WP/17/185

IMF Working Paper

Cyber Risk, Market Failures, and Financial Stability

by Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson

INTERNATIONAL MONETARY FUND

 WP/17/185

IMF Working Paper

Western Hemisphere and Monetary and Capital Markets Departments

Cyber Risk, Market Failures, and Financial Stability

Prepared by Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson

Authorized for distribution by Stephan Danninger and Nigel Jenkinson

Abstract

Cyber-attacks on financial institutions and financial market infrastructures are becoming more common and more sophisticated. Risk awareness has been increasing, firms actively manage cyber risk and invest in cybersecurity, and to some extent transfer and pool their risks through cyber liability insurance policies. This paper considers the properties of cyber risk, discusses why the private market can fail to provide the socially optimal level of cybersecurity, and explore how systemic cyber risk interacts with other financial stability risks. Furthermore, this study examines the current regulatory frameworks and supervisory approaches, and identifies information asymmetries and other inefficiencies that hamper the detection and management of systemic cyber risk. The paper concludes discussing policy measures that can increase the resilience of the financial system to systemic cyber risk.

JEL Classification Numbers: D5, D62, D82, G2, H41.

Keywords: Cyber risk, systemic risk, cyber insurance, cyber regulation, risk management, information asymmetries, market failure.

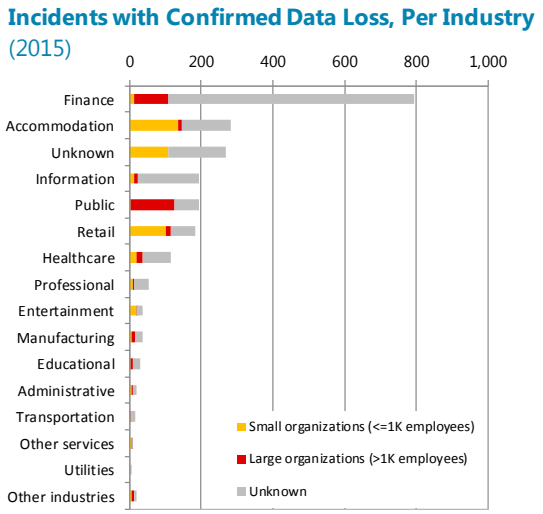
Author's E-Mail Address: ekopp@imf.org, lkaffenberger@imf.org, cwilson@imf.org.

Table of Contents

I. INTRODUCTION

Increased digitalization brings efficiency gains for financial institutions and fosters financial inclusion but it also creates a range of new and partially understood risks that evolve quickly and take multiple forms. One of the key risks is cyber-attacks against financial institutions. These are becoming more common and considerably more sophisticated.

Large-scale data breaches[1] feature prominently in the media. All types of banks—from small community and regional banks to the U.S. largest bank holding companies—money transfer services, and third party payment processors have seen their systems compromised. Financial market infrastructures have been attacked and, given the financial system's dependence on a relatively small set of technical systems, knock-on effects from downtimes and service disruptions due to successful attacks have the potential to be widespread and systemic.



Source: Verizon. IMF staff illustration.

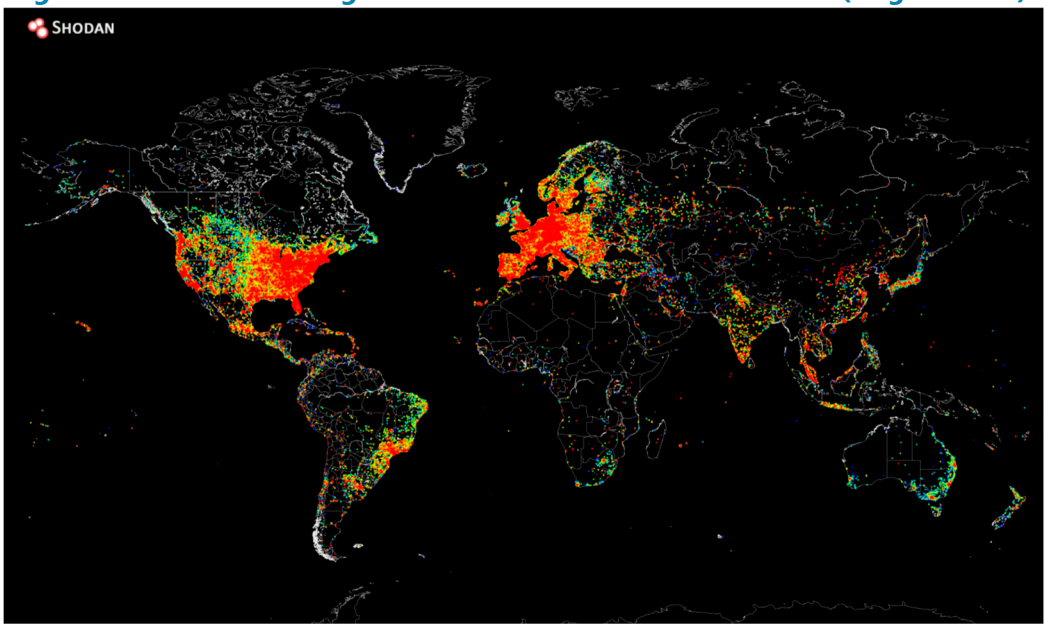
Cyber-attacks occur with increasing frequency amid ever-decreasing costs of technology. Box 1 gives examples of recent prominent cyber-attacks on the financial industry. Unsurprisingly, the financial sector is a popular target. According to a Verizon (2016) survey, the finance industry in 2015 has seen by far the most incidents with confirmed data losses.

Virtually everybody is exposed to cyber risk in some form. The economic aspects of cybersecurity are gaining increased importance and visibility, and the days when cyber risk was understood as a pure IT problem are now gone. Today, many countries set the development of a cybersecurity industry and standards as key policy objectives. Visualizing the number of electronic devices connected to the internet, Figure 1 illustrates the ubiquity of the *Internet of Things*.[2]

[1] *Incidents* are security events that compromise the integrity, confidentiality or availability of an information asset. *Breaches* are incidents that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party (see Verizon, 2013).

[2] The *Internet of Things* are everyday electronic devices that are connected to the internet, and send and receive data. Examples include cell phones, car electronics, and smart devices but also household appliances (thermostats, refrigerators, etc.).

Figure 1. Internet of Things: Devices Connected to the Internet (August 2014)[3]



Source: Shodan (2017).

Box 1. Recent Cyber Attacks on the Financial Services Industry

Financial sector institutions have experienced many cyberattacks including website Denial of Service attacks for extortion, fraudulent money transfer scams, and credit card fraud. Some of the most dangerous cyberattacks that the financial sector has so far experienced have affected financial infrastructures (messaging systems such as SWIFT), deliberately destroyed files and hardware (DarkSeoul), or compromised data and systems in a way that adversely impacts the provision of services (Corkow malware). These breaches have undermined confidence in the financial system or individual institutions.

Transfer fraud via compromised SWIFT servers: 2016 Bangladesh Bank

In early February 2016, criminals stole US$81 million from the central bank of Bangladesh. The criminals managed to get malware onto the bank's SWIFT server that defeated the business process controls, allowing the criminals to send transfer messages worth almost US$1 billion USD – some of the transfer messages were stopped due to a typographic error.[4] Another example is that of KfW, a German development bank, which in February 2017 erroneously transferred $5.4 billion to four other banks,[5] reportedly due of a technical problem that repeated single transfers multiple times. These events illustrate how perpetrators can gain financially if they obtain access to a bank's funds transfer system.

Destructive attacks against computer systems: 2013 Dark Seoul malware.

[3] Shodan (search engine for internet-connected devices). URL: https://imgur.com/aQUHzgu
[4] Reuters (2016).
[5] Bloomberg (2017).

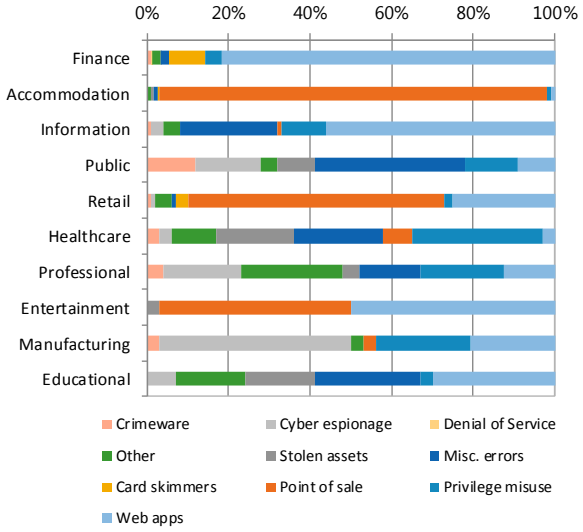
In March 2013, threat actors conducted cyberattacks against three South Korean banks. These attacks halted some bank branch operations when the virus erased files. The attacks also disrupted money transfer and ATM operations infecting 48,000 computers and inducing losses estimated at US$738 million.[6, 7]

Malware on a bank trading terminal: 2016 Corkow Malware

In September 2014, criminals compromised asset trading terminals in a Russian bank by using a malicious software called Corkow. Months later, the criminals used the Corkow malware to execute several high value dollar trades totaling $400 million. The trades occurred over a 14-minute period and caused a sudden 15 percent price swing in the USD/Ruble exchange rate.[8, 9]

Cyber-attacks evolve quickly and are highly dynamic by nature, which complicates risk assessment. Cyber incident patterns differ greatly across industries and over time. For instance, while all U.S. industries have seen an increase in web application attack patterns, the financial industry experienced a seismic shift in the importance of that method which, per Verizon (2017), increased from 31 percent in 2014 to 82 percent in 2015. Other means of attack have consequently lost importance. About two thirds of attacks on the U.S. financial sector involved ATMs, followed by databases and servers, at 20 percent each (Verizon, 2017). A notable exception from the financial motive are denial-of-service (DoS) attacks[10] which, per Verizon (2017) estimates, constitute 34 percent of all incidents (not breaches). This survey also showed that, while it takes perpetrators usually less than an hour to enter a system, 61 percent of attacks and 65 percent of breaches took weeks or more to discover. One in three breaches is discovered by external fraud detection providers, followed by law enforcement (20 percent), and the attacked firms' customers (15 percent). The fact that customers detect one in seven breaches in the survey results (double the cross-industry average) highlights that customers of financial services firms are very vigilant when checking statements and account data.

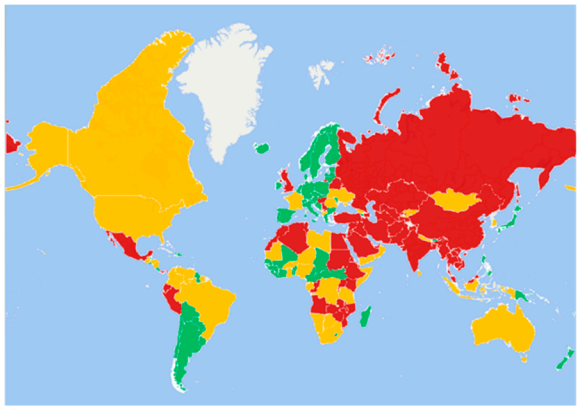
Patterns for Confirmed Breaches, Per Industry (2015)



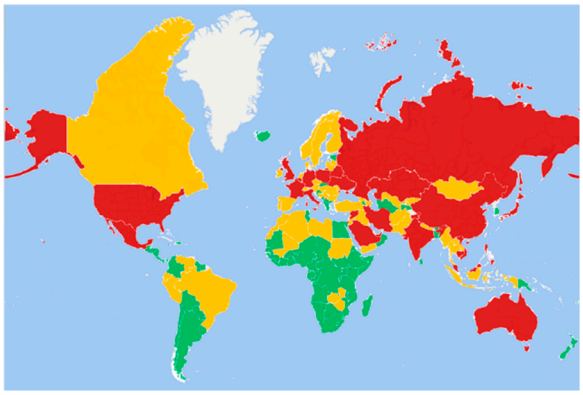
Source: Verizon. IMF staff illustration.

[6] http://english.yonhapnews.co.kr/northkorea/2013/04/10/49/0401000000AEN20130410007352320F.HTML
[7] http://english.yonhapnews.co.kr/northkorea/2013/10/15/16/0401000000AEN20131015003200315F.html
[8] Polozov (2016).
[9] http://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf
[10] DoS attacks do not involve direct stealing of data or money, but compromise the attacked firm's provision of services to customers as websites are knocked offline as the website is overwhelmed with traffic

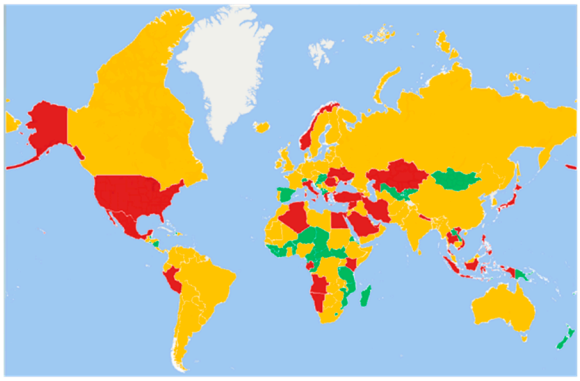
Figure 2. Sources of Threat by Type of Actor (March 2017)



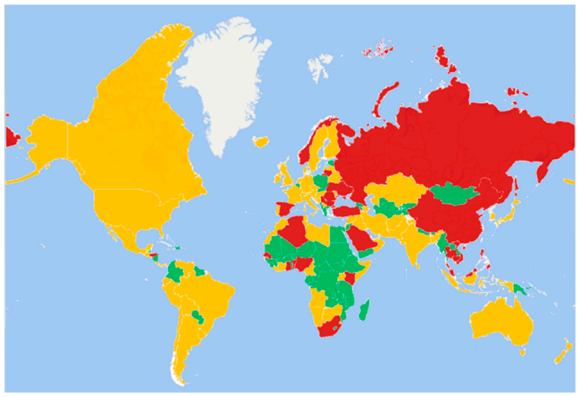
Communication Monitoring



Proxy Organizations



Cybercrime



Hacktivism

Source: IMF and Booz/Allen/Hamilton.

The internet is largely anonymous, which complicates the identification and attribution of cyber threats. The financial industry has been tackling the problem of non-identifiable perpetrators (cyberspace attribution problem) by trying to understand the motivations and capabilities of threat actors. Information gained about threat levels can then be combined and illustrated using cyber threat maps. For instance, Figure 2 gives a geographical illustration of the level of cyber threat that financial institutions and governments are exposed to. The color scale used for the charts range from green (low risk) to yellow (medium risk) to red (high risk).[11]

[11] *Communications monitoring* refers to the surveillance of communication generated over communications networks to a group of recipients by a third party. *Proxy organizations* are highly sophisticated and persistent attackers conducting espionage on behalf of a beneficiary. *Hacktivists* are online protestors that aim to advance a political or ideological cause.

There are structural difficulties in estimating the cost and likelihood of cyber events. These arise from inexperience with large events, unknown patterns of shock transmission, the lack of comprehensive and cohesive data about events and, especially, the uncertainties around long-term impacts of cyber breaches. Complex risk aggregation has been particularly challenging for estimating the cost of cyber events, especially for cyber insurance companies. Incentives are also skewed toward the target institution not revealing the scale or nature of cyber-attacks. Consequently, individual firms tend to underestimate the scope and scale of cyber risk by not fully acknowledging the nature and probability of tail risk losses.

Cyber risk is a textbook example of a systemic risk. Exposures to cyber risk are common across firms, and risks become highly correlated under stress. The existence of information asymmetries, misaligned incentives, strategic complementarities, and externalities can lead to an underestimation and mispricing of cyber risk. Also, these same imperfections mean that the market for cyber risk transfer can fail leading to an inefficient allocation of risk across the financial system. The main sources of systemic cyber risk are exposures to access vulnerabilities, risk concentration, risk correlation and contagion. Yet, it is unclear what the best policy response to systemic cyber risk may be, including how to design ex-ante regulation and assign ex-post liability, and on which levels firms, governments, and international financial institutions need to cooperate.

Effective risk management on various levels is crucial to ensure that investments in cybersecurity are commensurate with the underlying risk. As with other financial risks, firms must decide how to manage the cyber risk they are exposed to. The risks identified, analyzed, and evaluated in the risk assessment need to be actively managed, including through reduction, transfer, and avoidance of risk. This paper argues that, due to the existence of negative externalities in the private market, there is a clear role for the public sector to regulate the market properly such that information asymmetries are reduced and unexpected losses in individual entities do not give rise to systemic risk. International financial institutions—like the Bank for International Settlements, the World Bank, and the IMF—have a long track record in collecting and disseminating information and data among members and fostering policy coordination among countries. Thus, they appear to be well placed to help address some of the informational and cross-border coordination challenges created by systemic cyber risk.

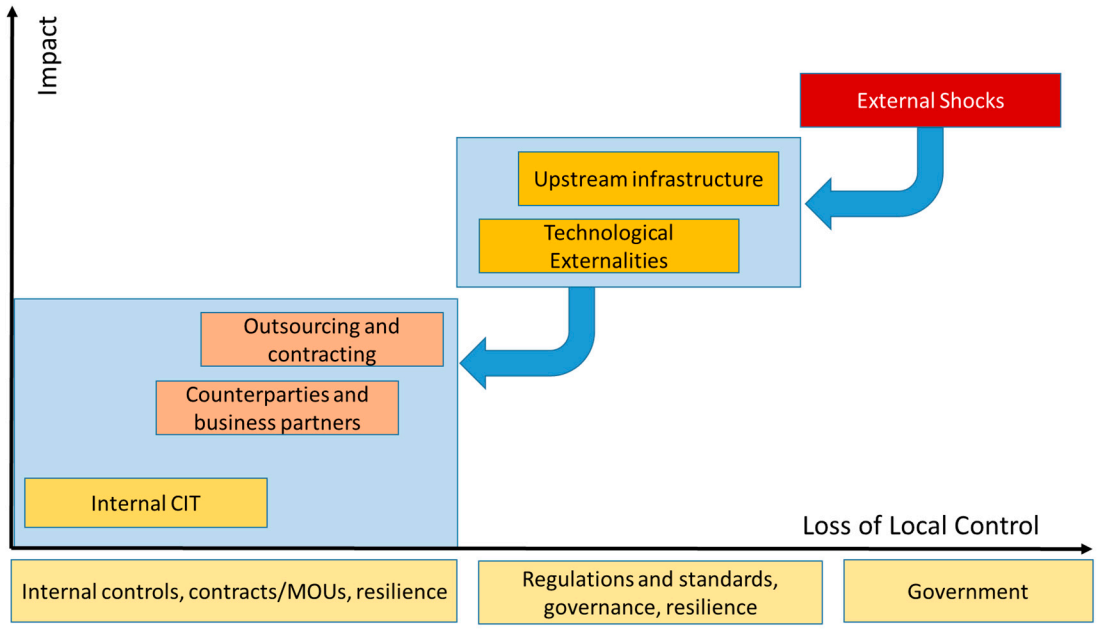
This paper considers the properties of cyber risk, including risk aggregation and intertemporal effects (section II), discusses why the private market can fail to provide the socially optimal level of cybersecurity and how systemic cyber risk interacts with financial stability risk (section III). Furthermore, this study takes stock of current regulatory frameworks and supervisory approaches, and evaluate their appropriateness to reduce systemic risk (section IV). Finally, section V discusses measures that can help increase resilience to cyber risk.

II. Cyber Risk

A. Cyber Risk Aggregation and Intertemporal Effects

Firms, including financial services institutions, have long viewed cyber risk mainly as an internal, IT security problem. Over time, this perspective has evolved to also include operational risks linked to the firm's immediate business partners—including counterparties and third parties to which certain cyber-security activities, like threat monitoring or data storing, have been outsourced. Thus, internal risk management processes and controls have extended to cover firms and customers that are immediately related to the firm's business. In many cases, firms use contracts or memoranda of understanding (MOU) to overcome information asymmetries (e.g. with business partners and third party vendors), to clarify cyber security standards for those firms, and to assign responsibilities (e.g., for response in the event of a cyber incident or payment in the event of financial loss).

Figure 3. Impact, Shock Transmission, and Control



Source: Based on Atlantic Council (2014); authors.

The true aggregation of risks related to cyberspace goes well beyond the internal monitoring and risk management capacities of an individual institutions (Figure 3). For example, there are risks stemming from upstream infrastructure (e.g., electricity, water supply, financial market infrastructures) or technological externalities (e.g., the entry of disruptive new technologies) which are outside the control of individual firms. In addition, even with MOUs and contracting arrangements it is virtually impossible to monitor cyber risk and vulnerability even of close business partners. So far, the industry has attempted to control risk arising from these external dimensions through regulations and standards.

Finally, risks can also arise from unanticipated external shocks, like international conflicts that give rise to cyber-attacks. Shocks on that level arise outside the system and control of institutions, affecting large parts of cyberspace, and require some form of government intervention and cannot be managed either by the private market or through ex-ante regulations. Table 1 gives a comprehensive picture of the different levels of risk aggregation in the cyber domain, illustrated with examples. The levels are ranked by the degree of control an individual institution may have over these sources of risk.

Table 1. Cyber Risk Aggregation Levels

	Description	**Examples**
Internal communication and information technology (IT)	Organization's internal IT systems	Hardware, software, servers, staff, data.
Counterparties and business partners	Risks due to dependence on other parties, or direct interconnections.	Relationship between financial institutions (e.g., through interbank lending); joint ventures; associations.
Outsourcing and contracting	Contractual relationships with external service providers, inducing concentration risk.	IT and cloud providers; outsourced legal, HR, or consulting activities.
Technological externalities	Disruption from or to new technologies which are not well understood.	Internet of Things; automatization of services; artificial intelligence.
Upstream infrastructure	Disruptions to basic infrastructure that the financial system relies on.	Electricity; telecommunication; internet access.
Feedback loops	Interrelationships between technologies and industries may give rise to cascading effects.	Unknown relationships suddenly become visible; dynamic range of failures.
External shocks	Risks arising outside the system and control of institutions, affecting large parts of cyberspace.	International conflicts; viruses, pandemics. Nearly impossible to predict.

Source: Based on Atlantic Council (2014); authors.

There is significant uncertainty surrounding the potential financial impact of cyber events. On the one hand, there are relatively well understood *direct costs* related to cyber incidents, including the cost of forensic investigation, legal assistance, customer notification, post-breach customer security and credit protection, and post-event measures to strengthen cybersecurity. *Indirect costs*, on the other hand, are less visible, more long-term and more difficult to quantify ex-ante. These include negative effects on brand name and customer relationships (reputational risk), the depreciation of intellectual property value, higher

ongoing operational expenses (to prevent future incidents), and the impact of a given incident on future cyber insurance premiums.

Table 2. Cost of Cyber Events

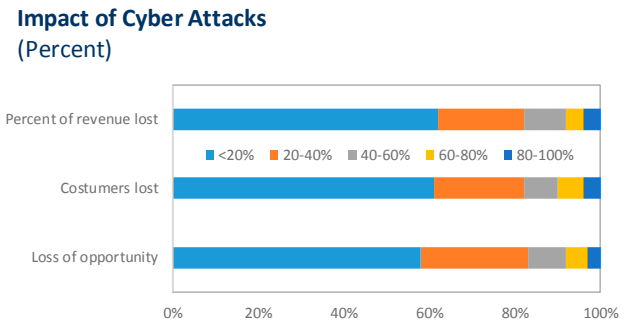
Phase	Direct Costs	Indirect Costs
Prevention (continuously)	• Cybersecurity costs (preventative safeguarding of systems and data) • Regulatory compliance cost	• Opportunity cost
Reaction (immediate)	• Technical investigation • Stop intrusion and initiate recovery of systems • Customer notification	• Cost of operational disruption • Opportunity costs • Loss in revenue • Loss in equity value
Impact management (short-term)	• Adjustment to infrastructure and processes • System and data recovery • Damage reduction • Post-breach customer protection • Initiation of cyber audit • Attorney and litigation cost	• Opportunity costs • Loss in revenue • Loss in equity value • Customer loss (turnover)
Business recovery and remediation (medium- to long-term)		• Increased funding costs • Lower future demand for breached firm's services • Redesign of business processes and systems • Rebuilding relationships, reputation and brand value • Investment in better security systems and preparedness capabilities

Source: Based on Deloitte (2016), and authors.

More than 90 percent of the total costs are attributable to indirect factors.[12] Costs manifest over time, and in four phases (Table 2):

- *Prevention* is the ongoing (ex-ante) effort to safeguard systems and data from cyber threats, which includes both preventative safeguarding and regulatory compliance costs.
- *Reaction* is the initial period after a cyber-attack is discovered. It includes a first analysis of what happened (forensics), followed by immediate measures to stop the intrusion and recover systems, develop communication strategies with customers, business partners and the general public, and prepare for potential (class action) law suits.
- *Impact management* involves efforts to address the direct impacts of the attack, including adjusting infrastructure and processes and initiating cyber audit processes and legal follow-up.
- *Business recovery and remediation* focuses on the repair of existing damage and the prevention of future events. This comprises a redesign of business processes and systems, rebuilding relationships and reputation, and investment in better security systems and preparedness capabilities.

The true cost of cyber-attacks manifests only over several years, which greatly complicates an ex-ante estimation of potential long-term costs of breaches. A Verizon (2017) survey showed that, in the U.S., revenue losses and the long-term cost of losing customers together make up three quarters of the estimated total cyber-event cost. The devaluation of the breached firm's brand name comes in third on the cost hierarchy. A survey on the impact of cyber-attacks[13] showed that around 60 percent of attacked firms report revenue and customer losses of up to 20 percent, and close to 10 percent report losses exceeding 80 percent of revenue. Opportunity costs show a similar pattern.



Source: Cisco 2017 Security Capabilities Benchmark Study

B. Impact Estimates for Cyber-Attacks

In contrast to many other financial and operational risks, loss data on cyber events is either not available or not useable for pricing cyber risk. For example, there is no

[12] Deloitte (2016), p. 3-7.
[13] Cisco (2017).

generally accepted framework that organizations can use to estimate and report the impact of cyber events.[14] Quantitative economic analysis in the field of cybersecurity has been hindered by the lack of useful data on the immediate and longer-term impact of cyber-attacks. Many cyber-attacks are reported late because in most cases attacks are discovered by third parties (like law enforcement and cybersecurity providers) and not by the breached firm itself. Separately, fearing an increase in insurance premiums or adverse effects on the firm's reputation or its customers' use of electronic services, firms often decide to withhold information about cyber events. Also, considering the speed with which cyber risk evolves, historic data is likely to be a poor predictor of future vulnerabilities or potential losses

Available cyber loss estimates show a wide range. Table 3 gives an overview of annual costs estimated in different studies. Globally, cyber losses have been estimated at $250 billion to $1 trillion. For the U.S., estimates range from $24 billion to a quarter trillion a year (0.1 to 1.3 percent of U.S. GDP). These costs can be compared with the GDP contribution of internet-related activities (Table 4): Internet-related activities contribute an estimated 4-7 percent to U.S. real GDP.[15] Therefore, being interconnected and digitized offers significant aggregate gains in output but it also gives rise to sizable vulnerabilities and potential losses. However, even for the upper range of cyber losses the net effect (both for the economy and individual institutions) is still likely to be positive.

Table 3. Estimated Annual Costs of Cyber Risk[16]

	Annual costs (USD bn)		Notes
	Global	U.S.	
McAffe (2013)	300-1000	24-120	Direct and indirect costs of cyber risk
McAffe (2014)	375-575	100	Direct and indirect costs of cyber risk
U.S. Department of Commerce		200-250	All kinds of IP theft, including cybercrime.
OECD (2012)	638		Cost of counterfeiting and data piracy.
Atlantic Council (2015)	250		Global cybersecurity costs.

[14] An exception is Borg (2009), who applies the concept of expected loss (Basel Committee on Banking Supervision, 1999) to cybersecurity risk and investment decisions.
[15] An OECD (2013) study found that internet-related activities contributed 7.1 percent of 2011 GDP, and Siwek (2015) estimated a 6 percent share of the U.S. economy's annual output. McKinsey (2011) estimated that over five years the internet contributed a cumulative 21 percent of GDP in advanced economies. Similar estimates were found for the G-20 and the European Union, see Hooton (2016). Dean and others (2012) estimated that the internet contributed 4.1 percent (or $3.1 trillion) of global GDP in 2011.
[16] McAffe (2014) is an update to the McAffe (2013) study.

Table 4. United States: Benefits, Costs, and Economic Net Benefit of Internet Use

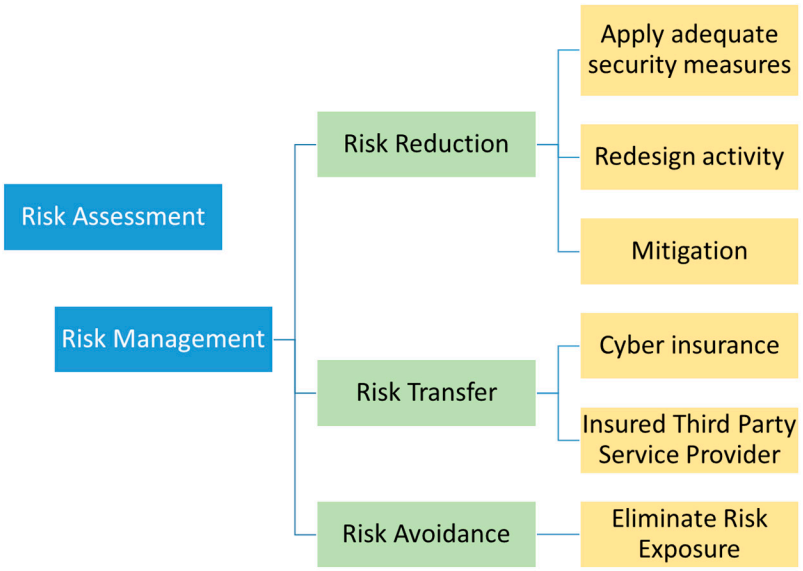
	Lower		Upper	
	Percent	Nominal	Percent	Nominal
Internet contribution to GDP	3.2%	573	6.0%	1,074
Cyber losses	0.6%	100	2.2%	400
Net benefit	**1.0%**	**173**	**5.4%**	**974**

Sources: Dean and others (2012); Hooton (2016); McAffe (2013, 2014); OECD (2013); Siwek (2015). IMF staff calculations.
Notes: Based on 2015 U.S. real GDP of $17.9 trillion. Nominal values are given in USD billions.

C. Cyber Risk Management

The risks identified, analyzed, and evaluated as part of a threat identification process need to be actively managed using largely common, risk management techniques. Active management is crucial to ensure that cybersecurity-related measures are appropriate for and commensurate with the underlying risk. The basic options are risk avoidance, risk reduction, and risk transfer (Figure 4).

Figure 4. Cyber Risk Management



Source: Authors.

Risk reduction. Risk can be reduced through active ex-ante risk management to align the likelihood and cost of a risk to a level that is consistent with the firm's preferred risk profile. This involves implementation of a range of security measures that can be physical (fences, locks), digital (security software like fire walls and data encryption), or human control measures (security training; role-based access rules). Risk mitigation activities can also include preparedness and business continuity planning that reduce the underlying cost in the

event a risk event materializes. These security measures are costly and often affect the systems usability and performance.[17]

Risk avoidance. A more fundamental management of exposure to cyber risk can involve redesigning the way activities are carried out. This may mean implementing adapting or changing products or processes, including a firm's business model, mechanism for processing payments, or the means to access certain systems. However, this is a dynamic process with new technologies and processes themselves creating new vulnerabilities that are only fully understood over time. .[18]

Risk transfer. This can involve buying cyber liability insurance or transferring the operational risk to a third-party service provider.[19]

- ***Cyber insurance*** (Box 2) can help arrive at a more efficient allocation of risks as it is a potential solution to the problem of information asymmetries. A functioning market for cyber risk transfer provides incentives for firms to invest in cyber defense systems, share data, and increase transparency since insurers reward both security investment and demonstrated openness by reducing premiums. In addition, it creates market incentives for insurers to collate data (including that shared with them by existing clients) to better understand the nature and frequency of cyber events. However, the current configuration of cyber liability policies may not allow for the most efficient transfer and allocation of risks. The evidence suggests that policies typically include conservative coverage limits (typically around $25 million[20]), and impose relatively restrictive exclusions and conditions. This, in turn, reflects the partial information that insurers have in pricing risk and the fast-changing nature of that risk. The combination of information asymmetries, difficulties in monitoring behaviors, and moral hazard problems that are typical of most insurance markets seem particularly binding in the case of cyber. This may mean there are effectively missing or incomplete markets for cyber risk insurance.

---

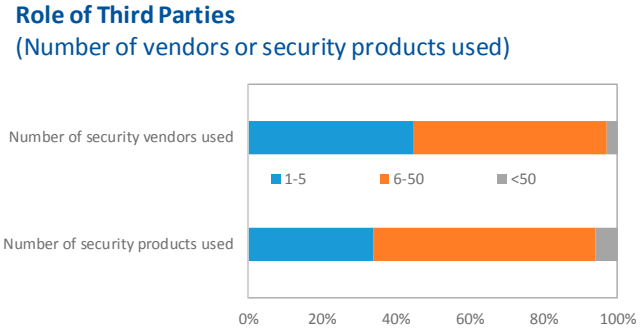
[17] For instance, fire walls reduce information flows, securing remote access considerably prolongs the process of accessing systems and data, impacting productivity. Other measures like encryption and cloud computing increase system complexity, and give rise to other technical risks. Importantly, security measures need to be adapted continuously as threats constantly change.

[18] These are ex-ante plans that outline which mechanisms will be used to reduce risk if a cybersecurity event materializes, how the adverse effects on economic or social activities can be limited and mitigated, and continuity and resilience of activities be enabled. The preparedness plan typically covers prevention, detection, response, and recovery.

[19] With indirect intermediary liability, third parties are held responsible for security incidents. This approach addresses the problem of non-identifiable perpetrators or otherwise liable parties that cannot bear the cost of security incidents. Third parties that are in a reasonably good position to detect threats or prevents incidents, and can sometimes even internalize negative externalities. Making vendors that supply security systems and frameworks are made indirectly liable, this can solve the principal-agent incentive problem discussed earlier.

[20] PwC (2015).

- Cybersecurity activities provided by ***third party service providers with indirect intermediary liability*** are an alternative to risk transfer mechanism. Rowe (2007) argues that if multiple organizations share the same service provider, economics of scale and information sharing can create positive externalities. In addition, if financial institutions use multiple suppliers to reduce concentration risk they have redundancies that increase resilience if one service supplier fails.[21] However, this dispersion of risk could get re-concentrated insofar as third party suppliers rely on a single firm, system or provider. For example, several cloud suppliers may use a common operating system so if that operating system has a vulnerability it could create a correlated risk across all cloud suppliers. Third party providers and software developers may or may not insure against cyber risk. However, even if the third-party providers are insured, low coverage limits and an inability to properly price risks could leave this firms still retaining a substantial amount of risk.



Source: Cisco 2017 Security Capabilities Benchmark Study

Box 2. Cyber Insurance

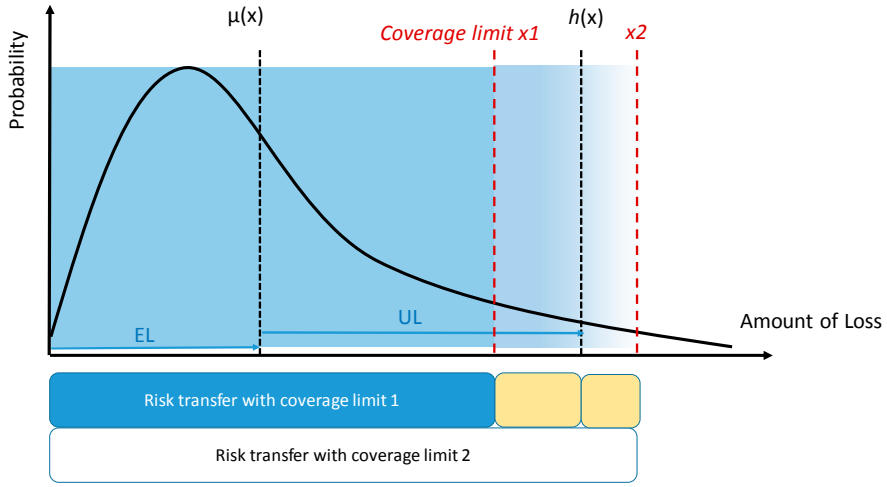
Cyber liability insurance is structured to transfer indemnifiable first and third party losses. Losses to the first party include the cost of crisis management, customer notification, network business interruption and associated direct cost,[22] systems recovery, and reconstitution of damaged software and digital assets (which would normally be covered under comprehensive crime insurance). Indemnifiable third party losses are those costs that are experienced by third parties. These include third party liability for security breaches and data privacy in general, defense costs, liability for failing to defend against a cyber-attack, but also investigation costs and, potentially, penalties and fines.

In 2016, 13 percent of all cyber insurance claims sampled by NetDiligence (2016) were caused by third-party vendors and 17 percent affected the financial services sector. Cyber insurance policies typically do not cover indirect costs from cyber-attacks that manifest over the medium- to long-term (like reputational damage, lost value of customer relationship, increased funding costs and insurance premiums, and the cost of having to beef up defense systems ex post to increase resilience against cyber risk). Such exclusions can be explicit or

[21] KPMG (2015), Cyber security: a failure of imagination by CEOs.
[22] Network interruption would not be covered under conventional business interruption insurance.

implicit by imposing coverage limits and very restrictive liability exclusions (in practice, even the largest financial firms have difficulties getting coverage limits of more than US$300 million[23]). This partial availability of coverage can render the market-based risk transfer mechanism inefficient, not covering unexpected losses in the tail of the distribution (Figure 5).

Figure 5. Coverage Limits and Effective Risk Coverage



Pricing cyber risk and liability insurance policies is challenging. Complex risk aggregation and the correlation of different risks in case of an event make cyber risk difficult to measure and even harder to price.[24] Also, the field is relatively new, and both firms and customers have very little experience with the characteristics of cyber risk or the longer-term effects of cyber-attacks and breaches on business relationships. Therefore, actuarial modeling techniques are underdeveloped compared to those for other insurable risks. Insurance companies have responded by adding a considerable cushion to the premium causing premiums to be higher relative to other types of coverage.[25] These difficulties in pricing can undermine the provision of financial protection, leaving gaps in coverage, and lead to an inefficient pricing and allocation of risks throughout the system. Further, there are concerns in the industry that risk exposures are becoming more concentrated in the insurance market and the insurance companies that are involved may not be able to withstand a large and correlated loss triggered by a systemic cyber-attack.

Cyber insurance is not a panacea for managing cyber risk. Despite its benefits, insurance coverage cannot replace active cyber risk management in financial firms. But as insurance companies gain more experience with cyber risk insurance, and the market matures, both the pricing of policies and the allocation of risks in the financial system will become more efficient, markets will be more complete, and cyber liability insurance will more efficiently transfer and pool risk.

[23] PwC (2015)
[24] OECD (2012).
[25] PwC (2015).

III. MARKET FAILURES

The market can fail to provide a socially optimal level of security due to information asymmetries, misaligned incentives, externalities, coordination failures and risk concentration. Furthermore, it is still under debate which approach works best in preventing the market from failing: ex-ante regulation and ex-post liability. Ex-ante regulation aims at preventing security risks to materialize, and can take the form of rules (laws) or guidance (compliance). While guidance is more adaptive when technologies or risks change rapidly, laws are more specific and easier to enforce. With ex-post liability, responsibility is assigned to a certain party. It is implicitly assumed that legal threats motivate the liable party to take security seriously, and invest accordingly. Critiques say that, with ex-ante regulation, the introduction of software liability would slow down innovation. and that it would basically be impossible for software developers to deliver a perfect product from the very start, as many bugs and inconsistencies are detected only when a new software is used in practice.

A. Information Asymmetries

Effective monitoring of others' activities in an anonymous and complex system like cyberspace is either impossible or extremely costly. Firms, including financial institutions, often lack the information needed to make informed decisions about how to best manage cyber risk, including how much to invest in cyber security. Firms cannot reliably judge ex-ante the extent of cyber risk they are exposed to, the effectiveness of defensive systems or third-party cybersecurity services, the resilience of market infrastructure the firm's operations rely on, or how high a liability insurance may be needed as to meet the long-term impacts of cyber-attacks. We know that asymmetry in information induces both moral hazard and adverse selection problems[26] which in turn can undermine the functioning of the system.[27] If asymmetrically distributed information is a systematic feature of the cyber system, the overall level of security of the system will be below the socially optimal level of security.

The information asymmetries in cyber are driven by a range of factors. First and foremost is the inexperience with cyber risk and events which complicates any quantification of cyber risk exposures. Also, the nature of the risks is diverse and evolving at a rapid pace which makes it difficult to characterize them in comparable terms (especially since risks stem directly from the firm and its business partners). In addition to these complications, there are other reasons not to share information to include legitimate concerns of reputational costs or an impact on the demand for that firm's services. These concerns lead firms to withhold information on the nature and costs of cyber events. Further, if a firm does have insurance, it

[26] Moore (2010), Böhme (2010).
[27] Borg (2016) observes a failure of markets involving software providers due to insufficient information about them.

must make a calculation of the net cost in terms of future premium increases that such a disclosure may create.

With both state and non-state actors involved in cyber areas there are strategic reasons why one country would prefer not to share information on the nature and size of its cyber losses or strategies in place to protect systems from cyber-attack. As highlighted in a U.S. Department of the Treasury (2017) report on financial regulation, there are important information asymmetries between different national regulators and across borders. The report pointed to the risk of fragmentation and overlap, and recommended better coordination of tools and examinations between federal and states' regulatory agencies. There is likely a need to harmonize the interpretation and application of existing rules by the different regulatory bodies. Since cyber risk is not limited by political or geographical barriers but a global risk, international policy coordination is needed as well—facilitating coordination, supporting information sharing, and designing coordinated policies

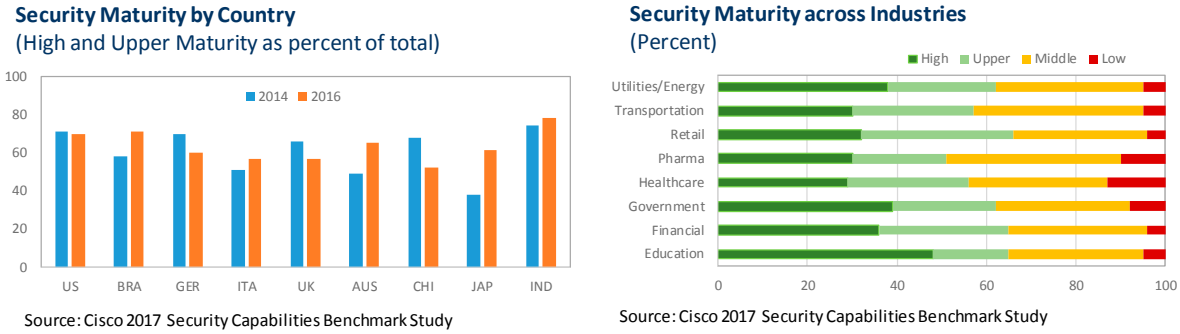
A final form of information problem is in judging the need or efficacy of particular types of cyber protection. Many firms, especially if they are smaller, lack the cyber-specific knowledge needed to make rational decisions about which software or cyber security provider to choose. Ex-ante, the net quality of different services or vendors is difficult to evaluate which can disincentive security investment[28] or cause firms to opt for cheaper (and perhaps less safe) solutions.

B. Strategic Complementarities, Coordination Failure, and Externalities

In general, externalities arise when one institution's behavior has side effects[29] that effect the net risk borne by others. Moore (2010) describes that investment in cybersecurity creates positive externalities within the same network: Individual firms' cyber risk decreases with additional investment in (i) the firm's own cybersecurity[30] and (ii) security in other organizations connected to the same network.[31] This is related to strategic complementarities (Cooper and John, 1988), where agents' decisions mutually reinforce one another and an agent's marginal return increases when the other agents' increase their action. This can lead to multiple equilibriums with different levels of cyber investment and underlying risk in the system. Through effective coordination, however, a better equilibrium could be achieved.

[28] See Varian (2004).
[29] Moore (2010).
[30] Such coordination failures create first-mover disadvantage as the utility of a particular cybersecurity investment depends on others' adoption of similar preventative measures.
[31] Security investment that generates positive externalities is described, for instance, by Kunreuther and Heal (2003), who argue that expected losses decrease with additional investment, but also with increasing security levels in organizations connected to the same network.

Figure 6. Maturity of Software Security



Moreover, software flaws create common exposures to cybersecurity risk. These externalities are not often internalized by the vendors and can induce negative externalities from exposure to the same network or technologies. Software developers do not particularly emphasize security until products achieve market dominance because it is more difficult and costly to develop applications for secure products.[32] As firms try to enter the market earlier than their competitors, new software is often pushed to the market with flaws not fully eliminated. Such flaws create common exposures to cybersecurity risk which are not internalized by the vendors and can induce negative externalities from exposure to the same network or technologies. Network externalities arise when a community of software users operate in the same large network, or use the same software or technologies. The choice of operating system or other software not only depends on its respective features but to a considerable extent on the number of users that already decided on that specific software. This also explains the dominance of certain systems in today's software markets. Figure 6 compares across countries (left chart) and industries (right chart) the maturity of software products, which are an indication of product security. According to a recent Cisco (2017) analysis, the U.S. is well above the 61 percent cross-peer country average. Software used by the financial sector typically show relatively high maturity, and the share of low- and middle-maturity products used is among the lowest.

Positive externalities can incentivize free-riding and cause under-investing. Böhme (2010) argues that if externalities persist, firms have incentives to free ride by under-investing in their own cybersecurity. If private costs are lower than social costs, with externalities not fully internalized and priced, market outcomes will not be efficient with an underinvestment in protection and the resulting negative externalities, should they be realized, being borne by the industry or society.[33]

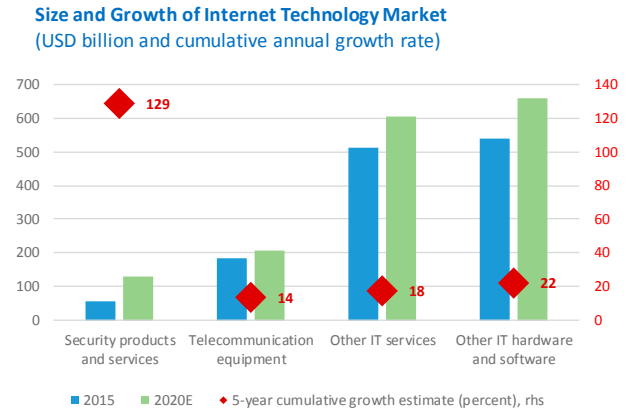
---

[32] The choice of operating system or other software not only depends on its respective features but to a considerable extent on the number of users that already decided on a specific software. This also explains the dominance of certain systems in today's software markets.

[33] Externalities often occur in situations where property rights have not been assigned. Access to and the use of the internet is largely non-rival and non-excludable, which are key properties of public goods. However, firms are aware of cyber risk and have clearly demonstrated their willingness to invest in cybersecurity, which indicates that there is a positive private return to cybersecurity.

C. Economies of Scale, Barriers to Entry and Risk Concentration

The market for cybersecurity services is dominated by a relatively small number of companies providing similar or indistinguishable products or services to an entire industry. In part this concentration is driven by a naturally increasing return in the provision of such services which can act as a barrier to entry for new companies, even if they have a superior technology (but an unproven track record). However, such oligopolies among providers can create correlated risks and common exposures for financial institutions since vendors and third-party providers frequently use similar software (including operating systems), hardware, and internet access modalities which creates significant common exposure to cyber risk. While the individual oligopolist has a strong incentive to protect its own systems, should that protection fail it can lead to systemic effects across the entire financial industry.



Source: Morgan Stanley (2016).

Insurance provision may also lead to a buildup of concentration risk. Among insurers, there are fixed costs and increasing returns in understanding cyber risks and developing insurance products to counter them. Since it is a specialized industry with a relatively small number of providers there is a risk of the insurance industry itself being a financial stability risk in the event of a widespread and coordinated cyber event. A.M. Best (2017) predicts that, in the U.S., the market for cyber insurance will see substantial growth, with coverages increasing up to $20 billion by 2020. In 2016, direct premiums written increased by one third year-on-year, expanding cyber insurance premium volume to $1.3 billion. The A.M. Best (2017) report on the U.S. cyber insurance industry points to considerable concentration risk in the market, with the largest three insurance writers (AIG, Chubb, and XL Group) covering 40 percent of the market, and the top-15 insurers serving 83 percent of the market. Although cyber insurance policies' direct loss ratio has recently seen a decrease (which has been attributed to a higher share of less-expensive forms of attacks, like ransomware), it is still around 50 percent. So far, the insurance industry has managed to fully cover incoming claims and make a profit—in part by building in sizable cushions in its premiums to account for these risks—but there is a legitimate concern that insurers may not be able to absorb highly correlated losses from a systemic attack on the financial system.

IV. Interactions of Cyber-related Market Failures and Financial Stability

Risk management in financial institutions has been focused on idiosyncratic risk. This is natural given an individual firms visibility and understanding of the broader systemic effects. However, this has meant insufficient attention in countering systemic cyber risks arising

from the dependence on complex infrastructure or disruptions to critical information. The predominance of cyber risk assessment on the level of individual institutions and entities signals a relatively narrow view that insufficiently considers the systemic dimension of cyber risk.[34]

Systemic risk arises where risk exposures are common or correlated across financial institutions. The main sources of systemic cyber risk to financial institutions are common exposures to access vulnerabilities, risk concentration, risk correlations, or contagion effects (including through reputational channels).

- ***Access vulnerabilities***. The financial system is one of the most connected systems in the global economy and, for business reasons, large parts of the industry's underlying systems can be accessed by customers and business partners from anywhere at any time. Hence, the system is characterized by inherent access vulnerabilities. Access protection is only as good as the safety level of its weakest link.

- ***Risk concentration*** is significant especially in key financial market infrastructures as well as for systemically important financial institutions. Certain financial market infrastructures, including central clearing platforms[35] (CCPs) or messaging systems like SWIFT are key hubs within the financial system. In addition, a small number of institutions handle a large share of the transaction volume in certain markets (e.g. for G7 foreign currency trading), much of it over proprietary electronic trading platforms. While they help standardize and enable global financial services they also generate concentration risk due to low (external) redundancy.[36,37] Although financial infrastructure systems are technically highly redundant, their function is clearly not. Problems in financial infrastructures can impact payment, clearing, and settlement of financial transactions, with negative externalities, exposing financial institutions, markets, and participants to unexpected shocks. As discussed before, cyber risk transfer via liability insurance has caused a build-up of risk exposures in the cyber insurance market. But systemic risk can also arise from technical and IT concentration, including from operating systems and programs; cloud servers; and electronic network hubs.

- ***Risk correlations and contagion***. Idiosyncratic cyber shocks can trigger funding liquidity risks, which can then morph into market liquidity shocks as firms are forced to shed

[34] The World Economic Forum (WEF) in 2015 offered one of the first definitions of systemic cyber risk: "*Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security."* See WEF (2015), p. 5.
[35] See Wendt (2015).
[36] If failing entities can be substituted with other (redundant) systems that perform identical or similar functions, systemic risk is lower compared to a situation in which there is no replacement.
[37] European and U.S. Regulators in 2016 achieved an agreement that links the CCPs across the Atlantic, and that extended CCP framework increases redundancies and lowers systemic risk.

assets, pulling down asset prices. It may also be the case that concerns over the integrity of counterparties leads firms to stop interacting with certain market participants, exacerbating pressures on the market-based recycling of liquidity. Materializing liquidity and market risk shocks can ultimately lead to solvency problems in financial institutions. Close direct connections through interbank and transfer markets, and indirect relationships (liquidity cascades) allow shocks to spread quickly throughout the system. An institution's inability to meet payment or settlement obligations—for example because their internal record-keeping or payments systems have been compromised—can cause a name crisis, which would have adverse effects on funding liquidity and knock-on effects to other institutions which were counting on the availability of these liquidity flows. Liquidity shortages can lead to fire-sales which then feed into asset valuations and spread to all kinds of market participants that are invested in or are trading a particular asset or asset class. Over time, liquidity risk-induced losses eat into firms' capital and end up weakening financial institutions' solvency positions.

As the connections between cyberspace and real economy intensify—amid a widely expected further increase in interdependency, interconnectivity and complexity—the probability for an external shock to transfer to the financial system and become a systemic event is likely to increase even if steps are taken to mitigate these risks.[38]

V. Financial Regulation of Cyber Risk

A. Cyber as an Operational Risk

Regulation of the financial services sector aims to promote long term economic growth and minimize the costs and negative externalities from financial instability.[39] A stable financial system is a prerequisite for a well-functioning economy that supports economic growth. In a stable financial system, institutions and markets will function, prices will reflect fundamentals and short-term stresses and fluctuations will only affect a limited circle of participants. To remain effective, however, regulation may need to adapt to new technological developments and risk factors such as cyber risk.

Given the pervasive role of technology in finance, regulators have established minimum standards for management of IT-related risks. An established regulatory framework for IT-related risks applies to the majority of financial services firms and regulators have traditionally thought about IT-related risks as a subset of operational risk which is a key pillar of the existing regulatory structure. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.[40] This formal definition includes legal risk, but excludes strategic and reputational risk.

---

[38] Reuters (2016).
[39] Minsky, Tommaso Padua-Schioppa.
[40] Basel Committee on Banking Supervision, 'International Convergence of Capital Measurement and Capital Standards', 2006.

Minimum standards for IT-related risks have traditionally focused on risk management including those that relate to handling major operational disasters (i.e., recovery and business continuity planning). Supervisors encourage financial services firms to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices.[41] Ideally, firms should adopt an integrated and risk-based approach to the management of IT-related risks which are identified, managed, and reported through the risk management function.

Operational risk frameworks include the need to quantify tail risks in the calculation of regulatory capital. The regulatory capital standards require banks to set aside capital for operational risk with the objective of absorbing unexpected losses. Banks are expected to calculate regulatory capital requirements as the sum of expected and unexpected losses. An integral part of this approach is the use of scenario analysis, in conjunction with external data, to evaluate its exposure to tail events. Scenario analysis is expected to be used to assess the impact of deviations from the correlation assumptions embedded in the bank's operational risk measurement framework. This includes evaluating potential losses that arise from multiple, simultaneous operational loss events. Over time, such assessments need to be validated and re-assessed through comparisons to actual loss experience. In conducting scenario analysis, banks are asked to estimate potential unexpected losses and set aside capital.

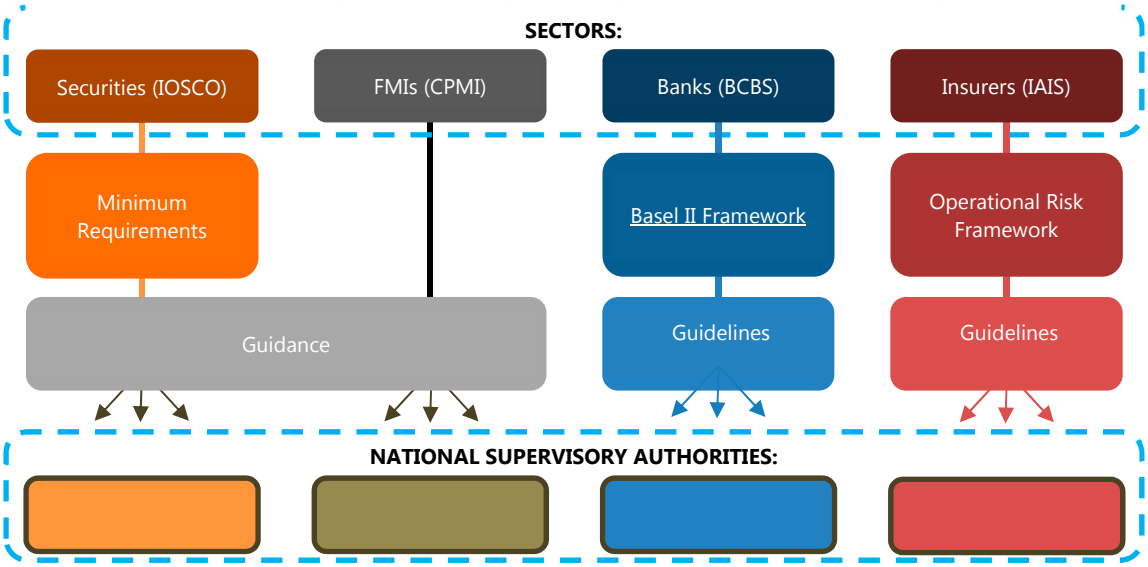
Risk management standards for IT-related risks are established by international standards-setting bodies (SSBs) and applied on a sectoral basis. For globally active financial services firms, SSBs have established a regulatory framework that sets minimum standards to encourage better risk management and allocate capital for unexpected losses, including risks from information technology. The existing framework for banks consists of a variety of guidance elements such as: Basel Core Principles[42], the Principles for the Sound management of Operational Risk[43], buttressed by the Basel Capital Accord[44] and various guidance papers dedicated to the topic of IT security and information management.[45] The requirements are applied on a sector by sector basis (see Figure 7).

[41] Basel Committee on Banking Supervision, 'Principles for the Sound Management of Operational Risk' June 2011.
[42] Basel Committee on Banking Supervision, Core Principles for Effective Banking Supervision, September 2012.
[43] Basel Committee on Banking Supervision, Principles for the Sound Management of Operational Risk, June 2011.
[44] Basel Committee on Banking Supervision, International Convergence of capital Measurement and Capital Standards, June 2006.
[45] Basel Committee on Bank... Management Principles for Electronic Banking, July 2003.

Minimum Requirements

Owing to the high reliance on technology in the securities and derivatives markets, explicit standards for cyber resilience have been implemented:[46] Operational problems in a payment, clearing, and settlement system may impede the control of, or even exacerbate, other types of risk such as market, liquidity, or credit risk in an unanticipated way that could pose a systemic risk, resulting in participants incurring significant losses. Payment and settlement related operational risks could spill-over into financial markets across a wide range of financial products with implications for global financial stability. For this reason, the IOSCO/CPMI guidance requires high standards of operational risk management for payments, clearing, and settlement systems.

Figure 7. Regulatory Architecture for Cyber Risk.



Source: Authors

Risk management standards for general IT-related risks are mature but cyber risks pose new challenges. Risks around cyber are different to traditional IT-related risks. The changing distribution channels and nature of cyber-related incidents require the regulations and supervisory approach to adapt to a rapidly changing risk profile. Effective management of technology-related operational risk is a fundamental element of a bank's risk management.[47]

The G7 has taken the first step toward standardized requirements for cyber risk. The G7 developed a set of non-binding, high-level fundamental elements designed for financial sector private and public entities.[48] The elements serve as the building blocks upon which an

[46] The Committee on Payment and Market Infrastructures and Board of the International Organization of Securities Commission's joint paper "Guidance on cyber resilience for financial market infrastructures, June 2016.
[47] Gracie (2015).
[48] Group of 7 (2016). The work program of the G7 Cyber Expert Group is progressing and will develop a set of a set of high level and non-binding fundamental elements for effective assessment of cybersecurity by October 2017 as well as work on third-party risks and the coordination with other critical sectors.

entity can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture. The elements include:

- Element 1: Cybersecurity Strategy and Framework
- Element 2: Governance
- Element 3: Risk and Control Assessment
- Element 4: Monitoring
- Element 5: Response
- Element 6: Recovery
- Element 7: Information Sharing

These are expected to be tailored by regulators and the financial institutions themselves to their own operational and threat landscape and legal and regulatory requirements. The elements also provide steps in a dynamic process through which the entity can systematically re-evaluate its cybersecurity strategy and framework as the operational and threat environment evolves. Public authorities within and across jurisdictions can use the elements to guide their public policy, regulatory, and supervisory efforts.

A reliable cyber risk reporting system is crucial. At the core of a well-functioning oversight system is the development of a cyber information asset prioritization program, a move to standardize data gathering, and build frameworks to model and price cyber risk. National authorities and regulations need to provide the right incentives to ensure cyber events are reported in a timely and accurate way. Standards for cyber risk should require financial institutions to provide internal cyber risk data, at first periodically, and eventually in real-time. Data reliability checks and automated processing would be responsibilities of the standard setters.

Due to the criminal nature of cyber-attacks, regulators will need to coordinate with relevant law enforcement agencies. Financial sector regulators should be able to quickly point out attacker(s) to appropriate enforcement agencies to ensure timely response, both from the legal and financial institution sides. Ideally there would be formal arrangements for a two-way exchange of information between law enforcement agencies and regulators.

Supervisors should have the flexibility to adapt their approach to cyber risk supervision in response to the fast-evolving nature of threats. Changing supervisors' mindset to fully embrace cyber as a business and economic risk is one of the main challenges in the transition from IT-based supervision. Another key factor is the ability of supervisors to develop a forward-looking cyber risk assessment based on available data and their understanding of

financial institutions' technology and business models, their evaluation of cyber risk appetites and breach trends, and their analysis of the evolution of the economic environment and implications for banks' activities and risk profiles. Perhaps more critical than other areas of financial supervision—given the speed of change in the overall landscape—is having the capacity and authority to adapt the supervisory response quickly as threats evolve.

Box 3. Approach to Critical Infrastructure

A differentiated approach for critical infrastructure is needed. Defining the scope of critical financial sector infrastructure and institutions is key to setting an effective cyber risk response. Certain types of financial institutions and infrastructures play a more pivotal role to the global financial and technological network, and thus may be responsible for spillover and contagion effects through the global financial system. Several jurisdictions (e.g., United States and Japan) have commenced this work by defining formally what constitutes critical infrastructure.[49] In Europe, the 2008 *Directive on European Critical Infrastructures* (ECI) established procedures for determining critical infrastructures, even though so far these have largely focused on energy and transportation (no financial ECI has been identified to-date). More recently, the *Network and Information Security Directive* addresses the need to identify critical infrastructure.

Public-private partnerships provide a pragmatic policy set-up, given limited incentives for coordination and cooperation across financial institutions. Public-private partnerships provide an effective channel for the sharing of information and coordination of cyber-threat prevention and identification across private entities, given there are limited private incentives to reveal instances of cyber-attacks. Such partnerships can be a good platform for exchanging information on cyber-threats and collaborating on cyber threat prevention and identification. In the United States a Cybersecurity Framework has been established, consisting of a set of voluntary risk-based industry-wide standards, guidelines and best practices.

Regulators and other policy-makers have taken important steps to improve the resilience of the financial sector to potential cyber threats. These include:

- In the U.S., the cybersecurity framework has been supported by more intense supervision and regulatory requirements to contain cyber risk-related vulnerabilities. The Federal Financial Institutions Examination Council (FFIEC) has initiated assessments to support smaller banks in addressing cybersecurity risks, inter alia via business continuity plans. For broker-dealers, the Securities and Exchange

[49] In the U.S., Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (February 12, 2013), established criteria for identifying critical infrastructure based on its ability to "reasonably result in catastrophic national effects on public health or safety, economic security or national security" in the event of a cyber-attack. In Japan, it was defined via the "Special Action Plan on Countermeasures to Cyberterrorism of Critical Infrastructure", adopted in December 2000.

Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) in 2014 announced broad examinations of cybersecurity preparedness.

- In Europe, the EU adopted a Cybersecurity Strategy in 2013, with emphasis on harmonization across states and on international cooperation. The EU also adopted a directive on Network and Information Security (NIS) in 2013, aiming at strengthening preparedness, cross-border cooperation and information exchange. In the UK, the authorities have set up a vulnerability testing framework to evaluate preparedness to simulated cyber-attacks. Through the so-called Waking Shark I and II exercises in 2011 and 2013, and more recently the CBEST vulnerability testing in 2014, the UK authorities have established a framework for bespoke, controlled cybersecurity tests across large UK financial institutions and FMIs. The framework also entails provision of detailed and reliable threat intelligence to the financial sector via the U.K.'s Certificateless Registry for Electronic Share Transfer (CREST).

- Japan has established a comprehensive cybersecurity policy, most recently enhanced by an updated Cybersecurity Strategy in 2013, which seeks to strengthen private-public information sharing; introduce business continuity exercises; establish a platform for evaluation and authentication of systems used by critical infrastructure; and enhance international cooperation.

- In Singapore, the government has introduced the National Cyber Security Masterplan 2018, with expected assessments of cybersecurity preparedness of critical sectors and the national infrastructure more broadly. In Australia, the government has established the Australian Cyber Security Centre (ACSC) to 'bring under one roof' the cybersecurity capabilities of various government agencies. In India, the government adopted a National Cyber Security Policy in May 2013 in an effort to establish a comprehensive cybersecurity mechanism.

- The Organization of American States (OAS) has established a secretariat to support better coordination across countries (including exchange of views and experiences) and the introduction of early warning mechanisms in each country.

B. Guidelines

For licensed financial institutions operating in the U.S., a sectoral approach to operational risk (including cyber) has been applied. Operational risks—including IT-related and cyber risks—are expected to be identified, managed and reported using an integrated approach to risk management.

The US authorities have stepped-up the focus on cyber resilience through targeted risk management standards and supervisory intensity for banks. U.S. bank regulators have implemented cyber security standards to protect financial markets and consumers from online attacks. The large bank holding companies (BHCs) are expected to have the most sophisticated defense capabilities and to be able to recover from any attack within two hours. Since 2013, banks include cyber risks and operational risks in the scenarios they submit in their annual stress tests. Banks prepare these scenarios as part of stress tests required under the Dodd-Frank Act. The agencies responsible for the supervision of BHCs (Federal Reserve, FDIC, and OCC) have issued an Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards.[50] The standards are tiered, with a set of higher standards for systems that provide key functionality to the financial sector. These enhanced standards do not apply to community banks.

Financial firms operating in securities markets also face a comprehensive supervisory framework. Owing to the high reliance on technology in the securities and derivatives markets a layered approach has been developed to build cyber resilience drawing on the Committee on Payment and Market Infrastructures and Board of the International Organization of Securities Commission's joint paper.[51] The general approach has been developed for the securities industry and financial market infrastructure but the framework is suitable for other financial sector participants. Key elements are requiring strong governance, the identification of systemic information assets ("crown jewels"); identifying cyber threats; building protections against cyber-attacks; the detection of abnormal events; reducing recovery costs through incident response planning; and comprehensive stress testing of systems and processes.

VI. Measures to Strengthen Resilience to Cyber Risk

A. Reducing Access Vulnerabilities while Boosting Resilience

Irrespective of the size of the financial institution, there are a few basic measures firms can take to address idiosyncratic cyber risk. Despite the enormous pace of technological progress over the last decades, the recipes and recommendations have been relatively constant. Different computer security experts effectively propose almost identical action lists that include:[52]

- Application whitelisting (only run pre-approved software on firms' computers);

[50] These standards apply to depository institutions and depository institution holding companies with total consolidated assets of $50 billion or more, the U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more, and financial market infrastructure companies and nonbank financial companies supervised by the Federal Reserve Board.
[51] CPMI and IOSCO (2016).
[52] See, for example, the Council on Cybersecurity (2014).

- Use of standardized secure system configurations (since complex configurations are more difficult to defend);

- Having processes in place to patch system and application software within a short period; and

- Limiting the number of individuals with administrator privileges.

Increased resiliency to cyber threats and attacks requires education efforts to change institutions' mindsets. Full security is an illusion, and firms should accept that cyber risks cannot be fully eliminated. Instead, firms need to take a risk-based approach in defensive measures and strengthen resilience to quickly bounce back from attacks. Incident response and continuity planning are key elements for successfully dealing with breaches. Firms should increase cybersecurity awareness and education efforts to increase their resiliency amongst their people. Due to the nature of their business, the financial services industry needs to take particularly strong measures to defend internal systems and prevent data breaches. Importantly, the relationships with counterparties, third-party security services, and upstream infrastructure should be controlled through contracts and agreements and integrated into broader risk management processes.

B. Lessening Information Asymmetries

Data collection and sharing, better risk modeling, and a forward-looking perspective with respect to new or emerging risks is needed. Cyber risk loss data is scarce and since its collection is not standardized it often cannot be used as an input into risk management models. Useful information would include statistics on the type and frequency of threats and breaches, together with their realized or expected monetary impact, both for the compromised firm itself and its stakeholders. Also, systematic and timely information sharing will increasingly determine how quickly and effectively systemic risks can be understood and contained.

Scenario analysis can help institutions understand potential risks, how these may transmit, where investments need to be made, and how best to respond when systems are breached. However, it is difficult to correctly calibrate these exercises if there is an incomplete quantitative understanding of the nature and size of risks that the industry faces. Information from scenario analyses can help improve financial and contingency planning but first there is a need to lessen the endemic information asymmetries through data and information sharing.

This gives rise to a clear public role to define cyber-related terms and standards, collect information, aggregate it to preserve confidentiality, and then disclose that information. Systematic collection and sharing of cyber data, including on the frequency and financial impact of cyber events, would help improve the understanding of the size and nature of the

risk and facilitate better risk management and modeling by both the public and private sector. First, to ensure that the classification of cyber events is consistent across firms and countries, there is a need to develop a common terminology and identical definitions of cyber risk terms. Second, information sharing should be institutionalized among law enforcement, supervisors, regulators and the private sector. Here, public-private partnerships can facilitate the distribution of information as well as national and international coordination, and help stakeholders design effective, coordinated cyber policies. And third, to overcome the industry's concerns about information sharing and potential reputational effects, individual firms' information must be anonymized and/or aggregated to a level that gives sufficient insights into the financial consequences of cyber-attacks and breaches while preserving confidentiality of firm-specific information. Finally, information and data should be made publicly available such that firms, supervisors, and regulators can use these sources as inputs into their risk management frameworks and models, and improve surveillance and early warning frameworks.

C. Designing Effective Policies

Cybersecurity risk needs to be managed using both ex-ante regulation and ex-post liability. Kolstad, Ulen, and Johnson (1990) and Shavell (1984) find that a mixture of both approaches should be used: ex-ante regulation appears ineffective where serious information asymmetries persist between regulator and firms, or if regulation fails to design effective standards. On the other hand, ex-post liability does not work when firms are not held accountable or if they don't have the means to cover the full scope of damages and losses (including because of the limited liability nature of corporate structures). Ex-ante regulation or ex-post liability could both slow down or prevent innovation given that new software and systems always embed new risks and vulnerabilities with inconsistencies detected only when a new software is used in practice. Therefore, it is important to find the right balance of ex-ante regulation and ex-post liability to improve resiliency without stifling innovation.

Given the differentiated nature of cyber risks, the regulatory architecture needs to adapt and be continually refined. Digitalization is moving fast, and the adoption of new technologies by the financial sector is moving alongside it. Risk management practices need to keep pace with the changing risk profile of IT reflected in the approach to regulation and supervision. The regulatory regime should encourage ongoing vigilance by boards and senior management to build resilience through investment in cyber security while giving institutions flexibility to address the risks in the way they see as optimal. However, actions by individual countries—and by financial sector participants alone—will not be sufficient. Constantly evolving industry-wide standards are needed to keep pace with evolving cyber risks, even if these create compliance costs for the affected institutions.

To encourage cyber-resilient financial systems, high level principles should be complemented with bespoke guidance at the firm level. The goal of policy and supervision should be to influence, incentivize, and shape financial institutions' cyber

security capability from elementary defenses to a state of cyber resilience. While cyber risks will never be eliminated, the regulatory framework and supervision activities need to adequately incentivize the implementation of risk management techniques, including to contain free-rider effects.

D. Address Coordination Failures and Manage Systemic Cyber Risk

In the highly interconnected IT and financial system, effective national and international coordination will be crucial. Governments need to ensure that different agencies collaborate coherently, avoid duplication, and pool initiatives.[53] As cyber risk is not limited by political or geographical barriers, international policy coordination is needed as well. Here, international organizations—like the Bank for International Settlements, the Financial Stability Board, or the IMF—can play a key role for facilitating coordination, supporting information sharing, designing coordinated policies, and helping solve disputes, if they emerge. The aggregation of cyber risk is too complex to be managed on the level of individual firms or countries. It is a global source of systemic risk that needs to be addressed on a multilateral level.

[53] OECD (2012).

REFERENCES

Atlantic Council, 2014, "Beyond data breaches: Global interconnections of cyber risk," in: Zurich, Risk Nexus, April 2014.

Atlantic Council, 2015, "Overcome by Cyber Risks? Economic Costs and Alternate Cyber Futures," in: Zurich, Risk Nexus, 2014.

A.M. Best, 2017, "Cyber Line Expected to be One of the Leading P/C Growth Areas," special report. URL: https://member.ambest.com/MemberCenter/sMC/Cust_Existing.aspx?URATINGID=&fs=0&altnum=0&altsrc=0&tl=7&b=0&nextpage=http://www3.ambest.com/ambv/sales/bwpurchase.aspx?record_code=263055

Basel Committee on Banking Supervision, 1999, "A New Capital Adequacy Framework," Consultative Paper, Basel, 1999.

Bloomberg (2017), "A German Bank Accidentally Transferred $5.4 Billion to Four Other Banks," Bloomberg News, March 24, 2017. URL: https://www.bloomberg.com/news/articles/2017-03-24/bank-known-for-lehman-blunder-transfers-5-4-billion-in-error

Böhme, R., 2010, "Security Metrics and Security Investment Models," in: I. Echizen, N. Kunihiro, R. Sasaki (eds.), *Advances in Information and Computer Security*. IWSEC 2010. Lecture Notes in Computer Science, Vol. 6434. Springer, Berlin, Heidelberg.

Borg, S., 2009, "The Economics of Loss," in C.W. Axelrod, J. Bayuk, and D. Schutzer (eds.), *Enterprise Information Security and Privacy*, p. 103-114.

Borg, S., 2016, "Cyber Threat Analysis and Cyber Consequences Analysis Course," course material, U.S. Cyber Consequences Unit, Mound, MN, U.S.A.

CISCO, 2017, "Annual Cybersecurity Report," CISCO Systems. January 2017. URL: http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017

CPMI and IOSCO, 2016, "Guidance on Cyber Resilience for Financial Market Infrastructures," June 2016.

Dean, D., S. Digrande, D. Field, A. Lundmark, J. O'Day, J. Pineda, and P. Zwillenberg, 2012, "The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity," The Connected World. BCG Report. The Boston Consulting Group. Available from:

https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/

Deloitte, 2016, "Beneath the Surface of a Cyberattack," Deloitte U.S.A., Cyber Risk Services. URL: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

Gracie, A., 2015, Speech at the Cyber Defence and Network Security Conference, Bank of England, London, U.K., January 23, 2015.

Group of 7 (G7), "Fundamental Elements of Cybersecurity for the Financial Sector," 2016.

Kunreuther, H. and G. Heal, 2003, "Interdependent Security," Journal of Risk and Uncertainty, Vol. 26(2-3), pp. 231-249. 2003.

Kolstad, C., T. Ulen and G. Johnson, 1990, "Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements," American Economic Review, Vol. 80(4).

KPMG, 2015, "Cyber Security: A Failure of Imagination by CEOs, URL: https://home.kpmg.com/xx/en/home/insights/2015/12/cyber-security-a-failure-of-imagination-by-ceos.html

McAffe, 2013, "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, McAffe.

McAffe, 2014, "Net Losses: Estimating the Global Cost of Cybercrime," Center for Strategic and International Studies, McAffe.

McKinsey, 2011, "Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity. Available from: https://www.nwoinnovation.ca/upload/documents/mgi-Internet-matters-report.pdf

Moore, T., 2010, "The Economics of Cybersecurity: Principles and Policy Options," International Journal of Critical Infrastructure Protection, Vol. 3(3-4, December 2010.

Morgan Stanley, 2016, "Cybersecurity Is About to Change in a Big Way," Morgan Stanley Blue Papers, Morgan Stanley, June 2016.

National Cybersecurity and Communications Integration Center (NCCIC), 2014, "Combating the Insider Threat," U.S. Department of Homeland Security, URL: https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf

NetDiligence, 2016, "2016 Cyber Claims Study," URL: https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf

OECD, 2012, "Cybersecurity Policy Making at a Turning Point," OECD Publishing, Paris.

OECD, 2013, "Measuring the Internet Economy: A Contribution to the Research Agenda". OECD Digital Economy Papers, No. 226, OECD Publishing, Paris.

Price Waterhouse Coopers (PwC), 2015, "Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience," Price Waterhouse Cooper Insurance, 2015.

Polozov, Y., 2016, "Trading Systems Manipulation: Metel/Corkow Trojan proof-of-concept attack," Wapack Labs, FS-ISAC.

Reuters, 2016, "SWIFT Says Bank Hacks Set to Increase", September 26, 2016. URL: http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11W1XY

Rowe, B., 2007, "Will Outsourcing IT Security Lead to a Higher Social Level of Security?," Workshop on Economics of Information Security 2007.

Shavell, S., 1984, "A Model of the Optimal use of Liability and Safety Regulation," RAND Journal of Economics, Vol. 15(2).

Siwek, S., 2015, "Measuring the U.S. Internet Sector". Internet Association. Washington, DC. Available from: http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf

U.S. Department of the Treasury, 2017, "A Financial System That Creates Economic Opportunities: Banks and Credit Unions," Report to the U.S. President, June 12, 2017.

Varian, H., 2004, "System Reliability and Free Riding," in: *Economics of Information Security*, Vol. 12, "Advances in Information Security," L. J. Camp, S. Lewis (eds.), Kluwer Academic Publishers, Boston, Massachusetts, pp. 1–15.

Verizon, 2013, "Data Breach Investigations Report 2013," Verizon Enterprise. URL: www.verizonenterprise.com/.../rp_data-breach-investigations-report-2013_en_xg.pdf

Verizon, 2016, "Data Breach Investigations Report 2016," Verizon Enterprise. URL: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Verizon, 2017, "Data Breach Investigations Report 2017," Verizon Enterprise. URL: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

Wendt, F., 2015, "Central Counterparties: Addressing their Too Important to Fail Nature." IMF Working Paper WP/15/21 (Washington: International Monetary Fund).

World Economic Forum (WEF), 2015, "Understanding Systemic Cyber Risk," Global Agenda Council on Risk & Resilience, October 2016.