# Chapter 2: The Economics of Cybersecurity[1]

This chapter presents the state of the art in the economics of cybersecurity. It elaborates the underlying concepts, as borrowed from economics. It answers the dissertation's central question theoretically, by reviewing what is known about the behavior, incentives, and role of intermediaries in cybersecurity.

## 2.1 Introduction

The Internet has enabled tremendous economic and social innovation yet the underlying systems, networks and services sometimes fail miserably in protecting the security of communications and data. Security incidents occur in many forms, including but not limited to the leaking and theft of private information, unauthorized access to information, malicious alteration of data, or software and service unavailability. Enumerating all the technical ways in which security may be breached would generate a lengthy list as the network, devices, users, and services can all be attacked. A typical network runs hundreds of protocols and hosts devices operating thousands of applications consisting of millions of lines of code. Looking for solutions opens up an equally unwieldy range of ideas, technologies, and complications. Not surprisingly, books on information security are typically voluminous. For example, Anderson's (2008) *Security Engineering* is over 1000 pages long. Despite its length, the book can address most topics only briefly. Even research focusing on specific problems and solutions can be dauntingly complex. For example, the design and use of passwords has generated hundreds of papers but the jury on best practices is still out (Bonneau et al. 2012). Achieving cybersecurity under these conditions may appear like a hopeless endeavor and failure unavoidable.

[1] To appear in: Asghari, Hadi, Michel J.G. van Eeten, and Johannes M. Bauer. 2016. "Economics of Cybersecurity". In *Handbook on the Economics of the Internet,* edited by Johannes M. Bauer & Michael Latzer. Cheltenham and Northampton: Edward Elgar. Reprinted with permission.

Given the complexity of the problem, it seems indeed improbable that security can be attained by eliminating all vulnerabilities. Moreover, preventative security measures are costly. Some level of uncertainty will therefore have to be accepted and choices need to be made trading off competing objectives and limited resources. Recent research has developed approaches to better explain why certain security failures occur and others do not. These contributions clarified that security is not merely a technical problem that can be fixed with engineering solutions but that is also has important economic and behavioral dimensions that need to be addressed (R. Anderson and Moore 2006). Examining the incentives of players in the information and communication technology (ICT) ecosystem has been particularly fruitful in explaining the landscape of vulnerabilities and attacks that can be observed. The core of this work is rooted in information security economics.

A key insight that catalyzed the development of this field is that many systems do not fail for technical reasons but because of the specific incentives shaping the behavior of individuals and organizations. For instance, if the individuals in charge of protecting a system do not have to bear any costs or other consequences in case of failure, they may exert insufficient care (R. Anderson and Moore 2006). Attackers similarly respond to the set of pertinent incentives, for example by selecting targets and attack strategies based on expected financial or political benefits and risks. Technical tools to carry out attacks are often chosen opportunistically as attackers will use whatever means happen to work in a given scenario. These insights and the abundance of technical and non-technical vulnerabilities and attack vectors imply that it is more promising to approach cybersecurity as a defender-attacker dynamic with an emphasis on the incentives of players rather than with a focus on the vulnerabilities. Another consequence is that for the foreseeable future information systems will need to be defended against attacks with a combination of technology and human vigilance.

Given the abundance of interdependencies in the ICT ecosystem, cybersecurity at the individual and system levels is influenced by how the incentives of different actors align. Sometimes individual and group incentives are compatible with both the private and social costs and benefits so that decentralized decisions will be workable and effective to achieve

desirable levels of security. However, more often such an alignment cannot be taken for granted and several questions arise. Are markets, networked governance, and individual organizational decisions—the predominant coordination mechanism in the Internet—sufficient to safeguard cybersecurity (Van Eeten and Mueller 2012)? Or does such decentralized coordination fail because market and non-market players are not prepared or capable to effectively deal with the risks? If market failure is pervasive, the incentives of decentralized players will be systematically biased and may result in underinvestment or overinvestment in security (Lewis 2005; Shim 2006). A classical response to market failure is government intervention but the incentives of government actors are not necessarily aligned with the common good. Parts of government, including secret services and the military, may have an interest to exploit vulnerabilities for surveillance purposes. Consequently, conflicts within government may prevent effective public sector responses to information security risks. Moreover, the global scale and connectivity of the Internet has created interdependencies that may require coordinated action beyond the national or global level to design effective responses, greatly compounding the challenges. Security economics has in the past decade successfully examined many of these questions and helped greatly in the design of rational responses.

Most of the work in the field has focused on information security as a means to fight criminal activities, rather than on the protection of national security and cyberwar. The two topics, while related, raise different theoretical and practical issues. Some scholars have argued that the societal impact of cybercrime is more important than the hype-prone concept of cyberwar. Cybercrime has been more amenable to empirical research; protecting national security in comparison is more about scenarios of potential impacts. It is important to understand the perspective used by each approach to conceptualize risk, costs and benefits, and the role of government (see, for example, Singer and Friedman 2013). Cybercrime is often discussed in a framework of risk management, using cost-benefit and trial-and-error approaches. This approach typically results in tolerating some level of risk and vulnerability. National security deals with massive economic and social disruptions, often focusing on worst-case scenarios. In such scenarios, prevention and resilience are often the main emphases (Van Eeten and Bauer 2009; Van Eeten and Bauer 2013).

In this chapter, we set out to survey the state of the art of the existing research with a focus on the criminal threats to cybersecurity.

The next section briefly outlines key topics addressed in economic analyses of information security. Sections 2.3 through 2.5 discuss software and platform security, end-user and organizational security, and Internet intermediary security. Attacker behavior is addressed in section 2.6 , followed by an exploration of policy options in section 2.7 and concluding remarks in section 2.8 .

## 2.2 Cybersecurity as an Economic Problem

Cybersecurity may refer to technical, legal, and organizational measures directed at maintaining or enhancing the integrity and security of information assets. It can be assessed at the level of individuals and organizational, or at aggregated levels such as nations or cyberspace as a whole. Many of the Internet's technical and behavioral standards, conventions, and norms emerge from decentralized repeated decisions of actors participating in it—ranging from component and hardware manufacturers to network operators, software vendors, application and service developers, content providers, and various users. These actors are heterogeneous and have different skillsets and motives. The architectural design adopted by Internet engineers created the socio-technical framework that constrains and enables these actors. While information security was initially not a pressing concern, the early choices that solidified the unique open design of the Internet inadvertently created later challenges of safeguarding cybersecurity (Lessig 1999; Hofmann 2010).

The field of economics of information security studies factors that actors perceive as relevant for security decisions ('incentives'), their influence on economic actions by individuals and organizations, and how these actions lead to emergent properties of the system. The early concepts and theories applied in the field originated from neo-classical microeconomics, and in particular the field of information economics. Economic sciences, however, constitute a wide discipline (Groenewegen 2007; Colander 2005). Concepts and theories from other fields, such as behavioral economics and new institutional economics, have also over the years made their way into the economics of information security. In this section, we look at four basic concepts.

*Externalities.* Cybersecurity has both private and public good characteristics: while investment in security protection entails private costs and benefits for the decision-maker, it may also benefit or harm other Internet actors. These interdependencies are called externalities—formally defined as the direct effect of the activity of one actor on the welfare of another that is not compensated by a market transaction (Rosen 2004). Much of the economic literature on security economics is concerned with externalities that can be negative or positive. In both cases, the price of the direct market transaction will not reflect the full social costs or benefits of the product or service, because the third party effects are not taken into account by the transaction partners. Consequently, systematic deviations from an optimal allocation of resources occur even in an otherwise functioning market economy (Musgrave and Musgrave 1973). Individual security measures may have positive and negative externalities, depending on whether attacks are targeted or non-targeted and whether the associated risk is interdependent or not (Kunreuther and Heal 2003). There are several ways to correct for such externalities and 'internalize' them into decision-making. A traditional response is collective action by government or the participants in an exchange. Many information markets are multi-sided ('platform') markets; the platform intermediary may have incentives to internalize externalities caused by others to improve its business case and competitiveness. In fact, these platforms can be seen as institutional arrangements to reduce transaction costs and address externalities (Rysman 2009).

*Information Asymmetry.* Another key focus in the information security literature relates to the situation in which information is incomplete and unevenly distributed among players; such as when buyers in a market do not have sufficient information to reliably separate between high quality and low quality products. For example, a subscriber looking to purchase Internet access may not be able to distinguish ISPs with strong security practices from those with lax ones. This makes buyers unwilling to pay a premium for the better product and consequently discourages suppliers from offering them—a situation dubbed a 'market for lemons' (Akerlof 1970). Information asymmetry afflicts many Internet services when it comes to security and privacy, where it is impossible to determine how secure a service is.

*Property Rights.* Although rarely explicitly recognized in the literature, a fundamental economic problem at the heart of many information security issues may be the absence of clearly defined property rights in personal and other information (Branscomb 1994). It is this absence that gives players in the Internet more or less free reign to appropriate information from users and store large amounts of data.

*Alignment of Incentives.* Cybersecurity can be improved by introducing measures that align incentives of individual actors so that deviations between private and social costs and benefits are reduced. If successful, such strategies can reduce or even eliminate security-related market failures and deficiencies. Table 2.1 presents selected high-level options for aligning incentives among Internet actors. One can strengthen the incentives for security investment and other protective measures among defenders. One can also disincentivize attackers by increasing the costs or reducing the benefits of cybercrime and other malicious actions. Although the differentiation between defenders and attackers is sometimes muddied—government agencies with an interest in vulnerabilities to spy on others, white hat hackers who attack with the goal to improve defenses—the approach is useful in exploring principal options.

In the next sections of this chapter, we survey the security economics literature organized around these actors. We shall provide examine the incentives of each actor, their interactions with the ecosystem, and security issues that they create or resolve. Among the attackers, our focus will be on cyber criminals, economically motivated and by far the largest group.

**Table 2.1. Improving cybersecurity by aligning incentives of actors**

| Improving Cybersecurity | |
|---|---|
| **Incentivizing Defenders** | **Disincentivizing Attackers** |
| *Who:* | *Who:* |
| - Software vendors | - Criminals |
| - End users and organizations | - Hacktivists |
| - Internet intermediaries | - Nation states |
| *How:* | *How:* |
| - Reducing information asymmetries | - Improved law enforcement |
| - Addressing negative externalities | - Reducing benefits of crime |
| - Education and capacity building | - Disrupting criminal resources |

*Approaches to Studying the Economics of Cybersecurity*

The security economics literature can be categorized into analytical, empirical, and experimental research.

*Analytical studies* employ methods such as game theory to deduct theoretically how actors behave in security dilemmas. Key variables, such as prices, regulation, and the type of competitive interaction are parameterized. Determining cooperative and non-cooperative equilibria of the game allows researchers to explore the conditions under which cybersecurity improves or deteriorates. As it may be difficult to derive solutions to games analytically, researchers also use computational and simulation methods to approximate outcomes. These methods offer interesting results but their practical use may be limited by the required simplifying assumptions. Results are often highly stylized and application to more complicated real world situations may need careful and cautious interpretation.

*Empirical studies* start by collecting and observing actual cybersecurity behavior and performance. While many of the efforts are descriptive, additional insights may be gained by combining datasets of Internet measurements or surveys with data analysis to unveil how a market functions and how its actors behave. Empirical studies are a promising avenue but they also have their unique challenges, which include the dynamic nature of the phenomenon, insufficient or unreliable data, and

problems of endogeneity that complicate establishing causality especially in cross-sectional comparative studies.

*Experimental studies* use lab or online experiments to test various hypotheses—with fewer assumptions and proxies than the other two methods. This raises challenges as to how generalizable the findings may be.

In subsequent sections of this chapter, we look at all three categories of works. We focus mainly on the recent literature as it usually also relates to earlier work and point to classics and influential work in the field. We have chosen this approach to keep the material more manageable but also because much of the earlier research has been updated and extended in recent years. Moore and Anderson (2012) and volume 3, issue 1 of IEEE Security & Privacy, published in 2005 are earlier surveys of the field. For the purposes of this chapter, relevant literature has been drawn from papers presented at a number of leading security conferences, including the annual Workshop on the Economics of Information Security (WEIS), a detailed examination of journals where scholars of the field typically publish and through keyword search in other journals.[2]

## 2.3 Software and Platform Security

The Internet and its services are run by software. Many security issues arise because of poorly written or misconfigured software. The Common Vulnerabilities and Exposures database, a 'dictionary of common names for publicly known information security vulnerabilities', lists 60 000 software vulnerabilities between 2005 and 2014 (CVE 2015). They can be found in all operating systems and pieces of software. Anderson (R. Anderson 2001) was one of the first to explore the fundamental economic reasons behind this phenomenon.

Software products share a number of interesting characteristics with other 'information goods' (Shapiro and Varian 1998). High initial devel-

[2] In addition to WEIS, proceedings of USENIX Security, IEEE S&P, ACM CCS, SOUPS were perused. Key journals that were reviewed in detail included IEEE Security & Privacy, Communications of the ACM, Telecommunications Policy, and Information Systems Research. Key search terms for other journals included 'economics, security' and 'internet, security'.

opment and production costs are accompanied by close to zero incremental costs for additional copies. Information goods often exhibit direct and indirect 'network effects'. Direct network effects exist if the utility of a software product increases with the number of users (e.g. because documents can be shared with a larger group). Indirect effects exist if, as the user base grows, more complementary software and products become available, further increasing the utility of the software. In the absence of cheap and efficient converter technology, network effects can lead to switching costs and consequently 'lock-in' effects (Gottinger 2003): The costs of equipping an organization with new hardware and software, the costs of switching from one solution or format to another including the associated costs of document conversion, and the costs of learning new skills all create rigidities that work in favor of sticking with the existing solution. This provides advantages for the first mover and disadvantages for competitors that enter a market late. Consequently, software markets have a 'winner-takes-all' dynamic that incentivizes vendors to move their products to market fast and to grow as quickly as possible.

In their battle for dominance, software vendors might initially give away their products for free or at a low price but change their pricing to generate a profit once they have a large user base and lock-in. Software vendors will attempt to lure developers to their platforms by making application programming interfaces (APIs) available for free or at a low cost as developers bring additional users. This might also imply that developers are given latitude and are permitted to work under lax rules for security technologies in the platform (R. Anderson and Moore 2006). Vendors will lure customers with bells and whistles that are visible features or provide convenience. Security is rather intangible and does not easily fit into these considerations, it might even reduce functionality. That is why in the short term the market does not value security. After a firm gains dominance, the incentive structure changes: The costs of releasing software patches and mending brand damage incentivize firms to change course. An example is Microsoft whose reputation was tarnished after a series of spectacular worm attacks in the early 2000s. In response, the company started an internal code-review campaign resulting in the release of Windows XP Service Pack 2 with many security enhancements in 2004 (Van Eeten and Bauer 2008). Nowadays, Windows vulnerabilities make fewer headlines. Vulnerabilities have moved 'up the stack' to other applications, including open-source software. But all

in all software vendors cause severe negative externalities as they do not bear much of the costs of insecure software.

Security software has an interesting extra hurdle. Since security is hard to measure, the average user basically has to take the word of a vendor claiming the product provides better security protection than another. Thus it becomes a classic lemons market (Schneier 2007). A running joke states that antivirus software competes on every feature except security. Judging by the large sums spent on security products (R. Anderson et al. 2013) consumers demand security. If they are lacking clear and reliable information they will likely underinvest in some key areas and overinvest in hyped ones.

A number of ideas have been presented for aligning incentives of the players in the software market. To be fair the responsibility rests not solely on software vendors as they are not instigating the attacks. Even in a perfect market some users might choose software with a lower degree of security and remedy remaining problems using other countermeasures. Anderson et al. (2008) name an obligation to provide free and timely software patches for security products, mandating 'secure by default', and responsible vulnerability disclosure as policy options. Previously software certification has been suggested but this has not worked as anticipated. We look at these options later in the chapter.

Zittrain (2008) raised concerns that the market might evolve toward users preferring locked-down devices to reduce the threats from malware and other side-effects of insecure software. Given the rise of mobile devices there is some evidence to that effect, as the major application stores are controlled by the respective firms or consortia (e.g. Apple's App Store, Google's Play Store, and Microsoft's Windows Store). Application stores for web-browsers are another example. Application stores have their own share of security problems and exhibit a wide variation in their security mechanisms. J. Anderson, Bonneau and Stajano (2010) compared the incentives of ten different application stores and concluded that soft liability and signaling have the best chance for improving security without stifling innovation. The shift towards software as a platform and the rise of application stores means that some software vendors become Internet intermediaries who have different incentives (e.g., Fershtman and Gandal 2012).

## 2.4 End-User and Organizational Security

Users may be individual end-users and organizations ranging from small to very large size. Our focus is on the incentives and decisions of organizations outside the IT security industry that need to protect information assets related to their core business. We start by looking at larger organizations with dedicated IT budgets and then turn our attention to smaller organizations and individuals with limited skills to assess and manage security risks.

*Information Security Investment in Large Organizations*

Rational large organizations would make security investment decisions based on several relevant factors, including the type of risk they are facing, the monetary and non-monetary consequences of failure, the resilience of their operations, etc. In practice, the available budget is often a key determinant of their security investments (Cavusoglu, Mishra, and Raghunathan 2004). The total cost of security includes investment in technology, the hiring of experts, as well as the indirect productivity costs that might be caused by security controls. Although security spending figures tell little about the rationality of expenses they are a useful proxy for the total resources available. Framing security as an investment problem eases communication with upper management and helps set limits as it might make sense not to defend against certain threats.

Gordon and Loeb (2002) first explored optimal security investment conceptually. They proposed a model in which information assets are categorized based on their value, potential loss in case of a breach, and their vulnerability. The authors showed that under varying assumptions firms will be better off concentrating efforts on information assets with mid-range vulnerabilities as extremely valuable information may be 'inordinately expensive' to protect. To maximize expected benefits a firm should spend only a small fraction of the expected loss on securing an asset (except in cases when law requires an asset to be protected regardless of value).

A number of scholars have extended this simple and elegant model, for instance by looking at the timing of investment, by proposing different caps for security investment, and by relaxing model assumptions. Ioan-

nidis et al. (2013a) show in a utility-theoretic model that security investment turns out to be cyclical when costly projects are deferred due to uncertainty related to the costs of future vulnerabilities. Böhme and Moore (2009) model the interaction between defenders that face investment decisions under uncertainty and attackers who repeatedly target the weakest link. They empirically validate their model and conclude that underinvestment can be reasonable under certain scenarios: When reactive investment is possible, when attacks are not catastrophic, and when uncertainty exists about attacker capabilities. Although difficult, quantifying cybersecurity risks and costs is an integral part of the investment models. Brecht and Nowey (2013) focus on establishing the costs of information security. They offer a comprehensive comparison of three alternatives to using surveys for determining such costs. Demetz and Bachlechner (2013) compared approaches using a configuration management tool as an example, and found that there is considerable potential for new approaches to complement existing ones. These selected findings illustrate the difficulties of operationalizing and implementing cost-benefit approaches to assessing security investment.

The level of investment aside, what security practices should an organization put into effect? A high-level distinction is between practices that have an observable impact on security, and those that are adopted for compliance reasons, due diligence, or keeping up with what are considered 'best-practices'. The security benefits of alternative approaches also depend on the goals of an organization, which might include protecting the organization's intellectual property, finances, and customers from attacks. Sometimes security solutions might be focused on other objectives than security, for instance on achieving customer lock-in, as is the case with security measures in printers designed to ensure that third party ink cannot be used. In the case of best practices or standards, security measures are not adopted per se for their effectiveness, but rather for the sake of compliance. Standards such as the ISO 27000 series, the common criteria, or sector specific security regulation may fall in this category if implemented mainly to disclaim liability in case of failure. From the perspective of policymakers such measures can still be useful for the ecosystem as a whole if an evaluation of their aggregate results indicates that they have desired effects on security.

The security incentives of large organizations are, in short, mixed. Tolerating some level of insecurity is economically rational, and as long as the organization accepts the risks and compensates the direct and indirect costs, it limits the externalities of its security decisions. An organization can also decide to transfer security risks to a third party via cyber-insurance. But this arrangement has not been widely adopted thus far. Other policies are required if incident costs are not borne by the organization and externalities are created. One means is data breach disclosure laws (sometimes referred to as security breach notification laws) intended to mitigate harms to third parties caused by an organization's underinvestment in security. Organizations are required to notify all affected customers in cases of breaches leading to compromise of personal information. If they fail to do so they become liable for damages and face fines.

### *Security in the Healthcare Sector*

Organizational security has also been studied in the context of particular sectors. The healthcare sector is a good example illustrating many key aspects of security decisions. It deals with confidential and sensitive patient data and has been subject to sector-specific regulation such as the U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act and the Health Insurance Portability and Accountability Act (HIPAA). While confidentiality has considerable importance for earning the trust of patients and professionals, it is not the core business of health organizations. Consequently, attitudes towards such regulations might mainly be driven by a desire to be compliant. Given the interest in how an attitude of compliance affects security decisions, the health care sector has been studied in detail by researchers.

Gaynor et al. (2012) studied around 200 reported data breaches in hospitals from 2006 to 2011 and found that increased competition was associated with a decline in data protection. They suggest that hospitals in competitive markets may be inclined to shift resources to visible activities rather than data protection. Kwon and Johnson (2011) analyzed two thousand healthcare organizations and found that proactive security investments, associated with longer intervals between subsequent breaches, were most effective when voluntarily done. Miller and Tucker (2011) looked at encryption as a tool for increasing data security, in particular in states that provide safe harbors when it is used. They found that data breaches perversely increased after healthcare organizations

adopted encryption software, possibly due to a false sense of security and/or a moral hazard problem. The effectiveness of sector regulation might be tied to the specifics of its formulation, as Kwon and Johnson (2013) suggest in a more optimistic study of the effects of the financial incentives created by the HITECH Act. They conclude that mitigating data breaches depends more on security resources and capabilities than regulatory compliance and reiterate that policy should provide guidelines to invest in a combination of security resources, capabilities, and cultural values, rather than impose single-solution requirements.

### *Individuals and Small Organizations*

End-users that lack dedicated IT staff often rely on a variety of heuristics to make security decisions. These decisions are prone to mistakes that fraudsters can exploit (Stajano and Wilson 2011). The sheer number of such users means that even a small vulnerable fraction can cause major security risks for others and in the aggregate. An example is the market for fake anti-virus software: hundreds of thousands of users have been conned into paying for malware that claims to be an anti-virus product (Stone-Gross et al. 2013).

Psychology and behavioral economics provide explanations for such behaviors. Understanding how end-users interpret error messages and make security decisions can be used to design user interfaces that nudge users towards better security choices (Sunshine et al. 2009; Camp 2013). Bravo-Lillo et al. (2011) provide an enlightening example: novice users perceive 'saving' a file as being more dangerous than 'opening' it, as it implies persistent changes to the system. Similarly, Wash (2010) discusses 'folk models' formed by users about security threats and how they influence online behavior.[3] Given these difficulties, end-users might be willing to pay for extra security services. Just as an example, Wood and Rowe (2011) estimated that customers of U.S. Internet service providers are willing to pay $4 to $7 a month premium for mitigating malware harms. However, this willingness often does not translate into actual purchasing behavior due to information asymmetries and the market for lemons problem.

[3] Due to the scope of this chapter, we will not delve further into these topics. The interested reader is referred to works presented at the annual Symposium on Usable Privacy and Security (SOUPS).

Users are not always wrong to ignore security advice (Herley 2009). Typical advice concerning passwords is outdated, almost all certificate error warnings appear to be false positives, and if users spent even a minute a day reading URLs to avoid phishing, the costs would greatly outweigh phishing losses. Florêncio and Herley (2010) investigated password policies concluding that websites with the most restrictive policies are insulated from the consequences of poor usability: for example, universities have stricter password rules than Google and Facebook, as they won't lose revenue if users have a hard time logging in. The latter defend against more attacks using other effective authentication controls that maintain convenience (such as the location of access). This example shows an interesting trade-off between different aspects of implementing security protections.

Due to carelessness and limits of human intuition, end users can create considerable externalities for the Internet economy. However, they also fuel the Internet economy by shopping online and clicking on ads. Improving end-user security at the expense of convenience might result in a negative net-gain, an economic trade-off that possibly can be done away by larger organizations. For example, when online merchants were pushed by Mastercard and VISA to adopt the 3D security anti-fraud measure or accept liability for the fraud losses, some found that the additional checks resulted in higher dropout rates during checkout. These exceeded the cost of accepting liability for the fraud, which led some merchants to opt out of the security program.

## 2.5 Internet Intermediaries

One of the most promising areas of security economics research has concentrated on Internet intermediaries. These entities provide the Internet's basic infrastructure and platforms, and enable communications and transactions between third parties and services. Players include Internet Service Providers (ISPs), hosting providers, payment systems, e-commerce platforms, search engines and participative platforms as show in Figure 2.1 (Perset 2010). The role of intermediaries has increased over the years gradually modifying the original vision of an 'end-to-end' design of the Internet. Most intermediaries are private businesses and IT

forms the core of their business. We will first make some general observations applying to all intermediaries, and then look at different types separately.

Intermediary markets are highly concentrated because of *network effects* and *economics of scale*. Network effects, as previously explained, reflect the increasing value of a service as more users adopt it. Economies of scale are cost advantages that firms gain due to their size. In many markets—for instance search engines, participative platforms or certificate authorities—a handful of companies control large market shares, sometimes up to eighty or ninety percent of the revenues or user base (Noam 2009). Some of the largest Internet intermediaries are among the world's top firms and well-known brands–e.g. Google, Facebook, eBay, Amazon, Apple and Microsoft.

Intermediaries raise interesting governance issues. They are in some sense gatekeepers of the Internet economy with direct access to end-users. They become de-facto standardization bodies and their mundane technical choices frequently have more profound effects on outcomes than formal Internet governance structures (Van Eeten and Mueller 2012). Their scale makes them focal points for regulation, whereas a network of thousands of organizations and millions of end users can hardly be regulated by traditional governance arrangements. However, like in the case of other players, the security incentives of Internet intermediaries are mixed. In some cases, security is a cost to avoid, in particular if it conflicts with business interests. In many cases however, intermediaries take security seriously and are among the largest defenders of users against attacks, as they have incentives in maintaining trust in the Internet economy. Often, their role as multi-sided platforms which are enabling other market players will generate strong incentives to internalize some of the externalities in the system. Moreover, many intermediaries have the resources, knowledge, and capabilities to provide security.

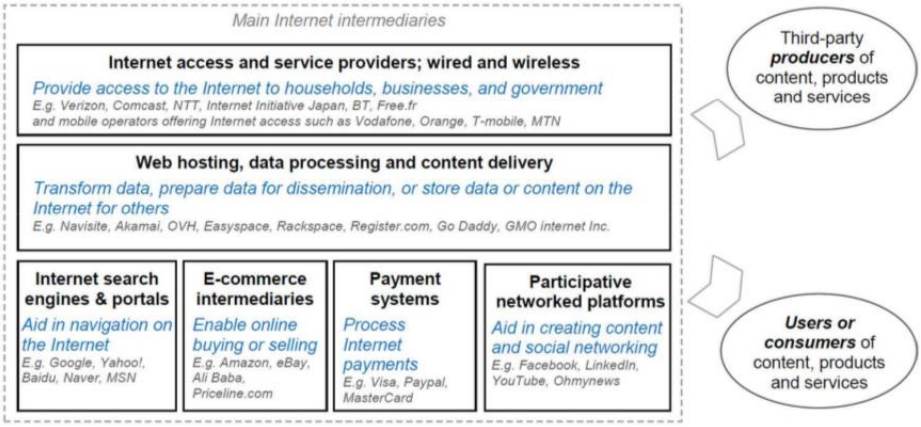


**Figure 2.1. Internet intermediary roles (Perset 2010, fig. 1)**

*Internet Service Providers*

Internet service providers (ISPs) are companies that connect subscribers to the global Internet. ISPs come in different sizes—from small regional ISPs to multinational tier-1 networks. There are several thousand ISPs worldwide but the 200 largest ones serve about 80 percent of broadband and mobile Internet markets (Van Eeten et al. 2010). Since ISPs have access to their subscribers' Internet traffic they are affected by and involved in policy debates on privacy protection, network neutrality, copyright enforcement, infrastructure resilience, the blocking of malware, and the disruption of botnets.[4] In many countries, ISPs have historically been regulated in a less intrusive fashion than traditional telecommunications companies. In the U.S. they were historically classified as 'information service providers' and in other countries as value-added service providers. As part of these legal arrangements, they were shielded from liability for traffic carried on their networks as long as they followed certain required business practices (e.g. notice and take-down procedures).[5] We shall focus this section on the role and incentives of ISPs with

[4] These debates are all important for the Internet economy; this chapter retains a focus on cybersecurity.

[5] In the U.S. these safeguards were contained in the safe harbor provision of the Digital Millennium Copyright Act (DMCA) of 1998. While American ISPs were reclassified as common carriers early in 2015 (see Federal Communications Commission, In the Matter of Protecting and Promoting the Open Internet, GN Docket No. 14-28, adopted February 26, 2015), they are subject to similar protections under common

regard to malware and botnets as some of the most pernicious cybersecurity threats.

Bots are computers infected with malware that puts them under remote control by attackers. The attackers may directly harm the owners of these machines through fraud or extortion. They may also combine infected computers into botnets of varying size or rent them out to other criminals. In either case, they become platforms to launch attacks on other parts of the Internet and therefore are a serious problem for the whole Internet ecosystem. Numerous botnets remain active despite more than a decade of countervailing measures. Depending on whether one differentiates according to the malware families used or by the number of different attackers using them, their number ranges between tens and thousands. The largest botnets may at peak consist of millions of bots (Symantec 2015).

The security community has had some success in seizing control over botnets through both technical infiltration and apprehension of the command and control infrastructure (Fryer, Moore, and Chown 2013). However, a key problem that remains is cleaning up the infected machines. Clayton (2011) contemplates alternative approaches to clean-up and concludes it might make sense for governments to subsidize ISPs or other third parties to clean up malware on end-user machines. In the same vein, there have been calls to treat botnets by employing a public health approach. In this framework, a 'cybersecurity health agency' would provide education, monitoring (e.g. infections and intrusion trends), epidemiology (e.g. malware analysis), immunization (e.g. patch coordination), and incident response (Sullivan 2012; Kelley and Camp 2012).

Van Eeten et al. (2010) evaluated the role and incentives of ISPs in botnet mitigation by comparing spam-bots in 200 ISPs between 2005 and 2009. They found that large retail ISPs are indeed effective control points but that the number of infected machines per subscriber differs significantly among ISPs. This difference was relatively stable over time, suggesting

carrier law. In the European Union, such protections are contained in the 'mere conduit' provision of the Electronic Commerce Directive.

that systematic differences exist in ISP policies and management practices as well as among users. The authors further found that larger ISPs have lower average infection rates, possibly due to automation of detection and clean-up that allow reducing the unit cost of providing security. Moreover, the data reveals that ISPs located in countries with an attentive regulator have cleaner networks. Other researchers have suggested that coordinated action by the largest networks can be very effective in stopping malware (Hofmeyr et al. 2013), and that a correlation exists between well managed networks and end user security (J. Zhang et al. 2014). Different approaches to incentivize ISPs and other networks to improve security practices have been proposed. Tang et al. (2013) perform a shaming and faming experiment with networks that have high outgoing spam, a sign of botnet activity. They report that performance improved in a treatment group that was subject to information disclosure. In recent years, public-private partnerships between ISPs and a national anti-botnet center have been the most called upon model for clean-ups (OECD 2012). By splitting costs, these models recognize the role of ISPs and the public sector, and that ISPs are not solely responsible for clean-ups. The verdict on the effectiveness of these models is still out.

### *Hosting Providers*

Hosting providers are organizations that operate servers used by customers to make content and services available to the Internet. Many hosting providers are also registrars: entities that sell and register domain names. As with virtually all services on the Internet, these businesses are abused by criminals. Phishing sites, command-and-control servers for botnets, and the distribution of child pornography, malware and spam all require such services. Like ISPs, hosting providers can thus play a key role in fighting cybercrime. Much of the criminal activity runs on compromised servers of legitimate customers but some run on servers rented by the criminals themselves. In either case, the hosting provider typically becomes aware of the problem only after being notified of the abuse. Responses to abuse reports vary widely, ranging from vigilant to slow to negligent (Canali, Balzarotti, and Francillon 2013; Stone-Gross, Kruegel, et al. 2009; Bradbury 2014). In a small number of cases, the hosting provider passively or actively facilitates the criminal enterprise and shields it from takedown attempts—a practice referred to as 'bulletproof hosting'.

While there is a wealth of research on security issues in hosting infrastructure, only a fraction has been done from an economic perspective. Moore and Clayton (2007) have studied hosting provider incentives to take down phishing sites. They found evidence for a 'clued-up' effect: it took time before a provider became aware and incentivized enough to start taking down sites. Once that effect occurred, takedown speed rapidly increased and stayed at this improved level. In a follow up study, Moore and Clayton (2009) expanded the research to other forms of Internet content and various notice and takedown regimes. The findings show that requester's incentives outweigh other factors in predicting takedown speed including the content, penalty, and evasion technology. Another study by Vasek and Moore (2012) looked at the responses of hosting providers to notifications of sites that were compromised with malware. It found that notifications that included comprehensive technical data of the detected problem were more likely to trigger takedown action on the side of the providers. This might be related to the competing incentives of providers: they do not want to disrupt service to their customers, while also protecting them and others from the negative consequences of compromised security. Extensive evidence helps them to legitimate countermeasures vis-à-vis their customers.

The overall effects of takedown actions seem limited. Criminal activity might be concentrated at some providers or registrars. Getting those providers to act can dramatically reduce the level of abuse in those networks, but the attackers are prepared for this and merely migrate their activities to other providers (Liu et al. 2011; Levchenko et al. 2011). The result is a game of whack-a-mole. Organizing collective action against criminal activities in the hosting sector is made more difficult because this market is not nearly as consolidated at many other online markets. In the absence of reliable reputation signals, it seems unlikely that market incentives alone will result in higher security levels across the thousands of hosting providers.

### *Payment Service Providers and Certificate Authorities*

Payment and other financial service providers (FSPs) are no strangers to attacks. Annual global losses from financial fraud amount to billions of dollars (R. Anderson et al. 2013). At the same time, these intermediaries have benefited tremendously from the growth of online payments, and in relative terms, fraud has been stable or diminishing (Financial Fraud

Action UK 2015). This is because they have become good at detecting fraud while maintaining convenience, for instance by profiling credit card transactions in real time in their back-end systems, rather than imposing additional security measures on the users directly. One advantage they have is that calculating the monetary gains and losses of certain trade-offs is easier for them than for other sectors. For example, after a data breach credit card issuers can calculate the relative cost of replacing cards or refunding victims of fraudulent cases (Graves, Acquisti, and Christin 2014). The FSPs have also been helped – perhaps paradoxically - by legal regimes in the U.S. and some European countries that limited the liability of consumers in cases of fraud. The burden of proof for fraud was put on the FSPs who actually had the capability to do something about it (Van Eeten and Bauer 2008). In short, financial service providers are in a position to internalize some of the externalities in the sector and thus absorb and mitigate the sector-wide costs of fraud.[6]

Related to payment providers and ecommerce platforms are certificate authorities (CAs)—organizations that issue digital certificates. Such credentials are intended to enable secure online communications, assuring confidentiality and integrity of information and transactions. A series of high profile breaches at CAs in recent years, most notably the breach and bankruptcy of DigiNotar in 2011 brought to light serious weaknesses in the current system (Arnbak and Van Eijk 2012). Vratonjic et al. (2013) looked at how TLS/SSL certificates are deployed on the top one million websites and found many misconfigurations. Durumeric et al. (2013) gathered all digital certificates in use in the public web and found hundreds of CAs with the authority to issue certificates that are recognized by browsers. If any of these CAs were to be breached, certificates can be maliciously issued for any other website, a serious negative externality. Arnbak et al. (2014) used the same data to calculate the market shares of CAs and connect them with their prices. Surprisingly, they found the market share of the most expensive CAs was much larger than cheaper CAs for identical certificates. This observation points to information

[6] Much research has been done into the technical aspects of online fraud, including analyzing malware, detecting fraudulent transactions and reverse engineering banking protocols. These topics touch upon economics but fall out of our scope. Crypto currencies are another topic that has received much attention in the literature due to its technical, economic, and regulatory aspects. The interested reader is referred to the conferences of the International Financial Cryptography Association (IFCA).

asymmetries that create advantages for the largest players. A technical fix to the protocols is required, but their adoption is complicated as long as CAs benefit from the status quo. Other intermediaries however, such as browser vendors and top websites, could play a role in pushing for new standards.

### *Search Engines and Participative Platforms*

Search engines, portals, and participative platforms are used to find content and connect to others. While these intermediaries have explored many different business models in the last decades, the market has converged on a business model in which users receive services for free while revenues are generated from targeted advertising. This development is driven by a combination of network effects and the 'economics of attention': in a world abundant with information, the scarcest resource is the attention of users (Shapiro and Varian 1998). These platforms fight for user attention (Davenport and Beck 2001). Since the marginal cost of information is close to zero, offering services at a low price or free is an economically rational strategy as it maximizes the size of the potential audience. Key players combine 'free' with a variety of nudging techniques to keep users on the platform (an interesting glimpse into this is the controversial study by Kramer et al. (2014) on changing the emotional content of Facebook news feeds to see how it effects users). Creating a revenue stream via advertisement is, of course, not new: broadcasting and newspapers have used the model for decades. The key difference is that targeted advertising can extract higher value (Goldfarb and Tucker 2011).

In terms of cybersecurity, these platforms overall seem to internalize costs to keep their users satisfied. Just to illustrate, Google has a team dedicated to protect users against state-sponsored attacks (Grosse 2012). This is not done out of nicety but as a competitive necessity: MySpace lost to Facebook partially as a result of increased spam and abuse on its network (Dredge 2015). Another example is handling 'click fraud'. When a bot imitates a legitimate user clicking an ad to generate revenue, the advertisers and the platforms are harmed financially and by the erosion of confidence. Chen et al. (2012) suggest that platforms will likely pay the costs of click fraud investigations thus internalizing some of the costs to the system at large. Schneier (2012) draws an analogy with

'feudal security' in the past: platforms provide users with security in exchange for allegiance. This approach has some benefits but it also comes with serious risks particularly with regard to privacy. Evidence of this tension is visible in how the platforms balance the interests of users and advertisers: Facebook Connect is preferred by many websites as a federated identity and password system over alternatives because of the user details it shares (Landau and Moore 2012).

## 2.6 Attacker Behavior

Over the past years, cybercrime has become highly differentiated and professionalized with a vast 'underground' (illegal) market that supplies various services required for an attack (Franklin et al. 2007). The division of labor can be illustrated with Zeus, an effective financial malware that caused considerable damage. It was coded by competent programmers that sold it as a do-it-yourself (DIY) kit for several thousand dollars (Riccardi et al. 2013). Fraudsters customized the malware and distributed it to their victims by either renting spamming services, directly deploying it via 'pay-per-install' services, or via other methods. After the malware was distributed, the attackers waited for victims and eventually managed to steal money and move it into other accounts. Finally, the money needed to be cashed out without leaving a trail. This was done using people known as 'money mules'. Thus, four major types of players were involved in Zeus, even though their roles may be carried out by vertically integrated players.

Cybercrime is also affected by the social relations among criminals. Because there is a risk of being cheated by a fellow criminal, Herley and Florêncio (2010) argue that prices in the underground markets are driven down to reduce the risks for buyers. In turn, this makes it less attractive to offer valuable items and creates a cycle of decay. The authors suggest this leads to a two-tier structure with IRC markets as the lower tier, filled with goods that are hard to monetize. Organization of criminal activities rather than ad hoc action is the route to profit. Repeated transactions are also a mechanism that incentivizes buyers and sellers to uphold their promises. Wondracek et al. (2010) looked at parts of the online adult industry employing practices that can be as best described shady: acquiring traffic and infecting visitors for a fee. Their measurements showed that traffic brokers honored the amount and origin of traffic they

were contracted for. Another mechanism, deployed in recent years on marketplaces active in the 'dark web', are seller ratings (Christin 2013). Similar to eBay, criminal buyers rate criminal sellers after a transaction; the reputation effect increases the incentives of criminals to stay honest. Despite these differences, both tiers of the underground market generate large negative externalities for society.

To be economically rational, the anticipated success rate and monetary value of an attack need to outweigh its costs. Florêncio and Herley (2013b) use this insight to explain the large gap between potential and actual harm online – the fact that most users do not get their accounts hijacked despite using pet names and birthdates as passwords. Automating attacks to scale is hard because of user diversity; it is also hard to know in advance which users offer sufficient financial prospects to be worth an attack. Herley (2012) presents this as the reason why Nigerian scams—the prince with five million dollars in dire need of your help—are so obvious. These scams are expensive to run and the attacker wants only the most gullible users. In short, many attacks cannot be made profitable on scale, which is one of the reasons why many doomsday scenarios did not unfold as predicted.

Focusing defender efforts on bottlenecks in the attacker monetization chain can be an ingenious way to reduce attacks. A monumental study has been the work of Levchenko et al. (2011) investigating the spam value chain. The team tracked a billion spam URLs and placed orders for the offerings (including Viagra). The study found that spammers fulfilled most purchases with real products (albeit generic versions). Interestingly, spammers refund unsatisfied customers to appease the scarcest resource in the spam value chain: the payment channel. Credit card companies put pressure on the acquiring banks who provide spammers with the ability to receive payments. Such financial relationships are very hard to replace, much harder than the technical infrastructure used for spamming and rogue pharmacies. Spam can be sent extremely cheaply via botnets, making conversion rates as low as one in 12.5 million viable (Kanich et al. 2008). Other elements are also readily available. But setting up relations within a credit card network turns out to be a bottleneck, as it requires legal documents, fees and time. Astonishingly, ninety-five percent of spam-advertised sales used merchant services from a handful

of banks. After the study was released, Pfizer and Microsoft, two big targets of spam advertised goods, asked VISA and MasterCard to act against these banks. This made a detrimental blow to spam profitability and production globally (K. Thomas et al. 2015).

Obviously, criminals do not like getting caught and paying a fine or spending time in jail reduces profitability. Law enforcement has been traditionally weak in cyberspace due to crimes crossing jurisdictions. This is gradually changing and law enforcement agencies are ramping up efforts, as evidenced by multiple high profile arrests in recent years (Krebs 2011). Anderson et al. (2013) believe investing in law enforcement abilities to arrest cybercriminals to be very efficient, as many attacks are run by a small number of gangs.

## 2.7 Policy Options

We have so far looked at the incentives of various actors in the Internet economy and how these affect their security decisions. We have seen that actors impose positive and negative externalities on others and the problems caused by asymmetric information. These are classic examples of market failures that weaken security incentives and will typically lead to suboptimal investment in security. We also saw that some actors, notably among Internet intermediaries operating in multi-sided markets, are willing to bear the costs of mitigating security failures of others. The unique competitive position of this group puts it in a position to make trade-offs between security and other qualities, possibly bringing the entire sector closer to a social optimum. However, in many situations no such endogenous mechanisms are available. This raises the question of whether and how forms of market failure can be remedied and what could be done to strengthen incentives to provide security. A traditional response to market failure is government intervention, but given the conflicting incentives of the state other forms of governance have been proposed as more effective (Brown and Marsden 2013; Moore and Anderson 2012). We continue with a brief discussion of theoretical and empirical contributions to the literature on policy options.

### *The Costs of Cybersecurity Breaches*

Ideally, private and public policy measures would take the actual and potential cost of cybersecurity breeches into account. This is one of the

preconditions of rational investment decisions by the private sector and of rational policy design. Unfortunately, while estimates and numbers abound, their reliability and representativeness is difficult to assess. Many reports are generated by players with a stake in inflating the numbers. They often are based on weak evidence and/or overly simplified strong assumptions. The employed methods typically are not publicly available, complicating an assessment of the validity and reliability of the information. Damage is typically assessed at a highly aggregated level and difficult to link to specific incidents. Florêncio and Herley (2013a) show that estimates are frequently biased by a few individual observations. Anderson et al. (2013) argue that the cost of prevention often exceeds the actual damage by orders of magnitude. With these caveats in mind, it is noteworthy that a joint study conducted by McAfee and the Center for Strategic and International Studies (CSIS) estimated the global costs of cybercrime at $445 billion, or about 0.6% of global GDP (CSIS and McAfee 2014).

Absent systematic and reliable metrics, it is at least possible to identify the types of costs good metrics would include. Because of the highly interconnected nature of the Internet, security incidents not only affect the immediate targets of an attack but also have second- and third-round effects on other stakeholders. From a policy perspective, the relevant cost is the total cost to society, which also includes the costs incurred by stakeholders other than those immediately affected. A comprehensive assessment of the costs and benefits of cybersecurity therefore should include the entire ecosystem of players including: users, private sector organizations, public sector organizations, Internet infrastructure providers (software vendors, ISPs, hosting providers, registrars), incident response units, society at large (including opportunity costs, lost efficiency gains, diminished trust and use of the Internet, etc.). It should also include revenues and profits made by cybercriminals, malevolent hackers, and all those seeking to profit from undermining the security of the Internet as these constitute 'bads' (that is costs) to society (Van Eeten, Bauer, and Tabatabaie 2009).

*Addressing Information Asymmetries*

Several approaches can help address information asymmetries, including mandatory breach disclosure, vulnerability disclosure, certification schemes, and the publication of security metrics.

*Mandatory Breach Disclosure.* Data breach disclosure and security breach notification laws aim to reduce harms caused to consumers resulting from breaches, and to incentivize organizations to invest in security to avoid bad reputation, by requiring them to notify all affected individuals when personal information has been compromised as a result of an attack or negligence. Critics of mandatory breach disclosure argue that they might perversely desensitize consumers or cause them to overreact. Data breach laws have been enacted in past years across a number of countries and most U.S. states. Romanosky, Telang and Acquisti (2011) found only weak empirical evidence in support of the effectiveness of disclosure laws. Between 2002 and 2009 disclosure requirements reduced identity theft by a mere 6.1 percent. This might be related to a finding by Nieuwesteeg (2013) that the vast majority of security breaches remain unreported, possibly due to firms calculating the risks of being discovered as smaller than notification and reputation costs. These costs include impacts of disclosure on stock market valuations of firms (Gordon, Loeb, and Zhou 2011). As other countries are considering adopting similar laws, there are discussions on how to design the details of such requirements. Thomas et al. (2013), for instance, recommend estimating and communicating the severity of breaches.

*Vulnerability Disclosure.* Should there be a mandate to publicly disclose a newly discovered software vulnerability? On the one hand, it forces vendors to acknowledge and prioritize releasing a patch; on the other hand it gives attackers information they might otherwise not have. Arora et al. (2010) looked at past evidence by analyzing the U.S. National Vulnerability Database (NVD) from 2000 to 2003. The data suggests that disclosures accelerated patch release. Ransbotham and Mitra (2013) evaluated differences between immediate disclosure and 'responsible disclosure', a procedure for first revealing the vulnerability in private to vendors before making it public after a certain period. Combining a dataset of intrusion detections from several hundred clients with the NVD for 2006 and 2007, the findings cautiously suggest that responsible disclosure is indeed beneficial.

*Certification Schemes.* Security certifications by trusted third parties have been proposed as fixes to the 'lemons market' problem affecting security aspects of products. Certifications schemes have been tried for software (R. Anderson and Moore 2006), for websites using various 'trust

seals', and the ISO 27000 information security standards. The success of these schemes hinges on who pays for the certification, who bears the costs of errors and what the certificates actually measure. Product sellers paying for certification have incentives to go to lax certification authorities. Even worse, Edelman (2011) observes an 'adverse selection' problem in that fraudulent websites have a higher probability of purchasing trust seals. Some certificates only demonstrate compliance with legal provisions. A great example of this is that DigiNotar passed the WebTrust EV audit for CAs just months before its spectacular collapse, while forensics revealed serious security problems (Prins 2011). This is not to say that security certification is not useful. It can still guarantee a basic level of good practices. However, it will not fully solve information asymmetry.

*Publishing Security Metrics.* Other market signals have also been proposed that simultaneously reduce asymmetry and allow organizations to self-evaluate. Organizations often believe they are doing enough to safeguard security. If they are presented with evidence that they do worse than their peers, they might increase efforts (e.g., Tang et al. 2013). The need for reliable measurements in cybersecurity has been known for a long time (Geer, Hoo, and Jaquith 2003; Pfleeger and Cunningham 2010). However, getting security metrics or measurements right is not an easy task. One should care not to confuse measurable properties with metrics that function as security indicators (Böhme 2010 provides a systematic overview). Designing, measuring, and reporting security metrics is a promising way to help markets produce security more efficiently.

### *Addressing Externalities*

Among the instruments proposed to help mitigate externalities are cyber insurance, liability rules, and better law enforcement.

*Cyber Insurance.* Insurance for cybersecurity incidents was proposed early on as a solution to align incentives, reduce information asymmetries, and enable firms to better manage risks (Schneier 2004; Böhme 2005). Scholars suggested that insurers would charge different premiums for different levels of cybersecurity and contingent on security practices, which would increase incentives for users to purchase more secure products and adopt better security policies. Nonetheless, these expectations did not materialize and the market for cyber insurance shrunk relative to the Internet economy (Böhme and Schwartz 2010). Shetty et al.

(2010) argue that quantifying cyber risks is fundamentally hard for insurers because of information asymmetries. In addition, the interdependent nature of cyber risks deviates from how risk is typically addressed in insurance markets, complicating the design of workable insurance policies.

*Assigning Liability.* Making users, organizations, and intermediaries liable for online harms caused by security breaches in their systems could tip security incentives toward higher investment. Fryer et al. (2013) examines the issue thoroughly by looking at liability theories and reviewing proposals in the security economics literature, for example, to make software vendors liable for bugs (August and Tunca 2011) or early calls to make users of bots liable for negligence attacks. In general, 'hard liability' will be a difficult sell in cybersecurity. In cases of clear negligence, it might make sense; however, tort law, existing 'duty to care' and consumer protection laws might be sufficient for the courts. Moreover, the forensics of establishing the facts of a case and measuring harm might not be easy. Due to the interdependencies, cascading harms might occur implying that firms may go bankrupt, become extremely risk-averse innovators, or resolve to create 'shell' companies. 'Softer' mechanisms—such as peer pressure, reputation effects, and regulatory coordination—might be much more effective. An alternative approach suggested by Ioannidis et al. (2013b) is to have an 'information steward' value harms to the ecosystem and allocate costs derived from externalities fairly among targets. Certain intermediaries such as Amazon Marketplace might be doing exactly this.

*Better Law Enforcement.* An alternative way to reduce externalities – and cybercrime – is to increase costs for attackers. This can be achieved by improving defenses, stricter law enforcement and by increasing the punishment for cybercriminals. Looking at the direct, indirect and defense costs imposed by cybercrime, Anderson et al. (2013) conclude that a more balanced approach is to spend less in anticipation of crime and more in response to it. Given the trans-border nature of many forms of cybercrime, this will also require improved international collaboration among law enforcement agencies.

## 2.8 Conclusion

In this chapter, we have seen that the economics of cybersecurity is a powerful tool to analyze security failures. By surveying the literature, we looked at the incentives of software vendors, organizations, end-users, Internet intermediaries, and attackers; where they align and produce security; and where the market fails. We highlighted the role of Internet intermediaries in securing the ecosystem. We then listed policy interventions proposed to address market failures. We further saw that the empirical evidence on policies is not always clear. In part, this is due to measurements difficulties, in part because aggregate outcomes are unclear, and in part because the responses of the dynamic system in which cybercrime develops are difficult to anticipate. For example, in the technology race between attackers and defenders tightened security eventually may lead to even more malicious forms of intrusion.

In the end, focusing on incentives rather than the technology helps understand trade-offs and develop sound cybersecurity policy. Given the dynamic nature of cybersecurity, all the issues discussed in this chapter are the subjects of ongoing research. Among emerging topics are security on mobile communications platforms, in the cloud, in the Internet of Things (IoT) and the industrial Internet, user behavior and education across life stages, the establishment of better national and international governance frameworks for security, and the development of better and more reliable metrics.

# References


Akerlof, George A. 1970. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84 (3): 488–500.

Anderson, Jonathan, Joseph Bonneau, and Frank Stajano. 2010. "Inglorious Installers: Security in the Application Marketplace." Paper presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), June 7-8, Harvard University. http://www.econinfosec.org/archive/weis2010/papers/session3/weis2010_anderson_j.pdf.

Anderson, Ross. 2001. "Why Information Security Is Hard - an Economic Perspective." In *17th Annual Computer Security Applications Conference (ACSAC 2001)*, 358–65. doi:10.1109/ACSAC.2001.991552.

———. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Tokyo, New York: Wiley.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. "Measuring the Cost of Cybercrime." In *The Economics of Information Security and Privacy*, edited by Rainer Böhme, 265–300. Berlin and Heidelberg: Springer. doi:10.1007/978-3-642-39498-0_12.

Anderson, Ross, Rainer Böhme, Richard Clayton, and Tyler Moore. 2008. "Security Economics and the Internal Market." Study commissioned by the European Union Agency for Network and Information Security (ENISA). http://www.enisa.europa.eu/publications/archive/economics-sec.

Anderson, Ross, and Tyler Moore. 2006. "The Economics of Information Security." *Science* 314 (5799): 610–13. doi:10.1126/science.1130992.

Arnbak, Axel, Hadi Asghari, Michel J.G. Van Eeten, and Nico Van Eijk. 2014. "Security Collapse in the HTTPS Market." *Communications of the ACM* 57 (10): 47–55.

Arnbak, Axel, and Nico Van Eijk. 2012. "Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain." Paper presented at the 40th Research Conference on Communication, Information and Internet Policy (TPRC 2012), September 21-23. doi:10.2139/ssrn.2031409.

Arora, Ashish, Ramayya Krishnan, Rahul Telang, and Yubao Yang. 2010. "An Empirical Analysis of Software Vendors' Patch Release

Behavior: Impact of Vulnerability Disclosure." *Information Systems Research* 21 (1): 115–32. doi:10.1287/isre.1080.0226.

August, Terrence, and Tunay I. Tunca. 2011. "Who Should Be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments." *Management Science* 57 (5): 934–59. doi:10.1287/mnsc.1100.1304.

Böhme, Rainer. 2005. "Cyber-Insurance Revisited." Paper presented at the Fourth Workshop on the Economics of Information Security (WEIS 2005), Harvard University. http://infosecon.net/workshop/pdf/15.pdf.

———. 2010. "Security Metrics and Security Investment Models." In *Advances in Information and Computer Security*, 10–24. Springer. doi:10.1007/978-3-642-16825-3_2.

Böhme, Rainer, and Tyler Moore. 2009. "The Iterated Weakest Link - A Model of Adaptive Security Investment." Paper presented at the Eight Workshop on the Economics of Information Security (WEIS 2009), June 24-25, University College London. https://www.is.uni-muenster.de/security/publications/BM2009_IteratedWeakestLink_WEIS.pdf.

Böhme, Rainer, and Galina Schwartz. 2010. "Modeling Cyber-Insurance: Towards a Unifying Framework." presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), June 7-8, Harvard University. http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf.

Bonneau, Joseph, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes." In *IEEE Symposium on Security and Privacy (SP) 2012*, 553–67. doi:10.1109/SP.2012.44.

Bradbury, Danny. 2014. "Testing the Defences of Bulletproof Hosting Companies." *Network Security* 2014 (6): 8–12.

Branscomb, Anne W. 1994. *Who Owns Information?: From Privacy to Public Access*. New York: Basic Books.

Bravo-Lillo, C., L.F. Cranor, J.S. Downs, and S. Komanduri. 2011. "Bridging the Gap in Computer Security Warnings: A Mental Model Approach." *IEEE Security and Privacy* 9 (2): 18–26. doi:10.1109/MSP.2010.198.

Brecht, Matthias, and Thomas Nowey. 2013. "A Closer Look at Information Security Costs." In *The Economics of Information Security and Privacy*, edited by Rainer Böhme, 3–24. Berlin and Heidelberg: Springer.

Brown, Ian, and Christopher T. Marsden. 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge, MA: MIT Press.

Camp, L Jean. 2013. "Beyond Usability: Security Interactions as Risk Perceptions." Paper presented at the Workshop on Risk

Perception in IT Security and Privacy, Newcastle, UK. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.385.7530&rep=rep1&type=pdf.

Canali, Davide, Davide Balzarotti, and Aurélien Francillon. 2013. "The Role of Web Hosting Providers in Detecting Compromised Websites." In *Proceedings of the 22nd International Conference on World Wide Web (WWW'13)*, 177–88. http://dl.acm.org/citation.cfm?id=2488388.2488405.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2004. "A Model for Evaluating IT Security Investments." *Communications of the ACM* 47 (7): 87–92. doi:10.1145/1005817.1005828.

Chen, Min, Varghese S. Jacob, Suresh Radhakrishnan, and Young U. Ryu. 2012. "The Effect of Fraud Investigation Cost on Pay-Per-Click Advertising." Paper presented at the Eleventh Workshop on the Economics of Information Security (WEIS 2012), June 25-26, Berlin. http://weis2012.econinfosec.org/papers/Chen_WEIS2012.pdf.

Christin, Nicolas. 2013. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." In *Proceedings of the 22nd International Conference on World Wide Web (WWW '13)*, 213–24. http://dl.acm.org/citation.cfm?id=2488388.2488408.

Clayton, Richard. 2011. "Might Governments Clean-up Malware?" *Communication and Strategies*, no. 81: 87–104.

Colander, David. 2005. "The Making of an Economist Redux." *The Journal of Economic Perspectives* 19 (1): 175–98.

CSIS, and McAfee. 2014. "Net Losses: Estimating the Global Cost of Cybercrime." Accessed July 14, 2015. http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/rp-economic-impact-cybercrime2.pdf.

CVE. 2015. "Common Vulnerabilities and Exposures List Master Copy." Accessed July 7, 2015. https://cve.mitre.org/cve/cve.html.

Davenport, Thomas H, and John C Beck. 2001. *The Attention Economy: Understanding the New Currency of Business*. Boston, MA: Harvard Business School Press.

Demetz, Lukas, and Daniel Bachlechner. 2013. "To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool." In *The Economics of Information Security and Privacy*, edited by Rainer Böhme, 25–47. Berlin and Heidelberg: Springer.

Dredge, Stuart. 2015. "MySpace – What Went Wrong: 'The Site Was a Massive Spaghetti-Ball Mess.'" *The Guardian*. March 6. http://www.theguardian.com/technology/2015/mar/06/myspace-what-went-wrong-sean-percival-spotify.

Durumeric, Zakir, James Kasten, Michael Bailey, and J Alex Halderman. 2013. "Analysis of the HTTPS Certificate Ecosystem." In

*Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13)*, 291–304.

Edelman, Benjamin. 2011. "Adverse Selection in Online 'trust' Certifications and Search Results." *Electronic Commerce Research and Applications* 10 (1): 17–25.

Fershtman, Chaim, and Neil Gandal. 2012. "Migration to the Cloud Ecosystem: Ushering in a New Generation of Platform Competition." *CEPR Discussion Paper*, no. DP8907. http://ssrn.com/abstract=2034125.

Financial Fraud Action UK. 2015. "Scams and Computer Viruses Contribute to Fraud Increases - Calls for National Awareness Campaign." http://www.financialfraudaction.org.uk/news-article.asp?genre=media&Article=2885.

Florêncio, Dinei, and Cormac Herley. 2010. "Where Do Security Policies Come From?" In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*, 10:1–10:14. http://doi.acm.org/10.1145/1837110.1837124.

———. 2013a. "Sex, Lies and Cyber-Crime Surveys." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 35–53. New York: Springer. doi:10.1007/978-1-4614-1981-5_3.

———. 2013b. "Where Do All the Attacks Go?" In *Economics of Information Security and Privacy III*, 13–33. Springer. doi:10.1007/978-1-4614-1981-5_2.

Fox-IT. 2012. "Black Tulip – Report of the Investigation into the DigiNotar Certificate Authority Breach." Version 1.0. By Hans Hoogstraaten and Others. Fox-IT. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update.html.

Franklin, Jason, Adrian Perrig, Vern Paxson, and Stefan Savage. 2007. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants." In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, 375–88. doi:10.1145/1315245.1315292.

Fryer, Huw, Roksana Moore, and Tim Chown. 2013. "On the Viability of Using Liability to Incentivise Internet Security." presented at the Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Georgetown University, Washington, DC. http://weis2013.econinfosec.org/papers/FryerMooreChownWEIS2013.pdf.

Gaynor, Martin S., Muhammad Zia Hydari, and Rahul Telang. 2012. "Is Patient Data Better Protected in Competitive Healthcare Markets?" presented at the Eleventh Workshop on the Economics of Information Security (WEIS 2012), June 25-26, Berlin. http://weis2012.econinfosec.org/papers/Gaynor_WEIS2012.pdf.

Geer, Daniel, Kevin Soo Hoo, and Andrew Jaquith. 2003. "Information Security: Why the Future Belongs to the Quants." *IEEE Security and Privacy* 1 (4): 24–32.

Goldfarb, Avi, and Catherine Tucker. 2011. "Search Engine Advertising: Channel Substitution When Pricing Ads to Context." *Management Science* 57 (3): 458–70. doi:10.1287/mnsc.1100.1287.

Goodin, Dan. 2009. "Superworm Seizes 9m PCs, 'Stunned' Researchers Say." *The Register*, January 16. http://www.theregister.co.uk/2009/01/16/9m_downadup_infections/.

Gordon, Lawrence A, and Martin P Loeb. 2002. "The Economics of Information Security Investment." *ACM Transactions on Information and System Security (TISSEC)* 5 (4): 438–57.

Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2011. "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" *Journal of Computer Security* 19 (1): 33–56.

Gottinger, Hans-Werner. 2003. *Economies of Network Industries*. London: Routledge.

Graves, James, Alessandro Acquisti, and Nicolas Christin. 2014. "Should Payment Card Issuers Reissue Cards in Response to a Data Breach?" Paper presented at the Thirteenth Workshop on the Economics of Information Security (WEIS 2014), College Park, PA. http://weis2014.econinfosec.org/papers/GravesAcquistiChristin-WEIS2014.pdf.

Groenewegen, John, ed. 2007. *Teaching Pluralism in Economics*. Cheltenham, UK and Northampton, USA: Edward Elgar Publishing.

Grosse, Eric. 2012. "Security Warnings for Suspected State-Sponsored Attacks." *Google Online Security Blog*. June 5. http://googleonlinesecurity.blogspot.com/2012/06/security-warnings-for-suspected-state.html.

Herley, Cormac. 2009. "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users." In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop (NSPW'09)*, 133–44.

———. 2012. "Why Do Nigerian Scammers Say They Are from Nigeria?" presented at the Eleventh Workshop on the Economics of Information Security (WEIS 2012), June 25-26, Berlin. http://weis2012.econinfosec.org/papers/Herley_WEIS2012.pdf.

Herley, Cormac, and Dinei Florêncio. 2010. "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy." In *Economics of Information Security and Privacy*, edited by Tyler Moore, David Pym, and Christos Ioannidis, 33–53. New York: Springer US. doi:10.1007/978-1-4419-6967-5_3.

Hofmann, Jeanette. 2010. "The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia." *London School of Economics Discussion Paper*, no. 62. http://ssrn.com/abstract=1710773.62.

Hofmeyr, Steven, Tyler Moore, Stephanie Forrest, Benjamin Edwards, and George Stelle. 2013. "Modeling Internet-Scale Policies for Cleaning up Malware." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 149–70. New York: Springer. doi:10.1007/978-1-4614-1981-5_7.

Ioannidis, Christos, David Pym, and Julian Williams. 2013a. "Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-Theoretic Approach." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 171–91. New York: Springer.

———. 2013b. "Sustainability in Information Stewardship." presented at the Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Georgetown University, Washington, DC. http://weis2013.econinfosec.org/papers/IoannidisPymWilliamsWEIS2013.pdf.

Kanich, Chris, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, and Stefan Savage. 2008. "Spamalytics: An Empirical Analysis of Spam Marketing Conversion." In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS '08)*, 3–14. http://dl.acm.org/citation.cfm?id=1455774.

Kelley, Timothy, and L. Jean Camp. 2012. "Online Promiscuity: Prophylactic Patching and the Spread of Computer Transmitted Infections." presented at the Eleventh Workshop on the Economics of Information Security (WEIS 2012), June 25-26, Berlin. http://weis2012.econinfosec.org/papers/Kelley_WEIS2012.pdf.

Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. 2014. "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks." *Proceedings of the National Academy of Sciences* 111 (24): 8788–90. doi:10.1073/pnas.1320040111.

Krebs, Brian. 2011. "72M USD Scareware Ring Used Conficker Worm." *Krebs on Security Blog*. June 23. http://krebsonsecurity.com/2011/06/72m-scareware-ring-used-conficker-worm/.

Kunreuther, Howard, and Geoffrey Heal. 2003. "Interdependent Security." *Journal of Risk and Uncertainty* 26 (2-3): 231–49.

Kwon, Juhee, and M. Eric Johnson. 2011. "An Organizational Learning Perspective on Proactive vs. Reactive Investment in Information Security." presented at the Tenth Workshop on the Economics of Information Security (WEIS 2011), June 14-15, George Mason University, Fairfax, VA.

http://weis2011.econinfosec.org/papers/An%20Organizational%20Learning%20Perspective%20on%20Proactive%20vs.%20Rea.pdf.

———. 2013. "Healthcare Security Strategies for Regulatory Compliance and Data Security." In *46th Hawaii International Conference on System Sciences (HICSS 2013)*, 3972–81. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6480324.

Landau, Susan, and Tyler Moore. 2012. "Economic Tussles in Federated Identity Management." *First Monday* 17 (10). http://uncommonculture.org/ojs/index.php/fm/article/view/4254.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic books.

Levchenko, K., A. Pitsillidis, N. Chachra, B. Enright, M. Felegyhazi, C. Grier, T. Halvorson, et al. 2011. "Click Trajectories: End-to-End Analysis of the Spam Value Chain." In *IEEE Symposium on Security and Privacy (SP) 2011*, 431–46. doi:10.1109/SP.2011.24.

Lewis, James Andrew. 2005. "Aux Armes, Citoyens: Cyber Security and Regulation in the United States." *Telecommunications Policy* 29 (11): 821–30. doi:10.1016/j.telpol.2005.06.009.

Liu, He, Kirill Levchenko, Márk Félegyházi, Christian Kreibich, Gregor Maier, Geoffrey M Voelker, and Stefan Savage. 2011. "On the Effects of Registrar Level Intervention." In *Proc. of the 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11)*. https://www.usenix.org/legacy/event/leet11/tech/full_papers/Liu.pdf.

Miller, Amalia R., and Catherine E. Tucker. 2011. "Encryption and the Loss of Patient Data." *Journal of Policy Analysis and Management* 30 (3): 534–56. doi:10.1002/pam.20590.

Moore, Tyler, and Ross Anderson. 2012. "Internet Security." In *Oxford Handbook on the Digital Economy*, edited by Martin Peitz and Joel Waldfogel, 572–99. Oxford: Oxford University Press. https://spqr.eecs.umich.edu/courses/cs660sp11/papers/moore-anderson-infoeconsurvey2011.pdf.

Moore, Tyler, and Richard Clayton. 2007. "Examining the Impact of Website Take-down on Phishing." In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit (eCrime '07)*, 1–13.

Moore, Tyler, Richard Clayton, and Ross Anderson. 2009. "The Economics of Online Crime." *Journal of Economic Perspectives* 23 (3): 3–20.

Musgrave, Richard A., and Peggy B. Musgrave. 1973. *Public Finance in Theory and Practice*. New York: McGraw-Hill.

Nieuwesteeg, Bernold F.H. 2013. "The Legal Position and Societal Effects of Security Breach Notification Laws." Master Thesis,

Delft University of Technology. http://repository.tudelft.nl/view/ir/uuid:38d4fa0e-8a3a-4216-9044-e8507a60ed66/.

Noam, Eli. 2009. *Media Ownership and Concentration in America*. New York: Oxford University Press.

OECD. 2012. "Proactive Policy Measures by Internet Service Providers against Botnets." OECD Digital Economy Papers 199. Paris: OECD Publishing. doi:10.1787/5k98tq42t18w-en.

Perset, Karine. 2010. "The Economic and Social Role of Internet Intermediaries." 171. OECD Digital Economy Papers. Paris: OECD Publishing. doi:10.1787/5kmh79zzs8vb-en.

Pfleeger, S.L., and R.K. Cunningham. 2010. "Why Measuring Security Is Hard." *IEEE Security and Privacy* 8 (4): 46–54. doi:10.1109/MSP.2010.60.

Ransbotham, Sam, and Sabyasachi Mitra. 2013. "The Impact of Immediate Disclosure on Attack Diffusion and Volume." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 1–12. New York: Springer. doi:10.1007/978-1-4614-1981-5_1.

Riccardi, Marco, Roberto Di Pietro, Marta Palanques, and Jorge Aguilà Vila. 2013. "Titans' Revenge: Detecting Zeus via Its Own Flaws." *Botnet Activity: Analysis, Detection and Shutdown*, Special Issue, Computer Networks, 57 (2): 422–35. doi:10.1016/j.comnet.2012.06.023.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management* 30 (2): 256–86. doi:10.1002/pam.20567.

Rosen, Harvey S. 2004. "Public Finance." In *The Encyclopedia of Public Choice*, edited by Charles Rowley and Friedrich Schneider, 252–61. Dordrecht: Kluwer Academic Publishers.

Rysman, Marc. 2009. "The Economics of Two-Sided Markets." *The Journal of Economic Perspectives* 23 (3): 125–43.

Schneier, Bruce. 2004. "Hacking the Business Climate for Network Security." *Computer* 37 (4): 87–89. doi:10.1109/MC.2004.1297316.

———. 2007. "A Security Market for Lemons." *Schneier on Security Blog*. April 19. https://www.schneier.com/blog/archives/2007/04/a_security_mark.html.

———. 2012. "When It Comes to Security, We're Back to Feudalism." *Schneier on Security Blog*. November 26. https://www.schneier.com/essays/archives/2012/11/when_it_comes_to_sec.html.

Shapiro, Carl, and Hal R. Varian. 1998. *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business School Press.

Shetty, Nikhil, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. 2010. "Competitive Cyber-Insurance and Internet Security." In *Economics of Information Security and Privacy*, edited by Tyler Moore, David Pym, and Christos Ioannidis, 229–47. New York: Springer US. doi:10.1007/978-1-4419-6967-5_12.

Shim, W. 2006. "Interdependent Risk and Cyber Security: An Analysis of Security Investment and Cyber Insurance." PhD diss, East Lansing, MI: Michigan State University.

Singer, Peter W, and Allan Friedman. 2013. *Cybersecurity: What Everyone Needs to Know*. Oxford: Oxford University Press.

Soghoian, Christopher, and Sid Stamm. 2012. "Certified Lies: Detecting and Defeating Government Interception Attacks against SSL." In *Financial Cryptography and Data Security*, edited by George Danezis, 250–59. Lecture Notes in Computer Science 7035. Berlin and Heidelberg: Springer. doi:10.1007/978-3-642-27576-0_20.

Stajano, Frank, and Paul Wilson. 2011. "Understanding Scam Victims: Seven Principles for Systems Security." *Communications of the ACM* 54 (3): 70–75. doi:10.1145/1897852.1897872.

Stone-Gross, Brett, Ryan Abman, Richard A. Kemmerer, Christopher Kruegel, Douglas G. Steigerwald, and Giovanni Vigna. 2013. "The Underground Economy of Fake Antivirus Software." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 55–78. New York: Springer. doi:10.1007/978-1-4614-1981-5_4.

Stone-Gross, Brett, Christopher Kruegel, Kevin Almeroth, Andreas Moser, and Engin Kirda. 2009. "Fire: Finding Rogue Networks." In *Anual Computer Security Applications Conference 2009 (ACSAC '09)*, 231–40.

Sullivan, Kevin. 2012. "The Internet Health Model for Cybersecurity." New York: EastWest Institute. http://www.ewi.info/idea/internet-health-model-cybersecurity.

Sunshine, Joshua, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. "Crying Wolf: An Empirical Study of SSL Warning Effectiveness." In *18th USENIX Security Symposium (Security '09)*, 399–416. http://static.usenix.org/legacy/events/sec09/tech/full_papers/sec09_browser.pdf.

Symantec. 2015. "Internet Security Threat Report Volume 20." Symantec. https://know.elq.symantec.com/LP=1542.

Tang, Qian, Leigh Linden, John S. Quarterman, and Andrew B. Whinston. 2013. "Improving Internet Security Through Social Information and Social Comparison: A Field Quasi-Experiment." presented at the Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Georgetown University, Washington, DC. http://weis2013.econinfosec.org/papers/TangWEIS2013.pdf.

Thomas, Kurt, Danny Yuxing Huang, David Wang, Elie Bursztein, Chris Grier, Tom Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. 2015. "Framing Dependencies Introduced by Underground Commoditization." Paper presented at the Fourteenth Workshop on the Economics of Information Security (WEIS 2015), June 22-23, Delft University of Technology, The Netherlands. http://weis2015.econinfosec.org/papers/WEIS_2015_thomas.pdf.

Thomas, Russell Cameron, Marcin Antkiewicz, Patrick Florer, Suzanne Widup, and Matthew Woodyard. 2013. "How Bad Is It? A Branching Activity Model to Estimate the Impact of Information Security Breaches (March 11, 2013)." *SSRN*. doi:10.2139/ssrn.2233075.

Van Eeten, Michel J.G., and Johannes M. Bauer. 2008. "Economics of Malware: Security Decisions, Incentives and Externalities." 2008/1. OECD Science, Technology and Industry Working Papers. Paris: OECD Publishing.

———. 2009. "Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications." *Journal of Contingencies and Crisis Management* 17 (4): 221–32.

———. 2013. "Enhancing Incentives for Internet Security." In *Research Handbook on Governance of the Internet*, edited by Ian Brown, 445–84. Cheltenham and Northampton: Edward Elgar.

Van Eeten, Michel J.G., Johannes M. Bauer, Hadi Asghari, and Shirin Tabatabaie. 2010. "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data." 2010/05. OECD Science, Technology and Industry Working Papers. Paris: OECD Publishing. doi:10.1787/5km4k7m9n3vj-en.

Van Eeten, Michel J.G., Johannes M. Bauer, and Shirin Tabatabaie. 2009. "Damages from Internet Security Incidents: A Framework and Toolkit for Assessing the Economic Costs of Security Breaches." Report for the Independent Post and Telecommunications Authority (OPTA, Now ACM). The Hague: OPTA. https://www.acm.nl/nl/download/publicatie/?id=9923.

Van Eeten, Michel J.G., and Milton L. Mueller. 2012. "Where Is the Governance in Internet Governance?" *New Media & Society* 5 (5): 720–36.

Vasek, Marie, and Tyler Moore. 2012. "Do Malware Reports Expedite Cleanup? An Experimental Study." In *5th Workshop on Cyber Security Experimentation and Test (CSET '12)*. https://www.usenix.org/system/files/conference/cset12/cset12-final20.pdf.

Vratonjic, Nevena, Julien Freudiger, Vincent Bindschaedler, and Jean-Pierre Hubaux. 2013. "The Inconvenient Truth about Web Certificates." In *Economics of Information Security and Privacy III*,

edited by Bruce Schneier, 79–117. New York: Springer. doi:10.1007/978-1-4614-1981-5_5.

Wash, Rick. 2010. "Folk Models of Home Computer Security." In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*.

Wondracek, Gilbert, Thorsten Holz, Christian Platzer, Engin Kirda, and Christopher Kruegel. 2010. "Is the Internet for Porn? An Insight Into the Online Adult Industry." presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), June 7-8, Harvard University. http://iseclab.org/papers/weis2010.pdf.

Wood, Dallas, and Brent Rowe. 2011. "Assessing Home Internet Users' Demand for Security: Will They Pay ISPs?" presented at the Tenth Workshop on the Economics of Information Security (WEIS 2011), June 14-15, George Mason University, Fairfax, VA. http://weis2011.econinfosec.org//papers/Assessing%20Home%20Internet%20Users%20Demand%20for%20Security%20-%20Will%20T.pdf.

Zhang, Jing, Zakir Durumeric, Michael Bailey, Mingyan Liu, and Manish Karir. 2014. "On the Mismanagement and Maliciousness of Networks." In *Proceedings of the Network and Distributed System Security (NDSS) Symposium 2014*. http://web.eecs.umich.edu/~jingzj/paper/jing_ndss14.pdf.

Zittrain, Jonathan. 2008. *The Future of the Internet–and How to Stop It*. New Haven, CT: Yale University Press.