Title

Cyber-Insurance for Cyber-Physical Systems

ISBN

9781538676981

Authors

Barreto, Carlos
Cardenas, Alvaro A
Schwartz, Galina

Publication Date

2018-08-21

DOI

10.1109/ccta.2018.8511535

Peer reviewed

2018 IEEE Conference on Control Technology and Applications (CCTA)
Copenhagen, Denmark, August 21-24, 2018

Cyber-Insurance for Cyber-Physical Systems

Carlos Barreto, Alvaro A. Cardenas, and Galina Schwartz

Abstract— **In this paper we review the emerging role of cyber insurance for Cyber-Physical Systems (CPSs) and discuss the obstacles, the needs, and the avenues forward. Specifically we focus on the unique characteristics and challenges that cyber-physical systems provide to the cyber-insurance industry (compared to classical information technology risks) and show how they change the incentives for security investments.**

I. Introduction

While investing in security protections is a challenge for most industries, there is a difference between industries that use conventional Information Technology (IT) systems and industries that work with CPS. Companies that use traditional IT (e.g., have a web-presence, or handle any financial transaction) are constantly targeted by increasingly sophisticated and well-organized criminal groups. For IT companies, cyber threats are recurrent events, so they constantly upgrade and improve the security of their systems to minimize losses. Disclosure of these attacks to the general public was facilitated by data protection laws enacted in several countries.

On the other hand, *most* industries in the CPS domain have rarely seen attacks sabotaging their physical process. While there have been attacks with the potential of causing catastrophic physical damage (e.g., Stuxnet [1], the attacks against the power grid in Ukraine [2], and the Triton malware attacking safety systems in the Middle East [3]), attacks with physical-world consequences are still rare, in part because they are hard to monetize by attackers.

In addition to being rare, attacks too CPS are not openly reported. This lack of actuarial data leads to low quality risk estimates; as the U.S. Department of Energy (DoE) stated in their Energy Delivery Systems Cyber Security Roadmap [4], "Making a strong business case for cyber security investments is complicated by the difficulty of quantifying risk in an environment of (1) rapidly changing, (2) unpredictable threats (3) with consequences that are hard to demonstrate."

Therefore, market incentives alone are insufficient to improve the security posture firms, and as a result, our CPS infrastructures remain fairly vulnerable to computer attacks and with technology that is decades behind the current security best practices used in enterprise IT domains. This market failure for improving the security of CPS has resulted in several calls for government intervention [5], [6], [7]

Instead of asking companies to follow specific standards, governments would demand firms to have cyber-insurance for their operations [8], [9], [10]. There is a popular view that under certain conditions, the insurance industry can incentivize investments in protection [11]. In particular, premiums would reflect the cyber security posture of CPS companies; if a company follows good cyber security practices, the insurance premiums would be low, otherwise, the premiums would be high (and this would in principle incentivize the company to invest more in cyber-security protections).

The purpose of this paper is twofold. On one hand, present a survey of mechanisms to manage risks, in particular, the risk of events with catastrophic consequences. On the other hand, we investigate how cyber insurance affects the protection of CPS against cyber threats. In a numerical case-study, we show how the self-interest of firms leads to low protection (low security investments), which in turn generate losses to society as a whole. We also find that with an active insurance market, firms will improve their profit; however, they will invest less in protection. To solve this problem, we show how asking operators for full liability for losses caused by cyber-attacks improves the security of CPS (operators will invest more in security protections). This shows that governments and regulatory bodies need to be careful in their design of insurance requirements.

The paper is organized as follows. In Section II, we discuss the problem of improving protections of CPS as a socially desirable problem and how insurance can help. In Section III we illustrate some of the main results from the theory of extreme events and how other industries have dealt with them. We present in Section IV an experiment of the impact of insurance in the security investment of CPS firms. In Section V we discuss further challenges and open problems for risk assessment and insurance for CPS, and in Section VI we conclude the paper.

II. Investments in Cyber Security and the role of Cyber Insurance

In decision theory, it is assumed that firms make decisions to maximize their expected utility. However, firms must cope with uncertain events (or risks), such as potential losses caused by cyber-attacks. For example, if we assume a Bernoulli risk distribution, a successful attack against a firm occurs with probability p and causes damage L; similarly, the attack fails with probability $(1-p)$. The risk under these conditions is $E[L] = p\,L$.

Common ways to manage risks include *risk reduction* (e.g., avoidance or mitigation) and *risk transfer* (e.g., insurance). A risk reduction strategy consists in procuring protections to reduce the probability of successful attacks, e.g., investing e resources in protection to reduce the probability of successful

C. Barreto, and A. A. Cardenas are with the Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA. email: carlos.barretosuarez, alvaro.cardenas@utdallas.edu.

G. Schwartz is with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley. email: schwartz@eecs.berkeley.edu.

attacks to $p_e \leq p$. A rational agent will invest in cyber-security protections as long as $p_e\, L + e < p\, L$.

On the other hand, firms can reduce their uncertainties transferring the risk through an insurance policy. In this case, the risk (expected loss) of the firm becomes $p(L - I) + P$ where I is an indemnity and P is a premium (payment to the insurance company). The premium that insurance industries compute is a measure of risk, which individuals, industries, and governments can use to make decisions (e.g., decide whether to start a business or move to a hurricane prone area). Therefore, insurance is seen as an essential tool for protecting societies against risk, and particularly, extreme events. Without insurance, nations would suffer larger material and non material losses [12].

A. Risk Reduction + Risk Transfer

Ehrlich and Becker [11] discuss the relationship between risk reduction and risk transfer. They find that insurance and self-protection are complements when investments in self-protection reduce the premium.[1] That is, with insurance we can incentivize investments in risk mitigation (protection), and transfer the remainder risk to a third party simultaneously.

The promise of insurance for managing the risks to cyber-events in classical IT systems has led to a growing interest on cyber-insurance [13], [14]. The cyber insurance market collected globally $\$75$ bn in premiums during 2015 [15], and while the cyber insurance market is small compared with the commercial insurance market, (which has $\$1.1$ trn in the U.S. alone [16]), it is expected to keep growing, since cyber crime has become more relevant in recent years.[2]

Cyber-insurance for CPS on the other hand is still in the future. Attacks to CPS with real physical world consequences are rare, therefore, insurers have insufficient information to estimate these risks (and the risk reduction resulting from investments in prevention). The classical insurance industry (e.g., health insurance or vehicle insurance) has achieved good risk estimates based on their access to large historical datasets of events, where they can identify the prevalence of certain types of accidents or risky human behavior. But these do not exist in CPS yet.

Besides inaccurate risk estimations, cyber threats on CPS also expose the insurer to *long tail risks* (events with low frequency and high cost, such as a blackout in the power grid). When these long tail risks reach unexpected high levels, they are called *extreme events*. By their nature, extreme events result in a *contagion effect* that affect other industries.

Therefore we need to start developing the theory and background necessary to discuss cyber-insurance for CPS, and we cannot think of insuring without clearly understanding the thresholds of indemnity that insurance companies will use to declare uninsurable events. To properly understand these problems we need to look at the theory of extreme events and at how other industries have dealt with them.

[1] Additionally, the probability of losses must be high enough (greater than $1/2$ for quadratic utility functions).

[2] For instance, the respondents of the survey [17] estimate that the probability of having losses in information assets is larger than in material assets (2.5% and 0.5% for maximum losses in each case).

III. Extreme Events

Extreme events are difficult to predict long time ahead and their impact can exceed the capabilities of the (re)insurer, leading to insolvencies [18]. For instance, events like Hurricane Katrina in 2005, the Fukushima Daiichi disaster in 2011, or terrorist actions, such as $9/11$, classify as extreme events because they reached unprecedented impacts and had repercussions in the international economy [19].

It is rational from a profit maximizing point of view to ignore extreme events. Effectively, extreme events are frequently explicitly excluded from insurance contracts. For example, earthquakes above certain Richter scale are excluded. For CPS security however there is not a clear cut way to exclude these events yet.

Below we introduce models used to estimate the risk of extreme events and mechanisms to deal with them. We focus on mechanisms used to protect against terrorist attacks, which unlike other risks, occur because of intelligent adversaries, rather than random events. These mechanisms can offer some guidelines to deal with attacks on CPS.

A. Modeling extreme events

The traditional statistical analysis based on Gaussian approximations is inappropriate to model extreme events, because some extreme events (in natural and social phenomena) follow power laws [20] and might have infinite variance (extreme events are capable of *black swan* behavior [21]). On the contrary, the analysis of extreme events focuses on characterizing the extremes (or tail of the distribution) rather than the mean, because losses of extreme events have more importance than the losses of smaller but frequent events.

Extreme value theory (EVT) is devoted to the analysis of extreme events with little information, such as natural catastrophes (e.g., windstorms, earthquakes, tsunamis, and volcanic eruptions), man made catastrophes (e.g., aviation crashes, explosions, terrorist acts, marine disasters), and financial events (e.g., sudden changes in the stock market) [22]. EVT is supported by a strong theoretical background, and in general, it is the best we can do with limited data [23], [24].

Some of the most important results in EVT are analogous to the central *limit theorem*, which states that the sum of iid samples have a distribution that converges to a Gaussian distribution as the number of samples increase. Similarly, EVT predicts that the distribution of extreme events (their tails more precisely) converge to a family of functions (see Table I). Below we show some of the main results of EVT, and refer the interested reader to [25], [26].

1) Generalized extreme value distribution: Suppose that we have a sequence of random variables $I_1, I_2, \ldots$ with an unknown distribution $G(x) = \mathbb{P}[I_i \leq x]$ (here I_i might represent losses or insurance claims. Let

$$M_n = \max_i \{I_1, \ldots, I_n\}$$

be the maximum among the n first observations. Furthermore, let us define the normalized maximum as $\frac{M_n - b_n}{a_n}$, where b_n

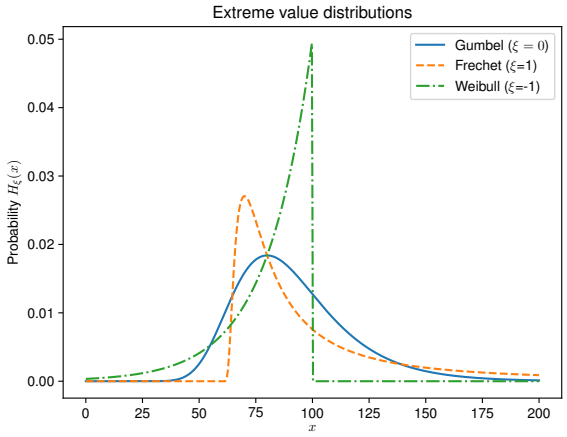


Fig. 1: Examples of the families of extreme value distributions.

and a_n determine the location and scale of the distribution. The Fisher-Tippett Theorem [27] states that if the distribution of a normalized maximum converges, then the limit belongs to the family extreme value distributions H_ξ, with some parameter ξ. That is,

$$G_{max}(a_n x + b_n) = P\left[\frac{M_n - b_n}{a_n} \leq x\right] \rightarrow H_\xi(x)$$

as $n \rightarrow \infty$. The family of *extreme value distributions* is defined as

$$H_\xi(x) = \begin{cases} \exp(-(1+\xi x)^{-1/\xi}) & \text{if } \xi \neq 0, \\ \exp(-e^{-x}) & \text{if } \xi = 0, \end{cases}$$

where ξ is the shape parameter of the distribution and x satisfies $1+\xi x > 0$. We can extend the family of distributions as $G_{max}(x) = H_\xi(\frac{x-\mu}{\sigma})$, which represents a distribution with location μ and scale σ.

We can classify the extreme value distributions in three subfamilies. I) If $\xi = 0$, then H_ξ belongs to the Gumbel family, which have medium tails. This distributions have a unlimited domain. II) If $\xi > 0$ then H_ξ belongs to the Fréchet family, which have heavy tails (its tail resembles a power law). The distributions in this sub family have a lower limit. III) If $\xi < 0$, then H_ξ belongs to the Weibull family, which have a short tail with an upper limit. Fig. 1 shows some examples of each family with $\mu = 80$ and $\sigma = 20$.

2) Generalized Pareto distribution (GPD): The GPD is another distribution of extreme events that describes observations exceeding a high threshold u. The probability that an event surpasses the threshold u is

$$G_u(x) = P\left[X - u \leq x | X > u\right] = \frac{G(x+u) - G(u)}{1 - G(u)}. \quad (1)$$

The Pickands-Balkema-de Haan Theorem [28], [29] states that G_u converges to a GPD as the threshold u increases. The GPD is defined as

$$G_{\xi,u,\sigma}(x) = \begin{cases} 1 - (1 + \frac{\xi x}{\sigma})^{-1/\xi} & \text{if } \xi \neq 0, \\ 1 - \exp(-\frac{x}{\sigma}) & \text{if } \xi = 0, \end{cases}$$

TABLE I: Statistical principles analogous to the central limit theorem used in extreme value theory.

Fisher-Tippet Theorem.	The distribution of extreme events (if it exists) converges to the extreme value distribution.
Pickands-Balkema-de Haan Theorem.	The tail of a distribution converges to the generalized Pareto distribution.

where $x \geq u$ and ξ and σ determine the shape and scale, respectively. This result suggest that we can use the GPD to model the tail of distributions, that is, the probability that an event exceeding u occurs. In such case we can fit the GPD to the data that exceeds the threshold u using some method like *maximum likelihood estimation* or *probability weighted moments*. From Eq. (1) we can approximate the loss distribution G for $y > u$ as

$$\hat{G}(y) = (1 - G_n(u))G_{\xi,u,\sigma}(y) + G_n(u)$$

where $G_n(u)$ is the empirical distribution evaluated at u.

Estimations of extreme events involve some level of judgment to select the threshold u because there is a trade-off between quality of the approximation and its bias. With less data the approximation will be less biased, but its quality will also deteriorate [25].

3) Catastrophe (CAT) models: We can enrich the data with hypothetical losses to observe the effect of unobserved adverse effects. For example, catastrophe models provide estimations of the cost of real or hypothetical catastrophes. These models are more complex than statistical models because they consider previous events, geographical information, and data about the infrastructures to emulate the damage of hazardous events [30]. Although the predictions tend to underestimate the losses of extreme events, these models are useful to generate data and overcome the lack of data from real events [25].

B. How can we manage extreme risks?

There are two main postures regarding the role of insurance in the management of extreme events [31]. On one hand, some authors believe that the insurance industry will be able to deal with the risk of extreme events. Private insurers have tried to use the international reinsurance market[3] and capital markets to diversify the risk of catastrophic risks [32], [33]. Particularly, the insurers transform their risk into *securities*, which are traded in capital markets. This has been used for natural catastrophes such as hurricanes, windstorms, and earthquakes [34].

On the other hand, some authors believe that, since losses of catastrophic events are highly correlated, they should be handled with social insurance (e.g., with assistance of the government).[4] Moreover, Ulrich Beck [35] argues that the modern risks, such as nuclear accidents, global warming,

[3] Reinsurance is the main mechanism to diversify catastrophe risk (40-50% of catastrophe losses in the U.S. are covered by reinsurance).

[4] For example, terrorism depends on the government's actions and has similarities with war, which is not insurable [31].

and terrorism are product of the human activity and are characterized by *radical uncertainty*, that is, we cannot deal with them through statistical analysis [36]. Such risks are beyond territory, time, and societies and the responsibility of their consequences are difficult to asses [35]. This theory is appealing due to the increasing frequency and impact of catastrophes, as well as the emergence of new forms of catastrophes, e.g., cyber risk.

Despite the characteristics of the new risks, the insurance industry has managed to insure against extreme events, such as terrorism (although governments usually act as insurers of last resort). However, the mechanisms to securitize the insurer's risk are in its infancy and their viability remains uncertain [22]. Below we describe some mechanisms to transfer and mitigate the risk of extreme events.

1) Risk-linked securities: CAT bonds are risk-linked securities, with payments made when some event occur, such as hurricanes or earthquakes. They work as follows: an insurer issues bonds that are sold through a reinsurer to the investors of the capital market. If no event occurs, the investors get a return (interest) for their investment. However, if a catastrophe occurs the loan is forgiven and the insurance company uses the collected capital to pay claims of the catastrophe (which cannot be covered only with premiums). The main advantage for the insurance company is to pass the risk to other agent and guarantee solvency in case of an accident. Furthermore, cat bonds are attractive investments to diversify because they avoid credit risks (risk that the loan is not paid) and have a low correlation with the market investment returns [18].

2) Proactive risk management: Firms and regulators seem to wait until accidents occur before they take action for managing risks of catastrophic events (because these events apparently are unimaginable or unlikely); however, there are signals that can alert about the risks of catastrophic events. For instance, although the 9/11 attacks are considered to be unpredictable, there where previous attempts of using airplanes in attacks [19]. Also, the tsunami risk of the Fukushima Daiichi nuclear plant was recognized (before the accident in 2011) through simulations that used updated estimations of threats. Furthermore, before the Fukushima accident other nuclear plants suffered floods, such as the Blayais Nuclear Plant in France in 1999 and the Madras Atomic Power Station in India in 2004 [37]. Although signals are easier to identify after the events, the previous examples show the importance of reevaluating risk management based on the evolution of both threats and best practices. Particularly, Paté-Cornell [19] highlights the importance of considering the risk of events that haven't happened yet and update their likelihood based on degrees of belief.

C. Insurance for terrorism

Perhaps the industry that is most relevant to insuring large-scale CPS, is the insurance industry focused on terrorism. Below we discuss some anecdotes and trends within this industry.

The terrorist attacks (truck bomb) by the Irish Republican Army (IRA) on Bishopsgate (London's financial district) in 1993 had a cost of £350 million and caused serious losses to insurance companies. After the attack, reinsurers announced exclusions of terrorism coverage from their contracts not only due to high costs, but because of their inability to estimate the risk.[5] Excluding terrorism from coverage would have profound consequences on the nation's economy. First, direct insurers won't accept risks without reinsurance [38], which in turn would expose businesses to additional attacks. Also, without protection the value of property would decline, as well as the interest in undertaking construction projects [38].

To avoid such crisis, the insurance industry (in cooperation with the British government) implemented the Pool resinsurance company (Pool Re), in which the government supports insurers acting as *reinsurer of last resort* for losses over £75 million. The government involvement allows to spread losses in the entire population through taxes. To date, Pool Re has covered claims from thirteen terrorist incidents contributing with more than £600 million [39].

A similar strategy was adopted in other countries that suffered terrorist attacks. For instance, The 'Consorcio de Compensacioń de Seguros' (CCS) is a catastrophic risk consortium created in Spain in 1941 to cover political risks (insurance against terrorism is compulsory). Sri Lanka created a fund known as the strike riot civil commotion and terrorism fund (SRCCTF). On the other hand, France has the 'Gestion de l'Assurance et de la Réassurance des Risques Attentats et actes de Terrorisme' (GAREAT) pool for terrorism risk. It was created after the attacks on 9/11 (again, having insurance against terrorism is compulsory).

Before $9/11$ the estimated probability of attacks on U.S. soil was close to zero, because from 1991-1998 the attacks on the U.S. were only 1% of attacks in the world. However, the attacks on $9/11$ unleashed a crisis in the insurance industry, because the attack occurred on U.S. soil and the insured losses amounted to $\$40 - \$70$ bn. After 9/11 reinsurers ceased terrorism coverage and insurers were reluctant to cover terrorism without federal assistance, which motivated the participation of the government as reinsurer of last resort through the Terrorism Risk Insurance Act (TRIA). The TRIA supports insurance claims caused by acts of terrorism. The total cap of federal coverage is $100 bn per year [40], [41]. Unlike Pool Re, the TRIA is mandatory and determines the government's payment once the attack took place. Table II shows a comparison between Pool Re and TRIA.

TABLE II: Characteristics of government reinsurance for terrorism.

	Pool Re	TRIA
Membership	Optional	Mandatory
Collect funds	Ex-ante	Ex-post
Premium	Based on risk	Based on total claims

[5] Unlike natural events, it is difficult to asses the frequency or the impact of terrorism because these acts are carried out intentionally.

D. Summary and Insights

We have discussed ways to model and quantify extreme risks, such as EVT, GPD and CAT models. We also introduced a variety of tools to manage risks, such as reinsurance markets, securities, risk-linked securities, and proactive risk management. Finally, we have summarized how the insurance industry dealt with catastrophic events arising from terrorism. One particular interesting point to take is that in several of these cases we need the government's intervention, like the TRIA act for terrorism in the U.S. Without it, the insurance market for terrorism could have collapsed. Therefore, the government may have to eventually play a similar role for nurturing a cyber-insurance market for protecting critical infrastructures such as the power grid from cyber-attacks.

IV. Experiment

In this example we illustrate how cyber insurance can affect investments in security protection. We assume that the insurer can estimate the risks accurately. As discussed before, most of the firms operating CPS have limited liability in case of a catastrophic attack, that is they do not bear the total damage caused to others.

We define the firm's utility function as

$$U(x) = 1 - e^{-ax},$$

where x is a real number and $a = 0.01$. The following parameters determine the wealth of the firm: i) the initial wealth $w_0 = 200$, ii) the losses, represented with the random variable L; and iii) the cost of protecting the system, denoted $C(z) = k_c z^\eta$, where $z \in [0, 1]$ is the degree of protection, $k_c = 50$, and and $\eta = 1.5$.

Here we model the losses of a firm L with a GEV distribution with parameters $\mu = 80$, $\sigma = 20$, and $\xi \in [0, 1]$. Hence, L has cdf

$$\mathbb{P}[L \leq x|\xi(z)] = G(x, \xi(z)) = H_{\xi(z)}\left(\frac{x-\mu}{\sigma}\right),$$

which depends on the shape parameter $\xi(z)$. For simplicity we assume that the shape parameter ξ changes linearly with the protection level z, i.e., $\xi(z) = 1 - z$, where $z \in [0, 1]$. Therefore, investments in security reduce the likelihood of extreme losses.

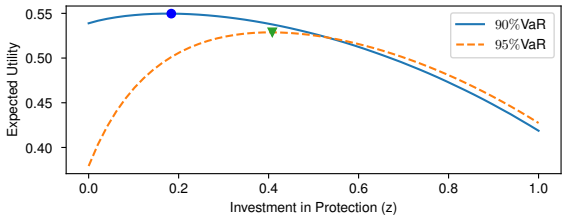
With the previous considerations the expected utility of the firm is

$$\mathrm{E}[U(w_0 - C(z) - L)] = \int_0^{Q_\alpha} U(w_0 - C(z) - x) dG(x, \xi(z)),$$

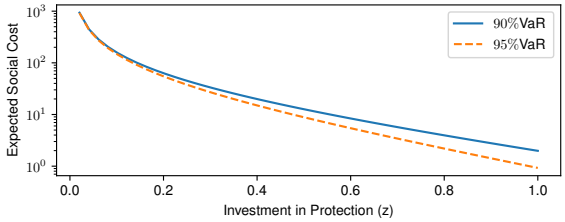
where Q_α is the maximum loss contemplated in the risk analysis. Here we assume that the firm uses *value-at-risk* (VaR) as the risk metric; hence, the firm discards extreme losses that occur with low probability. The maximum loss considered by the firm, Q_α, is defined as the $\alpha\%$ quantile of the loss distribution, that is,

$$\mathbb{P}[L \geq Q_\alpha|\xi(z)] = 1 - \alpha,$$

where α is the precision of the risk metric.



(a) Expected utility of the firm with different risk measures.



(b) Expected social cost (losses not covered by the firm).

Fig. 2: Expected utility of a firm and the social cost when a firm ignores the tail of the distribution. The firm invests more in protection and reduces the social cost when the risk measure α-VaR has large precision α.

A firm with $\alpha\%$-VaR might cover the losses up to Q_α; however, losses exceeding Q_α are imposed on third parties[6] who pay for the damage either by bearing the losses or by paying bail outs. In this case we define the social cost L_s as the expected losses not paid by the firm

$$L_s(z) = \int_{Q_\alpha}^{\infty} (x - Q_\alpha) dG(x, \xi(z)).$$

Fig. 2a shows the expected utility of a firm that ignores the tail of the distribution and Fig. 2b shows the social costs as a function of the investment z. Here, with lower $\alpha\%$-VaR the firm increases its profit by investing less in protection, which in turn increases the social cost.[7] This model thus captures the behavior we see in CPS and identifies the driving factors for the current underinvestment in security protections.

A. Effect of Insurance

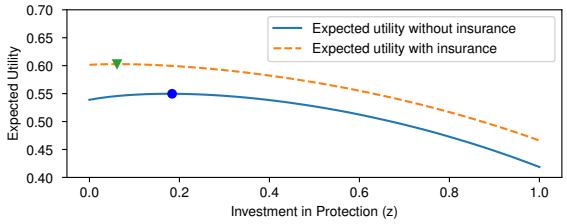
Now let us consider the effect of an insurance policy covering at most Q_α losses. In other words, the policy covers the losses that the firm considered in its risk analysis.[8] Also, we assume a fair premium, that is, the insurer charges the expected losses covered by the policy $P(z) = \int_0^{Q_\alpha} x\, dG(x, \xi(z))$.

Fig. 3 shows that firms with full liability invest more resources in protection than firms with limited liability. Therefore, a regulator or a government demanding full liability from their operators improves the security of systems. Moreover,

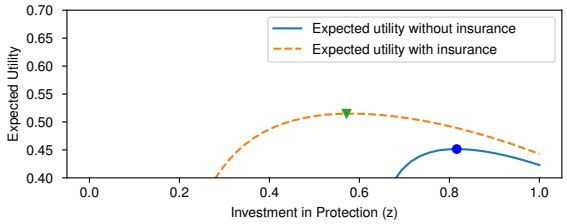
[6] E.g., shareholders, other firms, customers, or the government.

[7] In our experiments the firm contemplates losses up to 90%-VaR and 95%-VaR, therefore, the firm ignores events that occur once every 10 and 20 years, respectively.

[8] We assume that an insurer won't accept the risk of extreme events unless the firm is prepared for such events. Therefore, the policy covers only the maximum loss for which the firm took precautions.



(a) Limited liability (90%VaR).



(b) Full liability (99.9%VaR).

Fig. 3: Expected utility of a firm with (and without) insurance and different liability levels. The insurance improves the benefit of the firm, regardless of the liability; however, firms with insurance invest less in protection.

firms improve their profit with insurance, but invest less in protection (regardless of their liability). Therefore, insurance fails to improve the protection of firms, which might occur because the probability of extreme events is small. According to [11], insurance can incentive investments in protection when the probability of losses is high enough. Despite the failure of insurance to improve protection, insurance can still play an important role estimating the risk of companies in situations with asymmetric information.

V. Challenges and Opportunities

Below we describe some new and unique problems for managing risks in CPS.

A. Design of policies

1) Asymmetries in information: The U.S. Department of Homeland Security has sponsored some initiatives to facilitate and encourage voluntary data sharing, such as the Cyber Incident and Analysis Repository (CIDAR), Information Sharing Analysis Organizations (ISAO), Information Sharing Analysis Centers (ISAC), Cybersecurity Information Sharing Act (CISA) [42]. At present these initiatives are voluntary and face the following challenges: 1) ensure accurate reports (many organizations are reluctant to share meaningful information), 2) ensure anonymity and privacy of individuals, 3) maintain a voluntary nature and encourage participation, and 4) insurer's won't contribute data, because this information gives them a competitive advantage.

The government can regulate the cyber insurance market to reduce asymmetries in information. In particular, governments can implement regulations to mandate sharing of information [43], which in turn is expected to improve the insurability of cyber risks [44]. Particularly, [45] reports that federal regulation such as HIPAA and data breach disclosure laws increase demand for cyber insurance.

2) Development of response plans: It is also important to develop response plans to minimize the social impact of catastrophic events. Despite the fact that risk management practices would reduce losses (e.g., equipment damage), society still bears intangible damage, such as the suffering caused by catastrophic events. Therefore, it is necessary to raise awareness of cyber risks, so we can be prepared to face them [46].

B. Building CPS cyber-risk models

1) Estimation of cyber risks: Most works on risk management assume that risks can be estimated precisely, which implies knowledge of the likelihood of events and their impact. However, estimating risks in practice could be unfeasible due to a lack of information on attacks, and the complex interrelations among firms [47]. Furthermore, statistical properties of risks change upon observation in this type of adversarial system, because rational individuals react to acquired information. Hence, we need verify the precision of risk estimates (or develop better risk measures[9]) and design risk management strategies that consider uncertainties in the risk [48], [49]. Also, models should account for information feedback: i.e., changes in risk produced by the implementation of risk management actions.

2) Improve attack models: Traditional security studies consider that a system is partially secure if the cost of finding and exploiting a vulnerability exceed its benefits [50]. Furthermore, it is assumed that the cost of exploiting a vulnerability depends on the risk of being discovered (based the seminal work on the economics of crime by G. Becker [51]). However, the attackers responsible for cyber crimes often remain anonymous or cannot be prosecuted in their country of residence [52]. Hence, we need to design risk management strategies whee the attacker can remain anonymous.

While cyber-attackers may not be prosecuted, they still have limitations when attacking. For example, Axelrod and Iliev [53] explain that attackers face some risk when launching attacks, e.g., if the attacker uses some cyber-resource and is discovered, such resource would become useless in the future. On the contrary, if the attacker waits for too long, the defender might discover some protection against the vulnerability. Hence, the defender can prevent attacks by depleting the resources of its adversaries, without punishing them directly [54].

3) Dealing with evolving threats: Some research focuses on static settings, where protection decisions are made only once [55], [56]. However, unlike other static threats, cyber threats evolve in time because humans react to decisions made by the other parties. For example as an attack unfolds, the defender might discover new information to update its protection strategy. Likewise, attackers react to defense efforts by finding new vulnerabilities and attack strategies.

[9][48] shows that risk measures with VaR lack robustness and volatility, that is, forecasts are inaccurate and fluctuate between time periods.

Consequently, the information about previous attacks can become irrelevant for evaluating new risks [43].

We can model the evolution of threats by considering dynamics in the security of systems. For instance, [57], [58] consider problems of resource allocation in networks akin to viral spreading processes. On the other hand, [59], [60] analyze dynamics in the defense strategies, such as *moving target defense*, where changes are made to the configuration of the system to make it more difficult for attackers to launch successful attacks. Other works consider that the security of the system evolves according to a Markov process, in which the actions of both defender and attacker determine the security of the system [61], [54], [62]. We believe that we can design better protection schemes having into account the evolution of threats and the time restrictions mentioned in [53].

C. Challenges for investment in risk management

Firms with limited budgets face problems making sound security choices due to difficulties evaluating the risks. In addition, firms must choose between several mechanisms to reduce and transfer risks that perform different tasks and tackle different security problems. Hence, firms need to find the combination of risk management practices that bests suits them, however, individual firms often ignore the effectiveness both cyber insurance and mitigation technologies. Moreover, firms often ignore their exposure to risks. As a consequence, firms ignore the distribution tails (potential extreme events) and under invest in protection.

1) Determination of best practices: Cyber insurance policies can improve the security of systems if they promote effective security practices, e.g., through premium discounts. In such cases, the insurance industry can play the role of a regulator, which coordinates industries encouraging similar protections. However, the coordination of actions also introduces correlations in the risk, because the firms would have also the same vulnerabilities. Hence, insurers face a challenge in determining the best practices to cope with future unknown vulnerabilities. In general, a list of best practices should go beyond a list of requirements (e.g., standards, specific implementations of technologies), because the firms would focus on complying the requirements, rather than reducing the real risk.[10]

Nonetheless, investments in security can improve the protection even when the risk is misunderstood. For example, [63] finds that firms with a CISO (Chief Information Security Officer) have lower average costs of data breaches than companies without strategic security leadership. Indeed, [44] suggests that investments in mitigation explains why losses in the U.S. and Europe are lower than losses in Asia.

VI. Conclusions

In this paper we have focused on providing an overview of the unique characteristics that make cyber-insurance for CPS more challenging than cyber-insurance for classical IT networks.

We also saw how insurance can decrease security investments in protection; however, under the right setting (demanding to be fully covered for all liability losses) will actually motivate more investments in security protections and therefore will improve our public good.

Ultimately the success of a cyber-insurance market for CPS protection will depend on the ability of the insurance companies to estimate risks, and these estimates will have to address extreme events and the previous efforts on managing extreme risks.

[10]In many cases the specific configuration of the devices determines the risk, rather than their adoption

Acknowledgments

The authors are grateful with the anonymous reviewers, whose suggestions helped to improve the manuscript. This material is based upon work supported by NSF CNS-1547502.

References

[1] K. Zetter, "An unprecedented look at stuxnet, the world's first digital weapon," WIRED magazine, 2014. [Online]. Available: http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[2] ——. (2016, mar) Inside the cunning, unprecedented hack of ukraine's power grid. WIRED magazine. [Online]. Available: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[3] J. Finkle, "Hackers halt plant operations in watershed cyber attack," 2017.

[4] E. S. C. S. W. Group, "Roadmap to achieve energy delivery systems cybersecurity," U.S. Department of Energy, Tech. Rep., 2011.

[5] B. Schneier, "The internet of things will upend our industry," *IEEE Security and Privacy*, vol. 15, no. 2, pp. 108–108, 2017.

[6] K. Fu. (2016) Infrastructure disruption: Internet of things security. U.S. House of Representatives. [Online]. Available: http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-FuK-20161116.pdf

[7] M. Y. Vardi, "Cyber insecurity and cyber libertarianism," *Communications of the ACM*, vol. 60, no. 5, pp. 5–5, 2017.

[8] M. Daniel. (2013) Incentives to support adoption of the cybersecurity framework. https://obamawhitehouse.archives.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[9] "Executive order 13636: Improving critical infrastructure cybersecurity," https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf, Department of Homeland Security, Tech. Rep., 2013.

[10] (2014) Protection of critical infrastructure. European Commission. [Online]. Available: https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

[11] I. Ehrlich and G. S. Becker, "Market insurance, self-insurance, and self-protection," *Journal of political Economy*, vol. 80, no. 4, pp. 623–648, 1972.

[12] H. Kunreuther, "The role of insurance in reducing losses from extreme events: The need for public–private partnerships," *The Geneva Papers on Risk and Insurance Issues and Practice*, vol. 40, no. 4, pp. 741–762, 2015.

[13] "Cyber insurance: Recent advances, good practices and challenges," European Union Agency For Network and Information Security, Tech. Rep., 2016.

[14] C. Biener, M. Eling, and J. H. Wirfs, "Insurability of cyber risk: an empirical analysis," *The Geneva Papers on Risk and Insurance Issues and Practice*, vol. 40, no. 1, pp. 131–158, 2015.

[15] S. Morgan. (2015) Cybersecurity market reaches $75 billion in 2015, expected to reach $170 billion by 2020. Forbes. [Online]. Available: https://www.forbes.com/sites/stevemorgan

[16] "Insurance industry at a glance," Insurance Information Institute, 2015. [Online]. Available: https://www.iii.org/publications/insurance-handbook/introduction/insurance-industry-at-a-glance

[17] "2015 global cyber impact report," http://www.aon.com/attachments/risk-services/2015-Global-Cyber-Impact-Report-Final.pdf, Ponemon Institute, Tech. Rep., 2015, accessed: 2017-05-22.

[18] D. Jaffee and T. Russell, "Markets under stress: The case of extreme event insurance," *Economics for an Imperfect World: Essays in Honor of Joseph E. Stiglitz*, pp. 35–52, 2003.

[19] E. Paté-Cornell, "On "black swans" and "perfect storms": risk analysis and management when statistics are not enough," *Risk analysis*, vol. 32, no. 11, pp. 1823–1833, 2012.

[20] P. Andriani and B. McKelvey, "Beyond gaussian averages: redirecting international business and management research toward extreme events and power laws," *Journal of International Business Studies*, vol. 38, no. 7, pp. 1212–1230, 2007.

[21] N. N. Taleb, *The black swan: The impact of the highly improbable*. Random house, 2007, vol. 2.

[22] P. D. Bougen, "Catastrophe risk," *Economy and Society*, vol. 32, no. 2, pp. 253–274, 2003.

[23] A. J. McNeil, "Estimating the tails of loss severity distributions using extreme value theory," *ASTIN bulletin*, vol. 27, no. 01, pp. 117–137, 1997.

[24] P. Embrechts, S. I. Resnick, and G. Samorodnitsky, "Extreme value theory as a risk management tool," *North American Actuarial Journal*, vol. 3, no. 2, pp. 30–41, 1999.

[25] D. E. A. Sanders, "The modelling of extreme events," *British Actuarial Journal*, vol. 11, no. 3, pp. 519–572, 2005.

[26] P. Embrechts, C. Klüppelberg, and T. Mikosch, *Modelling extremal events: for insurance and finance*. Springer Science & Business Media, 2013, vol. 33.

[27] R. A. Fisher and L. H. C. Tippett, "Limiting forms of the frequency distribution of the largest or smallest member of a sample," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 24, no. 02, 1928, pp. 180–190.

[28] A. A. Balkema and L. De Haan, "Residual life time at great age," *The Annals of probability*, pp. 792–804, 1974.

[29] J. Pickands III, "Statistical inference using extreme order statistics," *the Annals of Statistics*, pp. 119–131, 1975.

[30] G. R. Walker, "Earthquake engineering and insurance: past, present and future," *Aon Re Australia)*, 2000.

[31] K. L. Petersen, "Terrorism: When risk meets security," *Alternatives*, vol. 33, no. 2, pp. 173–190, 2008.

[32] P. O'malley, "Governable catastrophes: a comment on bougen," *Economy and Society*, vol. 32, no. 2, pp. 275–279, 2003.

[33] R. V. Ericson and A. Doyle, *Uncertain Business: Risk, Insurance, and the Limits of Knowledge*. University of Toronto Press, 2004.

[34] "Understanding reinsurance: How reinsurers create value and manage risk," http://www.grahambishop.com/DocumentStore/SwissRe%20Understanding%20reinsurance.pdf, Swiss Re, Tech. Rep., 2004.

[35] U. Beck, *Risk society: Towards a new modernity*. Sage, 1992, vol. 17.

[36] J. M. Keynes, "The general theory of employment, money and interest," *The Collected Writings*, vol. 7, 1936.

[37] J. M. Acton and M. Hibbs, "Why fukushima was preventable," Carnegie endowment for international peace, Tech. Rep., 2012. [Online]. Available: http://carnegieendowment.org/files/fukushima.pdf

[38] W. B. Brice, "British government reinsurance and acts of terrorism: The problems of pool re," *U. Pa. J. Int'l Bus. L.*, vol. 15, p. 441, 1994.

[39] "Pool reinsurance company limited: Annual report 2015," https://www.poolre.co.uk/newsletters/Pool_Re_Annual_Report_2015.pdf, Pool Re, Tech. Rep., 2016, accessed:2017-05-28.

[40] J. D. Cummins and C. M. Lewis, "Catastrophic events, parameter uncertainty and the breakdown of implicit long-term contracting: The case of terrorism insurance," in *The Risks of Terrorism*. Springer, 2003, pp. 55–80.

[41] R. W. Klein, "Insurance market regulation: Catastrophe risk, competition, and systemic risk," in *Handbook of Insurance*. Springer, 2013, pp. 909–939.

[42] "Information sharing," https://www.dhs.gov/topic/cybersecurity-information-sharing, Department of Homeland Security, 2016.

[43] I. A. Tøndel, P. H. Meland, A. Omerovic, E. A. Gjære, and B. Solhaug, "Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research," SINTEF, Tech. Rep., 2015.

[44] M. Eling and J. H. Wirfs, "Cyber risk: Too big to insure? risk transfer options for a mercurial risk class," Institute of Insurance Economics, Tech. Rep., 2016.

[45] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, "Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?" 2017.

[46] T. Koppel, *Lights out: a cyberattack, a nation unprepared, surviving the aftermath*. Broadway Books, 2016.

[47] B. Johnson, A. Laszka, and J. Grossklags, "The complexity of estimating systematic risk in networks," in *2014 IEEE 27th Computer Security Foundations Symposium (CSF)*. IEEE, 2014, pp. 325–336.

[48] J. Danıelsson, "The emperor has no clothes: Limits to risk modelling," *Journal of Banking & Finance*, vol. 26, no. 7, pp. 1273–1296, 2002.

[49] J. Danielsson, "Blame the models," *Journal of Financial Stability*, vol. 4, no. 4, pp. 321–328, 2008.

[50] S. Schechter and M. Smith, "How much security is enough to stop a thief?" in *Computer Aided Verification*, 2003, pp. 122–137.

[51] G. S. Becker, "Crime and punishment: An economic approach," *Journal of Political Economy*, vol. 76, no. 2, pp. 169–217, 1968.

[52] K. Greene, "Catching cyber criminals," https://www.technologyreview.com/s/405467/catching-cyber-criminals/, MIT Technology Review, 2006.

[53] R. Axelrod and R. Iliev, "Timing of cyber conflict," *Proceedings of the National Academy of Sciences*, vol. 111, no. 4, pp. 1298–1303, 2014.

[54] C. Barreto, A. A. Cardenas, and A. Bensoussan, "Optimal security investments in a prevention and detection game," in *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp*, Apr 2017, pp. 24–34.

[55] M. Van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "Flipit: The game of "stealthy takeover"," *Journal of Cryptology*, vol. 26, no. 4, pp. 655–713, 2013.

[56] N. S. Rao, S. W. Poole, C. Y. Ma, F. He, J. Zhuang, and D. K. Yau, "Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models," *Risk Analysis*, vol. 36, no. 4, pp. 694–710, 2016.

[57] V. M. Preciado, M. Zargham, C. Enyioha, A. Jadbabaie, and G. J. Pappas, "Optimal resource allocation for network protection against spreading processes," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 1, pp. 99–108, March 2014.

[58] R. J. La, "Role of network topology in cybersecurity," in *2014 IEEE 53rd Annual Conference on Decision and Control (CDC)*. IEEE, 2014, pp. 5290–5295.

[59] H. Maleki, S. Valizadeh, W. Koch, A. Bestavros, and M. van Dijk, "Markov modeling of moving target defense games," in *Proceedings of the 2016 ACM Workshop on Moving Target Defense*. ACM, 2016, pp. 81–92.

[60] J. Rowe, K. N. Levitt, T. Demir, and R. Erbacher, "Artificial diversity as maneuvers in a control theoretic moving target defense," in *National Symposium on Moving Target Research*, 2012.

[61] M. Rasouli, E. Miehling, and D. Teneketzis, "A supervisory control approach to dynamic cyber-security," in *International Conference on Decision and Game Theory for Security*, 2014, pp. 99–117.

[62] C. Barreto and A. A. Cárdenas, "Optimal risk management in critical infrastructures against cyber-adversaries," in *2017 1st IEEE Conference on Control Technology and Applications (CCTA)*, aug 2017.

[63] S. J. Shackelford, "Should your firm invest in cyber risk insurance?" *Business Horizons*, vol. 55, no. 4, pp. 349–356, 2012.