CORPORATE RISK, INTELLIGENCE AND GOVERNANCE IN THE TIME OF CYBER THREAT

Christopher Bronk*

Abstract

Cyber security is an issue of foremost interest for policy makers in the world's governments, corporations, NGOs, academic institutions, and other associations, however remedy for the myriad cyber threats and vulnerabilities continues to elude technologists and policy makers alike. In this paper, we consider the concept of cyber risk intelligence, a general concept of understanding the varied phenomena that impact an organization's capacity to secure its digital communications and resources from eavesdropping, theft or attack. We also consider the deeper economics of information held and transmitted in digital form and how those economics may alter thinking on modeling of risk. Finally, we offer guidance of how organizations and entire sectors of business activity may want to alter their thinking on cyber security issues beyond a technological framing to an informational one aligned with business activities.

Keywords: Corporate Risk, Cyber Security, Cyber Attack, Governance

**Baker A. Institute III for Public Policy, Rice University, 6100 Main St, Houston, TX 77005*
Office Phone: 713.348.5939
Fax Number: 713.348.5993
E-mail: rcbronk@rice.edu

1 Where is cyber security today?

There is a conventional wisdom in cybersecurity that some major corporations either know they have had a cyber incident while others don't. Regardless, of that awareness, it is likely that all of them have had a significant cyber incident. Consider:

- Fifty businesses participating in a 2011 study on cybercrime experienced an average of more than one successful cyber attack per company per week – a 44 percent increase over the 2010 rate (Ponemon Institute, 2011).
- A 2010 survey of data breaches in 28 countries found that more than 721.9 million data records were compromised over the five years ending December 31, 2009. This works out to the inadvertent exposure of 395,362 records every day (Suzanne Wildup, 2010).
- In November 2011, a leading cybersecurity company reported detecting four times as many "targeted" cyber incidents as it detected just eleven months earlier, in January 2011. Defined as attacks directed at a specific person or organization rather than at random victims, targeted cyberattacks are considered especially dangerous because they are insidious, long-term electronic "campaigns" that can be extremely difficult to uncover and address (Symantec Corporation, 2011).

In light of statistics like these, it's reasonable to assume that most companies either have been or are at risk of being compromised by cyber means. There is great concern regarding cyber attack, as evinced by former defense secretary Leon Panetta's 2012 address on cyber issues in which he invoked the image of a "cyber Pearl Harbor," a massive surprise attack capable of crippling the United States capacity to defend itself or function politically and economically (Bumiller and Shanker, 2012). The sort of cyber attack Panetta speaks about is one that matters a great deal to the Department of Defense. It forces the international community to visit law on armed conflict and establish a bar over which cyber attacks gain the attention of national security interests (Bronk, 2013).

This is the frightening discussion that touches on the nascent domain of cyber warfare. A good working definition for this sort of threat is offered by Hathaway, et al., who present, "A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose" (Hathaway et al., 2011). It is not just militaries and defense firms that are the principal targets, but other types of companies, including those in telecommunications, utilities, information technology, oil & gas, aviation, and logistics. They should hold concern that they may face well-crafted malware and sophisticated cyber

attacks that are designed to *disrupt operations and purloin information*. Thus, there is a far broader definition of cyber attack that we often see that comes from the computer security and information assurance disciplines. This broad definition of attack may include everything from the targeted email message to a corporate officer meant to install monitoring software on her PC to the launching of massive, distributed denial of service (DDoS) campaigns designed to shut down websites and stifle communications.[45]

While most cyber incidents don't make national headlines, they can hurt a business in any number of ways, from simply vandalizing its website to shutting down networks, perpetrating fraud, and stealing intellectual property. The financial impact can be significant; however precise measurement is hamstrung by lack of uniform measurement or widespread disclosure of all varieties of incident. Then there are the less tangible costs. Cyber incidents can also deal a serious blow to a company's brand and reputation, with potentially significant consequences. Concerns about data security may prompt current and prospective future customers to take their business elsewhere, and negative reactions among investors may even drive losses in market value (Garg et al., 2002).

Although pricing market perception due to cyber incident reporting is complex and abstract, this does not mean that measurable phenomena don't exist in the cyber area, and in particular cyber crime. As hyperbolic theoretical costs have stretched into the tens and hundreds of billions of dollars, industry, government and academic sources have begun assembling data regarding the price of stolen information, compromised computers and websites, and the annual losses to electronic crime. (Moore et al., 2009). Russian cyber security firm Kaspersky Laboratories was able to construct a comprehensive pricing index for everything from installation of malware on host computers ($3 to $120 depending on the country of location) to spear phishing botnet access ($1,000 to $2,000 a month) in 2009 (ComputerWeekly.com, 2009). There are beginning to emerge a more robust set of economic indicators on cyber security.

Unfortunately, because of the constantly evolving source of cyber risk as well as the shift in computing platforms employed by enterprise to do business (such as cloud services and bring-your-own mobile devices), many organizations may not be as effective at managing cyber threat risk as they are at managing risk in other areas. A telling statistic in this regard is that fully 86 percent of the data breaches examined in a 2011 study were discovered, not by the victimized organization itself, but by external parties such as law enforcement or third-party fraud detection programs. As the researchers put it, "If [an] organization … must be told about [a breach] by a third party, it is likely they aren't as knowledgeable as they should be with regard to their own networks and systems" (Verizon, 2011). Despite internal efforts to elevate cyber defense capabilities, internal capacity for cyber risk intelligence is rare outside of niche firms in the information security business and government agencies.

Then there is a larger set of policy issues regarding corporate responsibility and the public interest. Recent communications from the U.S. Securities and Exchange Commission (SEC) support the view that cyber threat risk merits board-level consideration, at least from a disclosure standpoint. Noting that "risks … associated with cybersecurity have [recently] increased," the SEC released guidance in October 2011 intended to "assis[t] registrants in assessing what, if any, disclosures should be provided about cybersecurity" (U.S. Securities and Exchange Commission, 2011). This guidance, while not an actual reporting requirement, does highlight the extent to which worries about cybercrime's business impact have infused the public consciousness. In addition, various drafts of cyber security bills that circulated in the U.S. Congress in 2012 envisaged a far larger role for the Department of Homeland Security (DHS) in coordinating cyber incident event data to begin the process of stitching together stove-piped corporate cyber security capabilities to construct a holistic view of cyber threat.

2 Where Cyber Security stands in major organizations

In the wake of incidents, companies are typically able to adequately assess "What happened?" and "How did it happen?" These questions guide the post-incident and forensic activities that occur after something has gone wrong. These are important to understand, but they do not necessarily help firms to anticipate the cyber threats they face. Unfortunately, asking them indicates that a failure has occurred and a loss likely incurred as well. The "What?" and "How?" of cyber incident response needs to be informed by a broader set of questions.

In the geopolitical context of cyber incidents and conflict, perhaps the most important questions revolve around "Why?" In cyber defense activities, the typical mindset has been one in which risks are identified and mitigated based on known vulnerabilities and known threats. The enterprise does its best to put the biggest goalie possible in front of the net. Where organizations often fall short is pulling together all of the different inputs in understanding their vulnerabilities. In cybersecurity plans, processes and technologies, we do not often see adequate thinking in the framing of why an asset or capability would fall victim to cyber attack. It is

[45] The October 2012 DDoS attacks against several major US banks falling into this category are considered below.

the "Why did this happen?" question that must frame risk management that establishes cyber security and cyber defense strategy in firms.

This requires business process owners to do some hard thinking about what information they hold is most valuable and which employees would be most susceptible for targeting. On the network, not all users or pieces of information are created equal. Both senior leadership and cyber security practitioners must accept that reality. Not everything can be protected, and resources must be distributed in accord with a fundamental understanding of what items or people require the greatest protection.

3 The information economics of the risk space

Compromise of systems via cyber means should be accepted as a valid risk for almost any entity, but there is need for establishing the how an organization should think about cyber threat. For organizations, risk is not an alien concept. Financial institutions, technology firms, energy companies, and international NGOs all must think about the actions they take in doing their business in which negative outcomes are a possibility. Making the right trade, investment, play, or position involves risk. Organizations typically study the up- and down-side of significant activity before making decisions tied to significant investment. Corporations must measure myriad issues, such as competitive forces, technology development, workforce, infrastructure, environmental impact, regulation, and political factors before major capital bets are made. Cyber adds a new dimension of risk, in the crosscutting informational domain.

Elementary economics regarding the output of the firm identify all inputs under the categories of *capital* (K) and *labor* (L). Making products is a process of buying physical plant and technology as well as hiring people. The revolution in information technology over the last several decades has forced economic thinkers to assess where IT fits in how output is measured. Generally, IT is seen as a capital input that enables increased productivity from labor. In the 1980s Robert Solow argued that investment in IT could be seen everywhere but within the productivity figures, but his point was mooted by IT-driven productivity gains during the 1990s. Today it is quite clear that information connectivity is synonymous with productivity. Global firms depend on IT to interconnect production with distribution, producing highly efficient, low inventory supply chains. But a great many businesses are also in the business of information. Facebook acquired Instagram, a company 13 employees that had been operating for a little more than a year, for approximately $1 billion. The company's value was measured in the number of users of the service and their frequency of use of it – in other words, information.

Talk of the value of information in organizations is an evergreen topic. The organization's employees and their intellectual capacity and output create value for the organization. We used to see this as a body of individuals with repositories of information floating around in their heads. But we should ask now to what degree seeing inside the digital persona of an individual – their email, documents, social media posts, and Internet browsing habits – is useful in understanding their intent and therefore the direction of their organization. In the last few years, the United States government and the cyber security community of researchers, firms, and consultants has sounded the alarm regarding the theft of corporate intellectual property via cyber means. But what may be even more important is to address to where organizations are being fully compromised by digital means, as was the case with the Dalai Lama's (Deibert and Rohozinksi, 2009). The Ghost Net operation aimed at the Dalai Lama (and many others) indicates how the cyber vector is being employed to gain the inside view of organizations in ways that conventional espionage could hardly have imagined.

Beyond seeing inside the firm and purloining its intellectual output, there is a third, increasingly important concern, regarding the disruption of organizational activity. In cyberspace, this has traditionally been via the employment of distributed denial of service (DDoS) attacks in which externally facing web servers are overwhelmed by massive data queries. This is not a new problem. The February 2000 DDoS attacks against major Internet firms including Yahoo!, Amazon.com, and eBay, ostensibly launched by a single youth, have evolved (Gross, 2011). Today, protests against governments and corporations are undertaken by loose confederations of hacktivists, non-state actors and possibly governments as well. Several major U.S. banks experienced a degradation of their online banking Internet portals due to DDoS in September 2012. More recently, DDoS has been directed by Anonymous at the oil and gas industry.

The *Shamoon* malware indicates an even more serious threat to organizations, the development of *wiper* programs designed to widely propagate on an internal network and delete massive amounts of data. Shamoon is reputed to have impacted as many as 30,000 host computers connected to Saudi Aramco's internal network. While large, mature firms typically have resilient backup strategies in place to prevent data loss by unauthorized or accidental deletion, repairing the damage of a massive cyber incident carries a cost in locating the cause, and repairing the damage. Ensuring a clean bill of health for a system that has been compromised usually does not entail replacing hardware, but the cost in labor alone is no doubt significant for a Shamoon-type event. While we are left to guess on the final cost of Shamoon to

the companies impacted by it, there is one ground truth in cyber security, the best cyber incidents are the ones avoided.

4 Cyber risk intelligence: a proposed method for managing risk

Navigating around cyber incidents, from rather pedestrian cybercrime events and virus outbreaks to the highly sophisticated targeting of critical systems and senior executives or officers, is the problem of the moment. In an informal polling of cyber security specialists in industry and academia, there exists a general belief that the adversary has the initiative, and that response is ad hoc and often undesirably tardy. The Department of Homeland Security's Eric Cornelius recently asserted, "the delta *t* [or time] between compromise and detection is 420 days." Most of the cyber incidents Cornelius's office at DHS sees are more than a year in the running. This is plenty of time to exfilitrate massive quantities of data, emplace malware Trojans for future use, and observe the digital operations of the targeted organization.

Necessary then is a better way of undertaking the business of cybersecurity. While prescriptions of "don't click the link" employee awareness campaigns, procurement of security technologies and increased staffing are all valid, there is also a need to reassess strategy, for not just IT, but information. In other words, cyber security is not just an IT problem to be solved in a sub-segment of the organizational IT office. Cyber security is a culture. Organizations have these. In Houston, we see an industry-wide emphasis on the importance of safety on oil and gas operations and the conduct of the manned space program at NASA. Developing this culture will take time and by itself will not likely bring an end to major cyber incidents.

Military thinking on cyber incidents has emphasized development of the capacity to deter (Libicki, 2009). Deterrence, while useful in preventing major conflicts, largely breaks down in the cyber domain. There is much for the attacker to gain, often there is little to lose, and getting caught at all is not necessarily likely. With deterrence not yet practicable, the organizational default has been fortification, and hardening of the network, much as the world's great cities built walls to keep the undesirables out, from bandits to foreign invaders. The problem here is that walling off the network means severing connectivity and functionality. For the global organization, the capacity to conduct business is largely determined by the ability to pass data packets between offices and individuals. Digital connectivity is the lifeblood of global operations. Without the capacity to communicate quickly at a distance, the productivity gains of the last twenty years essentially evaporate. A massive cyber fault doesn't take us back to the Stone Age, but possibly to the 1980s.

This argument makes IT important, and it is if economists are willing to let information stand alongside capital and labor in the measurement of output. What this means is that cyber security needs to be considered in the broader scope of the organization. Considering what bad outcomes might occur in the cyber arena needs inputs not just from the IT space but the broader space of operation. We see a holistic model of inputs for cyber security that reaches far beyond IT-based indicators. Understanding what's going on within the network is important, however, seeing why the network is threatened is also important.

We see three general flows of information in determining an organizational frame for cyber risk intelligence: one that encompasses the awareness of the IT enterprise and its apparent health; a second that brings internal business activities into view; and a third that encompasses broader geopolitical and economic forces. These three areas can be combined into a common operating picture for cyber risk awareness. To the IT security community this no doubt seems daunting, but each of these areas is important.

Gauging the health of the organization's overall IT operations is what organizational chief information security officers and chief information officers are expected to know on a day-to-day basis. Such awareness is an output of increasingly advanced security hardware and software as well as increasingly specialized security practitioners inside the organization. No doubt, the larger the organization, the greater the resources and the larger the workforce, but bigger organizations are better known and frequently targeted. There's no reason to be complacent in size and spend alone.

More abstract is the need to incorporate the activities of the organization. Major manufacturers require global sourcing of materials and components, months or years of lead-time for product design, and frequently the aid of outside experts and vendors. Understanding cyber risk to the organization translates to understanding what the organization holds, what it values, and where it is headed. In addition, understanding business activities extends to partnerships and other relationships. This makes cyber security often a shared exercise, because of the role of external parties. Secret merger talks or a hushed product development may involve the participation of outside help, which leads to questions of how law firms, auditors, or other advisors are protecting information resources. The business factors are relevant cyber security factors as well.

Out third category addresses the broader economic and political forces at work. This is the broader space in which the organization is positioned. Today, few are the large organizations that do not also engage in international operations. They can expect that the threats they face, whether friendly competition, evolving market conditions, or overt

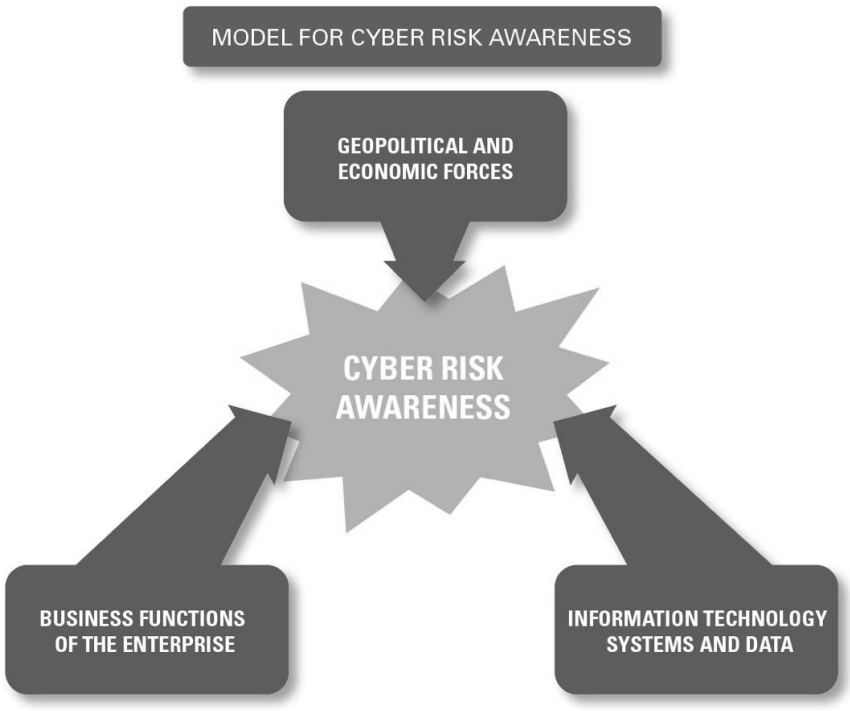
political acts, to increasingly migrate to cyberspace. Some proof of this may be offered in the widespread distributed denial of service (DDoS) attacks undertaken against the internet portals of some of the United States' largest banks during October 2012 that we alluded to before (Goodin, 2012).

Increasingly, we can infer that the cyber vector will be employed to express dissatisfaction and inflict harm, to operations, through the theft of information and the damage to organizational image.

With the rise of chief digital officer (CDO) positions in corporations, we see the indicators that organizations are reconsidering how they orient to the marketplaces dominated by the Internet. These CDOs will likely head up the activity of determining online strategy, but as currently conceived, the CDO position is likely one more oriented with marketing than corporate IT or security (Conneally, 2013).

How organizations will match their cyber security concerns with their overall digital strategy is an important question, but one perhaps not one being given much thought yet. That said, the hiring of talent, with the wherewithal to consider cyber security through multiple lenses rather than via a myopic IT-only view is under way, especially in global multinationals. This indicates that the lines between information security officers and security officers is probably blurring. The executive traveling abroad on business now needs adequate briefing on not only petty crime, kidnapping and terrorism, but also cyber threats.

Figure 1. Cyber Risk Awareness



5 Getting to Cyber Risk Intelligence

For more than a decade, organizational leaders have wondered how much is enough in cyber security. The good news is that we are now growing to better understand why the security of digital resources is a concern. Unsettling is that there is no means, short of digital disconnection, to completely mitigate the risk of a cyber incident. The current state for many or even most organizations is that they are coping with the cyber security problem. This raises the question of how organizations an move in front of it (Goel, 2011). We have several general observations drawn from the world of cyber security and also those from the field of intelligence.

First, cyber security has largely been viewed as a province of organizational IT. This is logical, as cyber security activities are designed to protect IT assets, but cyber security also addresses the protection of information, business operations, and larger issues of reputation and image. Organizations may need to consider how the cyber vector impacts their leadership with deeper thinking about the information at risk. The perception of cyber security activity as "an army of 'no'" inside the organization which seems to only be able to tell the general workforce what it can't do based upon known threats and vulnerabilities is one that requires remedy. The ability for an organizational IT security shop to consistently eschew innovation in the field in the name of security ignores the realities of increased productivity and profitability. This sort of risk avoidance runs contrary to the intuition of

organizations that embrace or accept risk in doing business.

There's an important lesson here from the US military's experience with social media. In 2009, the US Marine Corps banned its personnel from using social media sites such as Twitter and Facebook, and but less than a year later the ban was overturned. On the policy, the Chairman of the Joint Chiefs at the time, Michael Mullen, "Obviously, we need to find the right balance between security and transparency. We are working on that. But am I still going to tweet? You bet" (Bronk, 2009). Mullen's position underscores an important lesson for organizational information security officers, that the case for risk avoidance must be abundantly clear especially if it impacts organizational performance, which in the Marines' case is largely a measure of morale. Cyber risk intelligence should translate to a more informed dialog on the pros and cons of employing different information technologies rather than begrudgingly accepting new technologies because organizational leadership wants them.

In moving cyber security beyond the corporate IT function, a second issue must be entertained, which is how the organization is exposed to competition or harm. Organizations need to think about how their competitors and adversaries may gain from compromising information resources or computer systems. Where organizations generally detect the compromise of information systems is through discovery of atypical system behavior. This makes sense, but organizations will also need to approach the cyber issue from the business. When there is a pattern of failure, executives will need to begin asking, "Is there a cyber issue here?"

For organizations that take the above question seriously, this will be translated into cyber specialists who can not only understand the network operations and data management issues, but also interface with the business. They will need to embrace counter-intelligence thinking and practices and work with senior leadership on understanding where things aren't working and also determine what and why certain pieces of information may be vulnerable or compromised. In addition, they will have to understand the chains of custody for sensitive information so as to better understand how partners may be creating exposure to vulnerability. An organization with superb cyber security practices in place is vulnerable nonetheless if a law firm or accountancy it employs to conduct transactions does not have the same sort of capacity to protect information. Boilerplate legal language on the ethical and legal constraints on the transmission of information tacked on to the end of an email message are meaningless to the cyber adversary who has already accepted that she will function outside the law.

This issue of information custody speaks to the broader issues of how to build a more secure information ecosystem. We often discuss parameters for good hygiene or public health in cyberspace. These include technological practices such as deployment of anti-virus software, intrusion detection systems, and email spam countermeasures. There are also good organizational behaviors to foster, once again a common understanding on the importance of "Don't click the link," in countering phishing via email or other platforms. What will become more necessary is the construction of defensive policies and techniques that conform to the unique information resources, communication requirements, and computational infrastructure of the organization.

There is an issue here in scalability however. The largest corporations or government agencies can allocate far more in resources to the cyber security problem than smaller players. More important will be industry-wide efforts that identify key security concerns and meet them with collaborative response. Such activity can be labeled as another form of collective security, the same sort of thinking that guides countries to form military blocs or even broader political and economic organizations. The question in cyber security governance is how different industries and arrangements of organizations will come to confront the problem. This is a key problem that needs to be addressed. Without it, the large and well-resourced organizations, many of which are big targets, may be better off, but the smaller entities with which they work and upon whom they depend, will still render them vulnerable.

This collective action problem is at the core stumbling point for cyber security strategy. What will be interesting to see is how organizations accept the cyber vulnerability issue and are allowed to move beyond isolation in addressing threats and incidents. Today, organizations share data on cyber risk with others all the time. Consider the traffic in data from customers to the purveyors of anti-virus software. Without the constant connectivity between host computers and anti-virus labs, the struggle to contain malicious software of a general nature (as opposed to specifically designed pieces of malware) would be impracticable if not impossible. If the practice of cyber security is to improve, it will need to embrace the same things that the adversary willingly accepts: agile thinking; constant learning; and a willingness to collaborate beyond traditional boundaries when expertise is needed.

No single technology is likely to alleviate security concerns of the Internet-interconnected organization, nor is any single skill set able to do the same. Cyber security is akin to the other security concerns of our age, such as crime and terrorism. There are certain actions that may be taken by the individual and the organization to thwart them, and there are also certain common issues that only government can undertake, particularly when we consider punitive action in response to transgression.

But like the other forms of security threat, a fundamental component is in information.

Since the September 11, 2001 attacks, two air travelers have tried to blow up airplanes and been thwarted by fellow passengers and flight crew because there is a clear understanding of what is at stake. People aboard airliners now understand that successful hijacking may mean death. Threats in cyberspace are not so clear and so great in terms of life and limb. The case is clear that the world's organizations – governments, corporations, NGOs, universities, associations, and others – depend on IT to function. The question for preserving cyberspace is how those organizations pool their attentions and resources to preserve a vibrant and functioning cyberspace that may be used to enhance human endeavor. Without adequately studying new and even unorthodox approaches to security, we may eventually lament the loss of the cyber-connected world we once enjoyed.

References

1. Bronk, C. (2013), "Hacking Isn't Cyberwar, for Now", New York Times, February 28.
2. Bronk, C. (2009), "Marines' social-media ban is bad for morale - The ban might demoralize troops more than it improves security", Federal Computer Week, September 17.
3. Deibert, R. and Rohozinksi, R. (2009), "Tracking GhostNet: Investigating a Cyber Espionage Network", Information Warfare Monitor, March 29.
4. Bumiller, E. and Shanker, T. (2012), "Panetta Warns of Dire Threat of Cyberattack on U.S.", New York Times, October 11.
5. ComputerWeekly.com (2009), "Kaspersky reveals price list for botnet attacks," July 23, http://www.computerweekly.com/news/1280090242/Kaspersky-reveals-price-list-for-botnetattacks.
6. Conneally, T. (2013), "'Chief Digital Officer' is the next hot executive title, says Gartner", betanews, March 27, http://betanews.com/2012/10/22/chief-digital-officer-is-the-next-hot-executive-title-says-gartner/.
7. Garg, A., Curtis, J. and Halper, H. (2002), "The financial impact of IT security breaches: What
8. do investors think?" Information Systems Security, pp. 22-23, http://www.auerbachpublications.com/dynamic_data/2466_1358_cost.pdf.
9. Goel, S. (2011) "Cyberwarfare: connecting the dots in cyber intelligence", Communications of the ACM, Vol. 54, No. 8, pp. 132-140, http://dl.acm.org/citation.cfm?id=1978569.
10. Goodin, D. (2012), "DDoS attacks on major US banks are no Stuxnet- here's why", Ars Technica, October 3, http://arstechnica.com/security/2012/10/ddos-attacks-against-major-us-banks-no-stuxnet/.
11. Gross, D. (2011), "'Mafiaboy'" breaks silence, paints 'portrait of a hacker'", CNN, August 15, http://www.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html
12. Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., and Spiegel, J. (2011)
13. "The Law of Cyber-Attack", Yale Law School, November 16, http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf.
14. Ponemon Institute (2011), "Second annual cost of cyber crime study: Benchmark study of U.S. Companies", August, http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf
15. Libicki, M.C. (2009), "Cyber Deterrence and Cyberwar", RAND Project Airforce, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
16. Moore, T., Clayton, R., and Anderson, R. (2009), "The Economics of Online Crime", Journal of Economic Perspectives, Vol. 23, pp. 3-20.
17. Symantec Corporation, (2011), "Symantec Intelligence Report: November 2011", http://www.symanteccloud.com/mlireport/SYMCINT_2011_11_November_FINAL-en.pdf
18. U.S. Securities and Exchange Commission (2011), "CF Disclosure Guidance: Topic No. 2 – Cybersecurity", October 13, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
19. Verizon (2011), "2011 data breach investigations report: A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit", http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.
20. Wildup, S. (2010) "The leaking vault: Five years of data breaches", Digital Forensics Association, http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault-Five_Years_of_Data_Breaches.pdf.