# 14

# Enterprise Cyber Risk Management

Patrick L. Brockett, Linda L. Golden and Whitley Wolman
*University of Texas at Austin*
*USA*

## 1. Introduction

Cyber risk represents an ever-growing threat to public and private institutions alike due to its potentially disastrous effects on organizational information systems, reputational risk, and potential loss of consumer- and stakeholder's confidence. With the advent of the internet and the corresponding proliferation of information technology, firms, non-profits, and governmental entities were generally unprepared for identifying and addressing this risk, but the threat has increased in both frequency and severity over time, and the nature of attacks has also changed. In many early cases, the perpetrators of cyber attacks and information disruption campaigns interrupted business operations simply for their own amusement, or viewed breaking into the corporate information technology (IT) infrastructure as a challenge. They would deface websites or take down servers in order to aggravate or simply to challenge other cyber professionals in order to prove they could do it, not to profit (Hallam-Baker, 2008). However, as the Internet has grown and e-commerce has blossomed, employee access to company data has increased, and remote access to internal computer systems has become commonplace, cyber attackers have evolved, becoming more sophisticated and their effects becoming more devastating (Rhemann, 2011). Current cyber threats and attackers are increasingly focused on profiting from the consequences of their attack actions and either exploit the data they illicitly obtain for private gain or require payments from the victimized enterprise to restore service, access, or websites back to operational functionality (Maillart & Sornette, 2010).

The focus of this chapter will be on enterprise cyber risk management and risk mitigation (as opposed to individual consumer cyber risk, an extensive connected topic which is of interest in its own right but not addressed here). In this chapter we will investigate cyber risk of importance to enterprise to include information theft, compromise of consumer information, and the interruption of e-commerce. This chapter will focus on several important aspects of cyber risk and how these affect the economics and security of organizations. Cyber risk is unique among other operational enterprise risks due to its mobile location, scope of threat, and high-profile impact. With the proliferation of business services, systems, and data accessible via the Internet, cyber threats to enterprises (public and private) have grown immensely. Furthermore, companies have now realized that they run the risk of creating liabilities from any cyber event that could affect related services and products (e.g. the theft of email addresses from Epsilon on April 2011 also affected customers of numerous other businesses, such as Hilton Hotels, Citibank, etc., and has cast reputational risk on not only the original company but also on their clients, and has created increased potential legal liability as well.).

The ripple effect that cyber attacks can engender can influence suppliers, end users, and the organization itself, and could even have the potential to destabilize large swaths of the economy if the target of the cyber attacks were systemically important (such as a systemically important financial institutions, a utility operators, a water treatment facility, a transportation network, etc.). Additionally, cyber espionage techniques are developing rapidly, making enterprise trade secrets also vulnerable to competitor theft.

As with many other hazards faced by businesses, insurance companies who specialize in risk assumption and risk pooling saw a potential financial opportunity in filling the cyber risk hazard management needs of enterprises by providing insurance policies designed to protect or indemnify against the financial consequences of these Internet-related threats. Several insurance companies have started to offer connectivity-related policies that cover cyber information and security breaches. Early on, as the insurers tentatively waded into this new market, it was difficult to generate data on electronic losses. Although Internet-related insurance coverage is still in its infancy (as compared to other insurance classes), insurance companies over the past few years have now improved their ability to more accurately price policies and predict potential losses. These companies, including AIG, Chubb, Fidelity, Marsh, and Lloyds of London, have written policies that can hedge or transfer varying aspects of cyberspace risk (Gordon *et al.*, 2003). Further aspects of cyber-related insurance will be discussed in detail later in this chapter.

The chapter starts with a general discussion of cyber risk threats to organizations including trends and costs. These threats will be dichotomized into those cyber risk threats that arise internal to the organization (e.g., employee cyber-based financial theft, employee data theft, identity theft using internal company data, etc.), and those risk that arise external to the organization (e.g., hackers stealing data, money or trade secrets, or adversaries shutting down or disabling internal information technology, vulnerability of IT systems to external power surges, blackouts, etc.). Next in the chapter we shall discuss emerging cyber risk threats and trends, with particular attention on risk consequences of the emerging trend of organizations and individuals to use wireless mobile technology (smart phones, iPads, etc.) to conduct business to business transactions, access enterprise networks, do banking, and accomplish retail consumer purchases.

Having identified these major cyber risks, in this chapter we subsequently investigate the underlying economic considerations (and theory) related to cyber risk, including the extent to which these threat costs are internalized in stock prices and who bears the costs for such risks. One of the most important risk financing mechanisms utilized by enterprises for all the risks they face is insurance risk transfer. This is also the case to a certain (but more limited) degree with cyber risks as well. Consequently, after discussing the economic aspects of cyber threats, we next discuss cyber risk insurance, its availability, coverage and the economic issues related to cyber risk insurance such as moral hazard/adverse selection and issues concerning systemic risk causing correlation in the insurer's portfolio, such as the dominant use of particular software by multiple users (e.g., Microsoft Windows, Adobe Reader) so that hackers exploiting vulnerabilities in a single software product can cause losses for numerous insured clients. This reduces the risk pooling and diversification benefits that insurers depend upon when pricing their products (i.e., their estimates of aggregate loss probabilities based on independent loss occurrences which may differ substantially from those actually experienced when risks are highly correlated). The chapter concludes with comments about future trends and research.

## 2. Cyber risk threats

The cyber risk threat to enterprises is large and growing (Hallam-Baker, 2008; Rhemann, 2011). The Federal Bureau of Investigation (FBI) in the USA, universities, and other research organizations have delved deeply into the issues surrounding cyber security as a threat to public governments as well as private corporations. A 2002 Computer Security Institute/FBI joint study on cyber risk found that 90 percent of respondents had detected computer breaches within the past year, with an average loss of over $2M per organization (Power, 2002). In the then relatively new age of information technology and the Internet, most companies were not adequately prepared to face these types of costly losses. By 2008, however, the Computer Security Institute/FBI study found that the average loss had decreased to approximately $300,000, suggesting that companies and the security software they use have become more sophisticated in an effort to deal with the increasing threat of criminal cyber activity (Computer Security Institute, 2008). The 2008 CSI/FBI survey also found that companies significantly boosted their internal budgets associated with cyber security, which further implies that companies are spending more money, time, and manpower to mitigate these risks (Computer Security Institute, 2008). Cyber threats can shut down power grids, steal information and intellectual property, uncover competitors' bids, and disable web sites needed for business activity, causing substantial financial harm to unprepared enterprises. Accordingly, it is likely that companies will need to continue to focus on these cyber risk security issues as hackers continue to get more sophisticated causing more losses to business, on-line services, and operations, and especially as companies become more dependent on the Internet for e-commerce, mobile (or m-) commerce, or simply for daily operations, administration, and field contact with employees.

As the proliferation of information technology, the increasing facilitation of remote access to enterprise computers, and the corresponding risk of cyber threats have increased, so has the attention paid to these issues also increased. When focusing on these threat issues, for this chapter it is useful to broadly dichotomize cyber risk into 1) cyber risks that arise internal to the organization and 2) those that arise external to the organization. While certain risk mitigation techniques are common to both sources of cyber risk threats (e.g., securitization and password protection of sensitive information or technology, segmentation of information and its access within an organization, etc.), other techniques are more appropriate for one risk source rather than the other. The threats that each source of risk poses can be different and may often require different approaches. Moreover, as developing nations fight for parity with the more developed countries in terms of electronic Internet access and technological and industrial development, firms, non-profits and governmental entities and institutions are likely to see an increase in cyber threats from these sources outside the control or jurisdiction of the enterprise's host country. We shall discuss each risk source in turn.

### 2.1 Internal cyber risk threats

Ironically, a very high risk of cyber crimes comes from within rather than outside the organization. While an employee can be a company's greatest asset, employees are constantly exposed to vast amounts of confidential information and are, by necessity, trusted with proprietary company information, inventory and property. Sometimes the temptation for individual gain can be too great. Or, an employee who spent time developing the important proprietary company information can feel they have a right to this company

intelligence as a result of their time spent in research and development, product development, or technology transfer activities. Consequently, a company can be exposed to data or intellectual property theft from within rather than without.

Data theft is the term used when information is illegally copied or taken from a business or other individual. Employee theft of data, formulae, and process information can compromise the enterprise as readily as an external data theft attack, however because of their privileged position, the employee has more ability to act as the perpetrator since they already have trusted permission or password admittance into the cyber system of the enterprise for legitimate reasons, a permission that they may then turn against their employer. In fact, the FBI reports that employee theft is the fastest growing crime in America. The US Chamber of Commerce estimates about 75 percent of employees steal from their employer, with approximately 30 percent of corporate bankruptcies being the direct result of employee theft. The majority of involved individuals are higher level employees, and, on average, the time until discovery is approximately 18 months, giving substantial time for financial damage (Burke & Cooper 2010 p.433). Enterprises must be as vigilant against internal cyber threats as they are to external threats.

Removable media devices are the number one internal cyber security threat vehicle. Research conducted by Centennial Software in May 2007 found IT managers believe removable media devices now pose a larger security threat than either malware or viruses. In this 2007 survey quoted in Feig (2007), 38.4 percent of more than 370 respondents listed portable devices as their number one risk, up from the 25.7 percent in 2006. Due to this reality, in "IT Acceptability Policies" manuals, more organizations are now including security considerations of removable media devices in their risk management endeavors. Eighty percent of respondents reported that their organizations now dictate protocols for unauthorized use of removable media devices, with some prohibiting their use entirely. Other enterprises have modified their IT systems to either disable the USB ports or have installed software to prohibit downloading or uploading data without authorization via USB ports. The survey also found that 67 percent of IT staff use some form of removable media device on a daily basis and that the most popular type of device (65 percent) is the USB flash drive (Feign 2007). Never-the-less, despite the low cost, ease of use, ready availability to employees, and small size of USB devices, these devises were only used in 9 percent of data theft cases (Patel & Mischon De Reya 2011). Other larger, more sophisticated or faster devises are now also being used, such as iPods and MP-3 players.

Colorful names are often given by security professionals to the ingenious use of removable media drives for data theft. "Thumbsucking", for example, is the name given to data theft using a USB mass storage device, such as a USB flash (or thumb) drive to download confidential network information, literally "sucking" the data out of the network and onto the USB drive (Walsh 2011). This type of internal data theft threat has increased over the years. Whereas a previous limitation to the use of USB flash (or thumb) drives was one of memory space on the USB drive, this has been largely removed with modern USB drives. Price constraints have also been significantly alleviated on USB flash drives. Moreover flash drives are highly portable, compact, easily concealed, and instillation does not require the user to restart the computer system, making it a cheap and convenient tool for cyber theft (Walsh 2011).

Another fanciful name for a different, serious cyber theft risk is "pod-slurping". This involves using an iPod or MP3 type player to rapidly steal gigabytes of information from an enterprise's computer system (Giannoulis 2011). iPods are widely used by employees and often played (with approval) while attached to enterprise or office computers. However, they also can be used to download massive amounts of confidential company information. According to Mello (2005), a 2004 research report on security risks (conducted by Gartner technology research and advisory company) stated that portable devices posed serious threats for companies, and this report inspired a security engineer named Abe Usher to write a "proof of concept" program called "slurp.exe" that allows an iPod or other removable device to be used to "suck" 100 MB worth of data from the Windows "Documents and Settings" directory in a matter of minutes (Giannoulis 2011). Mello (2005) reports that Usher wrote in his blog (www.sharp-ideas.net) "Using slurp.exe on my iPod, it took me 65 seconds to copy all document files (*.doc, *.xls, *.htm, *.url, *.xml, *.txt, etc.) off of my computer as a logged in user. Without a username and password, I was able to use a boot CD-ROM to bypass the login password and copy the document files from my hard drive to my iPod in about 3 minutes, 15 seconds." While this "proof of concept" program illustrates the potential for data theft using these devices (virtually the entire set of business records of a small to medium sized company could be downloaded in minutes), there is also empirical evidence of its actual use. In 2005 a Chinese spy sought asylum from the Australian security forces saying that over a period of several months he had stolen confidential data using his MP3 player (Hughes & Allard 2005). Also, there have been several court cases involving using such devices to steal confidential company data.

Identification theft (ID-theft) is another well publicized cyber risk vulnerability of enterprises, from both internal and external sources. Employees (and successful external hackers) can obtain access to customer records such as names, phone numbers, addresses, usernames, passwords and PINs, credit card and other account numbers, as well as Social Security numbers (Miller 2008). This information can then be sold on the Internet or used by the intruder him/herself to commit identity fraud (or for blackmail or extortion purposes to the enterprise via threatening data exposure). For example, when an employee, in the normal course of business, gains access to credit card numbers they may be tempted to use this information to make purchases or obtain other lines of credit for their own benefit (Stroup 2011). The risk is not small. According to the identity theft research center (ITRC 2011), in 2011 there have been a total of 112 breaches and 5,460,925 records exposed, as of April 5, 2011. Moreover, using data from various sources such as social media sites (Facebook, etc.) the identity thief can gather sufficient information to match data records allowing them to break password cryptology security, obtain credit card numbers and make purchases using another's identity or credit cards. As a concrete illustration of the above mentioned internal cyber risk threat, we relate that in January 2009, Johns Hopkins University began receiving reports of identity theft activities in the Baltimore area surrounding their University (McMillan 2009). Ultimately, Johns Hopkins Hospital ended up having to warn over 10,000 patients about a woman that worked for the hospital who had access to Social Security numbers, names, addresses, dates of birth, telephone numbers, parents' names, and medical insurance information and who had used this information to commit fraud. Yet another example of this internal source of cyber risk is a Wells Fargo Bank employee (Roberta Dunsworth) convicted in federal court for identity fraud. She was charged on December 1, 2010 with ten counts of bank fraud, two counts of aggravated

identity theft, and two counts of fraudulent use of unauthorized access devices. Her fraudulent activities occurred while employed at the Wells Fargo Bank where she used the identity of a bank customer to obtain a credit card and a debit card and to open bank accounts (Admin 2011). Such employee related cyber risks can pose great financial, as well as and legal problems for employers if not adequately addressed preemptively.

An important internal covariate of internally perpetrated cyber risk is having disgruntled employees. These individuals may be motivated by revenge and will attempt to sabotage or destroy enterprise software or databases, thus depriving the enterprise of their property or costing the enterprise money. This more malevolent form of cyber risk should be addressed proactively by implementing a well-designed corporate security initiative, that includes policies such as, changing passwords prior to termination of employees with Internet access to enterprise computers and enforcing robust password strength requirements. Maintaining a log of user access to all corporate systems can be a preventative measure against cyber crime as well.

Internal data theft could also involve the employee as a victim of data theft. For example, New York Police Department employees became data theft victims in early 2009, when the personal records of approximately 80,000 police officers in a pension fund were stolen when an employee gained entry into a disaster recovery facility in Staten Island (InfoSecurity 2009). Similarly, in 2006 the McCombs School of Business at the University of Texas at Austin experienced a data breach with more than 197,000 personal records of faculty, staff, students, alumni and donors stolen. These examples illustrate the complex nature of cyber crime where inside intrusions include multiple types of data breaches such as customer data, employee data, and sensitive corporate data. Additionally, external components also may impact cyber security risk. We discuss the external components of cyber risk next.

### 2.2 External cyber risk threats

As developing nations fight for parity with the United States or other developed nations, American and other enterprises are likely to see an increase in targeted cyber attacks attempting to access their secret information or competitive knowledge (e.g., stealing competitive bids for strategic purposes). However, the risk from cyber threats goes beyond even the private sector into the public and governmental sectors. In 2010, President Obama declared threats to cyber-security a national security issue identifying "America's digital infrastructure [as] a 'strategic national asset' and [appointing] Howard Schmidt, the former head of security at Microsoft, as his cyber-security tsar" (The White House, 2010). In 2010, the President also directed the Pentagon to establish the U.S. military's Cyber Command to utilize a "full-spectrum" of operations in cyberspace (Economist, 2010). Additionally, the White House has directed several studies and initiated a national cyberspace strategy which stipulates the scope, process and development for using cyberspace (The White House, 2010).

The above pronouncement provides a further illustration of how flash drives, discussed previously as a threat in the internal risk section, can also pose cyber risk threats externally, even to the most secured enterprises. Flatley (2010) relates how an infected USB thumb drive was placed by a foreign intelligence agency in the parking lot of a Department of Defense facility in the Middle East. As might be expected by human nature, the person who

found it put it in their computer. The computer was connected to the US Central Command and, according to Deputy Defense Secretary William J. Lynn in *Foreign Affairs*, the malware that was embedded on the device was able to spread and pass "undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control." The same could occur with corporate or other enterprise computers as it exploits the natural human curiosity that would occur if one were to find a "lost" flash drive. It was the above incident that in part, motivated the White House to establish a Cyber Command. Corporations should also take note.

There also have been well-reported cases of cyber espionage by Chinese and Russian sources that have infected military networks and corporate networks alike. Certain elements in China have targeted military networks in order to gain access to military secrets and information on U.S. operations. Experts are unclear about whether the attackers are officially sanctioned by the Chinese government, but their locations have been traced back to mainland China.

National Journal reported,

> …Brenner, who works for Director of National Intelligence Mike McConnell, looks for vulnerabilities in the government's information networks. He pointed to China as a source of attacks against U.S. interests. 'Some [attacks], we have high confidence, are coming from government-sponsored sites,' Brenner said. 'The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction. It's a kind of cyber-militia.… It's coming in volumes that are just staggering' (Harris, 2008).

Cyber threats from Russia tend to come from organized crime groups that prey on unsuspecting websites or servers and even demand a ransom in order to restore functionality. Russian attackers have also sought to influence political movements through coordinated denial of service attacks that hinder political organizations. In a Wired magazine article, Don Jackson of Internet security firm SecureWorks is quoted as saying:

> "… the denial-of-service attacks managed to shut down more than 80 percent of Kyrgyzstan's bandwidth. While both sites now seem to be up and running, several commentators have speculated that the attack is meant to thwart Kyrgyzstan's embattled political opposition — which depends on the Internet to organize — or to pressure Kyrgyzstan's government, which hosts a U.S. airbase outside of the capital, Bishkek"(Hodge, 2009).

Another example of governments using cyber tactics to control political events was the recent revolution in Egypt in spring 2011. The Mubarak regime in Egypt essentially "pulled the plug" on the Internet throughout Egypt to control protests and political gatherings. If the Internet can be shut down, or severely disrupted, then most enterprises throughout the entire country will be put at risk. Proactive data back-up, record keeping, and other plans must be made to mitigate this damage should such an event occur.

Identity and personal information theft discussed previously from an internal risk perspective is also a substantial risk from external sources, and poses a growing cyber threat

to consumers and retailers using Internet technology. As recently as April 2011, computer database breaches affected millions of people. Epsilon, an online marketer, announced to customers that its email database had been hacked and intruders took millions of email addresses (Spicer & Aspan, 2011). The resulting damage not only affects the online marketer, but also the companies it services and the end users of their services. In the end, costs could grow into the millions if the company is found liable for negligence.

The Brookings Institution recently released a paper discussing the perils of identity theft and the need for consumer trust in online commerce (Friedman *et al.,* 2011). With the growth of social networking, online retail sites, and business services utilizing cyberspace, personal identity protection will continue to play a key role in the future of information technology development. Increasingly, a person's identity is used as the key to unlock various online portals of information, including secured corporate and governmental websites. Social security and bank account numbers are needed for online account creation, as well as government services. The potential for theft and fraud is greatly increased by the numbers of online users and the amount of information stored in electronic databases. Similarly, it is noted that users tend to use the same passwords for multiple Internet accounts, which could cause the risk to spread to other unsuspecting companies. Furthermore, websites are collecting larger amounts of data through "history sniffing" and the identities created from user-specific plug-ins (Friedman *et al*., 2011). This may be especially problematic because using smart phones to conduct business, (m-commerce) is substantially less secure, with employees possibly storing passwords and account numbers on the smart phones, and because smart phones (possibly containing account information and passwords) are lost or stolen at an alarming rate (Brockett *et al* 2011)

Whereas the traditional cyber risk threats discussed previously can be construed as exacerbated extensions of already existing risk control problems (physical risk perimeter securitization, employee theft risk control, corporate spying and intellectual property theft, etc.), the newly developing wireless or mobile technology is creating new (as opposed to merely enhanced) enterprise risk vulnerabilities that need enterprise wide attention. This is discussed in the next section.

## 3. Emerging cyber risk threats: Mobile Internet access, spear phishing and pharming

The ability to conduct business wirelessly (known as mobile or m-commerce) is revolutionary and growing in importance. Twenty two percent of consumers in 2010 used smart phones for price checking, 21 percent for doing product research, and 13 percent for making purchases using their phones (Schwartz, 2010), and enterprises including governmental entities, are changing web representations to accommodate this new interface modality. Reportedly 74 percent of online businesses have a mobile commerce strategy in place or are developing one (Marcus 2010 quoting a study by the National Retail Federation). Of those retailers not already involved in mobile commerce, one quarter say that they intend to begin within the next year (Siwicki 2010). Traveling sales people often access corporate data remotely using mobile smart devices, often smart phones, so the newly evolving wireless security risk is important to all enterprises.

There are, however, important distinctions between the risks associated with mobile Internet access and more familiar e-commerce or cyber risks. There are unique business challenges, cyber threats and data theft vulnerabilities embedded in this new modality. Mobile Internet connectivity uses a different communication channel (wireless) making business interface transactions more accessible at more times and places but also a different physical mode of communication than e-commerce. Due to the mobility of the communication, an interface between the accessing and accessed devises is more anonymous, making it more difficult to validate a transaction, and making it more difficult to secure the Internet transmission (eavesdropping on wireless communications is relatively easy if one is motivated to do so). Thefts are also more difficult to trace back to the perpetrator.

The Brookings Institution report "Online Identity and Consumer Trust: Assessing Online Risk" summarizes the difference in the physical characteristics of cyber risk and how those threats affect users:

> When communicating via a wireline, it is intuitive to most that the data traffic is leaving the computer through a data cord to an interface that connects with the Internet Service Provider…. It is quite difficult for a typical cyber criminal to intercept data … that he had not physically tapped. The same cannot be said of wireless network communications. Malicious actors can learn a great deal from unencrypted Wi-Fi links in their vicinity. …if the wireless connection is not itself encrypted using a modern standard …, then any nearby attacker can listen to all unencrypted traffic traveling between the computer and the wireless router. The data are being broadcast to the surrounding area by both the computer and the router in the same way that noise from a conversation is vulnerable to eavesdroppers. Thus, information that is not encrypted at the end points of the transaction can be intercepted. Tools to capture this traffic and reassemble the data packets into web pages are widely available, and usable to any moderately sophisticated computer user (Friedman *et al*., 2011).

Mobile communication differs in the types of devices used, the development languages, communication protocols, and even the technologies used (Coursaris and Hassanein 2002). These differences make mobile communication subject to new threats. A mobile business operating system provides the infrastructure for running smart phone applications and mobile access to company computers but, according to (Ghosh and Swaminatha 2001), the platforms and languages being developed for wireless devices have failed to utilize even the basic security concepts already present in hardwired desktops. Without a secure infrastructure for mobile devices, achieving secure mobile Internet communication or secure employee to employer communication may not be possible. Additionally, the nature of the software applications developed for mobile devices are important to overall security since logical flaws or oversights in these applications can present exploitable security loopholes allowing a point of entry by the malicious hacker, and consequently making enterprises (and individual mobile communication device users) vulnerable. Unfortunately, the devices' physical limitations often force application developers to make security and performance trade-offs. Limited power, processing cycles, memory, and bandwidth can force developers to give up security features like encryption in order to improve online performance (Ghosh and Swaminatha., 2001). The use of lower-level languages for phone communication development, as well as their often lacking built in non-functional security requirements ensures continuation of software vulnerabilities.

With mobile devices, there is also the potential to remotely access data on "always on" mobile phones, including passwords, contact lists and other information. The phone hacking scandal involving News International's paper *News of the World*, a subsidiary of Rupert Murdoch's international News Corporation organization in the UK in 2011 illustrates this threat is real. These news organizations hacked into the voice mail of such well protected people as members of the Royal Family. They also allegedly hacked into the phones of a murdered English schoolgirl, relatives of British soldiers who had died, and even some of the victims of the terrorist bombings in London on 7/7/2005. The police have a list of approximately 4,000 people they are contacting who may have been hacked, including celebrities, politicians, and sports stars (BBC 2011). This can be a substantial concern for commercial enterprises as well since executives and sales persons use their mobile phones for negotiations, contract bids, and other purposes requiring secrecy.

Given their size and portability, phones are also at risk of physical theft and loss, with an estimated two million phones lost or stolen each year (Siciliano, 2011b). Some of the data stored on such devices may be proprietary business data, and, additionally, there is an increased risk that someone that finds or intentionally steals these smart phones can use the stolen device to access internal corporate systems, including servers and file systems using passwords stored on the smart phone. An estimated 52 percent of smart phone users store passwords on their phones; and 87.5 million people do banking using their phones (Siciliano 2011a). Moreover, since most people (even employees with secured access) do not use PIN codes to lock their cell phones, and since most people use the same password for multiple "secured" sites, a great vulnerability is created by mobile access that is not present in otherwise Internet accessible enterprises. One problem with current mobile phones is there is no readily available mechanism to authenticate that a particular user belongs to phone being used (Ghosh and Swaminatha., 2001), so access to an employee's phone may open the entire enterprise to potential cyber risk.

Two other emerging cyber threats are spear phishing and pharming. Phishing occurs when a potential thief sends emails to people which masquerades as a legitimate request from the organization whose letterhead and logo they have hijacked. They ask the recipient to click on a link to supply information (account number, password, social security number, etc.) in order to verify some aspect of their account. The link (as well as the email) are phony, and once the recipient puts in their information, it is captured and used for accessing bank accounts, credit cards, identify theft, or downloading malware which can take over the computer remotely to access all information on the individual's computer (such as other passwords or corporate information). Spear Phishing is a refinement which is even more difficult counter. Using some inside information gathered by other means (e.g., hacking a corporation's computer, social media sites, etc.) they do a controlled and targeted phishing expedition rather than simply sending random emails. Using information particular relevant to this well defined smaller group of people they construct an email which is more specific and has an enhanced air of being a legitimate request by a supervisor or trusted superior (often it is designed to come from a higher-up in the organization so compliance is enhanced). Again, if any one of the many targeted individuals within the company responds and logs on, security is breached and computer programs can be downloaded that allow full access to company computers for espionage purposes, identity theft, malicious destruction of data, extortion, or financial thievery (FBI 2009).

Pharming is the name given to a different type of technique used to direct the unsuspecting victim to a malicious website where malware can be downloaded or password and account numbers can be harvested in bulk numbers. Unlike phishing where the individual phishing lines (emails) are set out to catch fish, in pharming a network node is hijacked and all traffic going through this node which thinks it is going, for example to CibiBank.com, will instead be directed to another website controlled by the criminal. Essentially the criminal harvests multiple users' information at once, and need never even contact the user or need the user to respond to an email. The way is works is this. On the Internet, the website addresses are a sequence of numbers representing the site (e.g., 123.456.7.8 might represent the web site for XYZCompany.com). There is a translation mechanism built into DNS servers that converts words we write (say XYZCompany.com) into numeric address of the web site we want to access (123.456.7.8). A pharmer hacks into the DNS server and changes the translation book so that when you (or anyone else using this server) types in XYZCompany.com, it automatically sends the communication to another site (say 987.654.3.2) instead of the real site (123.456.7.8). As the phony site looks the same as the original, the unsuspecting user logs in without knowing that their account information and password are compromised. Malware can be downloaded onto the requesting computer, compromising many business activities and trade secrets (Norton 2011). Companies involved in Internet commerce have major concerns with pharming and the consequent fraud as their clients get scammed. Online banking sites are particularity sensitive to this threat. Moreover, adware and spyware removal software and antivirus software is ineffective in protecting against this threat since the hijacking occurs on the DNS server away from the requesting or responding computers, and hence is not detected by either side of the transaction which was hijacked. With the growth of wireless routers (both in businesses and homes) and in public access wi-fi availability, the potential to hijack data and transactions in mass quantities via pharming is an increasing threat that requires very specific anti-pharming defenses by the enterprises involved.

Having delineated important cyber risks we now turn to an investigation of the financial and economic consequences of such risks. In many ways the development of the Internet (and the consequent development of cyber risk threats) has been generated by economic considerations. Mobile Internet devises are rapidly replacing hard wired desk top computers as the Internet devices of choice, and the economics of this transition is impactful. Additionally, economic theory can alert us to possible ways of handling cyber risk problems, such as the economic research into moral hazard associated with "free goods" or public goods. We shall next discuss the economic aspects of cyber risks.

## 4. The economics of cyber risk

Motivated by efficient market theory, (Garg *et al*., 2003) used event study methodology to indirectly measure the economic impact of Internet security breaches on stock process of breached firms (and also on Internet security providers). According to the efficient market hypothesis, all information about past and future events within a company (or industry) should be reflected in the stock price, which itself reflects investors' beliefs about future cash flows to investors. A security breach can cause a rethinking about future vulnerability as well as future legal risk, and hence reflect market assessment of impact on cash flows different from the reported financial loss (which may be biased or underreported).

Consequently, they reason, by looking at the abnormal (negative) return of a breached company's stock price, they can get an exogenous estimate of the permanent market assessed financial effect of the breach, different from the stated breach cost information. Moreover, such actual breach cost information, they argue, is not generally available to the market. Expenditures (and capability) in IT are not often reported. Also, most firms tend to underreport negative information containing security breach events simply because there is no incentive to correctly volunteer this information. Companies prefer not to seem vulnerable to their customers and competitors or to other potential predators. Why would these firms give an edge to the competition or a green flag to the cyber criminal if they do not have to? Additionally, in the age of management by stock price, firms also withhold this information to avoid lowering the price of the company's stock and falling out of favor with investors (Garg *et al*., 2003). Another reason for not releasing such information, of course, is pride. No one likes to have their shortcomings and failures broadcast to the media. Once the breach is public, markets can react, and their reaction reflects the decreased valuation of the enterprise. Using their event study methodology applied to 22 cyber security breach events Garg, et al (2003) found the lasting effects on stock prices of security breaches is an order of magnitude larger than other reported loss costs ($17-28 million as opposed to other reported estimates of $50K to $2 million per incident). Thus, the economic effects on breached firms are quite significant.

Economists have also used other microeconomics tools in order to price in certain aspects of information security. Bohme (2005) argues that insecure software technologies such as public access wi-fi availability in some cities are economically underpriced by the market due to costs of their negative externalities not being valued. Thus, public access wi-fi are similar to a public good since insecure nodes not only affect their own systems but those systems and users that are connected to it. This enables viruses and other attacks to proliferate much faster and more freely than other physical attacks. Since responsibility for preventing the attack is uncertain, no one user has an incentive to spend heavily on securing one's own infrastructure (Bohme, 2005) which would also benefit others. Consequently, Internet users are unlikely to procure expensive protection software that protects the next user. This implies that the incentives are misaligned and showcases the risks of these interdependent information networks. Economic theory suggests that the bearer of risk should be the entity that has best control of the risk. In the case of cyber risk, this is often the manufacturer of the devices used (smart phones, for example) and the provider of the free wi-fi. Regulators and governments can assist in this endeavor.

Having investigated the economic aspects of cyber risk, it is natural next to turn to the most common financial mechanism available for indemnifying enterprises against the potentially disastrous financial consequences of a successful cyber crime perpetrated against the enterprise. This mechanism is insurance, and the next section discusses the growing area of cyber risk insurance.

## 5. Cyber risk insurance

Once companies evaluate their current conventional insurance coverage, many firms then evaluate and purchase Internet and information security insurance to cover their specific insurable cyber risks. Along with determining their budgets for cyber insurance, firms must

choose between a blanket coverage policy and a more expensive, yet highly customized policy tailored to their business needs.

Anderson and Moore (2006) argue that cyber insurance is extremely difficult to price given the interconnectedness of the information security infrastructure and the interdependence on one piece of popular software (i.e. Microsoft Windows) whereby a general vulnerability in one product may expose every firm using that software to cyber threats (Anderson and Moore, 2006). Accordingly, an insurer insuring company X for cyber risk is also insuring against another company Y (e.g. Microsoft) who is not a client, and is not paying premiums, having created an exposure to cyber risk. Why should the insurance company pay for damages caused by another firm that infected or caused the infection of the covered firm? It seems that the law of large numbers which is often used to justify insurance company coverage could be defeated by the breadth and scope of the damages (and correlated risks of other insured companies using the same software) thus leading to the insurer's inability to pay claims and insolvency. If one flaw in a very common software system affects millions of users and propagates through several firms, the insurer might have difficulty paying all the resulting correlated damages for the sustained losses. It seems here that the network effect, typically lauded in economics, would have detrimental effects on the insured and insurers alike as it defeats the "independent identically distributed" (or at least uncorrelated) assumption which underlies insurance risk pooling and the general benefits of diversification. As our global interconnectedness grows, we must monitor the potential ripple effects that common interconnectedness can leverage on the global economy.

Firms have increasingly externalized the financial consequences of cyber risk by purchasing insurance to transfer that risk outside the company. Initially, insurance companies, given their lack of experience and practice associated with cyber risk insurance, have offered smaller coverage policies and packages. As firms and insurance companies develop more sophisticated analysis of cyber threats, the market for cyber insurance will likely grow. Indeed, many firms are pushing for the development of new markets and products with information security growth as a potential target (Gordon *et. al.*, 2003). As mentioned previously, several aspects of cyber-related insurance including pricing, information asymmetry, and correlations continue to influence the insurance market.

Traditionally, insurance premiums for commercial general liability are based on a firm's general features such as industry area, sales revenues, number of employees, and other similar characteristics (Baranoff *et al.*, 2010). Consequently, premiums typically do not reflect the firm's security activities, whether good or bad (Schwartz *et. al.*, 2010). If firms were more likely to demonstrate strict security practices, cyber risk coverage related premiums could be lowered, similar to the effect that a built-in safe or fire sprinkler system would have on a homeowner's policy, or a theft security system for an automobile would have on automobile insurance. For that reason, insurance companies find it necessary to separately assess and monitor these security precautions in order to verify the strength and level of protection.

Gordon, *et. al.* (2003) discuss their research on three aspects of cyber risk insurance including policy coverage pricing, adverse selection, and moral hazard. Since pricing depends heavily on actuarial estimates and historical data, pricing policies for Internet-related coverage are more uncertain than conventional insurance where data on claims have

been gathered by firms such as the Insurance Services Office (ISO) and where coverages are more standardized (and the risks do not change over time) making actuarial loss estimates more credible. However, some insurance firms have established insurance policies and quantified this difficult to assess risk (although critics argue over the accuracy of their projections). Also, (Gordon *et al*. 2003) discuss adverse selection for firms in terms of their "likelihood of a breach." If a firm has a higher likelihood of facing cyber threats, that firm may have an increased likelihood of purchasing insurance to transfer this risk, similar to a smoker or someone in poor health that would buy more health insurance because they know that they have a higher than average (for their risk pool) chance of loss, but are being charged the average risk pool premium. When someone else is paying part of the risk cost, it is economically rational to buy more insurance. Insurance companies can mitigate the risks associated with the above mentioned adverse selection by requiring a security audit of the firm.They might also be able to differentiate premiums based on a firm's current security profile (creating a separating equilibrium solution to the adverse selection problem).

Moral hazard is another economic problem that occurs with cyber insurance products. Moral hazard occurs when the actions the firm takes are different simply because they have insurance indemnification. Why spend money on cyber security when losses are (in large part) indemnified by the insurer and hence shared by the risk pool ex ante, but premium savings are entirely captured by the owners? Gordon *et al*. (2003) argue that the moral hazard problem faced by insurance companies offering cyber risk policies could be eased by offering premium reductions to firms that take appropriate security measures on their own. The firm should be given financial incentives that influence its decisions to mitigate the risk on its own (similar to what occurs in workers compensation and other insurance). The firm's expense on risk reducing processes and behavior would help the firm mitigate cyber risk and would potentially reduce the impact of a cyber event, thus lowering premiums. Additionally, deductibles, policy limits, and coinsurance are standard tools used by insurance companies when information asymmetry is present (Schwartz *et al*., 2010). This puts a higher financial burden on the insured party to mitigate the effects of adverse selection resulting from information asymmetry, and inaction caused by the insurer being unable to adequately monitor behavior (moral hazard).

Cyber insurance coverage typically involves both first party and third party coverage for potential damages from Internet-related activities. Retail names in the cyber insurance market include Chubb's Cyber Security, Lloyd's e-Comprehensive, and Marsh's NetSecure. As described previously, however, insurance companies are often reluctant to underwrite large amounts of damages due to the relative newness of this specific type of insurance, the degree to which the insured has control over the frequency and severity of losses, and the lack of well verified loss data upon which to make actuarial estimates (and the potential sizes of risk and correlation with other risks). Lloyd's of London, however, offers a $50,000,000 limit under its e-Comprehensive policy but will write a custom policy for up to $200,000,000 (Gordon *et. al*., 2003). As more actuarial and damages data becomes available and cyber risk protection protocols become more standardized, it is likely that firms will be able to compete more broadly on coverage and premiums.

In all risk situations, even including potentially catastrophic risk scenarios, the best (and most cost effective) approach is to act to avoid the risk (risk prevention) or to reduce the consequences (risk mitigation) of the risk even before the risk has been materialized and

potentially ruinous losses have been incurred. Risk mitigation- or risk prevention techniques can enhance the defenses of enterprises, and lower the cyber risk insurance premiums an enterprise pays to be indemnified after a loss event. In the next two sections, we discuss several risk prevention and risk mitigation methods for cyber risks.

## 6. Cyber threat risk prevention techniques

The adage "An ounce of prevention is worth a pound of cure" is especially true when dealing with cyber threats. If, for example, an enterprise's financial transaction over the Internet is hijacked and funds or information are stolen, it may be quite some time (if at all) before the theft is noticed. Additionally, it is likely that the proceeds will never be recovered nor will the thieves be apprehended (Clarke, 2008). It is much better to prevent the theft or cyber crime in the first place, and the first line of defense is purchasing a good suite of security software including, anti-spyware, adware detection, malware and antivirus protection that has been obtained from a reputable vendor. An automated update feature together with an automated routine scan of the system is also a must, and software patches should be installed when available. It is also good business practice to seek advice from advisors — cyber risk insurers, lawyers, accountants, and risk managers. For example, the cyber risk insurer Crum and Forster makes a private web portal that provides their clients with technical resources geared toward assisting them in preventing both network and private cyber losses, and provides support recovery if a cyber loss should occur. (Insurance Journal, 2011).

Concerning internal cyber theft of money, there are fundamental sound practices enterprises should follow to reduce the cyber risk associated with financial accounts, including implementing procedures to password protect checking accounts, accounts receivable checks, vendor and payroll checks and credit card receipts. Since many cyber breaches go undetected for long periods of time, there are additional procedures that can prevent ongoing cyber theft including separating the duties of check writing from reconciling checking accounts, as well as performing unannounced periodic audits of accounts payable and checks paid. Over a certain amount, the enterprise should also establish a dual signature requirement for checks made out, and establish limits on the credit card spending on employee credit cards. This prevents (or mitigates) large losses if a cyber thief enters the system as checks or fund transfers cannot be routinely done in secrecy. Similar controls also should be used to protect intellectual property and valuable information such as databases by restricting access or needing verification to obtain copies, or keeping an automated log of who has accessed a particular record or data set. Commercial and non-profit enterprises do not have the same legal protection against cyber thievery of bank accounts that individuals do (the bank must reimburse the individual but not the company) so proactive diligence is especially warranted by enterprises for transactions involving financial transfers over the Internet (Johnson 2011). While cyber theft insurance can provide a loss control mechanism against such risks, it will generally be subject to a deductible and hence still contain a loss potential for the enterprise

Additionally, many instances of internal cyber (or just plain employee) theft could have been avoided had employees, prospective employees (and even board members and trustees) undergone a criminal background check. Unwillingness to agree to such checks should be a red flag. Also it may be worthwhile to have employees (regardless of their

tenure), undergo a criminal background and credit check every five years or so, especially if they have access to financial accounts or check signing authority. As mentioned previously, disgruntled employees should be particularly scrutinized if they have sensitive information access. According to the 2012 Global State of Information Security Survey by Pricewaterhouse Cooper (PwC 2012), 15 percent of respondents (from over 9,600 CEOs, CFOs, CISOs, CIOs, CSOs, VPs and directors of IT and information security from 138 countries.) strongly agreed that the risks to company data had increased due to employee layoffs.

Additional prevention measures can include encrypting signals at both ends of the communication channel, and higher level authentication of identity before allowing entrance into cyber locations having potential for breach and information loss. Some banks, for example will, each time, use a secondary verification method before allowing access to accounts. In this process the individual is sent a text or email message with a specialized code which must be entered along with the password when attempting to log in to the account. Similar methods can prevent many forms of unauthorized access into enterprise computer systems, and thus prevent losses before they occur.

## 7. Cyber risk mitigation techniques

While not all risks can be prevented, the damaging effects can be mitigated by judicious planning. Typically, firms that are looking to counter their cyber risk will utilize risk management frameworks and techniques that identify information security vulnerabilities. The first step is a security audit performed by the firm (or a third party) which identifies risks and vulnerabilities within the company's systems. This step usually involves inspecting the physical computing environment for external risk threats, as well as examining electronic networks (including offsite access by employees and customers). Additionally, companies gather information on current risk profiles by interviewing IT managers and determining the financial costs of the risk management process. In many cases, firms take the recommended steps to coordinate their own in-house response by setting up access controls and enabling firewalls before they consult externally with insurers or security experts (Siegel *et. al.*, 2002).

A very important risk mitigation technique for enterprises to implement is the use of data encryption, essentially coding each document so that it cannot be read, even if stolen or hijacked in mobile transmission. Encrypting transmission and/or documents makes it almost impossible for third parties to productively hack into databases or mobile devices (Ohlhorst 2010). There are many ways to use encryption. Single files can be encrypted or entire archives can be encrypted. There are several different types of encryption. The two main leading types of encryption are private key cryptography and public key cryptography.

Private key encryption has a single key that is used for encryption and decryption. According to (Ohlhorst 2010) "Private key algorithms are generally very fast and easily implemented in hardware, so they are commonly used for bulk data encryption." Private key encryption is mainly used for file, directory, and partition encryption that is only known by the owner of the data. There are two general categories of private key algorithms: stream ciphers and block ciphers. A stream cipher individually encrypts every byte of the data and

is commonly used for wireless communications. Alternatively, block ciphers encrypt one block of data at a time and are used mainly for data encryption (Ohlhorst 2010).

Public key cryptography involves the use of two distinct but related keys: a public key and a private key. The public key can be shared with anyone and is used to encrypt data meant for the holder of the private key. The private key cannot be shared and is used to decrypt any data encrypted by the public key. Public key cryptography is primarily used for e-mail messages, file attachments, digital signatures and other transaction-related processes (Ohlhorst 2010).

Monitoring and detection is also a critical step in avoiding cyber risk. Many times firms are unaware of, or provide an inadequate response to, a possible breach that could have been thwarted. If the threatened firms used updated monitoring and intrusion techniques to detect attacks or threats in real-time, their performance rate would increase significantly. Security consultants can help both in delineating risk, outlining risk mitigation techniques, assessing the financial consequences of such risks, and performing and monitoring (as the environment is constantly changing) risk audits and assessing cyber vulnerabilities.

## 8. Some comments about future trends and research

Regulation and controls in cyber technology have developed at a much slower pace than actual growth and progress in the technology itself, thereby causing a lag in enforcement and justice. As mentioned previously, many of the cyber risk threats originate from countries different from the host country, and regulating or enforcing laws against such trans-border criminals can be difficult or even impossible. Governments and international regulatory bodies, such as the United Nations, are now trying to develop stricter regulations in order to deter these types of illicit cross national cyber risk threat activities. However, until there is broad consensus on enforcement and retribution, companies will be forced to tackle these risks on their own. Any risk manager looking into the future must be able to plan for these unique threats and their growing sophistication. Since the Internet allows potential access from anywhere, firms and governmental enterprises must be prepared to address both internal and external cyber risk threats.

Proactively, regulators and governments can also intervene to help reduce the risk of cyber theft or crime. As mentioned previously, currently software makers for mobile Internet devices (smart phones, iPads, etc.) do not adhere to security requirements that hardwired, Internet-connected computers use due to tradeoffs between security and the storage size, and speed of performing tasks on these devices. Security has taken a back seat in this trade-off, and most users are unaware. Regulators can impose standards, which make cyber theft via such mobile devices more difficult and have mobile Internet device manufacturers make software patches available as vulnerabilities become known. The exact form of such regulations is an important topic for future research.

The rather rapid emergence of the Internet and information technology over the last decade has contributed to more efficient communication, which has allowed companies to reach broader markets in the new global economy. As companies and organizations continue to rely increasingly on cyberspace for communications, on-line services, and electronic databases, and as employees continue their trend toward mobile or remote access to enterprise infrastructure

and assets, the importance of mitigating cyber risk for enterprises will continue to rise. Insurers have already begun to offer cyber-related coverage but what remains to be seen is how effective those policies will be in transferring the risk. Insurers will be concerned about moral hazard problems wherein an enterprise, which has cyber risk insurance takes less protective action because they have insurance and do not bear the entire risk costs.

Currently, individual firms are able to mitigate their risks through risk management processes tailored to mitigate or control cyber threats. If firms utilize firewalls, pin and password access systems, encryption, and secure ids, they have a greater (but non-zero) chance of avoiding a large-scale Internet-related attack and financial losses. As a result of such proactive policies, they are also likely to obtain lower premiums for cyber risk insurance coverage, and better security audits by insurers, which can reduce insurance costs. Never-the-less, the potentially widespread impact of an organized or coordinated cyber attack or information security breach could overwhelm any insurer with claims (and a cyber attack on infrastructure could also overwhelm governmental enterprises as well). Therefore, it is critical that enterprises establish policies that aid in pre-loss financing of these potential damages in ways that avoid insolvency.

It is clear that public and private institutions will increasingly feel the effects of cyber risk from their own actions or those of a connected supplier, distributor, or end user. And, as developing countries push for greater access to the global market, competing companies may see cyber information control as a means of accomplishing that goal (e.g., cyber information theft of such things as intellectual property, competitive bids, etc.). This vulnerability may be especially pertinent to those companies who engage in outsourcing in a manner that necessitates data access by foreign companies to host company computers. Even while the host country firm may have installed cyber threat protection the outsourced foreign firm may not have equivalent cyber protection, and their access vulnerability together with their permitted access to host computers may pose risks for the host enterprise. Due to substantial interconnectedness, enterprises must be cognizant of cyber risk management plans of their suppliers and their downstream distributors who have access to the enterprise's computer accounts.

As information technology evolves, enabling enterprises to utilize the benefits advancing technology provides, from enhanced marketing facilitation, to enhanced employee access to important enterprise information during negotiation processes, and to allowing customers to access personal records from anywhere, any time, we must remain vigilant and protect our enterprises from the cyber vulnerabilities that this new technology brings. As Dr. Martin Luther King, Jr. (1963) said, "All progress is precarious, and the solution of one problem brings us face to face with another problem." Even as new technology is creating opportunities for enhanced efficiency in enterprise activities via such advances as immediate employee access, targeted marketing ability, better customer service, and enhanced governmental transparency, Internet users should be aware that these advances create the new problem of enterprises becoming increasingly susceptible to cyber threats.

An important area of future research is how to enjoy the benefits of the information explosion without succumbing to the perils of cyber risk from inside and outside the organization. Benchmarking, state-of-the-art risk mitigation techniques, and proactive management will be necessities in the forthcoming world of interconnected commerce.

Cyber risk considerations should rise to the level of Boards of Directors in the near future as the consequences of failure are simply too large to ignore or do otherwise.

## 9. References


Admin[at]databreaches.net. (April 2011). Former Wells Fargo employee sentenced for ID theft, In: *Office of Inadequate Security,* September 19, 2011, Available from http://www.databreaches.net/?p=17654

Anderson, R., & Moore, T. (2006). The Economics of Information Security, *Science,* Vol. 314, No. 5799 October 2006 pp. 610-613, Available from http://www.sciencemag.org/content/314/5799/610.full.pdf

Baranoff, E., Brockett, P., & Kahane, Y. (June 2009). Risk Management for Enterprises and Individuals, In: *Flatworld Knowledge,* Available from http://www.flatworldknowledge.com/printed-book/1635

BBC News. (2011). *Q&A: News of the World phone-hacking scandal, BBC Mobile News UK,* (August 4, 2011), Available from http://www.bbc.co.uk/news/uk-11195407

Bohme, R. (2005). Cyber-Insurance Revisited, *Proceedings of the Workshop on the Economics of Information,* The Heartland Institute, Policy Documents, Chicago, Illinois, USA January 1, 2005, Available from http://heartland.org/policy-documents/cyber-insurance-revisited

Brockett, P. Golden, L., Manika, D & Song, A. (2011). Developments in Mobile Commerce: Economic Opportunities, Risk Analysis and Risk Management, *Working paper*, Center for Risk Management and Insurance, University of Texas at Austin, USA

Burke, R. & Cooper, C. (2010). *Risky Business, Psychological, Physical and Financial Costs of High Risk Behavior in Organizations,* p.433, Gower Publishing, Ltd., ISBN 978-0-566-08915-2, Surrey, England.

Clarke, R. (June 15-18, 2008). A Risk Assessment Framework for Mobile Payments, *21st Bled eConference e Collaboration: Overcoming Boundaries through Multi-Channel Interaction* Bled, Slovenia, April 29, 2011, Available from http://domino.fov.uni-mb.si/proceedings.nsf/Proceedings/FC5AA5C853A1CF3DC1257481003D0293/$File/06Clarke.pdf

Coursaris, C. & Hassanein, K. (2002). Understanding M-commerce - A consumer centric model, *Quarterly Journal of Electronic Commerce,* Vol. 3, No. 3 pp. 247-271

FBI (2009). Spear Phishers: Angling to Steal Your Financial Info, (April 1, 2009), *The FBI, Federal Bureau of Investigation,* Available from http://www.fbi.gov/news/stories/2009/april/spearphishing_040109

Feig, N. (2007). Banks Aren't Securing USB Ports, Study Reports, In: *Bank Systems and Technology,* June 17, 2007, Available from http://www.banktech.com/risk-management/201000516

Flatley, J. (2010). Thumb drive-based malware attack led to formation of US Cyber Command, *Engadget, AOL Tech*, August 26, 2010, Available from http://www.engadget.com/2010/08/26/thumb-drive-based-malware-attack-led-to-formation-of-us-cyber-co/

Friedman, A., Crowley, P., & West, D. (2011). Online Identity and Consumer Trust: Assessing Online Risk, *The Brookings Institution,* January 11, 2011, Available from http://www.brookings.edu/papers/2011/0111_online_identity_trust.aspx

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches, *Information Management and Computer Security,* Vol. 11, No. 2 pp. 74-83, Available from http://www.emeraldinsight.com/journals.htm?articleid=862842&show=abstract

Ghosh, A. & Swaminatha, T. (2011). Software Security and Privacy Risks in Mobile-Commerce, *Communications of the ACM,* Vol. 44, No. 2 (2001), pp. 51-57

Giannoulis, P. (2011). Pod slurping: The latest data threat, In, *SearchMidmarketSecurity.com*. April 11, 2011, Available from http://www.searchmidmarketsecurity.techtarget.com/tip/Pod-slurping-The-latest-data-threat

Gordon, L., Loeb, M., & Sohail, T. (2003). A Framework for Using Insurance for Cyber Risk Management, *Communications of the Association of Computing Machinery,* Vol. 46, No. 3, (March 2003), pp. 81-85, ISSN 0001-0782, Available from http://portal.acm.org/citation.cfm?id=636774

Hallam-Baker, P. (February 21, 2008). Famous for Fifteen Minutes: A History of Hacking Culture, In: *CSO Online-Security and Risk*, September, 11 2011, Available from http://www.csoonline.com/article/217058/famous-for-fifteen-minutes-a-history-of-hacking-culture

Harris, S. (2008). China's Cyber-Militia, *National Journal,* May 31, 2008, National Journal Group, Inc. 2011, Available from http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531

Hodge, N. (2009). Russian 'Cyber Militia' Takes Kyrgyzstan Offline? *Wired,* (January 28, 2009), Available from http://www.wired.com/dangerroom/2009/01/cyber-militia-t/

Hughes, G. & Allard, T. (2005). Fresh from the Secret Force, a spy downloads on China, *The Sydney Morning Herald*, (June 9, 2005), Available from http://www.smh.com.au/news/National/Fresh-from-the-Secret-Force-a-spy-downloads-on-China/2005/06/08/1118123901298.html

Identity Theft Resource Center. (2011). *Identity Theft Resource Center A Nonprofit Organization,* March 21, 2011, Available from http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml

InfoSecurity. (March 5, 2009). NYPD victim of data theft, In: *infoSecurity.com,* March 30, 2011, Available from http://www.infosecurity-us.com/view/555/nypd-victim-of-data-theft-/

Insurance Journal. (June 8, 2011). Crum & Forster Launches New Service to Protect against Cyber Risk, *Insurance Journal* August 17, 2011, Available from http://www.insurancejournal.com/news/national/2011/06/08/201793.htm

Johnson, S. (2011). Cyber-theft bedevils businesses: Commercial enterprises don't enjoy the same protections as consumers from online bank heists, In:The Miami Herald, Business technology section, September 17, 2011, Available from http://www.miamiherald.com/2011/04/04/2150009/cyber-theft-bedevils-businesses.html

King, Martin Luther, Jr. (1963). Quote taken from *Strength to Love*

MacMillan, J. (2009). Johns Hopkins Tells Patients: Employee Stole Data for Fraud, In: *CSO Online - Security and Risk* . CXO Media Inc., April 12, 2011, Available from

http://www.csoonline.com/article/492427/johns-hopkins-tells-patients-employee-stole-data-for-fraud

Marcus, S. (July 22, 2010). Top 5 Mobile Commerce Trends for 2010, April 30, 2011, Available from http://mashable.com/2010/07/22/2010-mobile-commerce-trends/

Maillart, T., Sornette, D. (2010). Heavy-tailed distribution of cyber-risks, *European Physical Journal B,* Vol. 75, No. 3 (June 2010), pp. 357–364, Available from http://www.springerlink.com/content/866j4814v275r582/fulltext.pdf

Mello, J. (September 29, 2005) Pod Slurping: Threat or Hype? In: *Welcome to TechNewsWorld,* March 27, 2011, Available from http://www.technewsworld.com/story/46417.html?wlc=1302480778

Miller, M. (June 30, 2008). Data Theft: How Big a Problem? In: *informIT,* Pearson Education, March 21, 2011, Available from . www.informit.com/articles/article.aspx?p=1220308

Ohlhorst, F. (February 10, 2010). Three encryption apps to keep your data safe - data encryption - PC World Business, In: *PC World Australia,* April 12, 2011, Available from http://www.pcworld.idg.com.au/article/335681/three_encryption_apps_keep_your_ data_safe/

Patel, H., Morrison, D. & Mischon De Reya, M. (n.d.). Information Theft: Are nervous employees sizing up your data? In: *KPMG: Cutting Through Complexity*. March 20, 2011), Available from http://www.datalossbarometer.com/14737.htm

Power, R. (2002). CSI/FBI computer crime and security survey. *Computer Security Journal,* Vol. 18, No. 2 (2002), pp. 7-30

PwC (2012). 2012 Global State of Information Security Survey, September 18, 2011, Available from http://www.pwc.com/gx/en/information-security-survey/key-findings.jhtml

Rhemann, M. (2011). "Cyber Trends" In: *Trends Digest,* September 11, 2011, Available from http://trendsdigeststore.com/CyberTrends.aspx

Richardson, R. (2008).CSI Computer Crime and Security Survey, *Computer Security Institute/Federal Bureau of Investigation* 2008, Available from http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf

Schwartz, M. (2010). The Mall in Your Pocket, *Gifts & Decorative Accessories Vol.* 111, No. 10 (2010) pp. 54-58

Schwartz, G., Shetty, N., & Walrand, J. (2010). Cyber-Insurance: Missing Market Driven by User Heterogeneity, *Submission to Workshop on the Economics of Information Security (WEIS),* February 2010, Available from http://www.eecs.berkeley.edu/~schwartz/missm2010.pdf

Siciliano, R. (February 15, 2011). Lost or stolen mobile devices can lead to identity theft, In: *McAfee Blog Central*, April 30, 2011, Available from http://blogs.mcafee.com/consumer/identity-theft/lost-or-stolen-mobile-devices-can-lead-to-identity-theft

Siciliano, R. (April 18, 2011). The Rise of Smartphones and Related Security Issues, In: *Infosec Island,* April 30, 2011, Available from https://www.infosecisland.com/blogview/13078-The-Rise-of-Smartphones-and-Related-Security-Issues.html

Siegel, C., Sagalow, T., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security, *CRC Press,* (March 4, 2002), Available from http://www.eprivacy.com/lectures/cyber-risk.pdf

Siwicki, B. (September 28, 2010). Mobile raises new fraud risks for merchants, In: *Internet Retailer,* April 10, 2011, Available from http://www.Internetretailer.com/2010/09/28/mobile-raises-new-fraud-risks-merchants

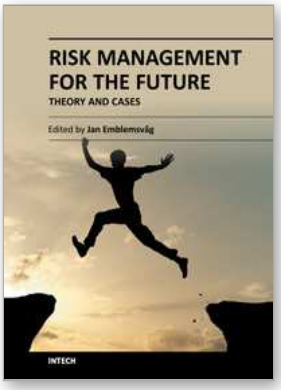
Spicer, J., Aspan, M. (2011). More customers exposed as big data breach grows, *Reuters*, 3 April 2011, Available from http://news.yahoo.com/s/nm/20110403/bs_nm/us_citi_capitalone_data

Stroup, J. (n.d.). Business Identity Theft: Your Risks from Employees, In: *Identity Theft - What You Need to Know to Protect Yourself from Identity Theft,* March 21, 2011, Available from http://idtheft.about.com/od/businessidtheft/a/IDT_EEs.htm

The Economist. (2010). War in the fifth domain: Are the mouse and keyboard the new weapons of conflict? *The Economist Newspaper Limited, London,* July1, 2010, Available from http://www.economist.com/node/16478792

The White House. (2010). Fact Sheet for National Strategy for Trusted Identities in Cyberspace, *Office of the Press Secretary,* June 25, 2010, Available from http://www.whitehouse.gov/the-press-office/fact-sheet-national-strategy-trusted-identities-cyberspace

Walsh, J. (n.d.) What is data theft? In: *article pros.* March 20, 2011, Available from http://www.articlepros.com/computers_and_Internet/data_recovery/article-131141.html




**Risk Management for the Future - Theory and Cases**
Edited by Dr Jan Emblemsvåg

ISBN 978-953-51-0571-8
Hard cover, 496 pages
**Publisher** InTech
**Published online** 25, April, 2012
**Published in print edition** April, 2012

A large part of academic literature, business literature as well as practices in real life are resting on the assumption that uncertainty and risk does not exist. We all know that this is not true, yet, a whole variety of methods, tools and practices are not attuned to the fact that the future is uncertain and that risks are all around us. However, despite risk management entering the agenda some decades ago, it has introduced risks on its own as illustrated by the financial crisis. Here is a book that goes beyond risk management as it is today and tries to discuss what needs to be improved further. The book also offers some cases.

**How to reference**
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Patrick L. Brockett, Linda L. Golden and Whitley Wolman (2012). Enterprise Cyber Risk Management, Risk Management for the Future - Theory and Cases, Dr Jan Emblemsvåg (Ed.), ISBN: 978-953-51-0571-8, InTech, Available from: http://www.intechopen.com/books/risk-management-for-the-future-theory-and-cases/enterprise-cyber-risk-management

INTECH
open science | open minds

**InTech Europe**
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

**InTech China**
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821