https://doi.org/10.48009/2_iis_2009_113-120

A THEORETICAL FRAMEWORK FOR UTILIZING DATA WAREHOUSING TO PREDICT INFORMATION SECURITY THREATS

Lee Jonathon Steen, Robert Morris University, ljsst8@mail.rmu.edu
Philip S. Kim, Robert Morris University, pxkst1@mail.rmu.edu

ABSTRACT

Many organizations have implemented information security countermeasures to detect, minimize, and defend against information security threats, or breaches. Most of these countermeasures have traditionally adopted a passive approach to securing corporate data. This paper proposes a theoretical framework for utilizing an information security data warehouse to identify security breach patterns, in order to predict when potential breaches are most likely to occur, thus taking a more proactive approach to securing information assets.

Keywords: Information Security, Security Breaches, Secure Data Warehousing, and Predictive Security Model.

INTRODUCTION

Information security has experienced exponential growth and consideration in recent years. Information has become a major financial staple for organizations as it is a driving force for companies to increase revenues or significantly reduce expenses. The PriceWaterhouseCoopers Global State of Information Security Study [21] describes organizational information or corporate data as the "new currency of business." The total cost spent on information security in 2006 was estimated to be approximately $45 billion [10], and that amount is expected to have increased substantially in 2007 and 2008. And in spite of the current worldwide economic state, security spending is one area that does not appear to be losing momentum [10] [18]. This has given organizations every reason to protect their information, and yet security threats and breaches will and do occur. Most security defenses are geared towards the prevention and/or mitigation of security breaches and often have to be policy-driven [8] [11] [25] [30].

The typical countermeasures for hardening security include layering defense systems, diversifying defense methods, ongoing management of hardware and software updates or patches, access controls with auditing, and authentication mechanisms [8] [11] [25] [30]. The issue with traditional information security countermeasures is that organizations often adopt a "passive" approach. This passive approach is operationally defined as putting security measures and countermeasures in place, and hope they work. If a breach occurs, these measures are updated to stop future breaches.

Almost all organizations that connect to the Internet have implemented some type of firewall. And yet simply deploying a firewall or several firewalls and not securing any further presents a single point of failure [24]. Other companies put up a myriad of defense mechanisms in place to prevent attacks without knowing what types of attacks will occur, or when they will happen. Still other firms try to stop or mitigate the attack happening in real time (e.g. Intrusion Detection Systems (IDS), or review logs and audits to see when attacks or breaches occurred). Even the IDSs are a passive approach because they ares reactive in nature, not pro-active. Each of these methods has an associated overhead cost with it and can be difficult to identify how effective they really are [26].

This paper presents a modified approach from the traditional passive information security measures to a more pro-active and risk-based approach to information security defense. The pro-active and risk-based defense has two parts. One is predicting when and where an attack is likely to occur, and the other to implement a risk-based methodology of safeguarding the most critical assets against an attack. This pr-active active approach allows an organization to actively look for where breaches are likely to occur. Once this is know, a risk-based approach allows the organization to focus more resources on the high vulnerable areas, and move away from less vulnerable ones. This makes the use of security resources more efficient and gives a better return on investment. Our focus for this paper is the prediction aspect, but we will discuss the significance of utilizing a risk-based approach to determining a corporation's critical assets.

The model presented in this paper for predictive security breaches involves the use of a data warehouse. The research will review current security threats, data warehousing, and present a predictive

model. The reader is encouraged to critique, adapt, and modify the model to their specific organization or industry. The paper concludes with the potential gaps within the model and topics for future research.

SECURITY THREATS

A security threat is "[a]ny circumstance or event with the potential to cause harm to an asset" [31]. The most common threats for organizations are not only from outside attackers trying to gain unauthorized access, but also from inside employees who already have access and intimate knowledge of the systems. Internal employees pose a significant threat not only due to internal access rights, but often because of simple human error. Unwitting internal employees who are untrained in the proper use of systems and corporate security procedures are a threat to the information security environment [8] [11] [25] [30].

Attacks can be triggered from the outside when the unauthorized party (attacker) is seeking access into the corporate network. A successful breach could result in loss of information. The attacker can use the stolen information to sell to the highest bidder, or use the data to negatively affect the organization's image, or possibly some other personal gain. Attacks can be initiated from the inside for the many of the same reasons including, employees seeking to profit from confidential or proprietary data, and disgruntled employee(s) seeking revenge against a co-worker or employer. Another growing threat is social engineering attacks, which can be successful when employees are not trained properly and are have little to no understanding of corporate security policies [8] [11] [17].

The first line of defense towards mitigating security threats are often enforced by standard policies and procedures. The policy and procedures should address how company technology and information assets are to be controlled and handled. Corporate policies and procedures should also include training employees on system and network updates for software and hardware, physical security practices, and updated information security policies and standards [8] [11] [25] [30].

DATA WAREHOUSING AND DATA MINING

A data warehouse is a repository of large amounts of data in a single, non-normalized location. The data warehouse gets its information from databases, transactional systems, data marts, and from other places in the organization where data is generated [1] [28].

The data warehouse information can be analyzed for patterns that emerge and for useful information by using data mining techniques. These techniques can use mathematical analysis and algorithms to discover patterns that are not easily identified by manual review.

In order for a data warehouse to be most effective, it has to contain relevant and up-to-date data that can lead to useful information. For the purpose of this theoretical framework, we are most interested in how a dedicated information security data warehouse can be a central repository for an organization's history or previous experience with security threats, attacks, and breaches. That is, the information security data warehouse will be a storehouse of any security breaches that have occurred and all of the possibly linked information to the security breaches. But gathering all data available may be too time-consuming and may prove to be unhelpful if it is not relevant. The question yet remains, what exactly is relevant and useful information as relates to the data warehouse?

In order to answer that question, it is worth analyzing applications within security that have built themselves around the use of a data warehousing and/or data mining. These applications include intelligent intrusion detection systems (IDS) [12] [15], internet protocol traffic and measurement analysis [2], identification of fraud within telecommunications [4], breach propagation detection for knowledge-sharing within an organization [30], and role identification for security administration [14].

ADAPTATION OF CURRENT APPLICATIONS

Intelligent intrusion detection systems (IDS) are designed to identify patterns within a computer network that appear to be inconsistent with a baseline and then analyze the pattern to determine if an intrusion is occurring or has occurred. Real-time IDS systems need to be accurate so they do not have many false alarms, efficient so they don't bog down network resources, and useable so that the individuals can utilize the tools [15]. Although IDS are considered a pro-active approach, they still do not anticipate breaches.

Lee, et al. [15] states that "[t]o improve accuracy, data mining programs are used to analyze audit data and extract features that can distinguish normal activities from intrusions." By utilizing data mining techniques, it is possible to detect breaches in real

time. It would be possible to take the current data mining process, store the same audit information in a data warehouse and perform queries to determine if there is an emergence of intrusion patterns. Organizations may be able to observe intrusion patterns by harnessing the ability to store, process, and query large amounts of information within the data warehouse. As more data are collected and intrusion patterns are identified, management could perceivably determine causal or corollary relationships to emergent security intrusions.

Another type of IDS uses data gathering agents to collect system logs and activity. The IDS then gathers and summarizes the data into an easy-to-understand common format [12]. Using this data, lower level agents classify the data and send it up to a higher level. What this means is at a low level, several agents analyze the data and summarize it by a common mean. The common mean summary is then passed one level higher. The higher level receives several summaries together and analyzes them, common means them again, and passes the data to the next higher level. This process is done until a single level makes a decision for the whole network. Adapting this to the information security predictive model would mean starting with the lowest level of security breach data, summarizing the data into meaningful information, and passing it up higher until it reaches the level of decision. The security breach data would need to be accessible and summarized at each level to determine if patterns exist within the breach (or intrusion).

Another area that is similar in design, measurement and analysis of data is the monitoring of internet protocol (IP) network usage and behavior. A current system of monitoring and measuring IP network usage and behavior is being used by AT&T [2]. This study describes how IP traffic is stored in a data warehouse and analyzed by data mining techniques to understand the behavior of IP traffic in a network. This type of data could be instrumental to understanding when a breach is likely to occur. If a specific segment of a network is experiencing unusually high traffic and the traffic begins to migrate, a pattern of movement may be emerging. Utilizing the data warehouse's real-time monitoring of IP traffic patterns would enable system administrators to determine, or "predict" where the traffic was heading. Once a known pattern is recognized, management would be able to mitigate the risk of attack by implementing additional defenses in that specific area.

Internal access to resources is another potential issue of security. Research has shown that by understanding the type of data stored and the level of authorized access held by an internal user, along with the frequency of access, an attacker can determine what function that user has within an organization [14]. For example, if a user continuously accesses financial data (type of data stored), at an access level that is high (level of authorized access), over a period of six months (frequency of access), the attacker and determine the user is a financial officer, or a manager of finance. The major purpose of "role mining" is to determine where a user falls within a set of business roles within an organization. A method to ensure all access and access attempts are legitimate, management could log and store the successful and unsuccessful access attempts within our theoretical information security data warehouse. Even with a brief history of internal access logs, the data warehouse could determine a pattern of invalid user access attempts. Similar to the IP traffic monitoring, management could then determine which internal resources had the highest number of unsuccessful access attempts to identify what types of forms, files, and data that users are after. Even if the user is not maliciously trying to access resources outside of his privileges, the history of user attempts data could point to future attempts or breaches by internal employees that do have malicious intent.

Another information security threat to organizations that share their data with other organizations is breach propagation [30]. The primary idea behind breach propagation is that as companies and organizations begin to share their information and data, knowledge sharing becomes an "inter-organizational" endeavor, which can positively increase the level and depth of knowledge. However the increase in inter-organizational reliance and information sharing can lead to an increase in breaches across many other partner organizations. Because the valuable data and knowledge is being shared, so too are the risks and vulnerabilities of a security breach [30]. To prevent this, the researchers present a model that attempts to minimize the effects of a security breach by centralizing security within a single "security hub" that controls access. In the event of a breach, the data can immediately be reported to the security hub and centralized to that node of the network. The security hub would allow all others hubs to be notified. To adapt the study's breach propagation defense, the data security hubs could be implemented as data marts that could directly feed into our theoretical information security data warehouse. The data warehouse would store data of all breaches that have occurred, when they

occurred, how they occurred, and any relevant circumstances surrounding the breach. This information could then be mined to determine if specific patterns of breach occurrences exist.

Another area that has recently been researched is how to analyze and control telecommunications frauds [4]. Telecommunications are essential to networking because they are the pathway to how networks connect and operate. A model for analysis and control of telecommunications fraud has six major components including a) detection, b) prevention, c) analysis, d) prediction, e) alarm, f) control [4]. What is particularly interesting is that this study included a potential model for prediction of fraud but did not appear to be discussed in detail. The various forms of relevant data in this study include customer data, fraud events, and customer data reports. This type of information could also be used to determine if any patterns are available that breaches (or fraud in this case) occur within the telecommunications system.

The final adaptation of current research to discuss is centered upon finding bugs in software that are used to exploit security vulnerabilities for attacks [32]. This method describes trends in ensuring software quality when systems are created by combining several different software components together to use specific features. This trend is known as service oriented architecture (SOA) and uses software as a service model. The implication with this study is the use information on software bugs to predict the service security risks, or breach prediction at given levels of service. The model is split into three areas, software security, service composition, and hacking exposure [32]. Each of these areas identified the most common breaches in security from the aspect of confidentiality, integrity, and availability. For example, a distributed denial-of-service (DDoS) attack is able to hinder system availability. From a hacking exposure perspective, it could mean that hackers may be able to easily identify the software, operating system, or software application an organization has deployed, and thus all known vulnerabilities can be exploited.

PREDICTION MODEL

The prediction model we propose will primarily use data collected on security breaches from multiple intra-organizational sources. The intra-organizational information security data warehouse would begin with a single organization and collecting data from its various departments, divisions, regions, and business units. The benefit of collecting the security breach data across the different departments is that it will lead to a more comprehensive representation of the organization's security breach environment. There is a wealth of information available even within one department's experience with security breaches, but the data may not be as useful across an enterprise if it is not being shared, stored, and utilized by other departments. The input data should not be limited to just security breaches or attacks.

Data input into the security data warehouse must also include organizational information such as marketing data, public data releases, or human resource activity such as incentive plans and bonuses, or new hires, promotions, and terminations. The data should also include when a company is introducing a new product line or information technology (IT) upgrades because these types of data may provide a direct link or correlation to an increase in security attacks or breach attempts.

The incoming data can be obtained electronically from an IDS or IPS system in real time [12] [15]. The data could be input into the data warehouse by a security administrator reviewing logs or by performing manual audits [4]. The data could also be automatically fed by other systems like security hubs, data marts, and even other predictive models already in place [14] [30] [32].

The multiple data feeds should be separated and scrubbed at the lowest level, and then combined and sent to a higher level for further scrubbing, and continued until the data reaches a level of meaningful summary [12]. The data will need to be organized and stored in a logical way that would allow the data warehouse administrator(s) to run multiple queries across various data sources. The results of the queries can then be reviewed to determine if there is any relationship between any security breach activities and other organizational activities. By collecting a brief history of security breach queries, an organization can examine these data and determine if an identifiable breach pattern emerges. The results should be used to inform management as to what data sources are most likely to be targeted and what, if any relationship exists between breach activity and intra-organizational happenings. If a significant pattern emerges, the organization may be able to not only defend against the attacks, but anticipate or predict when increased attacks may occur. The model is shown in figure 1 below.

In this model, the data sources shown at the top come from different areas of the overall corporation. This data is stored in some type of warehouse or data mart and is considered historical data of breaches and

other information. The forward looking corporate data is information that hasn't been released but can influence security. These items include news release statements that haven't occurred, potential purchases of different assets or other organizations, mergers, new technology being installed, or any other type of information that can influence security. All of this information is input to a security data mart and the information is scrubbed and transformed before being put into an enterprise data warehouse. Real time data, or data this is currently being streamed like IDS data, IP traffic data, news from other companies being released, and any other data will be stored later is streamed into a temporary or real time database. All the information from the enterprise data warehouse and the temporary database is input into a predictive algorithm. The temporary database is purged once data is stored long term or deemed no longer needed.

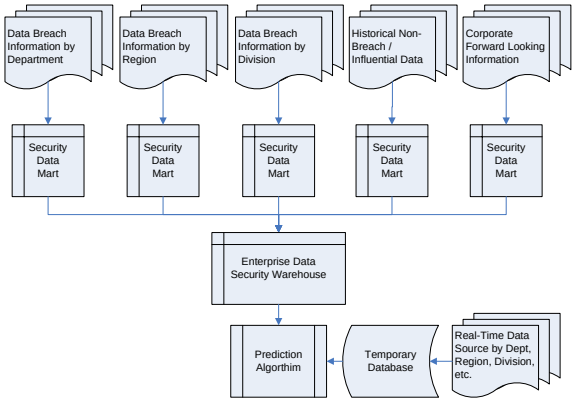

Figure 1 – Prediction Model

DISCUSSION

The security prediction model presented is from a high level. The actual input parameters would not be known until an organization is able to identify and risk-rate what data is relevant and what is not. The actual algorithms and queries used to mine the data, summarize the data, and identify the breach patterns are also open. Even if one system used a specific set of inputs and algorithms, it does not mean a second system would be identical. The systems are likely to vary by organization and industry. Depending on what breach patterns eventually emerge, an organization may have to adjust its definition of what is valuable or high-risk data. And as organizations continually adapt to the ever-changing information landscape [29], the prediction models will also evolve and mature.

The reason that news and other organizational data are important is because information thieves are becoming more opportunistic and some breaches occur because of the release of corporate data or news releases [3] [5]. A recent collection of information security breaches and the circumstances surrounding them reveals more than just technology security flaws [20]. Many of the cases of information theft or breaches involve other factors that are related to the incident such as involuntary terminations, massive corporate layoffs or downsizing, espionage or theft of proprietary information by a competitor. Recently, Circuit City, a US retailer of consumer electronics announced it would be closing its doors to business. A recent story was published regarding the arrest of three Circuit City employees suspected of stealing more than $50,000 in property from the retailer [23]. Police found TV's, video game systems, and computers while serving the warrant for arrest. According to report, store management determined that the employees were using Circuit City credit lines established by customers to make additional purchases. This incident was an example of a physical and logical security breach.

Another example involves an aerospace company. This breach involves three employees at NEC Toshiba Space Systems who were arrested for stealing data from Mitsubishi's antenna design for a high-speed Internet connection satellite [19]. Police report that one of the employees was able to guess a password to gain access to another organization's network that housed the proprietary data. It should be noted that it was public information that NEC and Toshiba were competing against Mitsubishi to develop Internet technologies and for bidding on Japan's National Space Development Agency (NASDA) future projects. NASDA prohibited both NEC and Toshiba from bidding on NASDA projects for a month [19].

Even virus attacks can be targeted based on news or current events. A recent virus by the name of Waledac.Trojan was introduced on February 10, 2009, and was targeted to those who sought to send electronic Valentine's Day greeting cards. According to Computer Associate's Security Advisor alerts, the Waledac Trojan has been observed to arrive in Valentine's Day-themed spam emails and spoofed websites [27]. Scenarios like those mentioned above could have been stopped or mitigated by the prediction model if the right information and patterns were identified prior to the security breaches.

Inter-Organizational Model

Ideally, this model would be more effective when multiple organizations are working together; creating

an inter-organizational security data warehouse that crosses organizational lines and numerous industries. By having multiple sets of data from different areas, the identification of patterns and prediction should be more accurate and reliable. Organizations that reveal and share breach information may find some commonality between the reasons or circumstances revolving around the breach incident. Also, if one organization is experiencing a specific breach and a still more organizations from the same industry begin to experience similar breaches, the system could identify and alert the breaches in real time, giving other enterprises within the industry a warning of what is likely to come. Real time is operationally defined in two ways, depending on the implementation. First, it can be real time streaming data that can be used in an algorithm to calculate probability, but not yet in a data mart. The second is to pull in real-time from a data mart. The difference will be decided by policies in an organization on how it is to handle data (e.g. from a data mart exclusively to the algorithm, or from streaming data).

But a few issues present themselves with organizations sharing breach information with other companies. The biggest issue is that companies do not want to release information when breaches happen. It is known that many companies will not publically release information on security breaches due to fear of threatening customer loyalty and negatively affecting the organization's reputation.

It is critical that the data warehouse that stores the breach information must be secure and follow specific security policies. A study on security and data warehousing was conducted which analyzed different aspects of online analytical processing (OLAP) data warehouse system [22]. Data warehouses crossed boundaries of various organizational units and thus security needs to come from front end access. Front end access means the graphical tools that display the data control what tables of data a user can access. This research is supported by another study which identified that meta data could be used for security purposes [13]. The meta data helps identify what information is sensitive and how it can be removed, or hidden from queries but still used. The research is also supported by further studies that identified that the actual "VIEW" of the data requested can be executed, but front end display tools for the view of the data can block out any data the user does not have access to [9] [25].

But even if the data was secure, preserving the privacy of the participating organizations is important as well. Privacy is an increasingly growing issue for integration and sharing of data [7]. Since multiple sources of data with varying degrees of proprietary and confidentiality will be coming into the data warehouse, the information must remain private. For example, if two companies who work in the defense industry as competitors decide to share a predictive data warehouse, since it would be beneficial to both, they need to establish practices that do not allow each other to query private data that is sensitive to their respective organizations [6] [33].

Even though security and privacy issues need to be addressed, the benefits of a predictive, if properly secured, the shared model can easily outweigh the risks. There may even be monetary rewards for those who share information on security breaches. Microsoft provides monetary awards, or bounties, to catch people who release worms that exploit known security vulnerabilities [18]. Because a shared information security model would not only share specific breach data, but also spread the load of responsibility for preventing future attacks. This concentrated cooperative effort could also aid in tracking the origins of outbreaks like worms and help identify the hackers who begin the attacks.

CONCLUSION

Information security is an area within IT that continues to grow in importance every day. As technologies advance, management must ensure that information security standards and practices also keep up to date. Although information security has usually "been the responsibility of IT departments, some companies have made it a business issue as well as a technological one" [16]. Most security defenses and countermeasures against threats have traditionally taken a more passive approach which puts implements standard pre-emptive security measures such as firewalls, proxy servers, IDS systems, and authentication protocols such as strong passwords and biometrics. While these industry-standard defense mechanisms serve as a foundational basis for information security, we argue that organizations should start to consider initiating a more pro-active approach to information security, specifically studying breach data, identifying trends, and predicting future security attacks or breaches before they occur.

This paper presented a first attempt at developing a security prediction model that utilizes a data warehouse to store attacks and breaches on an organization. The reader is encouraged to critique, adapt, and modify the model to their specific organization or industry. The issues with the

presented model may include privacy and sharing concerns, unknown attacks or breaches cannot be logged if they are not identified, accuracy of false-positives and false-negatives may be a problem, speed to which the prediction can respond, how the prediction should initiate a response, and not enough data stored to predict attacks. All of these issues should be researched further and a customized plan for each organization adopting this model should be utilized.

Future work will consist of designing the information security data warehouse and archiving security breach information from several intra- and inter-organizational units. The data will be analyzed manually and algorithms will be created to test the theory that breach patterns can be identified, and that the resulting future breaches can be predicted. Also, the issues listed above will be discussed with proposed solutions once the system is built.

Our proposed information security data warehouse model will be able to assist organizations in preparing for anticipated information security attacks or at a minimum to be more aware of attacks or breaches that have occurred in other companies and industries. Management could also utilize the data warehouse to determine its allocation of security resources, by providing more security in one area based on the risk and likelihood of an attack.

REFERENCES

1. Agosta, L. (2000). *The essential guide to data warehousing*. Upper Saddle River, NJ: Prentice Hall PTR.
2. Caceres, R., Duffield, N., Feldmann, A., Friedmann, J. D., Greenberg, A., Greer, R., Johnson, T., Kalmanek, C. R., Krishnamurthy, B., Lavelle, D., Mishra, P. P., Rexford, J., Ramakrishnan, K. K., True, F. D., & Merwe, J. (2000, May). Measurement and analysis of IP network usage and behavior. *IEEE Communications Magazine*, 38,144-151.
3. Campbell, K., Gordon, L.A., Loeb, M.P., and Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11 (2003), 431-448*.
4. Cao, L., Luo, C., Luo, D., & Zhang, C. (2004). Hybrid strategy of analysis and control of telecommunications frauds. *Proceedings of the 2nd international conference on information technology for application*, Harbin, China.
5. Casey, E. (2006). Investigating sophisticated security breaches. *Communications of the ACM, 49*(2), February 2006, 48-54.
6. Clifton, C., Doan, A., Elmagarid, A., Kantarcioglu, M., Schadow, G., Suciu, D., & Vaidya, J. (2004). Privacy-preserving data integration and sharing. *Proceedings of the 9th ACM SIGMOD workshop on research issues in data mining and knowledge discovery*, 19-26, Paris, France.
7. Clifton, C., Jiang, W., Muruguesan, M., & Nergiz, M. E. (2007). Is privacy still an issue for data mining?, *National science foundation symposium on next generation of data mining and cyber enabled discovery for innovation*, Baltimore, USA.
8. Cole, E., Krutz, R., & Conley, J. W. (2005). *Network security bible.* Indianapolis, IN: Wiley Publishing Inc.
9. Edwards, K.B. and Lumpkin, G. (2005). *Oracle white paper: Security and the data warehouse*. Redshores, CA: Oracle Corporation.
10. Galetsas, A. (2007). *Statistical data on network security*. European commission on information society and media directorate, Belgium Office.
11. Gallegos, F., Senft, S., Manson, D. P., & Gonzales, C. (2004). *Information technology control and audit (*2nd ed.). New York: Auerbach Publishing.
12. Helmer, G. G., Wong, J. S. K., Honavar, V., & Miller, L. (1998). Intelligent agents for intrusion detection, *Proceedings of Information Technology Conference*, 121-124, New York, USA.
13. Katic, N., Quirchmayr, G., Schiefer, J., Stolba, M., & Tjoa, A. M. (1998). A prototype model for data warehouse security based on metadata, *Proceedings of the 9th international workshop on database and expert systems applications*, 300, Washington DC, USA.
14. Kuhlmann, M., & Schimpf, G. (2003). Role mining: Revealing business roles for security administration using data mining technology, *Proceedings of the eighth ACM symposium on access control models and technologies*, 179-186, Como, Italy.
15. Lee, W., Stolfo, S. J., Chan, P. K., Eskin, E., Fan, W., Miller, M., Hershkop, S., & Zhang, J. (2001). Real time data mining-based intrusion detection, *Proceedings of DARPA information survivability conference and exposition II (DISCEX'01)*, Vol(1), 89-100, Anaheim, CA.
16. Lohmyer, D.F., McCrory, J., and Pogreb, S. (2002). Managing information security. *The McKinsey Quarterly 2002 Special Edition: Risk and Resilience*, 12-15.

17. Mitnick, K.D. and Simon, W.L. (2002). *The art of deception: Controlling the human element of security*. New York: John Wiley & Sons, Inc..
18. Neild, B. (2009). *$250K Microsoft bounty to catch worm creator*. Retrieved February 16, 2009, from CNN Web site: http://www.cnn.com/2009/TECH/ptech/02/13/virus.downadup/index.html.
19. Neohapsis. (2002). Aerospace workers arrested for hacking. Retrieved February 22, 2009 from http://archives.neohapsis.com/archives/isn/2002-q2/0291.html
20. Panko, R.R. (2004). *Corporate computer and network security*. Upper Saddle River, NJ: Pearson Education, Inc.
21. Price Waterhouse Coopers. (2008). Safeguarding the new currency of business: Findings from the 2008 global state of information security study. Retrieved from http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/Safeguarding_the_new_currency.pdf.
22. Priebe, T., & Pernul, G. (2000). Towards OLAP security design: Survey and research issues, *Proceedings of the 3rd ACM international workshop on data warehousing and OLAP*, 33-40, Virginia, USA.
23. Raguso, E. (2007). 3 arrested in circuit city theft operation customer credit used to steal more than $50K in electronics. Retrieved January 12, 2009 from http://www.modbee.com/local/story/66807.html.
24. Ranum, M.J. (1993). Thinking about firewalls, *Proceedings of second international conference on systems and network security and management (SANS-II)*, April, 1993.
25. Rosenthal, A. (2000). View security as the basis for data warehouse security, *Proceedings of the CAiSE international workshop on design and management of data warehouses (DMDW'2000)*, Stockholm, Sweden.
26. Samuelle, T. J. (2008). *Mike Meyers' certification passport: CompTIA Security+*. New York: McGraw Hill.
27. Shanbhaq, R. (2009). CA Issues Early Warning of Possible Waledac Trojan on Valentine's Day. Retrieved from February 19, 2009 from http://sip-trunking.tmcnet.com/topics/security/articles/50095-ca-issues-early-warning-possible-waledac-trojan-valentines.htm.
28. Simon, A. R. (1997). *Data warehousing for dummies*. Hoboken, NJ: Wiley Publishing Inc.
29. Skovira, R.J. (2004). Using informational landscape as a model to understand information use and design within organizations. *Issues of Information Systems*, *5*(1), 308-314.
30. Soper, D. S., Demirkan, H., & Goul M. (2007). An interorganizational knowledge-sharing security model with breach propagation detection. *Information Systems Frontier*, *9*(5), 469-479.
31. White, G., & Conklin, W. M. A. (2008). *All in one CompTIA security+ exam guide (2nd ed)*. New York: McGraw Hill.
32. Yin, J., Tang, C., Zhang, X., & McIntosh, M. (2007). On estimating the security risks of composite software services. International Business Machines (IBM). Retrieved from http://research.ihost.com/password/papers/Yin.pdf.
33. Zarsky, T. Z. (2003). "Mine your own business!": Making the case for the implications of data mining of personal information in the forum of public opinion. *Yale Journal of Law and Technology, 5*, 1-57.