARD	7035066	310	2124575	16	0	0	0	0
DISC	1550375	2105006706	385194087	1576141	21094488	12979387	3501561	0
HACK	348057288	5494774684	791295680	45231810	40900705	159979906	3350944	0
INSD	2407569	3508456	35671	40379	28506293	1059014	317	0
PHYS	58909	64007	4071	1023422	209616	35715718	24157	0
PORT	5852045	5836258	30244	238778	7683283	12645645	72176	0
STAT	100348	80108	9189	78177	3650	9604567	0	0
UNKN	421366	100155387	68000391	10352675	849587	109731	2501	10657026

2.4. Data modeling and yearly estimated loss

Breaches are characterized by their frequency and severity, which is measured by the number of compromised records in a single breach. As assessed in previous studies (Edwards et al., 2016; Carfora et al., 2019; Carfora and Orlando, 2022a,b, see), while the frequency of breach incidents is well modeled by a negative binomial distribution, the great heterogeneity in both the breach typology and the organization types requires a finer modeling for the breaches' severity; then, we decided to split the data into more homogeneous subsets and considered separate risk categories. Specifically, we only considered the three Business type organizations (BSF, BSO, and BSR), grouped together, and divided the incident types in two main groups, the 'negligent' breaches, caused by accidental exposures or inadequate vigilance (i.e., DISC, PHYS, PORT, STAT categories), and the 'malicious' ones that are a consequence of intentional attacks (i.e., CARD, HACK, INSD categories). Then, the severity of the breaches is modeled by skew-normal distributions with different parameters for the two groups.

After obtaining the best fit for the frequency and severity distributions of single breach events that belong to the considered data subset of Business organizations, we quantified the estimated yearly loss for a generic company in this subset: inspired by Farkas et al. (2021), we proposed a Monte-Carlo based simulation approach, described in the following paragraph, to reconstruct the losses distribution. Guided by the cited literature, we assumed that the probability for an organization of suffering $n_c \geq 0$ breaches in a year can be modeled by a geometric distribution with parameter p, whose value for the business categories is estimated as $p = 0.91$. Moreover, historical data from the PRC archive provided an estimate of the relative frequency f_m of malicious events (about 2/3) over the total number of events for the same group of organizations. Then, reliable estimates for the annual losses of a Business type organization are obtained by generating a huge number M of scenarios, in which the number of claims, their type (malicious or not), and severity are produced according to the given parameters. To obtain the financial loss that corresponds to the severity of each event, we follow Jacobs (Jacobs, 2014; Farkas et al., 2021) where two empirical regression rules are proposed.

We just remark that, in principle, one should distinguish between "third-party" and "first-party" ones. The OECD (OECD, 2017) provides a comprehensive summary of the various types of losses that result from a cyber incident: damage to both physical and non-physical assets, business interruption losses, and theft. Additionally, the report identifies liabilities to third parties including customers, suppliers, employees, and shareholders. In Jacobs' transformation, a single value that encompasses both the first-party and the third-party is considered (Jacobs, 2014; Farkas et al., 2021), and we make the same hypothesis. Finally, the expected yearly loss can be estimated as the average loss over all scenarios and, based on formula 7, $VaR(\epsilon)$ is also calculated as the empirical quantile of the distribution of annual losses across all scenarios. From these values, the proposed indicators are obtained. Figure 1 provides a visual representation of the entire procedure.

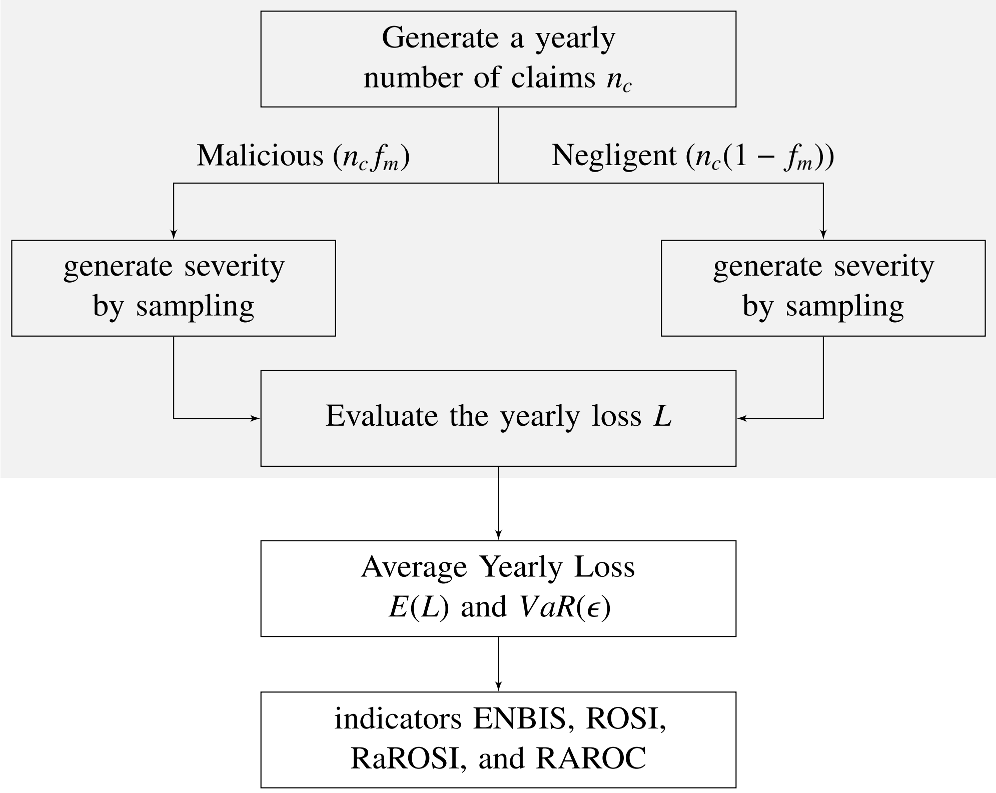
Generate a yearly number of claims n_c
Malicious ($n_c f_m$)
Negligent ($n_c(1 - f_m)$)
generate severity by sampling
generate severity by sampling
Evaluate the yearly loss L
Average Yearly Loss $E(L)$ and $VaR(\epsilon)$
indicators ENBIS, ROSI, RaROSI, and RAROC

Figure 1. Schematic of the Monte Carlo simulation approach used to estimate the proposed indicators. The gray block is repeated for each of the M scenarios.

3. Results

Based on the methodology described in Section 2.4, we report the estimated values of the expected loss $E[L]$ and the Value at Risk $VaR(\epsilon)$ along with their standard errors for ten groups of 1 Million scenarios in Table 2. In all simulations, we chose $\epsilon = 0.05$.

Table 2. Estimates ($) of the annual $E[L]$ and $VaR(\epsilon)$ for $\epsilon = 5\%$.

$E[L]$	$VaR(\epsilon)$
23647 ±38	135382±2245

$E[L]$ and $VaR(\epsilon)$ play a key role in quantifying the security investment metrics described in Section 2.2; the values on a yearly basis are reported in Table 3.

Table 3. Investment metrics (based on Equations 4, 3, 2, 5, 8, 9). G&L model parameters: $\alpha = 4 * 10^{-4}, \beta = 1.13$ and $\epsilon = 0.05$

z	% E[L]invested	% E[L]reduced	ENBIS	ROSI	RaROSI(ϵ)	RAROC(ϵ)
1182	5%	35%	7199	6.088	−54.920	10.64%
2365	10%	53%	10137	4.286	−17.982	13.36%
3547	15%	63%	11384	3.209	−8.401	14.51%
5103	**22%**	**71%**	**11815**	**2.315**	**−3.915**	**15.00%**
7094	30%	78%	11379	1.604	−1.841	14.50%
8276	35%	81%	10834	1.308	−1.281	14.00%
9459	40%	83%	10155	1.073	−0.941	13.78%
11824	50%	86%	8534	0.721	−0.592	11.88%

The first column shows the amounts of capital z invested to raise the security level, and each value corresponds to a percentage of the estimated loss before the investment, $E[L]$ ($\%E[L]$ invested, column 2). The reduction in the expected loss due to the investment z is reported as a percentage in column 4 ($\%E[L]$ reduced). This value is obtained by calculating $E_z[L]$ according to Equation 3. In the remaining columns, the estimates for the ENBIS, ROSI, RaROSI, and RAROC indicators are provided (Equations 2, 5, 8, and 9, respectively). Informed by the existing literature (Naldi and Flamini, 2017), we set the G&L model parameters as follows: $\alpha = 4 * 10^{-4}$ and $\beta = 1.13$. The bold line in Table 3 refers to the values of each variable calculated at the optimal investment level $z^* = 5103\$$ given by Equation 4. As shown, this invested capital corresponds to 22% of $E[L]$ (column 2, line 4), which result is consistent with what was demonstrated by Gordon and Loeb in their model (Gordon and Loeb, 2002), namely that the optimal investment was never more than 37% of the expected loss. As observed in the previous Sections, there comes a stage when it is no longer beneficial for a company to keep raising its spending on information security. Consequently, the ENBIS value (column 4), which is calculated based on Equation 2, reaches its maximum value of 11815$ (column 4, line 4) at the optimal investment amount of 5103$, and then decreases with z; this means that the investments which correspond to a higher percentage of $E[L]$ have a lower return in terms of a reduction of the expected loss (column 3).

Now, let us look at the ROSI (column 5), which is estimated based on Equation 5. First of all, it is important to highlight that, obviously, a ROSI greater than zero means that the company's security investments have produced a positive return. Indeed, a positive ROSI indicates that the security measures have successfully diminished the losses and enhanced the operational efficiency, thus leading to higher revenue for the company. An investment operation that results in a ROSI greater than one is particularly advantageous; this would mean that, in Equation 5, the benefit derived from the investment (numerator) is greater than the cost of the investment itself (denominator). Looking at Table 3, all the ROSI values are higher than one, except for the last value, which is obtained with an investment of 1184$ corresponding to 50% of the expected loss $E[L]$. The ROSI shows a significantly different behavior compared to the ENBIS in that it decreases as the investment z increases. The ROSI coming from the optimal investment $z^* = 5103$ is 2.315 (column 5, line 4).

Investing less than z^* provides a higher ROSI; however, we observe that the reduction in loss is also smaller with a smaller investment. On the other hand, investing more results in both a lower ENBIS and a lower ROSI, even if a greater reduction in the expected loss is obtained (column 3). Indeed, this reduction is not offset by the ENBIS and the ROSI values, thus indicating a diminished incentive to invest more.

Regarding the RaROSI (column 6), we observe negative values compared to whatever the amount of money invested z is. The reason lies in that this indicator accounts for unexpected losses characterized by a low probability but a high impact. As a consequence, the amount of invested money could be insufficient. The estimated values (Table 3) indicate that the higher the amount invested, the better the effect on the RaROSI, meaning that the negative impact of an unexpected loss decreases. Therefore, this indicator complements the investment evaluation analysis: even if a certain investment produces positive ENBIS and ROSI, it is important to consider the effects of an unexpected extreme loss, which also applies to the optimal investment z^*. In the last column, the RAROC values are reported. Based on Equation 9, we know that it is the ratio of the expected net benefit plus investment gains of an allocated capital at the risk free rate i and the capital itself. The allocated capital is a percentage of the probable extreme loss, $VaR(\epsilon)$, which is set aside to front the scenario of an actual loss greater than the expected one. In our example, we set the percentage at 80% and the risk free rate to 4%. We observe that the RAROC reaches its higher value, 15%, if the optimal amount $z^* = 5103$ is invested (column7, line 5).

Regarding the evaluation of security investments, the results show that it is appropriate to assess other profitability indicators in addition to the expected net benefit. This supplements the necessary information for making proper decisions while taking the return on the investment, the extreme unexpected losses, and the allocation of the capital needed to front probable extreme scenarios into account. Indeed, the optimal investment level assessed basing on the G&L model, characterized by the highest ENBIS, does not give the best results in terms of the ROSI and the RaROSI. If we look at the ROSI, it could be better to invest less; alternatively, if we look at the RaROSI, it could be preferable to invest more to front extreme scenarios. Therefore, the company must take both the available budget and its risk tolerance into account. Basing on that, the company might want to invest more to protect itself from the possibility of an incident causing a significantly higher-than-expected loss. Alternatively, it could decide to invest much less to achieve a high return on their investment while risking not being able to cope with the possibility of a significant extreme event. In any case, the results obtained by considering the optimal investment z^* are satisfactory, as we observe the maximum values of ENBIS and RAROC, a ROSI of 2.315 (meaning that for every dollar invested, benefits of just over 2 dollars are achieved), and an acceptable RaROSI value compared to the alternatives considered.

4. Discussion and conclusions

Cybersecurity has emerged as one of the top concerns for many companies. A successful cyber attack can be both damaging and costly, thus making investments in cybersecurity a logical choice. By implementing the right tools, processes, and solutions, an organization can significantly reduce the potential risk and impact of a cybersecurity incident. Security leaders must strategically balance investments with financial sustainability to ensure that spending is effectively translated into protection, rather than assuming that more investments always means better security. From a cost-benefit perspective, a key point is answering to the question: “How much is enough?” (Böhme and Nowey, 2008). A tentative answer was given by Gordon and Loeb that, in their seminal paper (Gordon and Loeb, 2002), proposed a theoretical model demonstrating that the optimal investment amount that maximized the expected net benefit of investing in security was less than 37% of the expected loss due to a cyber incident. Undoubtedly, from a measurement perspective, the high level of abstraction in the G&L model can be problematic. This is mainly because it directly links security investment amounts to the probability of loss, thus bypassing intermediate factors such as the actual level of security (Böhme, 2010). Despite this, its main benefit is a balanced methodology that merges rigor with simplicity, thus providing initial quantitative data that can be adjusted according to real-world experiences. Based on these considerations and in line with Gordon et al. (2016), we focused on understanding the G&L model's practical application. The contribution of our research is twofold:

- simulate a real-world scenario and propose a methodology to estimate the risk exposure of a company;
- extend the valuation of security investment benefits by considering other metrics than ENBIS.

As for the first point, we referred to a generic business type organization which bore the risk of data breaches, which are a great concern for companies (Allianz Global Corporate & Specialty, 2022). Based on previous studies (Carfora and Orlando, 2022b), we separated the breach data into two categories, thereby highlighting the different statistical nature (in terms of distribution parameters) of the negligent breaches and the malicious ones. Then, according to Farkas et al. (2021), we developed a Monte-Carlo based simulation to reconstruct the losses distribution. Nevertheless, the accuracy of the statistical data in this domain is hard to achieve, as companies are often reluctant to provide data on their security incidents (European Union Agency for Cybersecurity (ENISA), 2012). By means of the proposed methodology, we obtained rough estimates of the expected losses and the $E[L]$ and the $VaR(\epsilon)$, which played key roles in our investment analysis. Regarding the second point, we focused our analysis on the measurement of certain indicators such as ROSI and other metrics (RaROSI and RAROC) that consider the risk of significant unexpected losses, as measured by the VaR. In light of our findings, we can conclude that the expected net benefit of an investment, maximized at the optimal investment level, is not sufficient information to support appropriate decision-making. The use of metrics that account for the benefit relative to risk, as well as worst-case scenarios, provides additional insights. Indeed, taking the firm's risk profile and available budget into account might lead a company to invest an amount different from the optimal one. Our research is just a starting point and displays several limits, as highlighted in the previous sections. However, it allows us to focus on some key issues and offers room for future research.

Further steps will include testing the methodology to estimate the loss distribution on other datasets, thus allowing us to consider a richer range of types of incidents and make more extensive comparisons. Regarding the chosen model, we plan to deepen our analysis by considering the other security investment models proposed in the literature (Mazzoccoli and Naldi, 2022), which would also allow us to compare the results and better generalize our conclusions.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU

Author contributions

All authors contributed equally to this work.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

Allianz Global Corporate Specialty (2022) Allianz Risk Barometer: Top Business Risks for 2022. Report.

Böhme R (2010) Security metrics and security investment models. In *Advances in Information and Computer Security. IWSEC 2010. Lecture Notes in Computer Science*. Springer, Berlin. https://doi.org/10.1007/978-3-642-16825-3_2

Böhme R, Nowey T (2008) Economic security metrics. In Irene Eusgeld, F. F. and Reussner, R. H., editors, *Dependability Metrics. Lecture Notes in Computer Sciences 4909*, 176–187. Springer, Berlin Heidelberg. https://doi.org/10.1007/978-3-540-68947-8_15

Böhme R, Schwartz G (2020) Modeling the interdependent risks and investments in information security. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*.

Carfora M, Martinelli F, Mercaldo F, et al. (2019) Cyber risk management: An actuarial point of view. *J Oper Risk* 14: 77–103.

Carfora M, Orlando A (2022a) Cyber risk: Estimates for malicious and negligent breaches distributions. In Corazza, M., Perna, C., Pizzi, C., and Sibillo, M., editors, *Mathematical and Statistical Methods for Actuarial Sciences and Finance*, 140–145, Cham. Springer International Publishing. https://doi.org/10.1007/978-3-030-99638-3_23

Carfora M, Orlando A (2022b) Some remarks on malicious and negligent data breach distribution estimates. *Computation* 10. https://doi.org/10.3390/computation10120208

Edwards B, Hofmeyr S, Forrest S (2016) Hype and heavy tails: A closer look at data breaches. *J Cybersecurity* 2: 3–14. https://doi.org/10.1093/cybsec/tyw003

European Commission (2024) Dora regulation. Available from: ec.europa.eu/finance/docs/level-2-measures/dora-regulation-rts–2024-1532_en.pdf.

European Union Agency for Cybersecurity (ENISA) (2012) Introduction to return security investments. Available from: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/@@download/fullReport.

Farkas S, Lopez O, Maud T (2021) Cyber claim analysis using generalized Pareto regression trees with applications to insurance. *Insur Math Econ* 98: 92–105. https://doi.org/10.1016/j.insmatheco.2021.02.009

Fedele A, Roner C (2022) Dangerous games: A literature review on cybersecurity investments. *J Econ Surv* 36: 157–187. https://doi.org/10.1111/joes.12456

Feng N, Wang H, Li M (2022) Optimizing cybersecurity investment: An application of the Gordon-Loeb model in industry 4.0. *Comput Secur* 111.

Fernandez De Arroyabe I, Arranz C, Arroyabe M, et al. (2023) Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Comput Secur* 124: 102954. https://doi.org/10.1016/j.cose.2022.102954

Fortune Business Insights (2023) Cyber security market size, share & trends analysis report by component, by security type, by deployment mode, by enterprise size, by industry vertical, by region, and segment forecasts, 2023–2030.

Gordon L, Loeb M (2002) The economics of information security investment. *Acm T Inform Syst Secur* 5: 438–457. https://doi.org/10.1145/581271.58127

Gordon L, Loeb M, Zhou L (2016) Investing in cybersecurity: insights from the Gordon-Loeb model. *J Inf Secur* 7: 49–59. http://creativecommons.org/licenses/by/4.0/

Gordon L, Loeb M, Zhou L (2021) The impact of information security breaches on stock market returns: The role of financial analysts. *J Account Public Pol* 40.

Gordon L, Loeb P, Zhou L (2020) Integrating cost-benefit analysis into the nist cybersecurity framework via the gordon-loeb model. *J Cybersecurity* 6: 1–8. https://doi.org/10.1093/cybsec/tyaa005

Jacobs J (2014) Analyzing Ponemon cost of data breach. Available from: http: //datadrivensecurity.info/blog/posts/2014/Dec/ponemon/.

Javadnejad F, Abdelmagid A, Pinto C, et al. (2024) An exploratory data analysis of malware/ransomware cyberattacks: insights from an extensive cyber loss dataset. *Enterp Inf Syst* 18: 2369952. https://doi.org/10.1080/17517575.2024.2369952

Mazzoccoli A, Naldi M (2022) An overview of security breach probability models. *Risks* 10. https://doi.org/10.3390/risks10110220

Morgan J, Reuters (1996) RiskMetrics^{TM}.

Naldi M, Flamini M (2017) Calibration of the Gordon-Loeb models for the probability of security breaches. In *2017 UKSim-AMSS 19th International Conference on Computer Modelling & Simulation (UKSim)*, 135–140. https://doi.org/10.1109/UKSim.2017.18

OECD (2017) Types of cyber incidents and losses.

Orlando A (2021) Cyber risk quantification: investigating the role of cyber value at risk. *Risks* 9: 184. https://doi.org/10.3390/risks9100184

Privacy Rights Clearinghouse (2018) Chronology of data breaches. Available from: https://www.privacyrights.org/data-breaches.

Resti A, Sironi A (2012) *Risk Management and Shareholders' Value in Banking: From Risk Measurement Models to Capital Allocation Policies.* Wiley Finance. Hoboken: John Wiley Sons Ltd.

Shetty S, McShane M, Zhang R (2018) A portfolio approach to cybersecurity investment. *J Risk Insur* 85: 359–384.

Skeoch H (2022) Expanding the Gordon-Loeb model to cyber-insurance. *Comput Secur* 112: 102533. https://doi.org/10.1016/j.cose.2021.102533

Sonnenreich W, Albanese J, Stout B (2006) Return on security investment (ROSI) - a practical quantitative model. *J Res Pract Inf Tech* 38: 45–56.

Sun H, Xu M, Zhao P (2021) Modeling malicious hacking data breach risks. *N Am Actuar J* 25: N484–502. https://doi.org/10.1080/10920277.2020.1752255

World Economic Forum (2012) Risk and responsibility in a hyperconnected world-principles and guidelines.

Zaik E, Walter J, Retting G, et al. (1996) RAROC at Bank of America: From theory to practice. *J Appl Corp Financ* 9: 83–93. https://doi.org/10.1111/j.1745-6622.1996.tb00117.x

AIMS Press

© 2024 MF Carfora and A Orlando, licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0)