Journal of Information Security, 2016, 7, 81-102
Published Online March 2016 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2016.72006

Scientific Research Publishing

The "Iterated Weakest Link" Model of Adaptive Security Investment

Rainer Böhme[1], Tyler Moore[2]

[1]Department of Computer Science, Universität Innsbruck, Innsbruck, Austria
[2]Tandy School of Computer Science, University of Tulsa, Oklahoma, USA
Email: rainer.boehme@uibk.ac.at, tyler-moore@utulsa.edu

Received 24 February 2016; accepted 28 March 2016; published 31 March 2016

Abstract

We devise a model for security investment that reflects dynamic interaction between a defender, who faces uncertainty, and an attacker, who repeatedly targets the weakest link. Using the model, we derive and compare optimal security investment over multiple periods, exploring the delicate balance between proactive and reactive security investment. We show how the best strategy depends on the defender's knowledge about prospective attacks and the recoverability of costs when upgrading defenses reactively. Our model explains why security under-investment is sometimes rational even when effective defenses are available and can be deployed independently of other parties' choices. Finally, we connect the model to real-world security problems by examining two case studies where empirical data are available: computers compromised for use in online crime and payment card security.

Keywords

Optimal Security Investment under Uncertainty, Return on Security Investment

1. Security Investment in an Uncertain World

We hear about security breaches in the news almost daily, each bigger and more costly than the last. Does this reflect flawed technology, policy, or simply ineptitude? What if, instead, allowing some attacks to succeed is entirely rational for businesses? Rather than over-invest proactively, firms could wait to observe which attacks work and use this knowledge to better allocate security spending. In this article, we describe a model that weighs the merits of such an approach.

One key insight from the economics of information security literature is that attackers bent on undermining a system's security operate *strategically* [1]. Moreover, information systems are often structured so that a

system's overall security depends on its *weakest link* [2]. A careless programmer in a software firm can introduce a critical vulnerability. The Internet's global, distributed architecture leads to security being dominated by the weakest link—attackers compromise machines hosted at Internet service providers (ISPs) with lax enforcement policies or located in uncooperative countries. Attackers have repeatedly exhibited a knack for identifying the easiest way to bypass a system's security, even when the system's designer remains unaware of the particular weakness.

However, systems do not exist in a vacuum; rather, defenders respond to attacks by plugging known holes. And yet, as soon as one weakest link is fixed, another weak point is often identified and exploited. Therefore, a strong dynamic component is at play: attackers find the weakest link; defenders fix the problem; attackers find new holes which are then plugged, and so on. We see that this pattern emerges repeatedly. For instance, attackers construct networks of compromised machines (so-called botnets) to pester legitimate users by emitting spam, distributing malware and hosting phishing websites. Attackers concentrate their efforts at the most irresponsible ISPs, moving on to others only after the ISP cleans up its act or is shut down. Likewise, technical countermeasures to payment card fraud have evolved over time, causing fraudsters to adopt new strategies as old weaknesses are fixed. For example, when UK banks migrated to PIN verification of transactions rather than signatures, in-person retail fraud declined while overseas ATM fraud and card-not-present fraud skyrocketed.

In this article, we devise a model that reflects this dynamic interaction between attackers and defenders. Our model captures the *iterative* aspect of attack and defense; we exclusively study the case where security depends on the *weakest link*; consequently, we model the *iterated weakest link*.

Plugging known holes come at a cost for the defender. And as often experienced in real systems, this cost is not always proportional to the number of controls in place. For example, organization science suggests that complexity adds super-linear administrative costs, for instance to pay a manager who directs several employees where each is an expert for a particular control. Conflicting defenses also emerge from incompatible systems, e.g., running two virus scanners on the same machine to increase coverage slows down the machine and causes errors. Lastly, human behavior fundamentally limits the composability of defenses: a password policy that requires both special characters (defense 1) and frequent password changes (defense 2) encourages people to stick their password on their monitor. Our model can account for *interdependent* defensive countermeasures.

Practical security engineers will note that it is already difficult to obtain detailed information on cost structures, but what is even more unrealistic is attempts to determine the attackers' cost and plug them into decision tables. In the real world, defenders almost always operate with incomplete information, and oftentimes a rough gauge on the relative magnitude of known threats is all the information available to a decision maker.

So another key characteristic of our model is to reflect *uncertainty* about which components are weakest, and therefore, which components are most susceptible to attack. All chief information security officers (CISOs) know that the security of their computer systems is imperfect at best; the better ones have catalogued the many ways an attacker might penetrate their systems, mitigating risks where possible and accepting the rest. What they remain uncertain about is which, if any, of the vulnerable components an attacker will choose to exploit. We capture this uncertainty into our model and use it to analyze how defense strategies change as knowledge about the attacker varies.

We reach several interesting conclusions upon examining the model. By comparing the static case (a single round of attack and defense) to the dynamic one (multiple rounds), we find that different defender strategies may prevail. When the defender only gets one chance to protect a system, increasing uncertainty about which link is weakest causes the defender to protect more assets, but only up to a point. When uncertainty is too high, the defender does not know which asset to protect and so chooses to protect none. If instead we allow for repeated defensive investments, an uncertain defender will initially protect fewer assets and wait for the attacker to "identify" the weakest links to be fixed in later rounds. Hence, it can be quite rational to *under-invest* in security until threats are realized. Unlike in other theories, this type of under-investment is not driven by the interrelation with other market participants and resulting incentive systems. Of course, security countermeasures may require significant capital investment from the outset. When we consider unrecoverable costs in our model, we find that for moderate levels of uncertainty, high unrecoverable update costs can raise the proactive protection investment.

We then translate these findings about optimal defensive strategies into accepted security indicators such as annual loss expectancy (ALE) and return on security investment (ROSI). Return on investment drops as uncertainty about known attacks rises, even as the defender grows increasingly reactive when countering realized threats.

We *do not* deal with the problem of distributing costs if the defender is in fact a coalition of multiple parties (such as in the case of protecting global infrastructure) and the resulting incentive systems, which we regard as a separate problem to be studied independently. We refer the reader to the literature on externalities, such as [2]-[4].

The remainder of this article is organized as follows: Section 2 specifies the model, which is solved later on in Section 3. We apply the model to real problems in two case studies on current topics of information security, namely online crime (Section 5.1) and payment card security (Section 5.2). Section 6 puts our contribution into perspective with prior art, and Section 7 concludes the article.

Readers who want to glance over the article without getting into the formal details may find the model summary in Section 2.6 along with the interpretation of example results in Section 4 most useful. Also the case studies (Section 5) and the general conclusion (Section 7) do not require deep understanding of the model. A non-technical summary of the model's key ideas has also appeared in a magazine format [5].

2. Model

Imagine a simplistic world, in which a *defender* protects an *asset* of value *a* against a dispersed set of possibly heterogeneous *attackers*. There exist *n* possible *threats*, which can be regarded as distinct attack vectors against a single system.[1] Each threat can be warded off by investing in its corresponding *defense* (or control). In other words, we assume a one-to-one mapping between threats and defenses, and defenses are always effective.

2.1. Defender's Options

The model is "run" in an iterated player-versus-nature game with discrete time $t = (1, \cdots, t_{\max})$. In each round, the defender makes a security investment decision to define his *configuration* of defenses $\boldsymbol{d}_t$ and extracts a net return $r \cdot a$ from his asset before the attacker penetrates the system and, if successful, loots a fraction *z* of the asset. Gross returns are consumed or distributed so that the asset value does not accumulate over time. The defender seeks to maximize his expected return per round, where expectations are taken over the realizations of random variables and averages calculated over time.

Let elements d_i of the binary column vector $\boldsymbol{d} \in \{0,1\}^n$ indicate whether a defense against the *i*-th threat is implemented ($d_i = 1$) or not $(d_i = 0)$, and let $k = \sum_{i=1}^{n} d_i$ be the number of defenses in place.

The cost of defense c_t in round *t* can be calculated from an $n \times n$ upper triangular cost matrix $\boldsymbol{C}$ to reflect possible interdependent defenses,

$$c_t = \boldsymbol{d}_t \boldsymbol{C} \boldsymbol{d}_t \,. \tag{1}$$

Diagonal elements $C_{i,i}$ hold the cost to implement a defense against the *i*-th threat, and off-diagonal elements $C_{i,j}, j > i$ indicate the extra costs if the *i*-th defense is implemented together with the *j*-th defense. If all off-diagonal elements are zero, then the defenses are independent:[2]

$$\boldsymbol{C} = \begin{bmatrix} 1 & 0 & & 0 \\ 0 & 1 & & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & 1 \end{bmatrix}$$

(a) independent defenses

$$\boldsymbol{C} = \begin{bmatrix} 1 & 0 & 12 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -12 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

(b) conflicting defenses: 1 and 3
complementary defenses: 3 and 4

A nice property of the cost matrix is that for positive off-diagonal elements, decreasing marginal utility of defenses has become endogenous to our model. This compares favorably to, say, the Gordon-Loeb framework, in which this property appears as an assumption (A3 of [6], p. 443).

2.2. Defender's Knowledge

While the defender may possess some intuition about the relative difficulty of carrying out the *n* threats, such

[1] An alternative interpretation is that threats represent distinct targets in a distributed system that together form asset *a*.

[2] We do not consider higher-order interdependence such as extra costs if three or more defenses are involved.

knowledge may very well be blurred. To model this uncertainty, we order the threats $1,\cdots,n$ by *increasing expected cost of attack*, where the expectation is taken from the point of view of the defender. This constitutes our notion of an *attack profile*. This rank order is also convenient because it allows us to ignore the threats deemed too unlikely when deciding what to defend. This way, one can think of the n threats as those anticipated by the defender.

We define a simple functional form for the expected attack costs $\overline{x}_i$ of the i-th threat as follows,

$$\overline{x}_i = \overline{x}_1 + (i-1)\cdot\Delta x, \text{ with } \Delta x > 0\,. \tag{2}$$

The unknown true cost x_i, however, is modeled as a Gaussian random variable with mean $\overline{x}_i$ and standard deviation $\sigma/\Delta x$ (truncated to values $x_i \geq 0$),

$$x_i = \sup(0, \chi_i) \text{ with } \chi_i \sim \mathcal{N}(\overline{x}_i, \sigma/\Delta x). \tag{3}$$

The realizations χ_i are drawn only once and kept constant over time. We can vary the level of uncertainty by adjusting parameter σ. Modeling uncertainty in this way is crucial to the model, since it captures the difficulty defenders face in anticipating which of the undefended threats turns out to be the weakest link exploited by the attacker. **Figure 1** illustrates the role of uncertainty when ordering threats. The left graph plots a perfect matching between expected and realized costs of attack under certainty; under uncertainty, by contrast, the right graph shows that threat 4, not threat 3 as expected, is the weakest link if defenses 1 and 2 are in place.

The defender's knowledge about the attack profile will naturally increase over time once attacks occur, and so her uncertainty decreases as the observed attacks reveal which threat is in fact the weakest link with respect to a given configuration $\boldsymbol{d}_t$.

2.3. Unrecoverable Costs

So far we have assumed that the defender can upgrade his configuration $\boldsymbol{d}_t$ at any time. This may be necessary in order to adjust to new information on the threat level or to changing risk appetite. For example, a start-up company is exposed to so many risks that is might tolerate a moderate level of information security risk. As the venture grows and develops a brand name, its risk aversion will increase to reflect the higher damage caused by potential reputation losses. Conversely, market competition (alongside herd behavior and short-sighted incentives to management) may drive firms to decrease their risk aversion for the sake of higher expected profits.

As is argued in [6], security disinvestment is often possible to a certain degree, since personnel can be fired or equipment sold (though sometimes at high transaction costs). However, for many businesses, updating $\boldsymbol{d}_t$ may be very expensive and the costs are spent irrevocably. For instance, the vast majority of the cost to incorporate new security features into bank notes or payment cards are borne when the changes are first made. Producing and distributing tailored tokens or devices to a large and dispersed community is expensive, and unlikely to be repeated often. As unrecoverable costs considerably affect the strategy of security investment in an iterated setting, we include them in our model as follows:

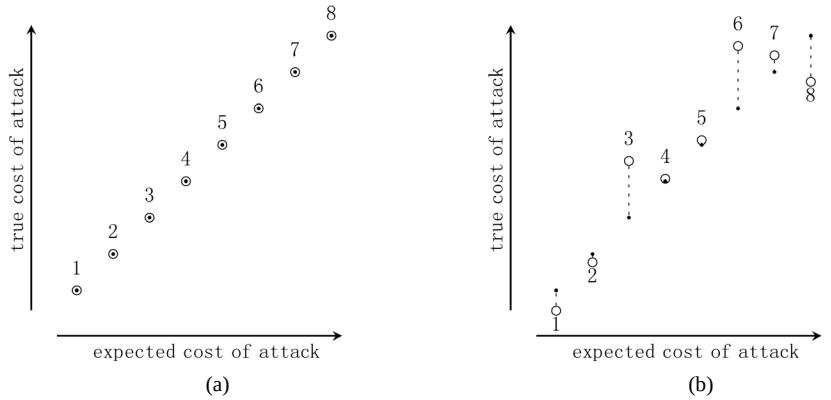

Figure 1. Attack profile. The defender forms expectations about the rank order of attack costs, but does not know the true costs until attacks are actually observed. (a) [certainty: $\sigma = 0$]; (b) [uncertainty: $\sigma = 1$].

$$s_t = \begin{cases} 0 & \text{if } t = 1 \text{ or } \boldsymbol{d}_t = \boldsymbol{d}_{t-1} \\ \lambda \cdot a & \text{else.} \end{cases} \tag{4}$$

Hence, parameter $\lambda \geq 0$ controls the amount of unrecoverable costs, on an *ex post* basis sometimes referred to as *sunk* costs.

2.4. Attacker's Options and Knowledge

Our attacker model is very simple: the attacker identifies and exploits the weakest link, *i.e.*, the threat least costly to the attacker. We do not require the attacker to make a trade-off between cost and potential gains by assuming the same utility is received for exploiting all threats. If the attacker succeeds, regardless of how, he profits $z \cdot a$, which is added to the defender's cost. Unlike the defender, the attacker is certain of the cost for each realization of x_i. The attacker does not operate indiscriminately; rather, he only attacks when it is profitable to do so; that is, if the term $\max_i(z \cdot a - x_i)$ is not negative.

These attacker assumptions are quite strong and probably unrealistic in some cases. For targeted attackers in particular, searching for the weakest link could be very expensive. So a more appropriate conception is the presence of many *opportunistic attackers* [7] who operate independently. Like in swarm intelligence, the chance that one of them finds the hole is quite high.

Moreover, the attacker's gain from successful attacks may only represent a small fraction of the defender's losses. But this is not crucial here since we do not consider attackers' profits; we simply need an asset-dependent quantity to relate to the cost x_i. A level shift of x_i could easily account for the negative balance (destruction of wealth) after successful attacks. This assumption is also common in the literature (e.g., [8]), and justified there by attackers who mainly care about inflicting harm on the defender. In summary, we consider it prudent to err in the direction of a more powerful attacker than an unrealistically weak one.

2.5. Simplifying Assumptions

To make the analysis more tractable, we restrict the space of possible cost matrices $\boldsymbol{C}$ by fixing all diagonal elements $C_{i,i}$ to a unit cost of value one and all off-diagonal elements $C_{i,j}$, $j > i$ to the same constant $\varrho \geq 0$. Hence, we can now derive from Equation (1) a simple expression for the cost per round to maintain *k* defenses,

$$c_t = \frac{\varrho}{2}k^2 + \left(1 - \frac{\varrho}{2}\right)k\,. \tag{5}$$

Observe that $c_t \sim \mathcal{O}(k^2)$ if $\varrho > 0$ and $c_t \sim \mathcal{O}(k)$ if $\varrho = 0$. Of course, if better knowledge on the cost of defenses is available in practical applications of the model, this assumption can be relaxed and $\boldsymbol{C}$ populated with real data.

We further assume a *risk neutral* defender, that is, one who maximizes inter-temporal utility as a linear function of (expected) revenues and costs. We defer consideration of other attitudes towards risk or different time preferences to future work in order to keep the core model lean.

2.6. Model Summary and Example Parameters

Our model can be applied to many scenarios. For now, we demonstrate its parameters in action by considering an imaginary online music store to demonstrate its parameters in action (we describe other scenarios in Section 5). The music store's asset is the library of audio files and the associated property rights. Let the total value of the asset be one million dollars. To avoid large numbers, we count in thousands of dollars, so asset value *a* = 1 000. Every year, indexed by *t*, the net return from online sales amounts to $r = 5\%$ of the asset value.

Surrounded by malicious competitors, professional cybercriminals and "curious customers", the store is exposed to various threats (say, $n = 25$). In case of a successful attack, the store loses $z = 2.5\%$ of the asset value, or $25,000, due to forgone sales and incurred damage. It is known (from industry sources) that, *on average* over all similar businesses, the cost of a successful attack is at least 15,000 dollars ($\overline{x_1} = 15$). This could be the price for an attack kit against standard software on the underground market for cybercrime supplies [9]. Attack costs also rise with novelty and difficulty of implementation, *on average* by 1000 dollars for each level of sophistication. Hence, the gradient of the attack cost is $\Delta x = 1$. However, these are only average values and it

is unknown how much the actual costs are to attack the particular business. This uncertainty can be expressed by the deviation σ of the attack costs around the average. To put this parameter in perspective, $\sigma = 0$ means that all attacks can be predicted perfectly, $\sigma = 1$ means 96% of the attacks can be predicted correctly,[3] and for $\sigma = 16$, predicting attacks is only 65% successful. This is still somewhat better than random guessing.

The store owner is not entirely helpless: he may spend on security measures to defend against each of the $n = 25$ threats. Each defense costs 1000 dollars per round (this is a constant that defines the unit, so no symbol is required). On top of that, defense interdependence with parameter $\varrho = 0.1$ accounts for additional cost for every pair of installed defenses. As a consequence, every investment in security must be carefully considered, since countermeasures added later cost more due to increased complexity and interoperability challenges. Finally, parameter λ controls (optional) unrecoverable costs. It describes the cost to update the defense configuration as a fraction of the asset value *a*. In the example of a music store, unrecoverable costs are negligible (*i.e.*, $\lambda = 0$) since security upgrades do usually not render existing investment useless. However, if the music store served a proprietary audio format targeted to specific playback devices, an exchange of all customers' physical playback devices to upgrade the defense configuration could be modeled as unrecoverable cost ($\lambda > 0$).

Table 1 summarizes the parameters of our model and their values used in the subsequent examples. The following section will show how defenders can optimize their security spending in this model. We are primarily interested in exploring how the optimal strategy changes based on the level of uncertainty σ; we also elaborate on the role of unrecoverable costs λ.

3. Analysis

We distinguish between *static* analysis, where the defender chooses the configuration in the first round ($t = 1$) and keeps it constant further on, and *dynamic* analysis, where the configuration can be updated in every round. In case of certainty ($\sigma = 0$), a static solution exists that is at least as good as any dynamic strategy. Unrecoverable costs are relevant in the dynamic setting only.

Table 1. Overview of model parameters.

Parameter	Symbol	Example values
Business model		
Asset value	a	1 000
Time in years	t	$1,\cdots,t_{\max}$
Return	r	5.0%
Attacker		
Number of threats	n	25
Loss given attack	z	2.5%
Expected minimum attack cost	$\bar{x}_1$	15
Gradient of attack cost	Δx	1
Level of uncertainty	σ	$0,\cdots,16$
Defense		
Cost of each individual defense	1	1 (unit definition)
Defense interdependence	ρ	0.1
Unrecoverable costs	λ	0

[3]All other parameters are as specified in **Table 1**.

3.1. Static Solution

We consider a defender with defense vector $\boldsymbol{d}$ where the k lowest cost threats are defended, leaving the remaining $n-k$ threats unprotected: $d_1,\cdots,d_k=1$ and $d_{k+1},\cdots,d_n=0$. Let $f(k)$ be the return function for this defender,

$$f(k)=a(r-zq)-c_t \tag{6}$$

$$=a(r-zq)-k-\frac{\varrho}{2}(k^2-k), \tag{7}$$

where q is an indicator variable that takes value one if the attacker is successful and zero otherwise. In the case of certainty, q is fixed for all rounds, so that two outcomes are possible:

$$f_{\text{att}}=a(r-z)\ (\text{attack})\ \text{and} \tag{8}$$

$$f_{\overline{\text{att}}}(k)=ar-k-\frac{\varrho}{2}(k^2-k)\ (\text{no attack}). \tag{9}$$

The cost term disappears in Equation (8) because if we accept attacks anyway, then there is no need to spend money to make it more difficult for the attacker (*i.e.*, $k = 0$). Otherwise, the minimal number of defenses k^* to defeat all attacks can be calculated by rearranging Equation (2) and comparing it to the attacker's gain za,

$$k^*=\sup\left(0,\left\lfloor\frac{za-\overline{x}_1}{\Delta x}+1\right\rfloor\right). \tag{10}$$

Typically, the best strategy for the defender is to follow whatever is higher, Equation (8) or (9), with $k=k^*$. When Equation (9) is lower than Equation (8), the defender finds it profitable to operate without investing in any security measures. We call this situation *indefensible*, which does not necessarily imply that the business is unsustainable. Rather like in self-insurance, the defender extracts positive gross return after deducting the losses due to successful attacks. Only when both equations are negative, the cost of attacks and the cost of defending them are both so high that the defender's business becomes *unviable*.

In the case of uncertainty ($\sigma>0$), q becomes a random variable and a risk neutral defender maximizes $E(f(k))$, where expectations are taken over the realizations of q. For a static solution, it is still rational to use configurations in which lower-order threats are defended first. So we can calculate $E(q)$ as a function of k as the probability that the cost of at least one of the unprotected threats falls below the threshold za,

$$E(q(k))=1-\prod_{i=k+1}^{n}\left(1-\Phi\left(z\cdot a;\overline{x}_1+(i-1)\cdot\Delta x,\sigma/\Delta x\right)\right),\ k<n \tag{11}$$

where $\Phi(x;\mu,\sigma)$ is the cumulative distribution function of the Gaussian normal distribution. The product term is the probability that none of the $n-k$ undefended threats materializes, so one minus this term is the probability of at least one successful attack. Inserting into Equation (7), we obtain

$$k^*=\arg\max_k E(f(k))=\arg\max_k a(r-zE(q(k)))-k-\frac{\varrho}{2}(k^2-k). \tag{12}$$

Figure 2 depicts expected returns of the static solution as a function of k for parameters as specified in **Table 1**. Each curve corresponds to different levels of uncertainty; the utility-maximizing selection of k^* for each uncertainty level is circled. In the case of certainty ($\sigma=0$), the optimal security investment amounts to $k=11$ defenses (Equation (10)). Increasing uncertainty affects the optimal strategy in a non-linear manner: while some noise in the predicted attack costs lets the defender take more proactive counter-measures ($\sigma=1,2$), the cost of this over-investment start to outweigh the protected revenues when uncertainty is too high ($\sigma=4,8$). Eventually, it becomes rational for more uninformed defenders to refrain from *any* defense and instead accept moderate losses in each round. In other words, knowing your enemy is a prerequisite for taking tailored countermeasures, and tailored defense is the only option if comprehensive defense (*i.e.*, $k=n$) is prohibitively expensive.

3.2. Dynamic (Iterated) Solution

When $\sigma>0$ (uncertainty), the static solution is often sub-optimal because observed attacks reveal additional

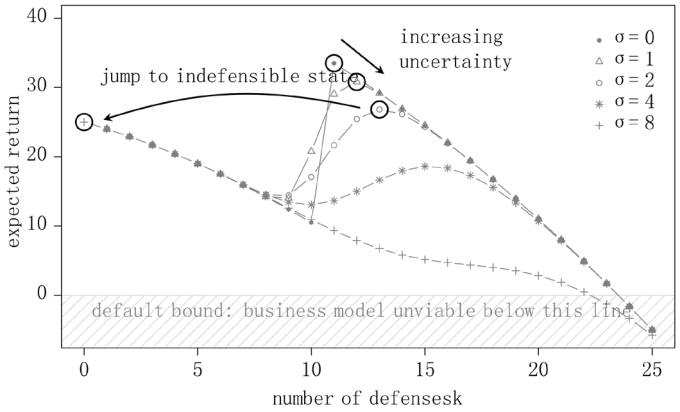

Figure 2. Static solutions for the parameters asset value a = 1000, return r = 5%, loss given attack $z = 2.5\%$, minimum expected cost of attack $\overline{x}_1 = 15$, gradient of attack cost $\Delta x = 1$, defense interdependence $\varrho = 0.1$, and $n = 25$. The optimal number of defenses k^* is circled for each curve.

information about the true cost of attack. This information could be used to reconfigure the defenses adaptively. In the dynamic case, uncertainty is repeatedly eliminated for targets revealed to be the weakest link. Consequently, this reduction in uncertainty for later rounds can lead to a better outcome for the defender than in the static case. In general, the inter-temporal outcome is the sum of all returns over a period of time $t = (1, \cdots, t_{\max})$,

$$y = \sum_{t=1}^{t_{\max}} f(\boldsymbol{d}_t, \boldsymbol{d}_{t-1}) = \sum_{t=1}^{t_{\max}} \left(a(r - zq_t) - c_t - s_t \right), \tag{13}$$

and can be maximized by adjusting $\boldsymbol{d}_t$ adaptively. At each point in time t, the defender learns about the materialized threat (if any) of period $t-1$. In Equation (13), c_t, s_t and q_t, are functions of the sequence of configurations $\boldsymbol{d}_t$ and the random realization of $\boldsymbol{x}$. Due to this stochastic component and its subsequent path dependencies through adaptation, the analysis must be based on expectations over all possible realizations. We will first discuss the simpler case without fully recoverable costs (*i.e.*, $\lambda = 0$) before moving on to the general case.

3.2.1. Special Case: All Costs Recoverable

The defender has to choose a *proactive defense* $\boldsymbol{d}_1$ against the k_1 most probable threats, so that $d_{i,1}, \cdots, d_{k_1,1} = 1$ and $d_{k_1+1,1}, \cdots, d_{n,1} = 0$. Unless this configuration is already secure, the defender would iteratively add another defense in each round as the attacker targets new weak links. The order of these *reactive defenses* is determined by the order of x_i, and thus by the realization of the random vector $\boldsymbol{x}$. This way, one weakest link is fixed after another. It follows from the path dependencies that once a secure configuration is found, the defender would not touch $\boldsymbol{d}$ anymore: in this model, it is always better to start with a lower proactive defense k_1 than tinkering with existing defenses after a couple of rounds. This is so because the uncertainty about the realization of $x_1, \cdots, x_{k_1}$ is not reduced, while the direct and indirect ($\varrho > 0$) cost of the k_1-th defense has to be born for all intermediate rounds.

Let t_{att} (with $0 \le t_{\text{att}} \le t_{\max}$) be the number of rounds with successful attacks, then $\boldsymbol{d}_{t_{\text{att}}+1} = \boldsymbol{d}_t \ \forall t > t_{\text{att}}$ is the final secure configuration that is eventually reached if $t_{\text{att}} < t_{\max}$. If all costs are recoverable, then Equation (13) can be rewritten as

$$y = \sum_{t=1}^{t_{\text{att}}} \left(a(r - z) - c_t \right) + \sum_{t=t_{\text{att}}+1}^{t_{\max}} \left(ar - c_t \right) \tag{14}$$

$$= t_{\text{att}} \cdot a(r - z) - \sum_{t=1}^{t_{\text{att}}} c_t + \left(t_{\max} - t_{\text{att}} \right) \left(ar - c_{t_{\max}} \right), \tag{15}$$

after inserting Equation (5) we obtain:

$$= t_{\text{att}} \cdot a\left(r - z\right) + \left(t_{\max} - t_{\text{att}}\right)\left(ar - c_{t_{\max}}\right) - \frac{\varrho}{2}\sum_{k=k_1}^{k_1+t_{\text{att}}} k^2 - \left(1 - \frac{\varrho}{2}\right)\sum_{k=k_1}^{k_1+t_{\text{att}}} k\,. \tag{16}$$

Equation (15) holds because c_t is constant when $\boldsymbol{d}_t$ is constant. A closed-form expression for Equation (16) can be obtained by replacing the remaining sums by first and second order arithmetic progression formulas. This expression gives the output y as a function of the proactive defense k_1 and the number of rounds under attack t_{att}. The latter parameter in fact depends on the random realization of $\boldsymbol{x}$. The expectation of the term in Equation (16) can be calculated by the sum of all possible values for $0 \le t_{\text{att}} \le t_{\max}$, weighted by the respective probability of occurrence $\mathcal{P}\left(t_{\text{att}}\right)$.

To calculate $\mathcal{P}\left(t_{\text{att}}\right)$, we interpret the condition for a successful attack $x_i \le z \cdot a$ as Bernoulli random variable with probability of attack

$$p_i = \Phi\left(z \cdot a; \bar{x}_1 + \left(i-1\right)\cdot \Delta x, \sigma/\Delta x\right). \tag{17}$$

Hence, $\boldsymbol{p}$ is the parameter vector of non-homogeneous independent Bernoulli variables. For reasonable parameter choices, the sum of these random vectors can be approximated by the Gaussian distribution with location $\mu = \sum_{i=1}^{n} p_i$ and variance $\varsigma = \sum_{i=1}^{n} p_i\left(1-p_i\right)$. This completes the analysis. Next, we compute the optimal choices for the proactive defense k_1^* (that maximize the expected inter-temporal outcome) numerically by searching for the supremum of $E\left(y\left(k_1\right)\right)$ in the integer range $k_1 = 0, \cdots, n$.

Figure 3 shows expected returns *per round* of the dynamic solution for the same parameters as in **Figure 2**, now as a function of the *proactive defense* k_1. Similar to **Figure 2**, the optimal proactive defense for each value of σ is circled. Obviously, in the case of certainty ($\sigma = 0$), the optimal proactive defense $k_1^* = k^* = 11$ equals the result of the static analysis. If there is no uncertainty, a defender does not gain any information from observed attacks and can define the optimal configuration entirely proactively. However, as soon as uncertainty arises, the optimal strategies in the static and dynamic case diverge. While some uncertainty ($\sigma > 0$, but small) makes a *static* defender more cautious (to reduce the probability of being vulnerable) and leads him to spend more, a *dynamic* defender knows that he will be able to adjust later and can thus take on more risk in the first place. The higher the uncertainty, the more valuable the information gleaned from observed attacks becomes and the lower the optimal share of proactive defense.

Moreover, observe that an indefensible state is already reached for $\sigma = 4$ in **Figure 2** for the static case, whereas much higher uncertainty is needed to let a defender refrain from all proactive investment in the dynamic case ($\sigma = 16$ in **Figure 3**). So we gain the insight that the sheer possibility of adjusting defenses reactively can stimulate proactive security investment when the uncertainty is high.

3.2.2. General Case

To consider unrecoverable costs in the analysis, Equation (13) is rearranged to the form of Equation (14) as

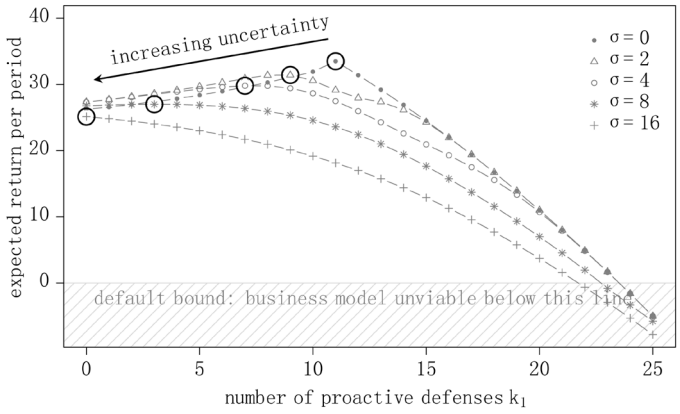

Figure 3. Dynamic solutions for the same parameters as in **Figure 2** ($a = 1000$, $r = 5\%$, $z = 2.5\%$, $\bar{x}_1 = 15$, $\Delta x = 1$, $\varrho = 0.1$, and $n = t_{\max} = 25$). The optimal number of proactive defenses is circled for each curve.

follows:

$$y = \sum_{t=1}^{t_{\text{att}}} \left(a(r-z) - c_t - s_t \right) + \sum_{t=t_{\text{att}}+1}^{t_{\max}} \left(ar - c_t \right). \tag{18}$$

The second sum does not include s_t because d_t remains constant for $t > t_{att}$. Rearranging and inserting Equation (4) yields

$$y = t_{\text{att}} \cdot a\left(r - z - \lambda\right) - \sum_{t=1}^{t_{\text{att}}} c_t + \left(t_{\max} - t_{\text{att}}\right)\left(ar - c_{t_{\max}}\right). \tag{19}$$

We proceed as with Equation (16) in the special case with all costs recoverable. It is possible to keep the same strategy of iterated investment because the elements of the random vector $\boldsymbol{x}$ are independent and observing one attack does not inform the defender on what the next weakest link will be. Also with unrecoverable costs at every update, it would be irrational to invest in bundles of reactive defenses if one had not done so proactively. However, if unrecoverable costs are not negligible, the effort spent on proactive measures changes substantially. For a finite horizons $t_{\max}$, however, it is rational for the defender to reflect on the strategy after having observed an attack in t_1: for very high λ, he might prefer not to defend at all and accept losses in the remaining $t_{\max} - 1$ rounds. This is like a reduction to Equation (8) of the static case. This lends to another interpretation of introducing unrecoverable costs in our model: they cause an increase in z for t_{att} rounds (if the iterated patching starts) combined with the option to fall back to the static case (without the increase in z).

Figure 4 illustrates the structure of the general decision problem and **Table 2** displays the corresponding expressions for calculating the costs at the different types of terminal nodes T_1, T_4. With unrecoverable costs, *ignore* becomes a valid choice as it may be cheaper than *disinvest*.

In **Figure 5**, we fix two settings for the level uncertainty, low ($\sigma = 2$) and high ($\sigma = 4$), and plot expected

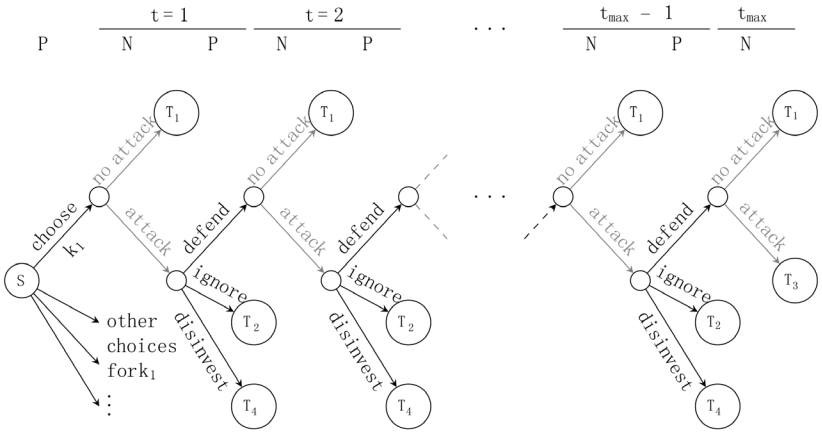

Figure 4. Decision tree of iterated weakest link model with unrecoverable costs. *S* is the start node, T_1, T_4 refer to terminal nodes, *P* denotes *player* (*i.e.*, defender) and *N* denotes *nature* (*i.e.*, attackers).

Table 2. Cost at terminal nodes as function of k_1 and t (if applicable).

T_1	$\left((t-1)\cdot az\right) + \sum_{i=0}^{t-1} c\left(k_1+i\right) + \left(t_{\max}-t\right)\cdot c\left(k_1+t-1\right) + \left(t-1\right)\cdot \lambda a$
T_2	$t_{\max}\cdot az + \sum_{i=0}^{t-1} c\left(k_1+i\right) + \left(t_{\max}-t\right)\cdot c\left(k_1+t-1\right) + \left(t-1\right)\cdot \lambda a$
T_3	$t_{\max}\cdot az + \sum_{i=0}^{t_{\max}-1} c\left(k_1+i\right) + 0 + \left(t_{\max}-1\right)\cdot \lambda a$
T_4	$t_{\max}\cdot az + \sum_{i=0}^{t-1} c\left(k_1+i\right) + \left(t_{\max}-t\right)\cdot c\left(k_1+t-1\right) + t\cdot \lambda a$

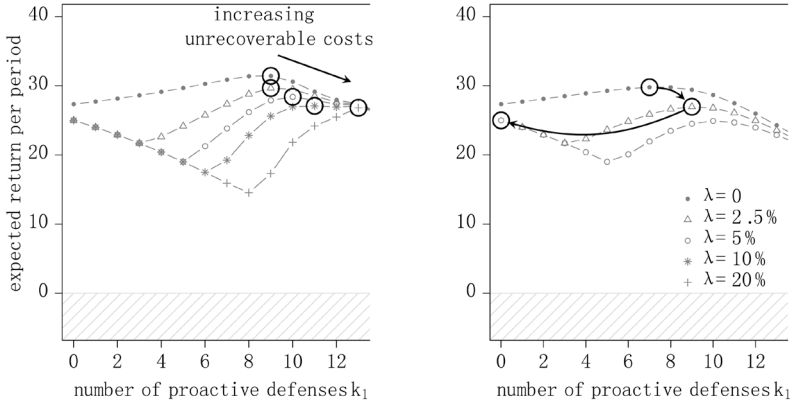

Figure 5. Dynamic solutions with unrecoverable costs for low (left) and high (right) uncertainty. All other parameters as in **Figure 2** ($a = 1000$, $r = 5\%$, $z = 2.5\%$, $\overline{x}_1 = 15$, $\Delta x = 1$, $\varrho = 0.1$, and $n = t_{\max} = 25$). λ controls the amount of unrecoverable update costs (as fraction of *a*), σ is a measure of uncertainty. The optimal number of proactive defenses is circled for each curve. (a) Low uncertainty: $\sigma = 2$; (b) High uncertainty: $\sigma = 4$.

returns per period as a function of the proactive defense k_1 for various settings of λ. Observe in **Figure 5(a)** that higher unrecoverable update costs triggers greater precaution and forces the defender to invest more in proactive security. This is consistent with common sense. However, if the uncertainty is high, then there exists a threshold for the unrecoverable costs above which a defender "surrenders" and prefers to cope with the attacks, as visible in **Figure 5(a)** for values of $\lambda > 1\%$ of the asset. The similarity to the static case can also be seen by comparing the similar shape of the curves. Note that these results should be interpreted with caution as they depend on a finite horizon $t_{\max}$, which might not apply to all business cases.

4. Security Investment Based on the Iterated Weakest Link Model

As we have analyzed the optimal strategies of the defender in the previous sections, we can now use the model to calculate some key indicators that relate to practical experience. **Table 3** compares typical security indicators derived from the model for different degrees of uncertainty (in columns) and different defense strategies (row sections—static/dynamic/dynamic with unrecoverable costs). The list of indicators includes:

- Optimal defense is a memo item that describes the optimal defense strategy $k^*_{(1)}$. All other indicators are computed on the assumption that a rational defender follows this strategy.
- Attack intensity measures the probability of a successful attack per round, averaged over all $t_{\max}$ rounds.
- Average gross return is the objective function of the optimization problem, scaled to a percentage of the asset value *a*. The average is computed over all $t_{\max}$ periods and expectations are taken over all realizations of the stochastic component $\boldsymbol{x}$, weighted by their respective probability of occurrence. Higher values are better.
- Average security spending is the average effort spent on defenses, comprising direct, indirect and unrecoverable costs (if applicable). Averages and expectations are computed as for gross returns. Lower values are not necessarily better; what matters is the efficiency of the security spending, *i.e.*, how security spending compares against prevented losses. This depends on how targeted the defense configuration is to the realization of the attack profile.
- Annual loss expectation (ALE) measures expected foregone profits per period [10].[4] ALE can be computed for two scenarios: ALE_0 is the (hypothetical) ALE if no defenses were deployed, and ALE_1 is the ALE of the respective defense strategy. Expectations are taken over realizations of the random vector $\boldsymbol{x}$.
- Return on information security investment (ROSI) is a summary measure to quantify the effectiveness of security investment. We follow the approach in [11] and normalize the indicators by the security spending, *i.e.*,

[4]We stick to the term "annual" to be consistent with the literature and assume that time periods in the model correspond to financial years.

Table 3. Key security investment indicators derived from the model.

	Level of uncertainty			
Indicator	$\sigma = 0$	$\sigma = 1$	$\sigma = 4$	$\sigma = 8$
Static defense				
Optimal defense k^*	11	12	0	0
Attack intensity (% rounds)	0.0	2.4	100.0	100.0
Avg. gross return (% asset)	3.4	3.1	2.5	2.5
Avg. security spending (% asset)	1.6	1.9	0.0	0.0
ALE_1	0.0	0.6	25.0	25.0
ROSI (% security spending)	51.5	31.2	-	-
Dynamic defense w/o sunk costs				
Optimal proactive defense k_1^*	11	9	7	3
Attack intensity (% rounds)	0.0	6.1	15.7	32.7
Avg. gross return (% asset)	3.4	3.2	3.0	2.7
Avg. security spending (% asset)	1.6	1.5	1.6	1.4
ALE_1	0.0	1.5	3.9	8.2
ROSI (% security spending)	51.5	52.8	35.2	18.9
Dynamic defense w/ sunk costs				
Optimal proactive defense k_1^*	11	10	9	0
Attack intensity (% rounds)	0.0	2.9	9.8	100.0
Avg. gross return (% asset)	3.4	3.1	2.7	2.5
Avg. security spending (% asset)	1.6	1.6	1.9	0.0
ALE_1	0.0	0.7	2.5	25.0
ROSI (% security spending)	51.5	50.6	15.7	-
Memo items: no defense				
Avg. gross return (% asset)	2.5	2.5	2.5	2.5
ALE_0	25.0	25.0	25.0	25.0

Parameters: asset value $a = 1000$, return $r = 5\%$, loss given attack $z = 2.5\%$, min. expected cost of attack $\bar{x}_1 = 15$, gradient of attack cost $\Delta x = 1$, defense interdependence $\rho = 0.1$, sunk costs $\lambda = 2.5\%$, $n = 25$, $t_{\max} = 25$. All figures rounded to one decimal digit.

$$\mathrm{ROSI} = \frac{\mathrm{ALE}_0 - \mathrm{ALE}_1 - \text{avg. security spending}}{\text{avg. security spending}}. \tag{20}$$

Higher values denote more efficient security investment. The indicator is not defined for cases where no defenses are optimal.

Unsurprisingly, the three modes of adaptivity concur in the case of certainty (leftmost column in **Table 3**). However, uncertainty creates some remarkable results, which we now discuss.

For low levels of uncertainty ($\sigma = 1$), replacing a static with a dynamic defense strategy primarily reduces security spending, which leads to more observed attacks. However, gross returns increase as well. In fact, security spending is better targeted, over-investment is reduced, and the overall efficiency of security investment (as measured by the ROSI indicator) improves. From this result, we can draw an alternative interpretation to the

omnipresent reports of security breaches in the media: rather than rashly framing them as engineering failures, one can also view them as unavoidable side-effects of smart defense strategies that balance the amount of proactive and reactive security investment.

Regarding attack intensity, a converse effect is observable when uncertainty is higher ($\sigma \geq 4$). Here, the attack intensity drops substantially from (almost) 100% in the static case to a very low rate in the dynamic case. At the same time, average returns increase. The reason for this is that high uncertainty lets some defenders refrain from deploying any defenses (and thereby absorbing losses). Only a staged approach gives these investors an incentive to defend against the most aggressive threats. Note that the model identifies the rational response to the *private* costs faced by defenders. We ignore the *public* costs created by insecurity. While not addressed by this article, negative externalities of poor security practices are widely considered to be a significant public problem [2]-[4]. Hence, while it may be narrowly better for some defenders to skimp on security when they are unsure whether they will be targeted, a public policy response may be necessary to compensate for the negative externalities of insecurity caused by such under-investment.

Unrecoverable costs muddy this picture somewhat. They raise incentives towards more proactive security investment. This leads to higher proactive defenses and thereby lower attack intensity. However, unrecoverable costs also eat up margins, so gross returns tend to decline. Even more importantly, the overall efficiency of the security investment drops, and the differential grows as uncertainty rises. So, some uncertainty combined with expensive infrastructure upgrades can stimulate over-investment—but only to a certain point. Eventually, high uncertainty can demotivate any security investment, similar to what happens in the static case. In the real world, we would expect to see relatively more weight on proactive security when updates case high unrecoverable costs (e.g., payment cards) and the uncertainty is low or moderate, compared to businesses where almost all costs are recoverable (e.g., websites). This prediction could be tested against cross-sectional empirical data in future work. In any case, the above-mentioned excuse of breaches as smart defense strategy does not apply to defenders with high unrecoverable costs. The related policy dimension here is to reduce the uncertainty when it is so high that it discourages security investment. This can be done, for instance, by encouraging information sharing so that the cost of reducing the uncertainty can be borne between several defenders [12] [13].

Note that all these conclusions remain fairly robust for other parameters than the example set in **Table 1**. For brevity, we refrain from discussing the influence of all other parameters. Instead, we demonstrate the validity of our model by applying it to two case studies where real data is available.

5. Empirical Evidence for Iterated Weakest Links

In the following, we will point the reader to past "iterated arms races" in the realm of information security. We argue that such dynamics, against the backdrop of our model, may in fact be rational and should not simply be framed as "failures". We have selected two cases, one where almost all costs are recoverable (Section 5.1) and another one where unrecoverable costs should not be ignored (Section 5.2).

5.1. Case 1: Phishing and Online Crime

Our first argument focuses on the security of computers comprising the Internet follow an iterated weakest link model. Fundamental to the Internet's design is the notion that any connected computer can communicate with every other computer. Attackers have relentlessly exploited this structure, constructing networks of compromised machines (so-called botnets) to pester legitimate users by emitting spam, distributing malware and hosting phishing websites. Internet service providers (ISPs) are usually well-placed to detect infection, because evidence of a user's infection flows over an ISP's communication systems. Moreover, large companies that act as Internet service providers have technical staff who can detect and clean up infected machines, while domestic users and small businesses are mostly helpless to even recognize when they are compromised; l*et al*one to take appropriate remedial action. However, for every responsible ISP that keeps a clean network, there are countless others who find it more cost-effective to ignore the problem and let infections flourish.

There is substantial evidence that attackers concentrate their efforts at the most irresponsible ISPs, moving on to others once the ISP cleans up its act or is shut down. For instance, until 2007, a lot of the world's malware was hosted by the Russian Business Network (RBN), which refused to comply with requests from international law enforcement [14]. After Russian Business Network suddenly went offline in late 2007, malware distribution shifted to other ISPs. In November 2008, a journalist from the Washington Post persuaded upstream bandwidth

providers to shut off their connection to San Francisco-based McColo, which led to a temporary fall of almost 70% in the volume of spam worldwide [15]. Apparently, many botnet herders had been using McColo to host their control machines. Spam volume has since recovered as the spammers found new safe havens. In 2008 EstDomains, which served as the primary domain name registrar for malicious websites hosted by Russian Business Network [16], became the first domain registrar to have its accreditation terminated by the Internet Corporation for Assigned Names and Numbers [17]. Unfortunately, other irresponsible registrars remain.

Attackers can often move on to exploit the next weakest link in the Internet far faster than defenders can knock them out. Moore and Clayton [18] showed how one leading group of online fraudsters, the rock-phish gang, operated. It registered many malicious web domain names to carry out attacks. Periodically, the gang picked a firm for registering Internet domain names that it had never used before and registered hundreds of web domains, using false names and stolen credit cards. These domains did not resemble normal bank names, so a registrar may not identify foul play, and the first domains to be used for false purposes were not removed quickly.

Figure 6 presents scatter plots of phishing site lifetime based on the date reported from data of [18]. Both .hk (Hong Kong) domains (left) and .cn (China) domains (right) lasted much longer in their first month of use than in later months. The gang targeted Hong Kong domains first in March 2007, followed by Chinese domains in May 2007 after the Hong Kong authorities wised up.

Such iteration over previously untargeted infrastructure operators is prevalent among many forms of cybercrime. Other researchers have found that websites hosting most malware move from one registrar to the next [19]. Liu *et al*. studied patterns in the registration and take-down of spam-advertised domains [20], finding that miscreants register many domains at previously untargeted registrars, repeatedly moving on to new ones following crack-downs. McCoy *et al*. examined the use of payment processors by unlicensed online pharmacies [21]. They showed that the operators of unlicensed pharmacies initially relied on a small number of payment processors. Once banks were made aware of the criminal behavior, many severed ties with the pharmacies, who quickly made arrangements with new processors.

5.2. Case 2: Payment Card Security

Financial transactions have long been subject to fraud, and banks and payment processors have recognized that fraud has to be managed rather than eliminated. In 2000, the UK banks decided to adopt the EMV card payment system designed by Europay, Mastercard and Visa, popularly known as “Chip and PIN” EMV. The EMV roll-out provides a compelling example of taking security decisions to tackle the weakest link, only to find that the attackers react by exploiting new holes previously ignored. A May 2007 internal report prepared by APACS (since rebranded as the UK Cards Association) compared the expected benefits from EMV adoption to fraud incidence over time. While the report was intended to be kept confidential, it was accidentally leaked and is now hosted on the Cryptome website [22]. We use the data gleaned from this report, as well as more recent public statistics [23] [24], to demonstrate how the banks’ fight against card fraud has essentially been a sequence of patches to plug weak links.

Figure 7 plots the annual percentage of transaction turnover found to be fraudulent from 1972 to 2014.

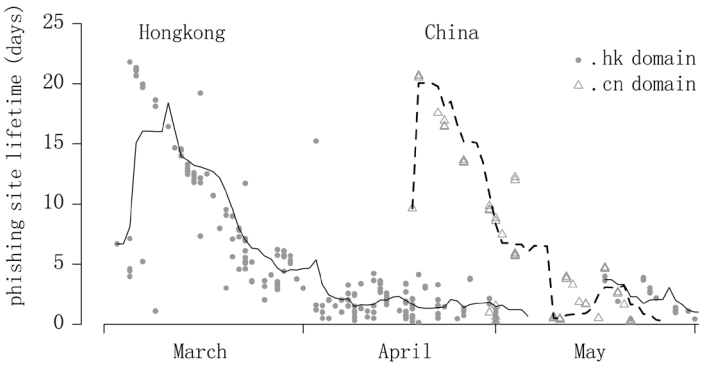

Figure 6. Take-down latency for phishing attacks targeting different registrars in spring 2007; lines are five-day moving averages broken down by top-level domain (Source: own aggregation based on data of [18]).

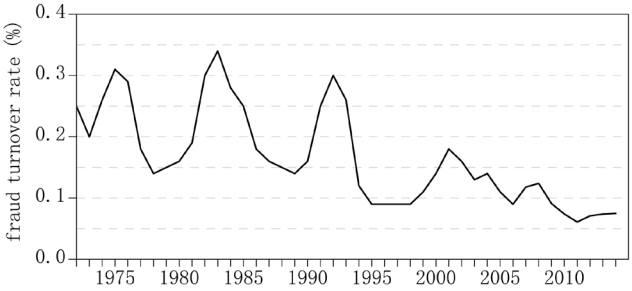

Figure 7. Long-term fraud rates as a fraction of overall turnover (Source: [22] [23]).

Notably, there are significant swings in the rate. According to the report [22], "the industry has responded to crises in card fraud by making significant investment in new preventative measures," including "terminalisation in the early 80s and, later, a major increase in levels of authorisation during the mid 90s." Such behavior is consistent with our model of iterating through successive weakest links.

Around 2000, a fear arose that another uptick in the fraud rate was imminent. The dashed line with triangle markers in **Figure 8** plots the forecast losses due to fraud based on maintaining the status quo as of 2000. To stem this expected rise in fraud, UK banks decided to adopt the EMV standard (Chip and PIN) over the course of the next few years. The estimated cost of implementing EMV across the UK was just over £1 billion, shared between the banks and retailers. We can interpret this investment to roll out EMV as unrecoverable costs. The dashed line with diamond markers in **Figure 8** plots the forecast losses following EMV adoption. The uptick to 2003 is due to the phased roll-out of the technology.

In fact, the actual losses look rather different (solid line in **Figure 8**). The anticipated explosion of fraud in the early 2000s did not materialize; strikingly, the full adoption of EMV (completed in 2005) did not significantly alter the fraud totals. Instead, a slow but steady increase was observed, both before and after EMV adoption.

Digging a little deeper, we can see that the switch to EMV did significantly alter attacker strategy, even if it did not significantly shift the aggregate fraud rates. Instead, as some types of fraud diminished, other techniques quickly filled the gap. For instance, EMV has caused a dramatic drop in face-to-face retail fraud, since forging a signature is easier than guessing the right PIN. In 2004, face-to-face fraud totaled £219 million; in 2006, after EMV became mandatory, it fell to £72 million (see **Figure 9**). However, card-not-present (CNP) fraud (where only the card number is used, as in online transactions) has sharply risen since the introduction of EMV, from £150 million in 2004 to £328 million in 2008, before falling modestly and reaching a new high of £332 million in 2014. This is not surprising, since PINs are not verified for CNP transactions.

Another example of attackers moving to weaker links can be found by looking at where ATM fraud takes place. With the adoption of EMV, ATMs in the UK stopped verifying PINs using magnetic stripes, requiring the PIN be verified using the more secure chip. However, many ATMs outside the UK continued to allow the less secure verification via magnetic stripe. As UK ATMs switched over during 2006, fraudsters immediately adapted to cashing out via less secure international ATMs. **Figure 10** shows how this transformation happened. In December 2005, when most UK ATMs still allowed magnetic stripe PIN verification, £6 million out of the total £6.5 million stolen from ATMs took place within the UK. By the end of the year, after the switch to more secure verification, the total monthly fraud increased to over £9 million, with nearly 75% of the losses occurring overseas. The shift to overseas fraud that is easier to carry out has continued since the EMV rollout. In **Figure 11**, we see that the share of the total fraud occurring overseas rose from £93M (18% of the total) in 2004 to a peak of £230M (37% of the total) in 2008. In fact, the share of overseas-originated fraud on UK cards in 2008 exceeded the total UK-originated fraud in 2004, just prior to the EMV deployment. This is compelling evidence of how quickly attackers can shift to find the next-weakest link once the biggest hole has been plugged.

The EMV standard actually provides several options for implementation that vary in the cost and security achieved. While the UK EMV implementation was certainly not inexpensive, its designers did opt for many of the lower-cost implementations offered by the standard. For instance, PIN verification is normally done offline, between the card's chip and the PIN entry device (PED). This enables a relay attack whereby a small, legitimate transaction authorized by a compromised terminal can be used to approve a simultaneous, much larger fraudulent

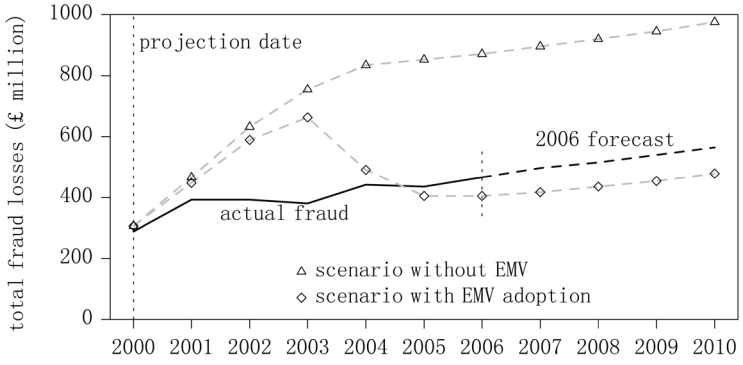

Figure 8. Ten-year fraud projections made in 2000 comparing whether EMV is adopted (marked dashed lines), plus actual fraud rates (solid line) (Source: [22]).

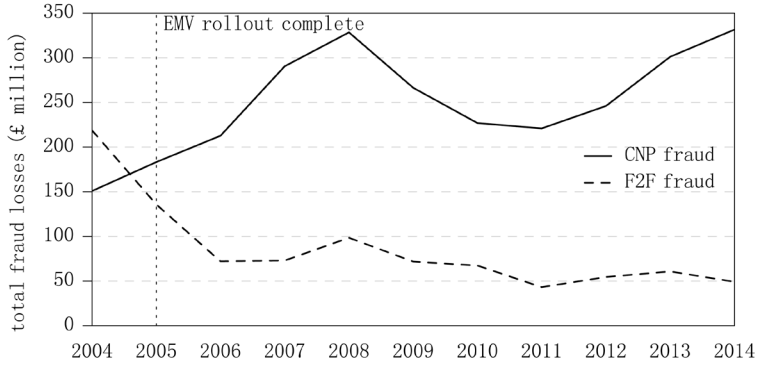

Figure 9. Fraud losses for UK face-to-face (F2F) retail transactions protected by EMV and for card-not-present (CNP) transactions not protected by EMV (Source: [23]).

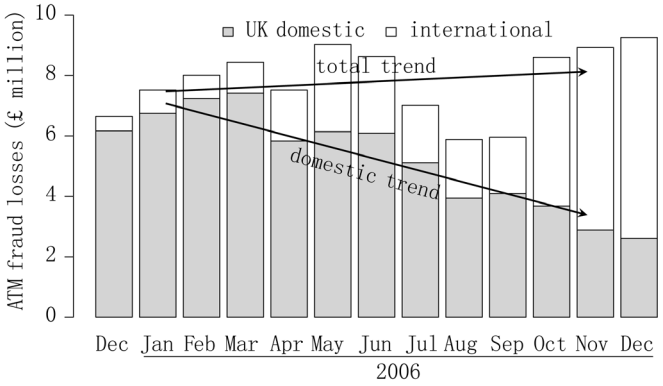

Figure 10. Shifting attacker strategy following EMV adoption. The bar graph shows how ATM fraud has moved overseas to ATMs which have not made the switch to chip verification, but still rely on less secure magnetic stripes (Source: [22], trend lines fitted with ordinary least squares).

transaction elsewhere [25]. Furthermore, the communications within the PED between the card's chip and the PED's processor are not encrypted. Combined with some shoddy tamper-proofed devices, this enables PINs to be read using a paper clip tapped inside the PED [26]. The same team later discovered an attack on the protocol that could enable a criminal to use a genuine card without knowing the PIN [24] [27]. While entirely practical, there is no evidence that these attacks are being used by attackers at present. Instead, they seem to be focusing on the more obvious weak links of card-not-present transactions and magnetic stripe verification at foreign

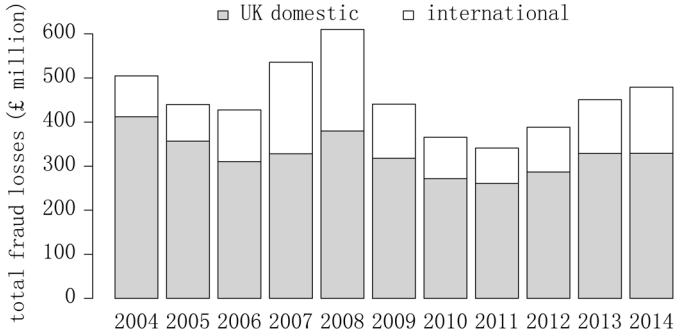

Figure 11. Total fraud losses split according to whether the fraud took place in the UK or not (Source: [23]).

ATMs. If (and when) these holes are plugged[5], one might expect these attacks to be deployed, which would trigger defensive countermeasures by the banks.

5.3. Attack Profiles for the Case Studies

Figure 12 plots the expected and realized costs of different attacks for the case studies just presented. **Figure 12(a)** plots a sequence of top-level domains that potentially targeted by the rock-phish gang. First, many Chinese domains were registered by the gang, followed by domains from Hong Kong (as shown in **Figure 6**). The next top-level domain targeted—Austria—came as a surprise. Austria has an extensive Internet security community, and its law enforcement has long cooperated with cyber investigations from other countries. Nonetheless, the rock-phish gang registered many .at domains, and they were not removed for a very long time. It turns out that the Austrian domain registrar nic.at balked at removing the illicit domains without more extensive evidence documenting their illegality. The domains were only removed following a public row between the e-mail-blacklist operator Spamhaus and nic.at [29]. Finally, after .at domains began getting removed promptly, the Turkish top-level domain .tk was targeted.

Meanwhile, many top-level domains have not been targeted by the gang. This includes domains such as Paraguay (.py), which we might have expected to be an easy target for attackers[6], as well as domains such as .se, .edu, and .gov that are harder to register.

The many threats to payment card security, along with their expected and actual costs, are shown in **Figure 12(b)**. Face-to-face retail fraud might reasonably be seen as the weakest link in the payment card environment; the reduction in face-to-face retail fraud following the adoption of EMV supports this view. Similarly, the banks correctly anticipated that losses due to credit cards lost or stolen inside the UK (L&S in the figure) would drop once PINs were required for use. By contrast, fraud rates due to cards stolen outside the UK were lower than the banks expected. Card fraud at UK ATMs is a bit harder than retail fraud since a PIN is required. One area where the banks' expectations were not met is with ATM fraud on UK cards outside the UK. It turns out that fraudsters can easily clone stolen UK cards and use them in foreign ATMs; hence the true cost of attack is lower than expected.

The banks' losses due to card-not-present fraud were much higher than forecast; unsurprisingly, many banks have now decided to deploy readers that verify PINs in order to carry out online banking. Meanwhile, uncertainty remains regarding the attacks on PIN entry devices uncovered in [25] and [26], though it is apparent that the costs are higher than for card-not-present fraud and foreign ATM fraud.

6. Related Work

The relevance of developing quantitative models of information security has been widely recognized in accounting [6] [30], information security [10] [31], and dependable computing [32]-[35]. Of this and subsequent

[5]Unfortunately, card readers used to secure online banking (and potentially all card-not-present e-commerce) have also been demonstrated to be insecure CAPFC [28].

[6]We do not intend to single out Paraguay; many smaller countries have not been targeted by the rock-phish gang.

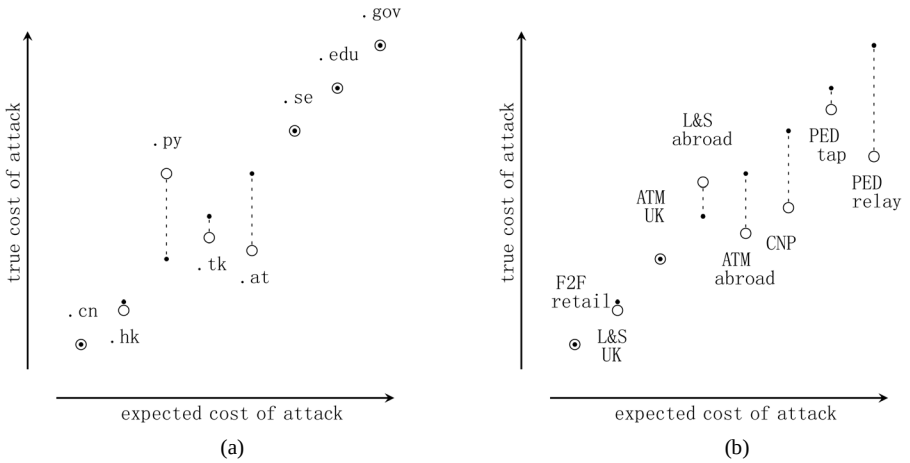

Figure 12. Hypothetical attack profiles (derived ex post from predictions and actual attacks). (a) Rock-phish domain costs; (b) EMV attack costs.

literature, we briefly describe several works with similarities to our model.[7]

Gordon *et al.*'s "wait-and-see approach" comes closest to our mode l [30] [39]. The authors explain deferred security spending in the framework of real option theory and conclude that "it is economically rational to initially invest a portion of the information security budget and defer remaining investments until security breaches actually occur". Similar to our argument, Gordon *et al.* [30] name uncertainty about the attack surface as main reason why one should "expect organizations to use security breaches as a critical determinant of their actual […] expenditures on information security." In this sense, our model can be regarded as a substantial extension of the two-period case study they discuss. Gordon *et al.*'s work differs from our approach in that they treat security spending as an allocation problem of a fixed security budget rather than seeing it as capital investment to be put into relation to the assets at risk. Also, the weakest link attacker model is unique to our work. We and Gordon *et al.* back our claims with empirical evidence. While they draw on cross-sectional survey data collected from senior information officers, we cite time series of actual attacks in Section 5 to emphasize the iterated dimension.

Herath and Herath [40] have transferred Gordon *et al.*'s [30] real option approach (ROA) to a case study of e-mail spam filtering. They compare net present values (NPV), which imply now-or-never investments, to ROA. Their results concur with our comparison between the static and dynamic solution: for their selected parameters, NPV suggests no security spending whereas ROA indicates positive returns for deferred partial security investment. Franqueira *et al.* [41] discuss a conceptual framework and tool support for implementing ROA in corporate security decision making.

Real options are in fact another tool to model uncertainty, learning, and sequential investment, so it is both plausible(and reassuring that models based on them come to similar conclusions. Both ROA and our iterated weakest link (IWL) have specific merits. While ROA is more general and builds on mainstream financial mathematics, IWL is more specific to information security and avoids the complexity of nested option contracts and abstract parameters, such as project volatility, which are difficult to interpret and even harder to estimate in practice. Both approaches are compatible, which allows a CISO to use IWL to make his decisions and express it in terms of ROA to convince his CFO.

Besides real options, the optimal timing of security investments has also been analyzed with other tools. [42] propose a graphical model for scenarios where defenders can learn from observed attacker behavior. The model shows the superiority of reactive defenses with concepts from online learning algorithms. Ogut *et al.* [43] use stochastic dynamic programming for the special case of reacting to signals from intrusion detection systems,

[7]For the sake of brevity, we do not review in detail the extensive literature explaining security underinvestment by interactions with other market players (e.g., by undersupply in a lemon market Anderson 2001 [36], moral hazard in risk sharing contracts Kunreuther 2003, market failure in residual risk transfer BS2010-WEIS [37], defense effectiveness conditional to other players' actions Varian 2004, or general externalities Bauer 2009). A trade-off between proactive and reactive measures is also studied in the literature on optimal configuration of response in intrusion detection and prevention systems Yue 2007 [38]. We deem this related, but not very relevant, due to the narrow scope of adjusting a technical decision threshold.

which are notorious for false alarms. They compare a myopic strategy, which prescribes a fixed dynamic reaction, to the optimal adaptive response. In this setting, the difficulty of finding the optimal adaptive response does not outweigh the security benefit of a fixed dynamic response. One step closer to practice, Zhu *et al*. [44] simulate reactive defense strategies based on reinforced learning algorithms for scenarios inspired by the discovery of the Heartbleed vulnerability in 2014. Kwon and Johnson [45] present the only empirical study we are aware of that specifically investigates proactive versus reactive security investment. Notably, their result contrasts the tenor of most analytical models! Proactive security investment was found to be more cost effective that reactive investment, and this effect is further amplified if indirect costs from breach disclosure are taken into account. It remains for future work to verify if these findings are due to the specific characteristics of the US healthcare sector, the subject of this study, or if they apply more broadly. In any case, it would be interesting to identify the driving factor behind this effect and tie it to the IWL model.

Recall that our model is technically not a "game", but a decision or optimization problem. Over the past couple of years, information security has become a rich application area for game theory [46]. Bier *et al*. [47] use a non-cooperative game-theoretic setting to study strategic interaction between a single attacker and a defender who optimizes the allocation of defenses to multiple targets (two in their formal model). Unlike in our model, only a single period is modeled; the model is designed to capture terrorism threats. Uncertainty of the defender is a common element in both models, in which the defender has to cope with uncertainty about an assumed hidden preference of the attacker to target a particular target. If our notion of asset is interpreted as a distributed system in which each target potentially gives the attacker access to the entire system (similar to our case study in Section 5.1), then targets can be interpreted as threats and (hidden) attack costs as preferences. A topic that has no counterpart to our work is Bier *et al*.'s reference to signaling theory to study whether the defense configuration should be kept secret or made public. The model by Cremonini and Nizovtsev [48] explains security investment decisions with uncertainty of the attacker. They too draw on signaling theory and conclude that a defense is good enough if, and only if, it looks strong enough to divert the attackers' attention towards other, seemingly weaker targets. In this sense, their work can be regarded as a kind of mirror image to our work, which deals with the uncertainty on the defender's side. Finally, Dijk *et al*. [49] have devised a continuous-time dynamic game of attacker-defender interaction, which increasingly attracts the attention of security researchers interested in game theory. Unlike in our setup, the game does not capture security investment in a narrow sense, but models the timing of cleanup operations. As it is formulated as a strategic game rather than an inter-temporal optimization problem against a probabilistic attacker, it becomes very hard to find stable equilibria for realistic strategy spaces. So far, we are only aware of partial solutions that are difficult to interpret in practice.

This article is an extended and updated version of our workshop version [50]. As a follow-up, [51] have studied a variant of this model which allows the defender to commission penetration tests that might reveal the next weakest link without risking the consequences of a successful attack.

7. Summary and Possible Extensions

We have presented an economic model that explains why and under which conditions under-investment in security can be rational, even against known threats for which defenses exist. Under-investment might reasonably occur when a) reactive investment is possible, b) uncertainty exists about the attacker's relative capability to exploit different threats, c) successful attacks are not catastrophic, and d) the costs to upgrade the defense configuration are largely recoverable.

Unlike in other work explaining security under-investment with market failures, the ingredients to our model solely draw on the relation between defender and attacker, and do not involve actions of other market participants. Our results do not contradict or invalidate the well-known explanations of market failure. It rather complements the picture and highlights that market failure is a sufficient, but not always necessary, cause for security under-investment.

We believe that an iterated weakest link model accurately captures the challenges facing many information security threats today. We discussed two timely examples in the article. First, miscreants committing high-volume online crime exploit the Internet's global, distributed architecture by compromising insecure machines and defrauding uninformed registrars, wherever they are located. Second, the security of payment cards has evolved over time by reacting to fraudster's actions. Empirical data on losses show how the introduction of

EMV in the UK has simply diverted attacker strategy to other methods, notably card-not-present and foreign ATM fraud.

As with any stylized model, ideas for extensions are abundant and implementation should be guided by the principle of parsimony, especially in the absence of reliable data to validate model assumptions. Nevertheless, a handful of extensions appear reasonable to make the model more applicable. One is to let the cost of attacks decrease over time to reflect learning and the creation of automated tools. Another direction could be to allow more ways for reducing uncertainty. This can be done either by including information gathering as an option for security investment (e.g., penetration testing or information sharing), or by relaxing the independence assumption between the stochastic realizations of the attack profile. The latter would allow the defender to infer knowledge about the probability of other threats from observed attacks, a phenomenon exploited by some technical early warning systems. If updates cause substantial unrecoverable costs, this opens new strategies of bundled investment in new defenses to better amortize the cost. Lastly, it may be of—at least academic—interest to consider other attack strategies. For example, attackers might not choose the weakest link to confuse the defender and trigger misallocations of security spending. Anecdotal evidence for such behavior can be found in the actions of some spammers, who send waves of messages with no other apparent purpose than to wear out self-learning spam filters.

One key future challenge is to find a case study where enough information is available to calibrate the model to empirical data. More generally, it may be worthwhile to explore further the question of when to deal with a problem. When is it better to move first and take proactive measures, and when is it better to defer and respond to other's actions?

Acknowledgements

We thank Chad Heitzenrater, the anonymous reviewers and participants of the 2009 Workshop on the Economics of Information Security (WEIS), and the anonymous reviewers of this special issue on Cybersecurity Investment for valuable comments and suggestions on earlier versions of this paper. All errors and omissions are the authors'.

References

[1] Anderson, R. and Moore, T. (2006) The Economics of Information Security. *Science*, **314**, 610-613. http://dx.doi.org/10.1126/science.1130992

[2] Varian, H.R. (2004) System Reliability and Free Riding. In: Camp, L.J. and Lewis, S., Eds., *Economics of Information Security*, Springer Verlag, New York, 1-15. http://dx.doi.org/10.1007/1-4020-8090-5_1

[3] Kunreuther, H. and Heal, G. (2003) Interdependent Security. *Journal of Risk and Uncertainty*, **26**, 231-249. http://dx.doi.org/10.1023/A:1024119208153

[4] Bauer, J.M. and van Eeten, M. (2009) Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options. *Telecommunications Policy*, **33**, 706-719. http://dx.doi.org/10.1016/j.telpol.2009.09.001

[5] Böhme, R. and Moore, T. (2010) The Iterated Weakest Link. *IEEE Security & Privacy*, **8**, 53-55. http://dx.doi.org/10.1109/MSP.2010.51

[6] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. http://dx.doi.org/10.1145/581271.581274

[7] Collins, M., Gates, C. and Kataria, G. (2006) A Model for Opportunistic Network Exploits: The Case of P2P Worms. Proc. of Workshop on the Economics of Information Security (WEIS), Cambridge, 26-28 June 2006. http://weis2006.econinfosec.org/docs/30.pdf

[8] Major, J.A. (2002) Advanced Techniques for Modelling Terrorism Risk. *Journal of Risk Finance*, **4**, 15-24. http://dx.doi.org/10.1108/eb022950

[9] Thomas, K., Huang, D.Y., Wang, D., Bursztein, E., Grier, C., Holt, T.J., *et al*. (2015) Framing Dependencies Introduced by Underground Commoditization. *Workshop on the Economics of Information Security* (*WEIS*), Delft, 22-23 June 2015.

[10] Hoo, K.J.S. (2002) How Much Is Enough? A Risk-Management Approach to Computer Security. *Workshop on Economics and Information Security* (*WEIS*), Berkeley, 16-17 May 2002. http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/

[11] Purser, S.A. (2004) Improving the ROI of the Security Management Process. *Computers & Security*, **23**, 542-546.

http://dx.doi.org/10.1016/j.cose.2004.09.004

[12] Gal-Or, E. and Ghose, A. (2005) The Economic Incentives for Sharing Security Information. *Information Systems Research*, **16**, 186-208. http://dx.doi.org/10.1287/isre.1050.0053

[13] Laube, S. and Böhme, R. (2015) Mandatory Security Information Sharing with Authorities: Implications on Investments in Internal Controls. 2*nd ACM Workshop on Information Sharing and Collaborative Security*, Denver, 12-16 October 2015, 31-42. http://dx.doi.org/10.1145/2808128.2808132

[14] The Economist (2007) A Walk on the Dark Side. http://www.economist.com/displayStory.cfm?story_id=9723768

[15] Krebs, B. (2008) Major Source of Online Scams and Spams Knocked Offline. Washington Post, 11 November 2008. http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html

[16] Krebs, B. (2008) EstDomains: A Sordid History and a Storied CEO. Washington Post, 8 September 2008. http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html

[17] ICANN (2008) Termination of Registrar EstDomains to Go Ahead. http://www.icann.org/en/announcementsannouncement-12nov08-en.htm

[18] Moore, T. and Clayton, R. (2007) Examining the Impact of Website Take-Down on Phishing. *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, Pittsburgh, 4-5 October 2007, 1-13. http://www.cl.cam.ac.uk/~rnc1/ecrime07.pdf http://dx.doi.org/10.1145/1299015.1299016

[19] Day, O., Palmen, B. and Greenstadt, R. (2008) Reinterpreting the Disclosure Debate for Web Infections. In: Johnson, M.E., Ed., *Managing Information Risk and the Economics of Security*, Springer, New York, 179-197.

[20] Liu, H., Levchenko, K., Félegyházi, M., Kreibich, C., Maier, G., Voelker, G.M. and Savage, S. (2011) On the Effects of Registrar-Level Intervention. *Proceedings of the 4th USENIX Conference on Large-Scale Exploits and Emergent Threats*, *LEET*'11, Berkeley, 5.

[21] McCoy, D., Dharmdasani, H., Kreibich, C., Voelker, G.M. and Savage, S. (2012) Priceless: The Role of Payments in Abuse-Advertised Goods. *Proceedings of the* 2012 *ACM Conference on Computer and Communications Security*, *CCS*'12, Raleigh, 16-18 October 2012, 845-856. http://dx.doi.org/10.1145/2382196.2382285

[22] APACS (2007) 2007 UK Chip and PIN Report. http://cryptome.org/UK-Chip-PIN-07.pdf

[23] The UK Cards Association. Card Fraud Figures. Retrieved on 29 December 2015. http://www.theukcardsassociation.org.uk/plastic_fraud_figures/

[24] LLC EMVCo. EMV 4.1, June 2004. http://www.emvco.com

[25] Drimer, S. and Murdoch, S.J. (2007) Keep Your Enemies Close: Distance Bounding against Smartcard Relay Attacks. *Proceedings of* 16*th USENIX Security Symposium*, Boston, 6-10 August 2007, Article No. 7.

[26] Drimer, S., Murdoch, S.J. and Anderson, R. (2008) Thinking Inside the Box: System-Level Failures of Tamper Proofing. *IEEE Symposium on Security & Privacy*, Oakland, 18-22 May 2008, 281-295. http://dx.doi.org/10.1109/sp.2008.16

[27] Murdoch, S.J., Drimer, S., Anderson, R. and Bond, M. (2010) Chip and PIN Is Broken. 2010 *IEEE Symposium on Security and Privacy* (*SP*), Oakland, 16-19 May 2010, 433-446. http://dx.doi.org/10.1109/sp.2010.33

[28] Drimer, S., Murdoch, S.J. and Anderson, R. (2009) Optimised to Fail: Card Readers for Online Banking. In: Dingledine, R. and Golle, P., Eds., *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, Vol. 5628, Springer, Berlin, 184-200. http://dx.doi.org/10.1007/978-3-642-03549-4_11

[29] Spamhaus (2007) Report on the Criminal "Rock Phish" Domains Registered at Nic.at (Press Release). http://www.spamhaus.org/organization/statement.lasso?ref=7

[30] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) Information Security Expenditures and Real Options: A Wait-and-See Approach. *Computer Security Journal*, **14**, 1-7.

[31] Schechter, S.E. (2005) Toward Econometric Models of the Security Risk from Remote Attacks. *IEEE Security and Privacy*, **3**, 40-44. http://dx.doi.org/10.1109/MSP.2005.30

[32] Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., *et al*. (1994) Towards Operational Measures of Computer Security. *Journal of Computer Security*, **2**, 211-229.

[33] Jonsson, E. and Andersson, M. (1996) On the Quantitative Assessment of Behavioural Security. In: Pieprzyk, J. and Seberry, J., Eds., *Information Security and Privacy*, Lecture Notes in Computer Science, Vol. 1172, Springer-Verlag, Berlin, 228-241. http://dx.doi.org/10.1007/bfb0023302

[34] Jonsson, E. and Olovsson, T. (1997) A Quantitative Model of the Security Intrusion Process Based on Attacker Behaviour. *IEEE Transactions on Software Engineering*, **23**, 235-245. http://dx.doi.org/10.1109/32.588541

[35] Avižienis, A., Laprie, J.-C., Randell, B. and Landwehr, C. (2004) Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, **1**, 11-33. http://dx.doi.org/10.1109/TDSC.2004.2

[36] Anderson, R. (2001) Why Information Security Is Hard—An Economic Perspective. *Annual Computer Security Applications Conference* (*ACSAC*), New Orleans, 10-14 December 2001, 358-365. http://www.cl.cam.ac.uk/~rja14/econsec.html http://dx.doi.org/10.1109/acsac.2001.991552

[37] Böhme, R. and Schwartz, G. (2010) Modeling Cyber-Insurance: Towards a Unifying Framework. *Workshop on the Economics of Information Security* (*WEIS*), Harvard University, Cambridge, 7-8 June 2010.

[38] Yue, W.T. and Çakanyildirim, M. (2007) Intrusion Prevention in Information Systems: Reactive and Proactive Responses. *Journal of Management Information Systems*, **24**, 329-353. http://dx.doi.org/10.2753/MIS0742-1222240110

[39] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective. *Journal of Accounting and Public Policy*, **34**, 509-519. http://dx.doi.org/10.1016/j.jaccpubpol.2015.05.001

[40] Herath, H.S.B. and Herath, T.C. (2008) Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems*, **25**, 337-375. http://dx.doi.org/10.2753/MIS0742-1222250310

[41] Franqueira, V.N.L., Houmb, S.H. and Daneva, M. (2010) Using Real Option Thinking to Improve Decision Making in Security Investment. In: Meersman, R., Dillon, T.S. and Herrero, P., Eds., *On the Move to Meaningful Internet Systems*: *OTM*, Lecture Notes in Computer Science, Vol. 6426, Springer, Berlin, 619-638. http://dx.doi.org/10.1007/978-3-642-16934-2_46

[42] Barth, A., Rubinstein, B.I.P., Sundararajan, M., Mitchell, J.C., Song, D. and Bartlettm, P.L. (2010) A Learning-Based Approach to Reactive Security. In: Radu, S., Ed., *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, Vol. 6052, Springer, Berlin, 192-206. http://dx.doi.org/10.1007/978-3-642-14577-3_16

[43] Ogut, H., Cavusoglu, H. and Raghunathan, S. (2008) Intrusion Detection Policies for It Security Breaches. *INFORMS Journal on Computing*, **20**, 112-123. http://dx.doi.org/10.1287/ijoc.1070.0222

[44] Zhu, M., Hu, Z. and Liu, P. (2014) Reinforcement Learning Algorithms for Adaptive Cyber Defense against Heartbleed. *Proceedings of the* 1*st ACM Workshop on Moving Target Defense*, Scottsdale, 3-7 November 2014, 51-58. http://dx.doi.org/10.1145/2663474.2663481

[45] Kwon, J. and Johnson, M.E. (2014) Proactive versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, **38**, 451-471.

[46] Manshaei, M.H., Zhu, Q., Alpcan, T., Basar, T. and Hubeaux, J.-P. (2013) Game Theory Meets Network Security and Privacy. *ACM Computing Surveys*, **45**, Article No. 25. http://dx.doi.org/10.1145/2480741.2480742

[47] Bier, V., Oliveros, S. and Samuelson, L. (2007) Choosing What to Protect: Strategic Defensive Allocation against an Unknown Attacker. *Journal of Public Economic Theory*, **9**, 563-587. http://dx.doi.org/10.1111/j.1467-9779.2007.00320.x

[48] Cremonini, M. and Nizovtsev, D. (2006) Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. *Workshop on the Economics of Information Security* (*WEIS*), Robinson College, University of Cambridge, 26-28 June 2006. http://weis2006.econinfosec.org/docs/3.pdf

[49] van Dijk, M., Juels, A., Oprea, A. and Rivest, R.L. (2013) FlipIt: The Game of "Stealthy Takeover". *Journal of Cryptology*, **26**, 655-713. http://dx.doi.org/10.1007/s00145-012-9134-5

[50] Böhme, R. and Moore, T. (2009) The Iterated Weakest Link: A Model of Adaptive Security Investment. *Workshop on the Economics of Information Security* (*WEIS*), University College London, 24-25 June 2009. http://weis09.infosecon.net/files/152/paper152.pdf

[51] Böhme, R. and Félegyházi, M. (2010) Optimal Information Security Investment with Penetration Testing. In: Alpcan, T., Buttyán, L. and Baras, J.S., Eds., *Decision and Game Theory for Security*, Lecture Notes in Computer Science, Vol. 6442, Springer, Berlin, 21-37. http://dx.doi.org/10.1007/978-3-642-17197-0_2