risks

MDPI

Article

An Overview of Security Breach Probability Models

Alessandro Mazzoccoli † and Maurizio Naldi *,†

Department of Law, Economics, Politics and Modern Languages, LUMSA University, Via Marcantonio Colonna 19, 00192 Rome, Italy

* Correspondence: m.naldi@lumsa.it

† These authors contributed equally to this work.

Abstract: Cybersecurity breach probability functions describe how cybersecurity investments impact the actual vulnerability to cyberattacks through the probability of success of the attack. They essentially use mathematical models to make cyber-risk management choices. This paper provides an overview of the breach probability models that appear in the literature. For each of them, the form of the mathematical functions and their properties are described. The models exhibit a wide variety of functional relationships between breach probability and investments, including linear, concave, convex, and a mixture of the latter two. Each model describes a parametric family, with some models have a single parameter, and others have two. A sensitivity analysis completes the overview to identify the impact of the model parameters: the estimation of the parameters which have a larger influence on the breach probability is more critical and deserves greater attention.

Keywords: breach probability function; cybersecurity; investment; vulnerability

Citation: Alessandro Mazzoccoli, and Maurizio Naldi. 2022. An Overview of Security Breach Probability Models *Risks* 10: 220. https://doi.org/10.3390/risks10110220

Academic Editor: Mogens Steffensen

Received: 13 October 2022
Accepted: 14 November 2022
Published: 17 November 2022

1. Introduction

Cyberattacks are continuously increasing, as highlighted by several sources. The COVID-19 pandemic over the last three years accelerated an existing trend, as highlighted in the survey by Georgescu (2021). The number of companies experiencing more cybersecurity incidents is up to 60%. In particular, a 13% increase in ransomware was observed Verizon Risk Team (2022). Moreover, a threefold increase in Remote Desktop Protocol (RDP) attacks occurred Georgescu (2021). Though the shift to remote work during the pandemic may be considered the trigger for many of the latest trends, the rising trend of cybersecurity incidents has been going on for several years. After analyzing data provided by Advisen, a US-based organization that acquires and sells cyberloss and incident data to insurers, it was found that reinsurers, brokers, and cybermodeling firms, Palsson et al. (2020) experienced a steady increase in cyberincidents over the years, covering since 2018. Xu et al. (2018) tried to find a model for the time series of hacking breaches, observing a sharp decrease in the interarrival time of incidents (hence, an increase in their frequency) starting in 2016. Going a bit backwards, Wheatley et al. (2016) highlighted that the overall frequency of large data breaches has increased in the period ending in 2015 (due especially to outside-the-US events), driving the growth in the overall volume of breached records. Finally, Maillart and Sornette (2010) identified faster-than-exponential growth from 2000 to 2006, i.e., roughly twenty years ago. That marks a very long period of practically uninterrupted growth of cybersecurity issues. It has to also be noted that not all cyberincidents are reported: Sangari and Dallal (2022) have proposed an approach to estimate unaccounted incidents and correct the count of incidents. Bothos et al. (2021) adopt an econometric model to predict the probability of an attack, considering bug bounties and the prizes offered for white-hat hackers in a time series model. A contagion model for the attack is instead suggested by Chiaradonna and Lanchier (2021), where contagion spreads through the edge of the network, moving with different probabilities towards lower-level and higher-level assets. Contagion is similarly analyzed by Xu and Hua (2019), where both Markovian and

non-Markovian models are employed. Machine learning is instead employed to predict attacks in (Yeboah-Ofori et al. 2021).

Aside from the technical disruption caused by cyberattacks, their economic consequences have been a significant issue of concern in cybersecurity management since long ago, as reported in the economic-grounded cyber-risk management framework put forward by Jerman-Blažič et al. (2008); Rodrigues et al. (2019). Costs related to cybercrime belong to several categories, as listed by Eling and Wirfs (2019). The measurement (or estimation) of the losses caused by cyberattacks has been addressed by several authors. The use of Value-at-Risk as a metric for cyberlosses has been advocated by Erola et al. (2022). A similar approach addressing extreme risks is considered by Strupczewski et al. (2018), who exploit the SAS OpRisk Global Database. Additional metrics, such as the risk-adjusted return on security investment and risk-adjusted return on capital, have been proposed by Orlando (2021). Giudici and Raffinetti (2022) proposed the use of ordinal regression and Shapley values instead to describe the level of cyber-risk as a means to progress towards explainability. In addition to the immediate consequences of attacks, being exposed to cyberattacks has far-reaching consequences on the market value of companies, as investigated by Arcuri et al. (2017) and Hovav and D'Arcy (2003). Lin et al. (2021) have reversed this point of view, using the public stock market response to estimate cyberlosses. A similar reverse approach has been put forward by Woods et al. (2021), who use particle swarm optimization to derive a cyberloss distribution from cyberinsurance prices. The estimation of the actual costs is a research theme itself, as shown in several papers, e.g., by Hua and Bapna (2013); Kamiya et al. (2020); Poufinas et al. (2018); World Economic Forum (2015) and The Ponemon Institute (2016). An econometric approach relating cyberlosses to company size has been proposed by Yamada et al. (2019). The availability of data, especially through open access databases, has been highlighted as a further problem that hampers all attempts to tackle cyber-risk and devise a proper cyber-risk management strategy Cremer et al. (2022).

From an economic point of view, strategies to manage cyber-risks have the natural aim of minimizing the overall loss, where the term *overall* implies that we must factor in the economic values of many terms in the budget equation. Under this aspect, the set of strategies that we may consider in cyber-risk management is not at all different from the taxonomy of strategies available for general risk management Scala et al. (2019), i.e., the three categories of risk avoidance, risk transfer, and risk mitigation (or a combination thereof), as described by Paté-Cornell et al. (2018) and Refsdal et al. (2015). A historical survey of cyber-risk management with an eye on the future is reported by McShane et al. (2021).

While risk avoidance is not a viable option in many cases, since it would imply a significant sacrifice of usability, as shown by Murphy and Murphy (2013), we can focus on the latter two.

Risk transfer is typically carried out by buying an insurance policy, where risk is transferred from the insured to the insurer upon paying a premium. Several efforts have been devoted to premium computation formulas. An approach based on the first two statistical moments of loss (mean–variance) has been employed by Mukhopadhyay et al. (2019), while an approach based on a more accurate (and demanding) statistical characterization of losses (up to the fourth moment) has been proposed by Naldi and Mazzoccoli (2018) and Mazzoccoli and Naldi (2020a). Instead, Young et al. (2016) have proposed incorporating a discount in premium formulas and incentivizing all actions aimed at reducing the loss. That proposal has been advocated by Rosson et al. (2019) in the context of the power sector. While these approaches assume loss to be known (or at least estimated), Antonio et al. (2021) have proposed to incorporate the network structure into pricing to account for the presence of clusters in the diffusion of attacks. Lopez and Thomas (2022) have analyzed the possible use of parametric insurance, where a parameter related to the loss is employed instead of the true loss to determine compensation; the parametric approach allows setting up insurance policies when the amount of information about risk is limited. Moreover, the adoption of security audits to design insurance contracts more accurately has been put forward by Khalili et al. (2018). Additionally, the relationship between insurance and pricing

sustainability has been investigated by Mastroeni et al. (2019). The traditional distinction between insured and insurer is abandoned in (Vakilinia and Sengupta 2018), where a coalitional approach is proposed, with organizations playing the role of insured and insurer at the same time, adopting crowdfunding, or outsourcing a common insurance platform. An excellent survey of cyberinsurance has been carried out by Marotta et al. (2017).

Risk mitigation is instead carried out by investing in tools and procedures that can help to reduce the probability of success for cyberattacks and/or the extent of losses when cyberattacks succeed. Mayadunne and Park (2016) have related those investment decisions to the risk-taking attitude of the company. Naldi et al. (2018) have investigated the liability consequence of not investing enough in security. The optimization of investment has been the subject of many papers, which mainly differ on the relationship between investment and security performance. The seminal paper for such an approach is due to Gordon and Loeb (2002). A mixed-integer linear programming formulation has been adopted in the context of Industry 4.0 supply chains by Sawik (2020). Instead, most papers adopt a straightforward net profit maximization. Wu et al. (2015) employ a game-theoretic approach to analyze the investment strategies of two interconnected firms under different types of attack (targeted vs opportunistic). The optimal trade-off between investing in knowledge and expertise versus investing in deploying mitigation measures has been investigated by Wang (2019). The spread of attacks is described through a Susceptible–Infected–Susceptible (SIS) model in Mai et al. (2021), where security investment, recovery costs, and economic losses are considered.

The mixed approach, consisting in investing in reducing the vulnerability and buying an insurance policy to cover the residual risk, was first dealt with by Young et al. (2016), and has been further explored by Mazzoccoli and Naldi (2020b), who have examined the robustness of risk management strategic choices when the information about the system under attack is uncertain. Skeoch (2022) has also embraced a similar approach, but employing a utility function (either logarithmic or exponential) and adopting a percentage premium. The analysis has then been extended by Mazzoccoli and Naldi (2021) to the case of a firm with multiple branches and interdependencies, chasing the problem introduced by Xu et al. (2019). The importance of interdependencies is also examined by Uuganbayar et al. (2021), who examine the possible incentivizing impact that cyberinsurance has on security investments in the case of interdependence. While these studies are concerned either with the variety of attacks or the variety of targets, a slightly different subject is analyzed by Yaakov et al. (2019), who consider choosing among a variety of countermeasures, i.e., including specific mitigation tools (such as intrusion detection systems and firewall) and reporting the results of a game played by fictional decision makers.

When pursuing a mitigation approach (or a mixed one), a crucial role is played by the so-called security breach function, i.e., the function describing the impact of investments on the probability that the attack is successful. Since that function returns a probability value, modeling the vulnerability through the security breach probability function allows us to fulfill the risk description step, which is the third step involved in any risk analysis process, as set in Aven (2011). Moreover, it allows us to evaluate the risk through the computation of the expected value of losses when we associate a loss with each breach event. The choice of a suitable model for the security breach probability function is then a fundamental step in a probabilistic risk assessment (PRA) approach to risk analysis. Though several functions have been proposed for that task, we cannot list a single attempt to line them up and examine them using the same systematic approach. The correct choice of the function, often tailored to the specific type of attack, is essential to properly choose the amount to invest in security. In this paper, we propose a description and analysis of all the breach probability functions that appeared in the literature by adopting a unifying approach. In particular, we provide the following contributions:

- We propose a list of properties that a breach probability function might/should have (Section 2.2);
- We report the breach probability functions appearing in the literature (Sections 2.3–2.11);

- We analyze their properties as above (Sections 2.3–2.11);
- We examine the impact of their parameters (Section 3);
- We report a comparison of models through different aspects with the purpose of helping the reader choose the most suitable for the case at hand (in the Conclusions).

It is to be noted that we strongly advocate the principle that there is no one size fits all. The range of investment choices may be very large, since they may differ not just for their size (monetary value) but also by the device (e.g., investing in antivirus software rather than in a network firewall), the technology employed (e.g., adopting a software based on known malware signatures rather than on a machine learning approach), or the system location where the security devices are placed (e.g., on any single machine or through a centralized approach). Moreover, the impact of each investment choice depends on the type of attack, so some choices are better suited to defend against a specific type of attack.

2. Security Breach Probability Models

The security breach probability function describes how the vulnerability of the system (here embodied by the probability of a breach) is reduced when the company invests in security, i.e., the relationship between investments and security levels. Though several models have been proposed for that function, there are some common features that those models share, i.e., some fundamental properties. In this section, we first outline those properties that any security breach probability function should possess and then provide a detailed survey of the models proposed in the literature.

2.1. Definitions

Before dealing with the properties of the security breach function, we define what it describes more precisely. We adopt the glossary provided by the Society for Risk Analysis Aven et al. (2018), but we provide a bridge with the terms employed in the cybersecurity literature where the standards in the two communities differ.

The event of interest here (see the Definition 1.7 of Aven et al. (2018)) is a data breach, i.e.,[1] "an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner." This definition is consistent with what the authors of the three papers providing the model described here state. Namely, Gordon and Loeb define the security breach probability function as the function providing the probability that an information set is breached Gordon and Loeb (2002). Hausken and Wang follow suit, providing alternative models for exactly the same event Hausken (2006); Wang (2017). For all purposes, the information set breach they consider can be considered a synonym of a data breach.

We do not deal here with the adverse consequences of that breach. The severity of the damage could be quantified (as Gordon and Loeb do) by the amount of money that is lost as a consequence of the breach (see Definition 1.8 of Aven et al. (2018)). As an example of studies considering the influence on consequences other than vulnerability, Wang (2019) analyze separately the role of investments in separately reducing threats (i.e., the probability of an attack), vulnerability (i.e., the probability that an attack succeeds), and impact (i.e., the loss if an attack succeeds).

The threat here is represented by the intention of the attacker (who wishes to get hold of the data) to initiate an attack (see the Definition 1.18 of Aven et al. (2018)).

The vulnerability in the risk analysis context (as reported in the Definition 1.19 of Aven et al. (2018)), i.e., conditional on the risk event, is the probability that a data breach occurs. In the cybersecurity economics literature Gordon and Loeb (2002); Hausken (2006); Wang (2017), a distinction is made between the vulnerability when an investment in security is made (which is the breach probability function for which we later provide the relevant models) and the vulnerability when no investments are made (which is simply called vulnerability in the cybersecurity economics literature). For the sake of maintaining the distinction while employing the SRA terminology, we refer to the breach probability

function as simply the vulnerability, and use the term *a priori vulnerability* to denote the vulnerability in the absence of investments.

The vulnerability is expected to be lower than the a priori one, as investments are made in cybersecurity. If we indicate the investment by $z \in \mathbb{R}^+$, and the a priori vulnerability as $v \in [0,1]$, the resulting vulnerability is $S(z,v)$, also known as as security breach probability function. Its notation explicitly shows that it is a function of both the a priori vulnerability and the investment. Both the a priori vulnerability and the vulnerability are measured as probabilities. Its range is then defined as $S : \mathbb{R}^+ \times [0,1] \to [0,1]$.

The way we act on the risk here is just through mitigation (see Definition 3.5 of the SRA glossary Aven et al. (2018)). Risk is not canceled but just reduced. No risk avoidance or risk transfer measures are contemplated here. We can envisage several mechanisms to reduce risks. Money can be spent on any of the countermeasures typically adopted to prevent breaches from occurring. For example, data breaches may be reduced by:

- Purchasing antivirus software;
- Installing firewalls inside the network;
- Deploying tighter access control policies;
- Renewing and updating the ICT infrastructures;
- Having employees attend training courses to increase their awareness of cybersecurity risks and develop more cautious behavior.

Coming back to the security breach probability function, it may be more convenient to deal with the normalized breach probability function, since we are mainly interested in how investments reduce the breach probability down from v:

$$S^*(z,v) = \frac{1}{v} S(z,v). \tag{1}$$

2.2. Fundamental Properties

We expect any security breach probability function to possess several essential characteristics. Here, we consider a superset of those established in Gordon and Loeb (2002), which we may include some alternatives. These properties are reported hereafter in full:

$\mathbb{P}1$: $S(z,0) = 0, \forall z \geq 0$;
$\mathbb{P}2$: $S(0,v) = v, \forall v$;
$\mathbb{P}3$: $\lim_{z\to\infty} S(z,v) = 0, \forall v \in (0,1)$
$\mathbb{P}4$: $\frac{\partial S(z,v)}{\partial z} < 0, \forall v \in (0,1)$ and $\forall z > 0$;
$\mathbb{P}5.1$: $\frac{\partial^2 S(z,v)}{\partial z^2} > 0, \forall v \in (0,1)$ and $\forall z$;
$\mathbb{P}5.2$: $\frac{\partial^2 S(z,v)}{\partial z^2} \begin{cases} < 0 & \text{if } z < z_i \\ > 0 & \text{if } z > z_i \end{cases} \quad \forall v \in (0,1)$
$\mathbb{P}5.3$: $\frac{\partial^2 S(z,v)}{\partial z^2} < 0, \forall v \in (0,1)$;
$\mathbb{P}5.4$: $\frac{\partial^2 S(z,v)}{\partial z^2} = 0, \forall v \in (0,1)$ and $\forall z$.

Property $\mathbb{P}1$ concerns the impact of the a priori vulnerability. If the information set is completely invulnerable, it will remain perfectly protected for any information security investment, including a zero investment.

Property $\mathbb{P}2$ concerns the behavior of the system if no investment in security is made. In that case, the vulnerability of the system equals its a priori vulnerability v.

Property $\mathbb{P}3$ states that the probability of a security breach can be made to be arbitrarily close to zero by investing sufficiently in security.

Property $\mathbb{P}4$ embodies the general requirement that information is made more secure as the company invests more in security.

Properties $\mathbb{P}5.x$ all concern the second derivative, i.e., the change in the decay of the breach probability as the company invests more in security. It is to be noted that these properties are alternative to each other.

Under Property $\mathbb{P}5.1$, the vulnerability decreases at a slower rate as the investment grows. This property embodies the law of diminishing returns. If the breach probability follows this property, investing beyond a certain threshold does not pay because the reduction in the expected loss due to the cyberattack is not enough to justify the additional investment.

Property $\mathbb{P}5.2$ again concerns the rate at which the effectiveness of security investments changes. In this case, the breach probability decreases first at a slow rate (when investments are very low) but then gathers momentum and is significantly abated as the investment grows to end up approaching zero slowly when investments get even bigger.

Under Property $\mathbb{P}5.3$, the negative slope of the security breach function becomes even more negative as investments grow. Coupling Property $\mathbb{P}4$ with $\mathbb{P}5.3$, we obtain a concave breach probability function, where investments have larger effectiveness as they grow. Of course, a continuing concavity would bring the breach probability below zero, which would violate probability principles, so that this model is valid up to the value z^* such that $S(z^*, v) = 0$.

Finally, Property $\mathbb{P}5.4$ simply embodies the case of a linear breach probability function.

In the literature, we found nine functions that possess all these properties (i.e., Properties $\mathbb{P}1$ through $\mathbb{P}4$ and one of the $\mathbb{P}5.x$ alternatives):

- Gordon–Loeb Class One;
- Gordon–Loeb Class Two;
- Hausken Class Three;
- Hausken Class Four;
- Hausken Class Five;
- Hausken Class Six;
- The Exponential Power Class;
- The Proportional Hazard Class;
- The Wang Transform Class.

In the following subsection, we describe each of them and analyze their properties. For each model, we roughly follow the same pattern: (a) introducing the mathematical function that describes the model; (b) checking that it possesses the five fundamental properties; (c) identifying the functional formal that relates the breach probability to the a priori vulnerability and investments; and (d) describing the role of parameters.

2.3. Gordon–Loeb Class One Model

The first security breach probability function we examine is the Gordon–Loeb Class One function (GL1 for short), introduced by Gordon and Loeb (2002). It has the following expression

$$S_{GL1}(z, v) = \frac{v}{(\alpha_1 z + 1)^{\alpha_2}} \tag{2}$$

where the parameters $\alpha_1 > 0$ and $\alpha_2 \geq 1$ measure of the productivity of information security.

This function possesses Properties $\mathbb{P}1 - \mathbb{P}4$ and Property $\mathbb{P}5.1$:

$\mathbb{P}1$: $S_{GL1}(z, 0) = \frac{0}{(\alpha_1 z+1)^{\alpha_2}} = 0$;

$\mathbb{P}2$: $S_{GL1}(0, v) = \frac{v}{(\alpha_1 \cdot 0+1)^{\alpha_2}} = v$;

$\mathbb{P}3$: $\lim_{z\to\infty} S_{GL1}(z, v) = \lim_{z\to\infty} \frac{v}{(\alpha_1 z+1)^{\alpha_2}} = 0$;

$\mathbb{P}4$: $\frac{\partial S_{GL1}(z,v)}{\partial z} = -\frac{\alpha_1 \alpha_2 v}{(\alpha_1 z+1)^{\alpha_2+1}} < 0$;

$\mathbb{P}5.1$: $\frac{\partial^2 S_{GL1}(z,v)}{\partial z^2} = \frac{\alpha_1^2 \alpha_2^2 v}{(\alpha_1 z+1)^{\alpha_2+2}} > 0$.

The model is graphed in Figure 1. It depends linearly on the a priori vulnerability. The relationship with investments is a bit more complex since we have a modified (scaled and shifted) power-law functional form.

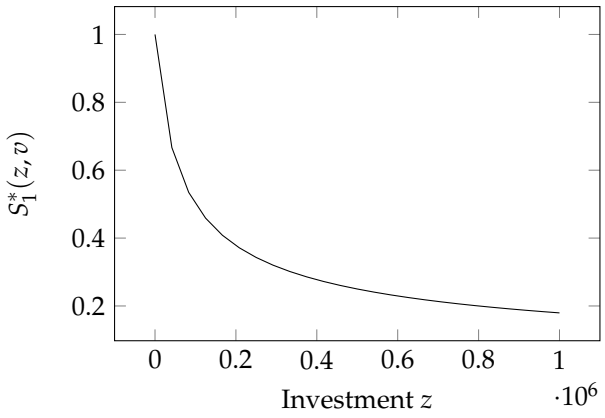

Figure 1. Impact of the investment in security z on the normalized GL1 security breach probability function.

The two parameters α_1 and α_2 modulate the relationship with the investments. Values provided for them in the seminal paper by Gordon and Loeb (2002) are $\alpha_1 = 10^{-5}$ and $\alpha_2 = 1$. It is to be noted that, since α_1 acts as a scaling factor for z, its value also depends on the unit of measurement chosen for the investment (which is dollars in Gordon and Loeb (2002)).

A special form of the GL1 model (namely, when $\alpha_2 = 1$) has been independently derived by Huang and Behara (2013) for the case of targeted attacks on a particular node (one-to-one attacks). The mathematical equivalence of the GL1 model and the model proposed by Huang and Behara has been proven by Naldi et al. (2018). In their paper, Huang and Behara (2013) employ the value $\alpha_1 = 5 \times 10^{-6}$.

This model was used by Mayadunne and Park (2016) to analyze the information security investment through the simplified functional form of the security breach probability function used in Huang and Behara (2013). The GL1 model was also employed by Hua and Bapna (2013) to determine the sensitivity of the investment in security. Then, it was employed by Gao et al. (2015), who extended the GL1 model, combining the latter function with factors that took into account risk and investment correlation among multiples companies. Gordon et al. (2015) used this function to analyze the investment in security considering some target level of cybersecurity. In the same year, Wu et al. (2015) demonstrated, using this model, that the optimal security investment level of an interconnected firm against targeted attacks is different from that against opportunistic attacks and discussed two economic incentives to motivate firms, or rather liability and security information sharing. Recently, this model was used in a risk management framework by Gordon et al. (2020) to derive a cost-effective spending level on cybersecurity activities. A dynamic extension has also been proposed by Krutilla et al. (2021). Mai et al. (2021) employ a simplified version of this model, where $v = 1$ and $\alpha_2 + 1$.

2.4. Gordon–Loeb Class Two Model

The second security breach probability function is again due to Gordon and Loeb. It was introduced along with the GL1 model in their seminal paper (Gordon and Loeb (2002)). Accordingly, we call it the Gordon–Loeb Type Two function (GL2 model for short). Its mathematical expression is

$$S_{GL2}(z, v) = v^{\beta z + 1}, \tag{3}$$

where $\beta > 0$ is a coefficient that measures the effectiveness of security investments: the larger β is, the more effective the investment. The coefficient β roughly plays the same role as α_1 in the GL1 model, i.e., a scaling factor for the investment z. It is, however, the only parameter in the function, while the GL1 model has two.

Unlike the GL1 model, the GL2 model bears a nonlinear relationship with both the investment, and the a priori vulnerability v.

As in the case of the GL1 model, the GL2 model possesses all the properties of $\mathbb{P}1 - \mathbb{P}4$ and $\mathbb{P}5.1$:

$\mathbb{P}1$: $S_{GL2}(z,0) = 0^{\beta z+1} = 0$;
$\mathbb{P}2$: $S_{GL2}(0,v) = v^{0+1} = v$;
$\mathbb{P}3$: $\lim_{z\to\infty} S_{GL2}(z,v) = \lim_{z\to\infty} v^{\beta z+1} = 0$;
$\mathbb{P}4$: $\frac{\partial S_{GL2}(z,v)}{\partial z} = \beta \ln(v) v^{\beta z+1} < 0 \quad \text{since} \quad \ln(v) < 0$;
$\mathbb{P}5.1$: $\frac{\partial^2 S_{GL2}(z,v)}{\partial z^2} = \beta^2 \ln^2(v) v^{\beta z+1} > 0$.

Similarly to the GL1 model, Huang and Behara (2013) derived a model whose mathematical expression is identical to the GL2 model for attacks that propagate epidemically over a scale-free network (opportunistic attacks). Again, the equivalence of the GL2 model and that proposed by Huang and Behara (2013) was proven by Naldi et al. (2018).

The model is graphed in Figure 2.

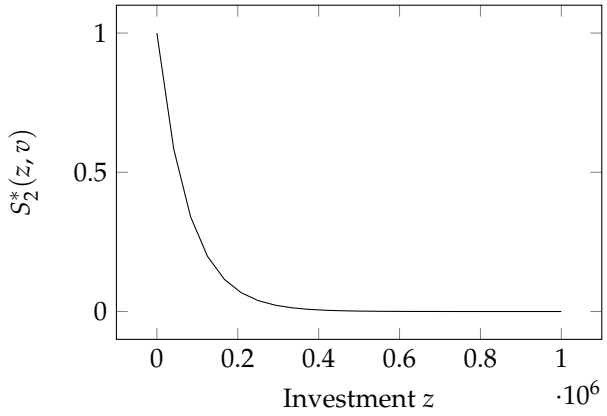

Figure 2. Impact of the investment in security z on the normalized GL2 security breach probability function.

This model was used, e.g., by Gordon et al. (2015); Mayadunne and Park (2016); Mazzoccoli and Naldi (2020b); Rosson et al. (2019); Sawik (2020); Wu et al. (2015); Xu et al. (2019); Young et al. (2016) and Mazzoccoli and Naldi (2021). Young et al. (2016), Rosson et al. (2019), and Mazzoccoli and Naldi (2020b) used this model to evaluate the optimal investment in security together with the presence of insurance coverage against cyber-risks, either through simulation or through closed mathematical formulas. As for the first model, Gordon et al. (2015) use this function to analyze the optimal investment in security for some target level of cybersecurity. Mayadunne and Park (2016), as with the GL1 model, used this function to estimate investment in security by the functional form employed in Huang and Behara (2013). Wang (2019) also adopted this model to describe the impact of investments on vulnerability alone. Sawik (2020) presented a mixed-integer linear programming formulation for the optimization of cybersecurity investment in Industry 4.0 supply chains. He employed this security breach probability function to transform a nonlinear stochastic combinatorial optimization model into its linear equivalent using a recursive linearization procedure. Mazzoccoli and Naldi (2021) extended the structure of the optimization model used in Mazzoccoli and Naldi (2020b) for a single firm, considering a multi-branch firm in which branches have a risk and investment correlation with the headquarters.

2.5. Hausken Class Three Model

Hausken (2006) introduced an alternative breach probability function that replaces one assumption of both GL models, namely the law of diminishing returns embodied by Property $\mathbb{P}5.1$. That assumption is replaced by Property $\mathbb{P}5.2$, where small investments have a very small impact, but vulnerability is greatly lowered when investments reach a critical mass. If investments get even bigger, the law of diminishing returns applies again

in full. The model proposed by Hausken, called by Hausken himself Class Three (hereafter H3 model for short) to follow the numbering initiated by Gordon and Loeb, is

$$S_{H3}(z,v) = \frac{v}{1+\gamma_1(e^{\gamma_2 z}-1)} \tag{4}$$

where $\gamma_1 > 0$ and $\gamma_2 > 0$ are coefficients that measure the productivity of the information security. Again, the coefficient γ_2 is a scaling coefficient for the investment and plays then the same role as α_1 in the GL1 model and β in the GL2 model. The resulting breach probability function follows a logistic decrease, as can be seen in Figure 3.

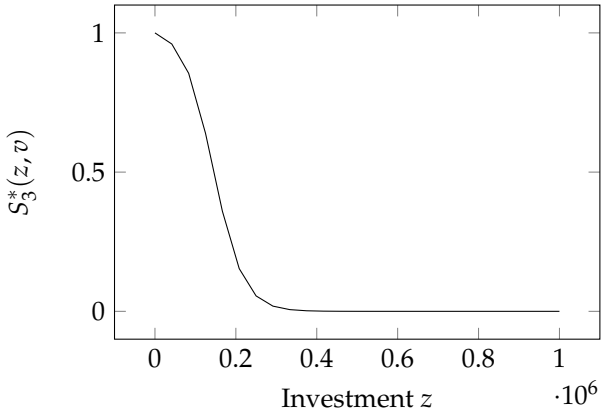

Figure 3. Impact of the investment in security z in the Hausken Class Three model.

This function satisfies Properties $\mathbb{P}1 - \mathbb{P}4$:

$\mathbb{P}1$: $S_{H3}(z,0) = \frac{0}{1+\gamma_1(e^{\gamma_2 z}-1)} = 0$;

$\mathbb{P}2$: $S_{H3}(0,v) = \frac{v}{1+\gamma_1(e^{\gamma_2 0}-1)} = v$;

$\mathbb{P}3$: $\lim_{z\to\infty} S_{H3}(z,v) = \lim_{z\to\infty} \frac{v}{1+\gamma_1(e^{\gamma_2 z}-1)} = 0$;

$\mathbb{P}4$: $\frac{\partial S_{H3}(z,v)}{\partial z} = -\frac{v\gamma_1\gamma_2 e^{\gamma_2 z}}{(1+\gamma_1(e^{\gamma_2 z}-1))^2} < 0$.

As hinted, it also possesses Property $\mathbb{P}5.2$ in place of $\mathbb{P}5.1$. The intermediate investment z_i appearing in Property $\mathbb{P}5.2$ can be found by zeroing the second derivative with respect to the investment z of the security breach probability function:

$$\begin{aligned} &\frac{\partial^2 S_{H3}(z,v)}{\partial z^2} = 0 \\ &-\frac{\gamma_1\gamma_2^2 v e^{\gamma_2 z}(1-\gamma_1 e^{\gamma_2 z}-\gamma_1)}{(1+\gamma_1(e^{\gamma_2 z}-1))^3} = 0 \\ &z_i = \frac{1}{\gamma_2}\ln\left(\frac{1-\gamma_1}{\gamma_1}\right) \end{aligned} \tag{5}$$

This security breach probability function was used by Hua and Bapna (2013) to determine the sensitivity of the optimal investment in security to confront losses caused by cyberterrorists and hackers, similarly to what they did for the GL1 model.

2.6. Hausken Class Four Model

This is again a model proposed by Hausken (2006) and is called Class Four, following the numbering initiated by Gordon and Loeb.

Its mathematical expression is

$$S_{H4}(z,v) = \begin{cases} v(1-\varepsilon z^{\phi}) & \text{if} \quad z \le z_u := \varepsilon^{-\frac{1}{\phi}} \\ 0 & \text{if} \quad z > z_u \end{cases} \tag{6}$$

where $\phi \in (0,1)$ and $\varepsilon > 0$.

The model is graphed in Figure 4. It combines some functional relationships seen in the previous models since it is linear in the a priori vulnerability but exhibits a shifted-and-scaled power-law dependence on the investment. A new feature is, however, the possibility of achieving total invulnerability (i.e., zero breach probability) if the investment is large enough (namely larger than z_u). Hausken himself admitted that such total invulnerability is quite unrealistic, which leads to two conclusions: (a) the threshold z_u must be set at very high values; (b) the interesting part of the model is that where $z < z_u$.

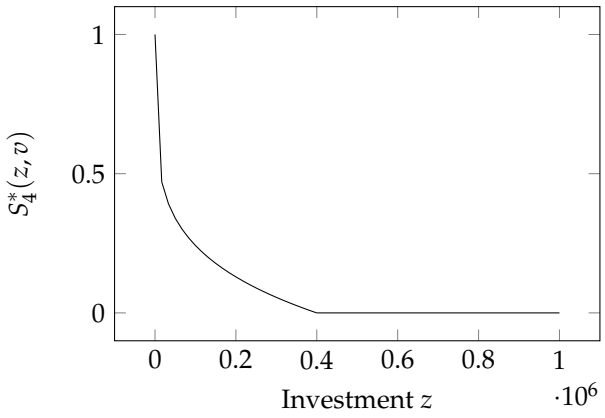

Figure 4. Impact of the investment in security z in Hausken Class Four model.

Keeping in mind condition (b), the properties stated in Section 2.2 must be checked under the hypothesis that $z < z_u$. In that case, we see that the Hausken Class Four model possesses Properties $\mathbb{P}1 - \mathbb{P}4$ and, again, $\mathbb{P}5.1$, as the GL1 and GL2 models:

$\mathbb{P}1$: $S_{H4}(z,0) = 0(1-\varepsilon z^{\phi}) = 0$;
$\mathbb{P}2$: $S_{H4}(0,v) = v(1-\varepsilon 0^{\phi}) = v$;
$\mathbb{P}3$: $\lim_{z\to\infty} S_{H4}(z,v) = S_{H4}(z,v)|_{z>z_u} = 0$;
$\mathbb{P}4$: $\frac{\partial S_{H4}(z,v)}{\partial z} = -\varepsilon\phi v z^{\phi-1} < 0$;
$\mathbb{P}5.1$: $\frac{\partial^2 S_{H4}(z,v)}{\partial z^2} = -\varepsilon\phi(\phi-1)vz^{\phi-2} > 0$.

2.7. Hausken Class Five Model

Here, we again have a model proposed by Hausken (2006). The breach probability appears to have the same mathematical expression as the Hausken Class Four model:

$$S_{H5}(z,v) = \begin{cases} v(1-\omega z^k) & \text{if} \quad z \le z_u := \omega^{-\frac{1}{k}} \\ 0 & \text{if} \quad z > z_u \end{cases} \tag{7}$$

The coefficient ω plays the same role of scaling the contribution of the investment as α_1 in GL1, β in GL2, and γ_2 in H3. In addition, it assumes again (as in the H4 model) that the system can be made invulnerable by investing enough in security. Namely, the threshold beyond which the breach probability is zero is z_u. However, the exponent k now lies in the $k > 1$ range, which has an impact on the sign of the second derivative of the breach probability function.

This function possesses the properties $\mathbb{P}1 - \mathbb{P}4$ plus $\mathbb{P}5.3$:

$\mathbb{P}1$: $S_{H5}(z,0) = 0(1-\omega z^k) = 0$;
$\mathbb{P}2$: $S_{H5}(0,v) = v(1-\omega 0^k) = v$;
$\mathbb{P}3$: $S_{H5}(z,v) = 0$ when $z > z_u$;
$\mathbb{P}4$: : $\frac{\partial S_{H5}(z,v)}{\partial z} = -v\omega k z^{k-1} < 0$;
$\mathbb{P}5.3$: $\frac{\partial^2 S_{H5}(z,v)}{\partial z^2} = -v\omega k(k-1)z^{k-2} < 0$.

Small investments are then relatively ineffective but become increasingly effective as they grow, till reaching the point of complete invulnerability when $z > z_u$, as can be seen in Figure 5.

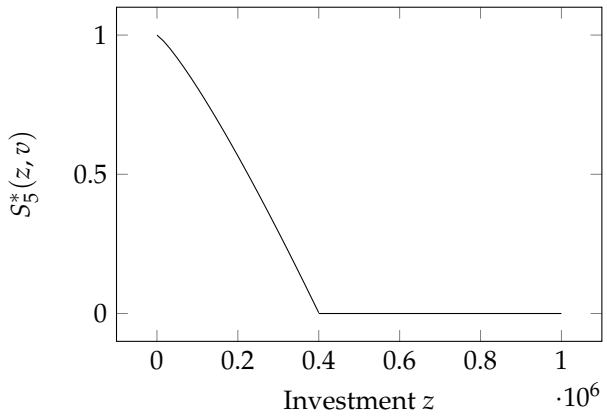

Figure 5. Impact of the investment in security z on Hausken Class Five model.

2.8. Hausken Class Six Model

Here, we have the last of the models proposed by Hausken (2006), which we call hereafter H6 for brevity. The breach probability is a linear function of the investment

$$S_{H6}(z,v) = \begin{cases} v(1-\lambda z) & \text{if} \quad z \leq z_u := 1/\lambda \\ 0 & \text{if} \quad z > z_u \end{cases} \tag{8}$$

This model can be seen as a special case of the H4 model, with the simple name change in the scaling coefficient $\mu = \lambda$, and when we remove the limitation on the exponent k and set it as $k = 1$. The model is graphed in Figure 6.

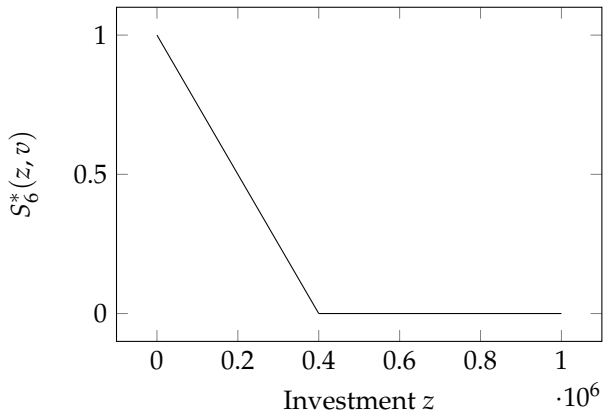

Figure 6. Impact of the investment in security z in Hausken Class Six model.

The H6 model keeps the same assumption as models H4 and H5 that total invulnerability can be achieved if investments are large enough, namely beyond the threshold z_u. As in the previous cases, we are interested in examining the properties of this function when it still exhibits a degree of vulnerability, i.e., when $z < z_u$.

It possesses the following properties:

$\mathbb{P}1$: $S_{H6}(z,0) = 0(1-\lambda z) = 0$;
$\mathbb{P}2$: $S_{H6}(0,v) = v(1-\lambda 0) = v$;
$\mathbb{P}3$: $S_{H6}(z,v) = 0$ when $z > z_u$;
$\mathbb{P}4$: : $\frac{\partial S_{H6}(z,v)}{\partial z} = -\lambda v < 0$;
$\mathbb{P}5.4$: $\frac{\partial^2 S_{H6}(z,v)}{\partial z^2} = 0$.

2.9. The Exponential Power Class Model

This model is one of the three proposed by Wang (2017). Its formulation is a bit different from the models examined so far, since Wang assumes that the system is totally vulnerable if there is no investment in security, i.e., $v = 1$. In addition, Wang considers a benchmark investment B and defines the breach probability as a function of the normalized investment $\hat{z} = z/B$. His breach probability function is then

$$\hat{S}_{\text{EP}}(\hat{z}) = \hat{S}_{\text{EP}}(1)^{\hat{z}^{\eta}}. \tag{9}$$

where $\eta > 0$.

The model is plotted in Figure 7.

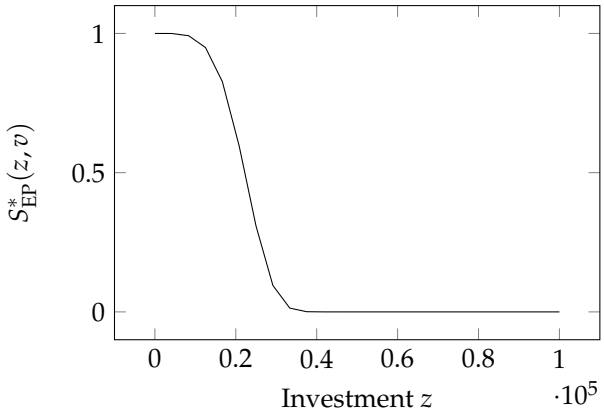

Figure 7. Impact of the investment z on the W1 security breach probability function.

We can safely remove the former assumption to make the model more general. Since removing the assumption that $v = 1$ is akin to removing the normalization concerning the a-priori vulnerability, the breach probability function $S_{\text{EP}}(z, v)$ can be seen as the un-normalized version of the original function proposed by Wang:

$$\begin{aligned} S_{\text{EP}}(z, v) &= v\hat{S}_{\text{EP}}(z/B) = v\hat{S}_{\text{EP}}(1)^{\left(\frac{z}{B}\right)^{\eta}} \\ &= v\zeta^{z^{\eta}}, \end{aligned} \tag{10}$$

where $\zeta = \hat{S}_{\text{EP}}(1)^{\left(\frac{1}{B}\right)^{\eta}}$.

Similarly to the Hausken Class Three model, the Exponential Power Class possesses Properties $\mathbb{P}1 - \mathbb{P}4$ and $\mathbb{P}5.2$

$\mathbb{P}1$: $S_{\text{EP}}(z, 0) = 0 \cdot \zeta^{z^{\eta}} = 0$;

$\mathbb{P}2$: $S_{\text{EP}}(0, v) = v\zeta^0 = v$;

$\mathbb{P}3$: $\lim_{z\to\infty} S_{\text{EP}}(z, v) = \lim_{z\to\infty} v\zeta^{z^{\eta}} = 0$ since $\zeta < 1$;

$\mathbb{P}4$: $\frac{\partial S_{\text{EP}}(z,v)}{\partial z} = \eta v \ln(\zeta) z^{\eta-1}\zeta^{z^{\eta}} < 0$, again since $\zeta < 1$;

$\mathbb{P}5.2$: $\frac{\partial^2 S_{\text{EP}}(z,v)}{\partial z^2} = v\eta\zeta^{z^{\eta}} z^{\eta-2} \ln\zeta[\eta \ln\zeta z^{\eta} + \eta - 1] \gtrless 0$.

As to Property $\mathbb{P}5.2$, we note that the term preceding the square bracket is always negative, since $\zeta < 1$, so that the second derivative is negative if $\eta \ln\zeta z^{\eta} + \eta - 1 > 0$, i.e., if the investment is

$$z < \left(\frac{1-\eta}{\eta \ln\zeta}\right)^{1/\eta} \tag{11}$$

We then have a breach probability function that is concave for low investments and convex (concave upward) for high investments; the marking point between low and high investments being given by Equation (11). This inflection point marks the switch to a lower marginal impact of investments.

The Exponential Power Class function has been employed by Feng et al. (2020) to investigate the competition between two cloud providers trying to sell their cloud security services while optimizing their investments to maximize their profits. Feng et al. (2020) adopted $\hat{S}_{\mathrm{EP}}(1) = 0.5$ and $\eta = 0.5$ as example values for the model parameters.

Wang (2019) derived an optimal mix of cybersecurity investments in *knowledge and expertise* versus *deploying mitigation measures* using this function.

2.10. The Proportional Hazard Class Model

Wang (2017) introduced a second model, which he called the Proportional Hazard class, again adopting normalized investment as the independent variable (with the same benchmark investment B as a normalization parameter). Its form is

$$\hat{S}_{\mathrm{PH}}(\hat{z}) = (1 - (1 - \hat{S}_{\mathrm{PH}}(1))^{\hat{z}^{-\eta}}), \tag{12}$$

the parameter $\eta > 0$ is the same as that appearing in the Exponential Power Class and is invariant to changes in the benchmark investment B. The model is graphed in Figure 8.

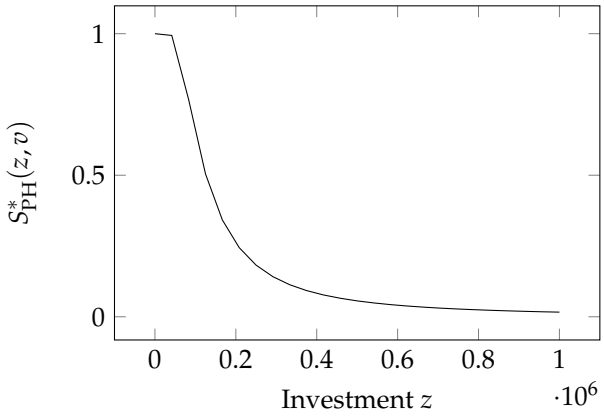

Figure 8. Impact of the investment z on the W2 security breach probability function.

Following the same transformation indicated in the first step of Equation (10), we obtain the breach probability function exponential power class

$$\begin{aligned} S_{\mathrm{PH}}(z,v) &= v\hat{S}_{\mathrm{PH}}(z/B) \\ &= v\left\{1 - \left[1 - \hat{S}_{\mathrm{PH}}(1)\right]^{\left(\frac{z}{B}\right)^{-\eta}}\right\} \\ &= v\left(1 - \xi^{z^{-\eta}}\right) \end{aligned} \tag{13}$$

where $\xi = \left[1 - \hat{S}_{\mathrm{PH}}(1)\right]^{\left(\frac{1}{B}\right)^{-\eta}}$.

The security breach probability function follows properties $\mathbb{P}1 - \mathbb{P}4$ and $\mathbb{P}5.2$, since the domain of this function is $z \neq 0$. The Property $\mathbb{P}2$ must be verified computing the limit in $z = 0$

$\mathbb{P}1:\ S_{\mathrm{PH}}(z,0) = 0 \cdot \left(1 - \xi^{z^{-\eta}}\right) = 0;$

$\mathbb{P}2:\ S_{\mathrm{PH}}(0,v) = \lim_{z\to 0} v\left(1 - \xi^{z^{-\eta}}\right) = v$ since $\xi < 1;$

$\mathbb{P}3:\ \lim_{z\to\infty} S_{\mathrm{PH}}(z,v) = \lim_{z\to\infty} v\left(1 - \xi^{z^{-\eta}}\right) = v \cdot 0 = 0$, again since $\xi < 1;$

$\mathbb{P}4:\ \frac{\partial S_{\mathrm{PH}}(z,v)}{\partial z} = v\eta z^{-\eta-1}\ln(\xi)\xi^{z^{-\eta}} < 0;$

$\mathbb{P}5.2:\ \frac{\partial^2 S_{\mathrm{PH}}(z,v)}{\partial z^2} = v\eta\ln(\xi)[(-\eta-1)z^{-\eta-2}\xi^{z^{-\eta}}$
$- \eta z^{-2\eta-2}\ln(\xi)\xi^{z^{-\eta}}] = -v\eta\ln(\xi)\xi^{z^{-\eta}}z^{-\eta-2}$
$\times [\eta + 1 + \eta z^{-\eta}\ln(\xi)] \gtrless 0.$

The second derivative in Property $\mathbb{P}5.2$ is negative if $\eta + 1 + \eta z^{-\eta} \ln(\xi) > 0$, i.e., if the investment is:

$$z = \left(-\frac{\eta + 1}{\eta \ln(\xi)} \right)^{-1/\eta} \tag{14}$$

It has been employed by Feng et al. (2020).

2.11. The Wang Transform Class

The last security breach probability function we analyze employs the Wang Transform. It was introduced by Wang (2017) and then used in the paper by Feng et al. (2020), WT, and has the form

$$\begin{aligned} S_{\mathrm{WT}}(z, v) &= v\Phi[\Phi^{-1}(\hat{S}_{\mathrm{WT}}(1)) - \eta \ln(z)] \\ &= v\Phi[\Phi^{-1}(\rho) - \eta \ln(z)] \end{aligned} \tag{15}$$

where $\rho = \hat{S}_{\mathrm{WT}}(1)$, $\Phi(*)$ is the cumulative distribution function for the standard normal distribution, and $\eta > 0$ has the same meaning as in the Exponential Power and the Proportional Hazard classes. The model is plotted in Figure 9.

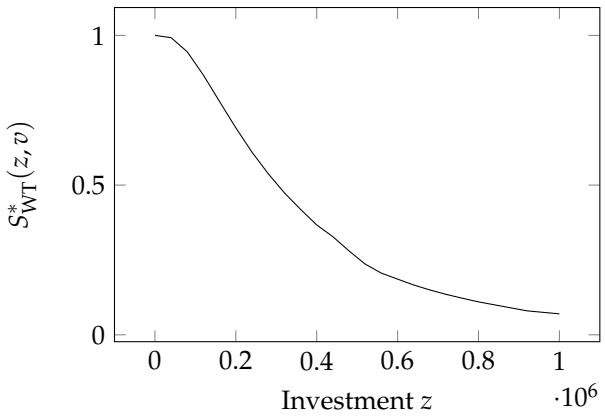

Figure 9. Impact of the investment z on the W3 security breach probability function.

This function possesses the four fundamental properties $\mathbb{P}1 - \mathbb{P}4$ and $\mathbb{P}5.2$

$\mathbb{P}1:$ $S_{\mathrm{WT}}(z, 0) = v\Phi[\Phi^{-1}(\rho) - \eta \ln(z)]$
$0 \cdot \Phi[\Phi^{-1}(\rho) - \eta \ln(z)] = 0;$
$\mathbb{P}2:$ $S_{\mathrm{WT}}(0, v) = \lim_{z \to 0} v\Phi[\Phi^{-1}(\rho) - \eta \ln(z)] = v;$
$\mathbb{P}3:$ $\lim_{z \to \infty} S_{\mathrm{WT}}(z, v) = \lim_{z \to \infty} v\Phi[\Phi^{-1}(\rho) - \eta \ln(z)] = v\Phi(-\infty) = 0;$
$\mathbb{P}4:$ $\frac{\partial S_{\mathrm{WT}}(z,v)}{\partial z} = -\frac{v\eta}{\sqrt{2\pi}z} e^{-\frac{1}{2}[\Phi^{-1}(\rho) - \eta \ln(z)]^2} < 0;$
$\mathbb{P}5.2:$ $\frac{\partial^2 S_{\mathrm{WT}}(z,v)}{\partial z^2} = -\frac{v\eta}{z\sqrt{2\pi}} e^{-\frac{1}{2}[\Phi^{-1}(\rho) - \eta \ln(\rho)]^2}$
$\times \{-1 + \eta[\Phi^{-1}(\rho) - \eta \ln(z)]\} \gtrless 0.$

Additionally, zeroing the second derivative with respect to the investment z of the security probability breach function, the intermediate investment z can be found

$$z = \exp\left\{ \frac{1}{\eta} \left[\Phi^{-1}(\rho) - \frac{1}{\eta} \right] \right\}. \tag{16}$$

This model has been employed by Feng et al. (2020).

3. Sensitivity of the Security Breach Probability Functions

As summarized in Table 1, all the security breach probability models reviewed in Section 2 depend on either a single parameter or two parameters. Though those param-

eters do not change the functional relationship between the breach probability and the investments, their correct determination is essential for the accurate representation of reality. Some effort has been devoted to their correct calibration, e.g., by Naldi and Flamini (2017). Similarly, some effort should be spent on analyzing how their value influences the above relationship, i.e., the sensitivity of the breach probability to those parameters. Any calibration task is unavoidably marred by a degree of incertitude on the correct value of the parameters. Those parameters that bear a greater impact on the breach probability must be determined with greater accuracy. In this section, we analyze the sensitivity of the breach probability functions to their parameters in all the models examined. For that purpose, we employ the quasi-elasticity function. After defining that function, we evaluate it for all the models described in Section 2.

Table 1. Summary of security breach probability models.

Model	Formulation	Num. of Parameters
Gordon and Loeb (GL1)	$\frac{v}{(\alpha_1 z+1)^{\alpha_2}}$	2
Gordon and Loeb (GL2)	$v^{\beta z+1}$	1
Hausken (H3)	$\frac{v}{1+\gamma_1(e^{\gamma_2 z}-1)}$	2
Hausken (H4)	$\begin{cases} v(1-\varepsilon z^{\phi}) \text{ if } z < \varepsilon^{-\frac{1}{\phi}} \\ 0 \text{ if } z > \varepsilon^{-\frac{1}{\phi}} \end{cases}$	2
Hausken (H5)	$\begin{cases} v(1-\omega z^{k}) \text{ if } z < w^{-\frac{1}{k}} \\ 0 \text{ if } z > w^{-\frac{1}{k}} \end{cases}$	2
Hausken (H6)	$\begin{cases} v(1-\lambda z) \text{ if } z < \frac{1}{\lambda} \\ 0 \text{ if } z > \frac{1}{\lambda} \end{cases}$	2
Exponential Power (EP)	$v\hat{S}_{\mathrm{EP}}(1)^{(\frac{z}{B})^{\eta}}$	1
Proportional Hazard (PH)	$v[1-(1-\hat{S}_{\mathrm{PH}}(1))^{(\frac{z}{B})^{-\eta}}]$	1
Wang Transform (WT)	$v\Phi[\Phi^{-1}(\hat{S}_{\mathrm{WT}}(1))-\eta\ln(\frac{z}{B})]$	1

In the following, we use the values reported in Table 2 to plot the quasi-elasticity functions. Unless otherwise stated, we assume $v = 0.65$ and $z = 10^5$.

Table 2. Values of the parameters used.

Class	Parameter	Value
GL1	α_1	2.7×10^{-5}
	α_2	0.5
GL2	β	2.7×10^{-5}
H3	γ_1	0.2
	γ_2	2.7×10^{-5}
H4	ϵ	0.08
	ϕ	0.2
H5	ω	1.89×10^{-7}
	k	1.2
H6	λ	2.5×10^{-6}
EP	η	4.5
PH	η	1.8
WT	η	1.2

3.1. Quasi-Elasticity

The notion of sensitivity in economics has typically been measured through elasticity, i.e., the measure of the percentage change in the response variable when an input variable changes by 1%. The description is well reported in textbooks, such as in Chapter 17 of

Arnold (2008) or Chapter 6 of Krugman and Wells (2009). It has been widely employed in the context of cybersecurity risk to measure the sensitivity of the optimal investment with respect to the two parameters in the GL1 model in Mazzoccoli and Naldi (2020b).

However, here we are concerned with the sensitivity of the breach probability function, which intrinsically lies in the [0,1] range, so it is more appropriate to employ the quasi-elasticity instead, which measures the absolute change in the response variable when the input variable undergoes a relative change. Quasi-elasticity has been employed by Naldi et al. (2019) to measure the trade-off between fairness and profit in project selection.

In our case, we define the quasi-elasticity of the security breach probability function with respect to a generic parameter x of the breach probability function:

$$\varepsilon_x = x\frac{\partial S}{\partial x}. \tag{17}$$

By multiplying the quasi-elasticity by 100, we obtain the change in the security breach probability due to a 1% increase in the breach probability function parameter.

3.2. Gordon–Loeb Class One Model Elasticity

Since the Gordon and Loeb Type One model is governed by two parameters (α_1 and α_2), we compute the quasi-elasticity function according to Equation (17) for both.

The resulting quasi-elasticity for α_1 takes the following form

$$\varepsilon^{\mathrm{GL1}}_{\alpha_1} = \alpha_1\frac{\partial S_{\mathrm{GL1}}}{\partial \alpha_1} = -\frac{\alpha_1\alpha_2 vz}{(\alpha_1 z+1)^{\alpha_2+1}} \tag{18}$$

From this formula, we already see that the quasi-elasticity is always negative: the breach probability decreases when α_1 grows. However, the rate of change depends very much on the other parameter. In Figure 10, we see that α_1 plays an ever more important role as α_2 grows, but it does not alter the breach probability significantly. In that picture, as well as in the following 3D pictures representing quasi-elasticity values, the colour coding describes the level of quasi-elasticity, with red representing regions of insensitivity (quasi-elasticity close to zero) and blue representing the opposite extreme, i.e., regions of high sensitivity.

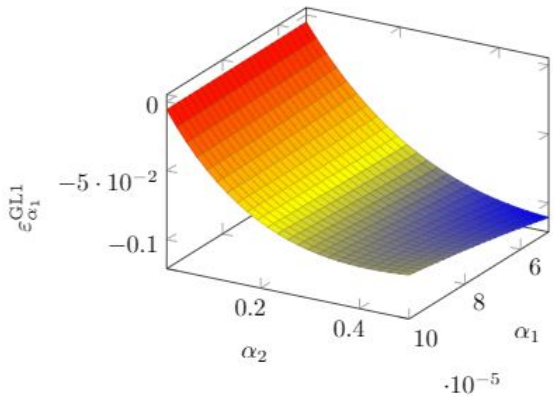

Figure 10. Quasi-elasticity in the GL1 model with respect to α_1.

We now turn to the other parameter (α_2). The quasi-elasticity is

$$\varepsilon^{\mathrm{GL1}}_{\alpha_2} = \alpha_2\frac{\partial S_{\mathrm{GL1}}}{\partial \alpha_2} = -\frac{\alpha_2 v\ln(\alpha_1 z+1)}{(\alpha_1 z+1)^{\alpha_2}} \tag{19}$$

Again, we have a negative quasi-elasticity: the breach probability decreases when α_2 grows. In Figure 11, we also see that the dependence on α_1 is very small.

We can then confirm that the parameter α_2 is by far the most critical between the two, especially at its lowest values.

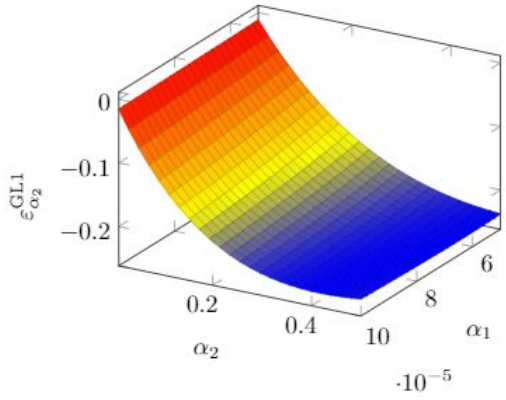

Figure 11. Quasi-elasticity in the GL1 model with respect to α_2.

3.3. Gordon–Loeb Class Two Model Elasticity

In the GL2 model, we have a single parameter (β). If we recall the breach probability function of Equation (3), we can compute the quasi-elasticity

$$\varepsilon^{\mathrm{GL2}}_{\beta} = \beta \frac{\partial S_{\mathrm{GL2}}}{\partial \beta} = \beta z v^{\beta z+1} \ln v, \tag{20}$$

which is always negative. Again, larger parameter values lead to a lower breach probability.

In Figure 12, we see that the elasticity is not monotone and exhibits a negative peak (which, by the sign of the quasi-elasticity, implies the maximum influence), slightly above $\beta = 2 \times 10^{-5}$ in the picture.

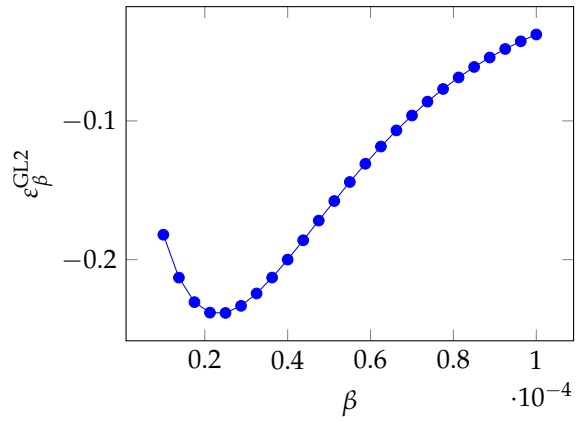

Figure 12. Impact of the effectiveness of security investment β in the GL2 model.

By exploiting the very same breach probability function of Equation (4), we can derive that $\beta z = \ln S / \ln v - 1$ and rewrite the quasi-elasticity as

$$\varepsilon^{\mathrm{GL2}}_{\beta} = (\ln S - \ln v) S. \tag{21}$$

By taking a look at Figure 13, we see that the influence of β reaches a maximum for an intermediate value of the breach probability. Precisely, we have the maximum influence when $\partial \varepsilon^{\mathrm{GL2}}_{\beta} / \partial S = 0$, i.e., when the breach probability is reduced to $S = v/e$. The correct estimation of β is then least critical when the investment is either small or large (which means that the reduction in the breach probability is, respectively, minimal or so large as to be beyond the $1/e$ factor).

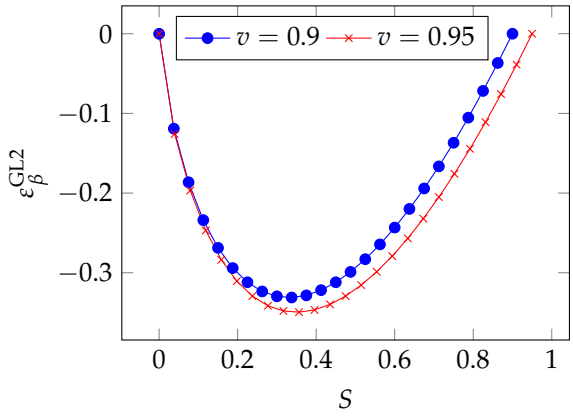

Figure 13. Quasi-elasticity with respect to β in the GL2 model as a function of S.

3.4. Hausken Class Three Model Elasticity

With the Hausken Class Three model, described in Section 2.5, we return to a two-parameter model such as the GL1. The two parameters are here named γ_1 and γ_2. After recalling the definition of Equation (4), we can compute the quasi-elasticity for γ_1, which is

$$\varepsilon_{\gamma_1}^{\mathrm{H3}} = \gamma_1 \frac{\partial S_{\mathrm{H3}}}{\partial \gamma_1} = -\frac{\gamma_1 v(e^{\gamma_2 z} - 1)}{[1 + \gamma_1(e^{\gamma_2 z} - 1)]^2}. \tag{22}$$

The relative relevance of the two parameters follows what we have already seen for the GL1 model. In Figure 14, we see that the sensitivity to γ_1 is quite driven by γ_1 itself and becomes heavier when γ_1 grows.

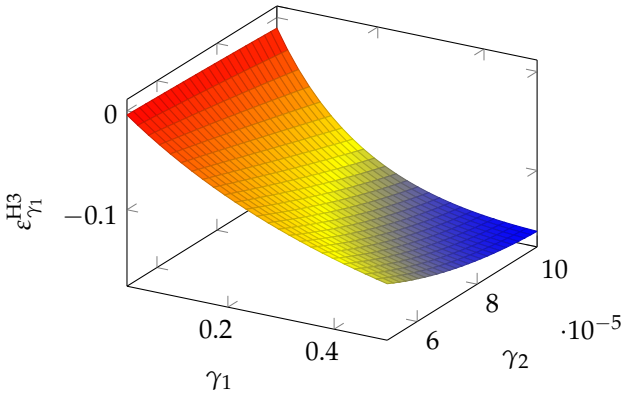

Figure 14. Quasi-elasticity $\varepsilon_{\gamma_1}^{\mathrm{H3}}$.

We can also analyze the regions of greatest sensitivity by rewriting Equation (22) as a function of the breach probability S. After a few algebraic manipulations, we obtain

$$\varepsilon_{\gamma_1}^{\mathrm{H3}} = -S\left(1 - \frac{S}{v}\right), \tag{23}$$

which is plotted in Figure 15 for two values of the a priori vulnerability v. As observed in the Gordon–Loeb model, we see that the peak of sensitivity occurs for intermediate values of the breach probability (between 0.4 and 0.6). We can obtain the precise location of the peak by zeroing the derivative

$$\frac{\partial \varepsilon_{\gamma_1}^{\mathrm{H3}}}{\partial S} = -\left(1 - \frac{S}{v}\right) - S\left(-\frac{1}{v}\right) = -1 + 2\frac{S}{v} = 0, \tag{24}$$

which gives us

$$S = \frac{v}{2} \tag{25}$$

The maximum influence of γ_1 on the breach probability function S is reached when the investments are such as to reduce the vulnerability by half.

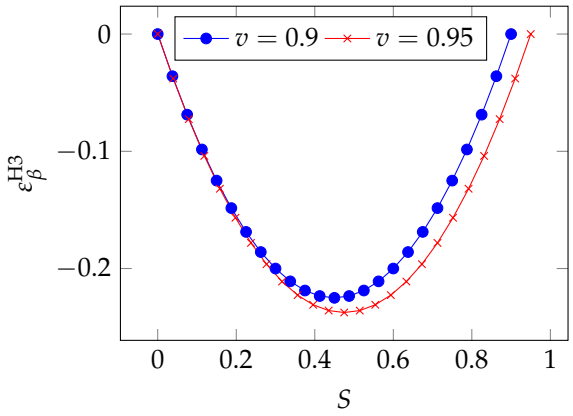

Figure 15. Quasi-elasticity with respect to γ_1 in the H3 model as a function of S.

If we turn to the second parameter, we obtain the quasi-elasticity

$$\varepsilon_{\gamma_2}^{\mathrm{H3}} = \gamma_2 \frac{\partial S_{\mathrm{H3}}}{\partial \gamma_2} = -\frac{\gamma_1 \gamma_2 v z e^{\gamma_2 z}}{(1 + \gamma_1 (e^{\gamma_2 z} - 1))^2}, \tag{26}$$

which is plotted in Figure 16. We see that γ_2 is most influential when both parameters are large.

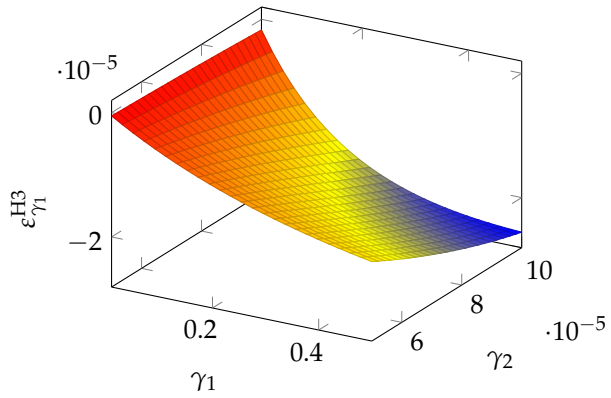

Figure 16. Quasi-elasticity $\varepsilon_{\gamma_2}^{\mathrm{H3}}$.

3.5. Hausken Class Four Model Elasticity

Here, we have another two-parameter model. The parameters are now ϵ, not to be confused with the symbols used for the quasi-elasticity, which is always accompanied by the variable, the model, and ϕ.

By recalling the definition of the breach probability function in Equation (6), we have

$$\varepsilon_{\epsilon}^{\mathrm{H4}} = \epsilon \frac{\partial S_{\mathrm{H4}}}{\partial \epsilon} = \begin{cases} -\epsilon v z^{\phi} & \text{if } z < \epsilon^{-1/\phi} \\ 0 & \text{if } z > \epsilon^{-1/\phi} \end{cases} \tag{27}$$

$$\varepsilon_{\phi}^{\mathrm{H4}} = \phi \frac{\partial S_{\mathrm{H4}}}{\partial \phi} = \begin{cases} -\phi v \epsilon z^{\phi} \ln(z) & \text{if } z < \epsilon^{-1/\phi} \\ 0 & \text{if } z > \epsilon^{-1/\phi} \end{cases} \tag{28}$$

We have a negative quasi-elasticity again for both parameters, excepting the regions where the quasi-elasticity is null because the breach probability function is null itself (actually, the model validity stops when $z > z_u$, since the mathematical expression would lead to a negative breach probability function).

We examine first the sensitivity with respect to ϵ. In Figure 17, we see that the sensitivity to that parameter grows with both parameters in such a way that keeping either parameter very low makes the breach probability function nearly inelastic to ϵ.

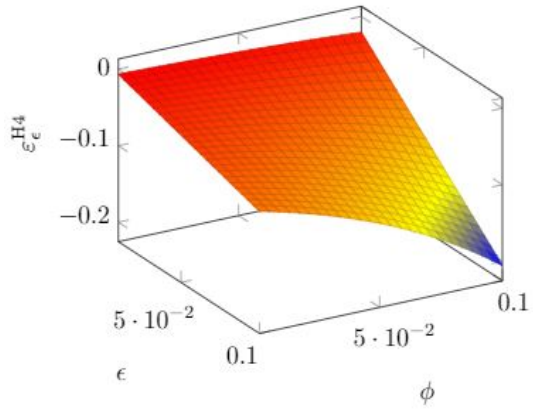

Figure 17. Quasi-elasticity $\varepsilon_\epsilon^{H4}$.

We can also find for which investment range the choice of ϵ may be more critical. If we use the breach probability function definition in Equation (6), we obtain $\epsilon v z^\phi = v - S_{H4}$, so that the quasi-elasticity can be expressed as

$$\varepsilon_\phi^{H4} = -(v - S_{H4}) \qquad z < \epsilon^{-1/\phi} \tag{29}$$

A linear relationship appears, which means that the sensitivity to ϵ is very small when investments are small (so that the reduction in vulnerability is itself small) but gradually grows when investments increase.

If we turn to the effect of ϕ, we see similar behavior in Figure 18: the quasi-elasticity becomes significant when both parameters grow.

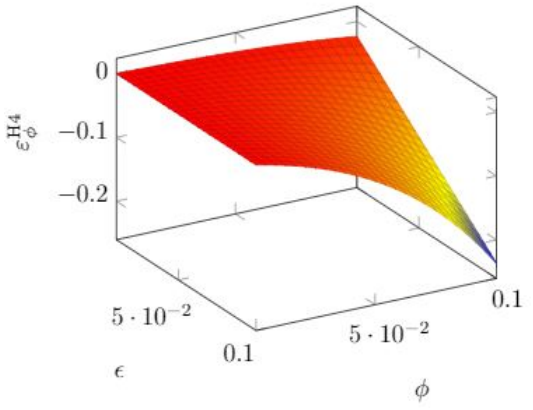

Figure 18. Quasi-elasticity ε_ϕ^{H4}.

3.6. Hausken Class Five Model Elasticity

As shown in Section 3.6, the H5 model has the same mathematical expression as the H4 model, but they differ in the parameter range for k. Hence, we obtain the same expression for the quasi-elasticity. Since the models assume that we can reach complete invulnerability, the limiting value for the investment $z = \omega^{-1/k}$ is due to the mathematical need to avoid negative values for the breach probability. The expressions for the quasi-elasticity are then

$$\varepsilon_{\omega}^{\mathrm{H5}} = \omega \frac{\partial S_{\mathrm{H5}}}{\partial \omega} = \begin{cases} -\omega v z^{k} & \text{if } z < \omega^{-1/k} \\ 0 & \text{if } z > \omega^{-1/k} \end{cases} \tag{30}$$

$$\varepsilon_{k}^{\mathrm{H5}} = k \frac{\partial S_{\mathrm{H5}}}{\partial k} = \begin{cases} -k v \omega z^{k} \ln(z) & \text{if } z < \omega^{-1/k} \\ 0 & \text{if } z > \omega^{-1/k} \end{cases} \tag{31}$$

In Figure 19, we see that the sensitivity to ω grows rapidly when the other parameter k exceeds 1.2 roughly and ω is itself in the higher range ($\omega > 2$ roughly).

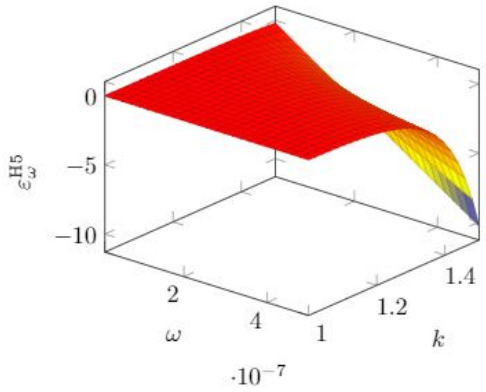

Figure 19. Quasi-elasticity $\varepsilon_{\omega}^{\mathrm{H5}}$.

Quite a similar behavior is observed for the quasi-elasticity with respect to k, as can be observed in Figure 20.

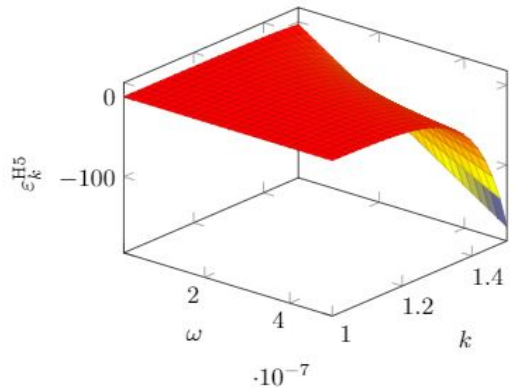

Figure 20. Quasi-elasticity $\varepsilon_{k}^{\mathrm{H5}}$.

Given the identity of the mathematical expressions of the breach probability function of the H4 and H5 models, we can write the quasi-elasticity with respect to ω as

$$\varepsilon_{\omega}^{\mathrm{H5}} = -(v - S_{H5}) \qquad z < \omega^{-1/k}, \tag{32}$$

which shows again a linearly growing sensitivity when the breach probability reduces due to larger investments.

3.7. Hausken Class Six Model Elasticity

We consider here what is probably the simplest breach probability model, described by the linear relationship with a single parameter (λ) shown in Equation (8).

The computation of the quasi-elasticity gives us again a linear function:

$$\varepsilon_{\lambda}^{\mathrm{H6}} = \lambda \frac{\partial S_{\mathrm{H6}}}{\partial \lambda} = \begin{cases} -\lambda v z & \text{if } z < \frac{1}{\lambda} \\ 0 & \text{if } z > \frac{1}{\lambda} \end{cases} \tag{33}$$

The quasi-elasticity function is amenable to be expressed as a function of the breach probability function. After a few simple manipulations, we obtain again, however, a linear function, as we did for the H4 and H5 models:

$$\varepsilon_{\lambda}^{\mathrm{H6}} = -(v - S_{H6}). \tag{34}$$

Hence, the impact of the parameter is stronger when investments are so large as to reduce the breach probability down to low values.

3.8. Exponential Power Class Elasticity

If we write the breach probability function as

$$S = v\gamma^{\left(\frac{z}{B}\right)^{\eta}}, \tag{35}$$

where γ is the breach probability obtained when the investment equals some benchmark value B, we can compute the quasi-elasticity with respect to the exponent η.

After a few algebraic manipulations, we obtain

$$\varepsilon_{\eta}^{\mathrm{EP}} = \eta \frac{\partial S_{\mathrm{EP}}}{\partial \eta} = \eta v \gamma^{\left(\frac{z}{B}\right)^{\eta}} \ln \gamma \left(\frac{z}{B}\right)^{\eta} \ln\left(\frac{z}{B}\right) \tag{36}$$

In Figure 21, we see again the pattern where the sensitivity is higher for intermediate values of investments. If we push investments still further to reduce the breach probability, the influence of η goes down till becoming negligible.

We can also analyze the regions of greatest sensitivity by rewriting Equation (36) as a function of the breach probability S. We first derive the following relationship by taking the logarithm of both sides of Equation (35):

$$\ln S = \ln v + \left(\frac{z}{B}\right)^{\eta} \ln \gamma \rightarrow \left(\frac{z}{B}\right)^{\eta} = \frac{\ln(S/v)}{\ln \gamma} \tag{37}$$

After some algebraic manipulation, we obtain

$$\varepsilon_{\eta}^{\mathrm{EP}} = S \ln\left(\frac{S}{v}\right) \ln\left(\frac{\ln(\frac{S}{v})}{\ln(\zeta)}\right) \tag{38}$$

In Figure 22, we see the same pattern as in the GL2 model, though a significant asymmetry is observed here, with the maximum influence taking place for lower values of the breach probability.

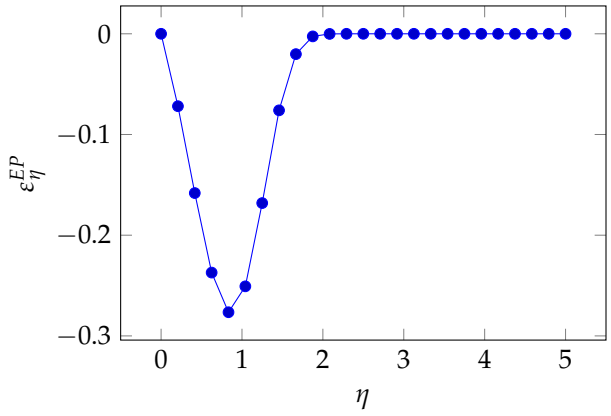

Figure 21. Quasi-elasticity ε_{η}^{EP}.

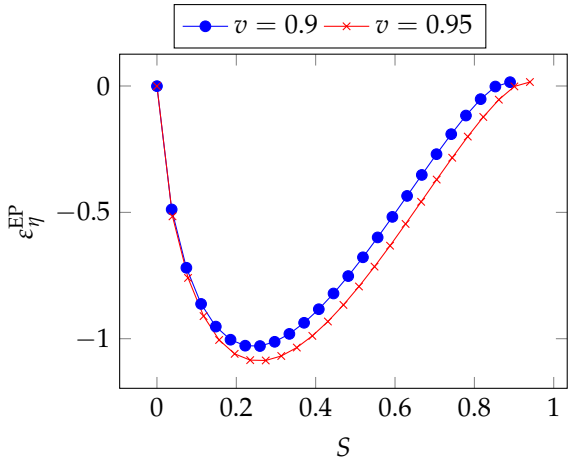

Figure 22. Quasi-elasticity with respect to η as a function of S in the Exponential Power Class model.

3.9. Proportional Hazard Class Elasticity

Here, we have again a two-parameter model, whose breach probability function is reported as Equation (12). First, we obtain the quasi-elasticity with respect to the parameter η as

$$\begin{aligned}\varepsilon_\eta^{\mathrm{PH}} &= \eta \frac{\partial S_{\mathrm{PH}}}{\partial \eta} = \eta v (1-\gamma)^{\left(\frac{z}{B}\right)^{-\eta}} \\ &\times \ln(1-\gamma)\left(\frac{z}{B}\right)^{-\eta} \ln\left(\frac{z}{B}\right) \\ &= -v(1-S/v)\ln(1-S/v)\ln\left(\frac{\ln(1-S/v)}{\ln(1-\gamma)}\right)\end{aligned} \tag{39}$$

The resulting function is plotted in Figure 23, where we observe a pattern similar to that of the Exponential Power Class, i.e., the greatest sensitivity for intermediate values of the parameter η.

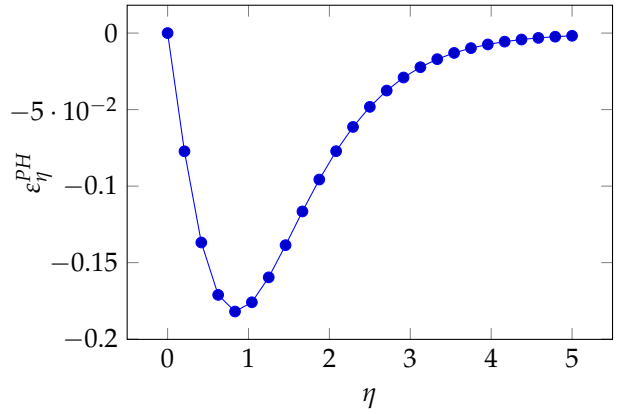

Figure 23. Quasi-elasticity ε_η^{PH}.

If we write the breach probability function in its original form

$$S = v[1-(1-\gamma)^{\left(\frac{z}{B}\right)^{-\eta}}], \tag{40}$$

where γ is the breach probability function when the investment z equals the benchmark value B, we can derive the following relationship, which proves useful to express the quasi-elasticity in a suggestive way:

$$\left(1-\frac{S}{v}\right)=(1-\gamma)^{\left(\frac{z}{B}\right)^{-\eta}}\rightarrow\left(\frac{z}{B}\right)^{-\eta}=\frac{\ln(1-S/v)}{\ln(1-\gamma)} \tag{41}$$

By exploiting this relationship and recalling Equation (39), we obtain

$$\varepsilon_{\eta}^{\mathrm{PH}}=-v(1-S/v)\ln(1-S/v)\ln\left(\frac{\ln(1-S/v)}{\ln(1-\gamma)}\right) \tag{42}$$

In Figure 24, we find the same trend as in the Exponential Class.

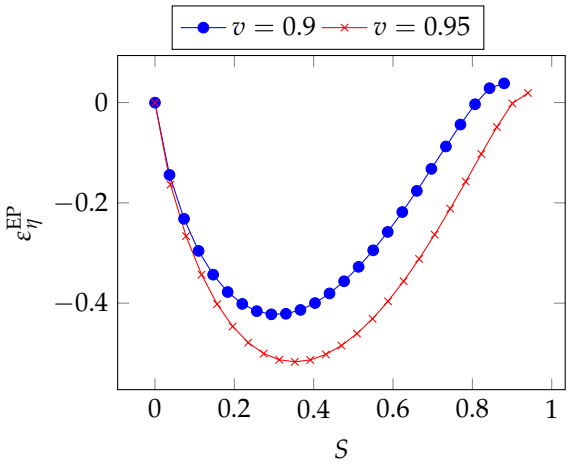

Figure 24. Quasi-elasticity with respect to η as a function of S in the Proportional Hazard Class model.

3.10. Wang Transform Class Elasticity

Finally, we conduct the same analysis for the Wang Transform model, which is a two-parameter model. As in the EP and PH models, however, we focus on η. The pertaining quasi-elasticity is

$$\begin{aligned}\varepsilon_{\eta}^{\mathrm{WT}}&=\eta\frac{\partial S_{\mathrm{WT}}}{\partial\eta}=-\eta\frac{\ln(z)}{\sqrt{2\pi}}\\&\times\exp\left\{-\frac{\Phi^{-1}(\gamma)-\eta\ln(z)}{2}\right\}\end{aligned} \tag{43}$$

We find the same pattern as seen for the EP and the PH model, i.e., a peak of sensitivity followed by a fast retreat to zero sensitivity as η grows, as can be observed in Figure 25.

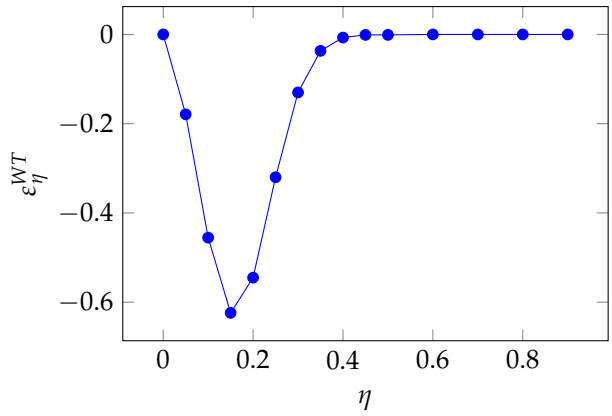

Figure 25. Quasi-elasticity ε_η^{WT}.

If we write the breach probability function as

$$S = v\Phi[\Phi^{-1}(\gamma) - \eta \ln(z)], \tag{44}$$

we find the following relationship:

$$-\eta \ln(z) = \Phi^{-1}(S/v) - \Phi^{-1}(\gamma), \tag{45}$$

which proves useful to express the quasi-elasticity as a function of the breach probability.

$$\varepsilon_\eta^{\mathrm{WT}} = \frac{\Phi^{-1}(S/v) - \Phi^{-1}(\gamma)}{\sqrt{2\pi}} e^{-\frac{1}{2}(\Phi^{-1}(S/v))^2} \tag{46}$$

In Figure 26, we see a trend again similar to what we found in the EP and PH models.

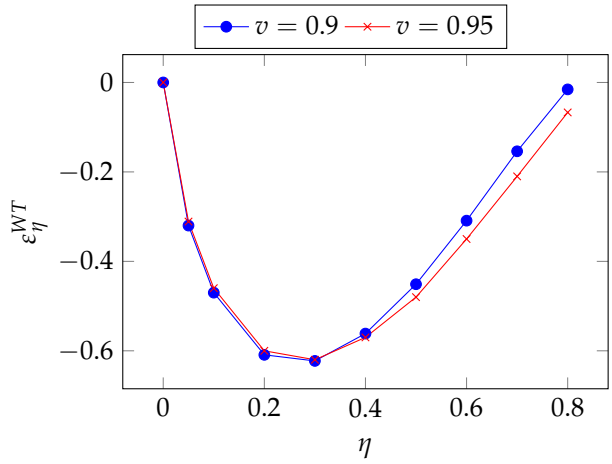

Figure 26. Quasi-elasticity with respect to S as a function of S in the Wang Transform Class.

4. Conclusions

We provided a presumably complete view of the breach probability functions proposed in the literature to model the effect of cybersecurity investments on the actual vulnerability to cyberattacks. The variety of forms taken by these functions allows us to be reasonably confident that they can be used to fit many contexts adequately.

We can take different approaches to compare them and choose what is probably the best for us. In this conclusion, we examine all of them.

First, we can examine the properties they exhibit. In Table 3, we report how the different models comply with the properties we set in Section 2.2. We notice that all models exhibit Properties $\mathbb{P}1$ through $\mathbb{P}4$, i.e., all models assume that investing in security does

always improve the robustness of the system till the point of turning mitigation into a nearly complete shield against attacks. However, they differ in the additional impact that further investments get. We have just one model (H6) assuming that returns on investments are linear: the same additional investment leads to the same vulnerability decrease, regardless of the initial situation. All other models assume that the impact of further investments depends on the starting point. Both the models by Gordon and Loeb and the Hausken Class Four consider diminishing returns, which inevitably leads to a point after which it does not pay to invest more in security. On the other end of the spectrum, we have the Hausken Class 5, which implies a snowball effect: we obtain a more-than-proportional reduction in vulnerability by investing more. In between, all other models (H3, EP, PH, and WT) predict a strong initial reduction in vulnerability, followed by diminishing returns.

A major element to assess the importance of those models is their usage. In the literature, we found applications reported for the GL1, GL2, H3, PH, and WT models. Aside from their proponents, we did not find applications of H4 through H6, or EP models, which have yet to prove their relevance.

An additional way to compare them is to look at the complexity of the model, as embodied by the number of parameters. This is actually a two-sided argument. When the number of parameters grows, we obtain more parameters to estimate, but the model becomes more flexible at the same time. Anyway, in the array of models we examined, the number of parameters is two at most. We have three models that are fully characterized through a single parameter: Gordon–Loeb Class 2, Hausken Class 6, and Wang Transform. All other models have two parameters. In the case of two-parameter models, one is typically more critical than the other, since their influx on the overall breach probability is larger, requiring more attention in their estimation.

Table 3. Comparison of properties.

	GL1	GL2	H3	H4	H5	H6	EP	PH	WT
$\mathbb{P}1$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{P}2$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{P}3$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{P}4$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{P}5.1$	✓	✓		✓					
$\mathbb{P}5.2$			✓				✓	✓	✓
$\mathbb{P}5.3$					✓				
$\mathbb{P}5.4$						✓			

A fundamental limitation of the models presented here is that they are all derived from first principles. A strong trend in risk analysis is the shift to a more data-centric approach Aven and Flage (2020), as underlined by Ale (2016), Choi and Lambert (2017), and Nateghi and Aven (2021). Unfortunately, data are still scarcely available in the cybersecurity world. In addition, the models should be developed using a counterfactual approach, comparing the outcome of the investments in cybersecurity with what would have happened if no investments were carried out. An attempt to calibrate a security breach probability function by relating the investment with the resulting vulnerability has been proposed in Naldi and Flamini (2017).

In addition, all the current models are of the one size fits all kind. They do not differentiate among cybersecurity countermeasures: an investment in a firewall is considered as valuable as an investment of the same amount in antivirus software or one in cybersecurity education. The time has come to progress towards a finer description of the return on security, considering the different possibilities that a cybersecurity officer has.

Though the current models have opened the path to a greater awareness of the economic trade-offs of investing in security, the increase in spending, dictated by the

growth of cyberthreats, calls for more careful investment decisions, which in turn requires more accurate models if they have to become operational tools rather than just indicative.

Author Contributions: Conceptualization, A.M. and M.N.; methodology, A.M. and M.N.; software, A.M.; validation, A.M. and M.N.; formal analysis, A.M. and M.N.; investigation, A.M. and M.N.; resources, M.N.; data curation, A.M.; writing—original draft preparation, A.M. and M.N.; writing—review and editing, A.M. and M.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Note

[1] See the definition provided at https://www.trendmicro.com/vinfo/us/security/definition/data-breach, accessed on 16 November 2022.

References

Ale, Ben. 2016. Risk analysis and big data. In *Safety and Reliability*. London: Taylor & Francis, vol. 36, pp. 153–65.

Antonio, Yeftanus, Sapto Wahyu Indratno, and Suhadi Wido Saputro. 2021. Pricing of cyber insurance premiums using a markov-based dynamic model with clustering structure. *PLoS ONE* 16: e0258867.

Arcuri, Maria Cristina, Marina Brogi, and Gino Gandolfi. 2017. How does cyber crime affect firms? the effect of information security breaches on stock returns. Paper presented at First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy, January 17–20, pp. 175–93.

Arnold, Roger A. 2008. *Economics*, 8th ed. Mason: Thomson South-Western.

Aven, Terje. 2011. *Quantitative Risk Assessment: The Scientific Platform*. Cambridge: Cambridge University Press.

Aven, Terje, and Roger Flage. 2020. Foundational challenges for advancing the field and discipline of risk analysis. *Risk Analysis* 40: 2128–36.

Aven, Terje, Yakov Ben-Haim, H. Boje Andersen, Tony Cox, Enrique López Droguett, Michael Greenberg, Seth Guikema, Wolfgang Kröger, Ortwin Renn, Kimberly M. Thompson, and et al. 2018. *Society for Risk Analysis Glossary*. McLean: Society for Risk Analysis.

Bothos, Ioannis, Vasileios Vlachos, Dimitris M. Kyriazanos, Ioannis Stamatiou, Konstantinos Georgios Thanos, Pantelis Tzamalis, Sotirios Nikoletseas, and Stelios C. A. Thomopoulos. 2021. Modelling cyber-risk in an economic perspective. Paper presented at 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, July 26–28; pp. 372–77.

Chiaradonna, Stefano, and Nicolas Lanchier. 2021. Exact insurance premiums for cyber risk of small and medium-sized enterprises. *arXiv* arXiv:2110.08910.

Choi, Tsan-Ming, and James H. Lambert. 2017. Advances in risk analysis with big data. *Risk Analysis* 37: 1435–42.

Cremer, Frank, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy, and Stefan Materne. 2022. Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance-Issues and Practice* 47: 698–736.

Eling, Martin, and Jan Wirfs. 2019. What are the actual costs of cyber risk events? *European Journal of Operational Research* 272: 1109–19.

Erola, Arnau, Ioannis Agrafiotis, Jason R. C. Nurse, Louise Axon, Michael Goldsmith, and Sadie Creese. 2022. A system to calculate cyber-value-at-risk. *Computers & Security* 113: 102545.

Feng, Shaohan, Zehui Xiong, Dusit Niyato, Ping Wang, Shaun Shuxun Wang, and Xuemin Sherman Shen. 2020. Joint pricing and security investment in cloud security service market with user interdependency. *IEEE Transactions on Services Computing* 15: 1461–72.

Gao, Xing, Weijun Zhong, and Shue Mei. 2015. Security investment and information sharing under an alternative security breach probability function. *Information Systems Frontiers* 17: 423–38.

Georgescu, Tiberiu-Marian. 2021. A study on how the pandemic changed the cybersecurity landscape. *Informatica Economica* 25: 42–60.

Giudici, Paolo, and Emanuela Raffinetti. 2022. Explainable ai methods in cyber risk management. *Quality and Reliability Engineering International* 38: 1318–26.

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

Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2020. Integrating cost–benefit analysis into the nist cybersecurity framework via the gordon–loeb model. *Journal of Cybersecurity* 6: tyaa005.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. 2015. Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity* 1: 3–17.

Hausken, Kjell. 2006. Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers* 8: 338–49.
Hovav, Anat, and John D'Arcy. 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review* 6: 97–121.
Hua, Jian, and Sanjay Bapna. 2013. The economic impact of cyber terrorism. *The Journal of Strategic Information Systems* 22: 175–86.
Huang, C. Derrick, and Ravi S. Behara. 2013. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics* 141: 255–68.
Jerman-Blažič, Borka. 2008. An economic modelling approach to information security risk management. *International Journal of Information Management* 28: 413–22.
Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M. Stulz. 2020. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139: 719–49.
Khalili, Mohammad Mahdi, Parinaz Naghizadeh, and Mingyan Liu. 2018. Designing cyber insurance policies: The role of pre-screening and security interdependence. *IEEE Transactions on Information Forensics and Security* 13: 2226–39.
Krugman, Paul, and Robin Wells. 2009. The rational consumer. *Microeconomics* 269–90.
Krutilla, Kerry, Alexander Alexeev, Eric Jardine, and David Good. 2021. The benefits and costs of cybersecurity risk reduction: A dynamic extension of the gordon and loeb model. *Risk Analysis* 41: 1795–808.
Lin, Zhaoxin, Travis R. A. Sapp, Rahul Parsa, Jackie Rees Ulmer, and Chengxin Cao. 2021. Pricing cyber security insurance. *Journal of Mathematical Finance* 12: 46–70.
Lopez, Olivier, and Maud Thomas. 2022. Parametric Insurance for Extreme Risks: The Challenge to Properly Cover Severe Claims. HAL Preprint no. 03524677. Available online: https://hal.sorbonne-universite.fr/hal-03524677 (accessed on 9 October 2022).
Mai, Van Sy, Richard J. La, and Abdella Battou. 2021. Optimal cybersecurity investments in large networks using sis model: Algorithm design. *IEEE/ACM Transactions on Networking* 29: 2453–66.
Maillart, Thomas, and Didier Sornette. 2010. Heavy-tailed distribution of cyber-risks. *The European Physical Journal B* 75: 357–64.
Marotta, Angelica, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. 2017. Cyber-insurance survey. *Computer Science Review* 24: 35–61.
Mastroeni, Loretta, Alessandro Mazzoccoli, and Maurizio Naldi. 2019. Service level agreement violations in cloud storage: Insurance and compensation sustainability. *Future Internet* 11: 142.
Mayadunne, Sanjaya, and Sungjune Park. 2016. An economic model to evaluate information security investment of risk-taking small and medium enterprises. *International Journal of Production Economics* 182: 519–30.
Mazzoccoli, Alessandro, and Maurizio Naldi. 2020a. The expected utility insurance premium principle with fourth-order statistics: Does it make a difference? *Algorithms* 13: 116.
Mazzoccoli, Alessandro, and Maurizio Naldi. 2020b. Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. *Risk Analysis* 30: 550–64.
Mazzoccoli, Alessandro, and Maurizio Naldi. 2021. Optimal investment in cyber-security under cyber insurance for a multi-branch firm. *Risks* 9: 24.
McShane, Michael, Martin Eling, and Trung Nguyen. 2021. Cyber risk management: History and future research directions. *Risk Management and Insurance Review* 24: 93–125.
Mukhopadhyay, Arunabha, Samir Chatterjee, Kallol K. Bagchi, Peteer J. Kirs, and Girja K. Shukla. 2019. Cyber risk assessment and mitigation (cram) framework using logit and probit models for cyber insurance. *Information Systems Frontiers* 21: 997–1018.
Murphy, Diane R., and Richard H. Murphy. 2013. Teaching cybersecurity: Protecting the business environment. Paper presented at 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, Kennesaw, GA, USA, October 12; pp. 88–93.
Naldi, Maurizio, and Alessandro Mazzoccoli. 2018. Computation of the insurance premium for cloud services based on fourth-order statistics. *International Journal of Simulation: Systems, Science and Technology* 19: 1–6.
Naldi, Maurizio, and Marta Flamini. 2017. Calibration of the Gordon-Loeb Models for the Probability of Security Breaches. Paper presented at 2017 UKSim-AMSS 19th International Conference on Computer Modelling & Simulation (UKSim), Cambridge, UK, April 5–7; pp. 135–40.
Naldi, Maurizio, Gaia Nicosia, Andrea Pacifici, and Ulrich Pferschy. 2019. Profit-fairness trade-off in project selection. *Socio-Economic Planning Sciences* 67: 133–46.
Naldi, Maurizio, Marta Flamini, and Giuseppe D'Acquisto. 2018. Negligence and sanctions in information security investments in a cloud environment. *Electronic Markets* 28: 39–52.
Nateghi, Roshanak, and Terje Aven. 2021. Risk analysis in the age of big data: The promises and pitfalls. *Risk Analysis* 41: 1751–58.
Orlando, Albina. 2021. Cyber risk quantification: Investigating the role of cyber value at risk. *Risks* 9: 184.
Palsson, Kjartan, Steinn Gudmundsson, and Sachin Shetty. 2020. Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance-Issues and Practice* 45: 564–79.
Paté-Cornell, M-Elisabeth, Marshall Kuypers, Matthew Smith, and Philip Keller. 2018. Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis* 38: 226–41.
Poufinas, Thomas, and Nikolaos Vordonis. 2018. Pricing the cost of cybercrime—A financial protection approach. *iBusiness* 10: 128.
Refsdal, Atle, Bjørnar Solhaug, and Ketil Stølen. 2015. Cyber-risk management. In *Cyber-Risk Management*. New York: Springer, pp. 33–47.

Rodrigues, Bruno, Muriel Franco, Geetha Parangi, and Burkhard Stiller. 2019. Seconomy: A framework for the economic assessment of cybersecurity. In *International Conference on the Economics of Grids, Clouds, Systems, and Services*. New York: Springer, pp. 154–66.
Rosson, Jack, Mason Rice, Juan Lopez, and David Fass. 2019. Incentivizing cyber security investment in the power sector using an extended cyber insurance framework. *Homeland Security Affairs* 15: 1–25.
Sangari, Seema, and Dr Dallal. 2022. Correcting for reporting delays in cyber incidents. *arXiv* arXiv:2201.10348.
Sawik, Tadeusz. 2020. A linear model for optimal cybersecurity investment in industry 4.0 supply chains. *International Journal of Production Research* 60: 1–18.
Scala, Natalie M., Allison C. Reilly, Paul L. Goethals, and Michel Cukier. 2019. Risk and the five hard problems of cybersecurity. *Risk Analysis* 39: 2119–26.
Skeoch, Henry R. K. 2022. Expanding the gordon-loeb model to cyber-insurance. *Computers & Security* 112: 102533.
Strupczewski, Grzegorz. 2018. Current state of the cyber insurance market. In *Proceedings of the 10th Economics and Finance Conference*. Number 6910062. Rome: International Institute of Social and Economic Sciences.
The Ponemon Institute. 2016. *2016 Cost of Data Breach Study: Global Analysis*. Technical Report. Traverse City: The Ponemon Institute.
Uuganbayar, Ganbayar, Artsiom Yautsiukhin, Fabio Martinelli, and Fabio Massacci. 2021. Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security* 101: 102121.
Vakilinia, Iman, and Shamik Sengupta. 2018. A coalitional cyber-insurance framework for a common platform. *IEEE Transactions on Information Forensics and Security* 14: 1526–38.
Verizon Risk Team. 2022. *2022 Data Breach Investigations Report*. Technical Report. New York: Verizon.
Wang, Shaun. 2017. Optimal Level and Allocation of Cybersecurity Spending: Model and Formula. SSRN Preprint no. 3010029. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3010029 (accessed on 16 November 2022).
Wang, Shaun S. 2019. Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal* 57: 101173.
Wheatley, Spencer, Thomas Maillart, and Didier Sornette. 2016. The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B* 89: 1–12.
Woods, Daniel W., Tyler Moore, and Andrew C. Simpson. 2021. The county fair cyber loss distribution: Drawing inferences from insurance prices. *Digital Threats: Research and Practice* 2: 1–21.
World Economic Forum. 2015. *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats*. Technical Report. Davos: World Economic Forum.
Wu, Yong, Gengzhong Feng, Nengmin Wang, and Huigang Liang. 2015. Game of information security investment: Impact of attack types and network vulnerability. *Expert Systems with Applications* 42: 6132–46.
Xu, Lu, Yanhui Li, and Jing Fu. 2019. Cybersecurity investment allocation for a multi-branch firm: Modeling and optimization. *Mathematics* 7: 587.
Xu, Maochao, and Lei Hua. 2019. Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal* 23: 220–49.
Xu, Maochao, Kristin M. Schweitzer, Raymond M. Bateman, and Shouhuai Xu. 2018. Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security* 13: 2856–71.
Yaakov, Yoav Ben, Xinrun Wang, Joachim Meyer, and Bo An. 2019. Choosing protection: User investments in security measures for cyber risk management. In *International Conference on Decision and Game Theory for Security*. New York: Springer, pp. 33–44.
Yamada, Michihiro, Hiroaki Kikuchi, Naoki Matsuyama, and Koji Inui. 2019. Mathematical model to estimate loss by cyber incident in japan. Paper presented at ICISSP 2019, Prague, Czech Republic, February 23–25; pp. 353–60.
Yeboah-Ofori, Abel, Shareeful Islam, Sin Wee Lee, Zia Ush Shamszaman, Khan Muhammad, Meteb Altaf, and Mabrook S. Al-Rakhami. 2021. Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access* 9: 94318–37.
Young, Derek, Juan Lopez, Mason Rice, Benjamin Ramsey, and Robert McTasney. 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection* 14: 43–57.