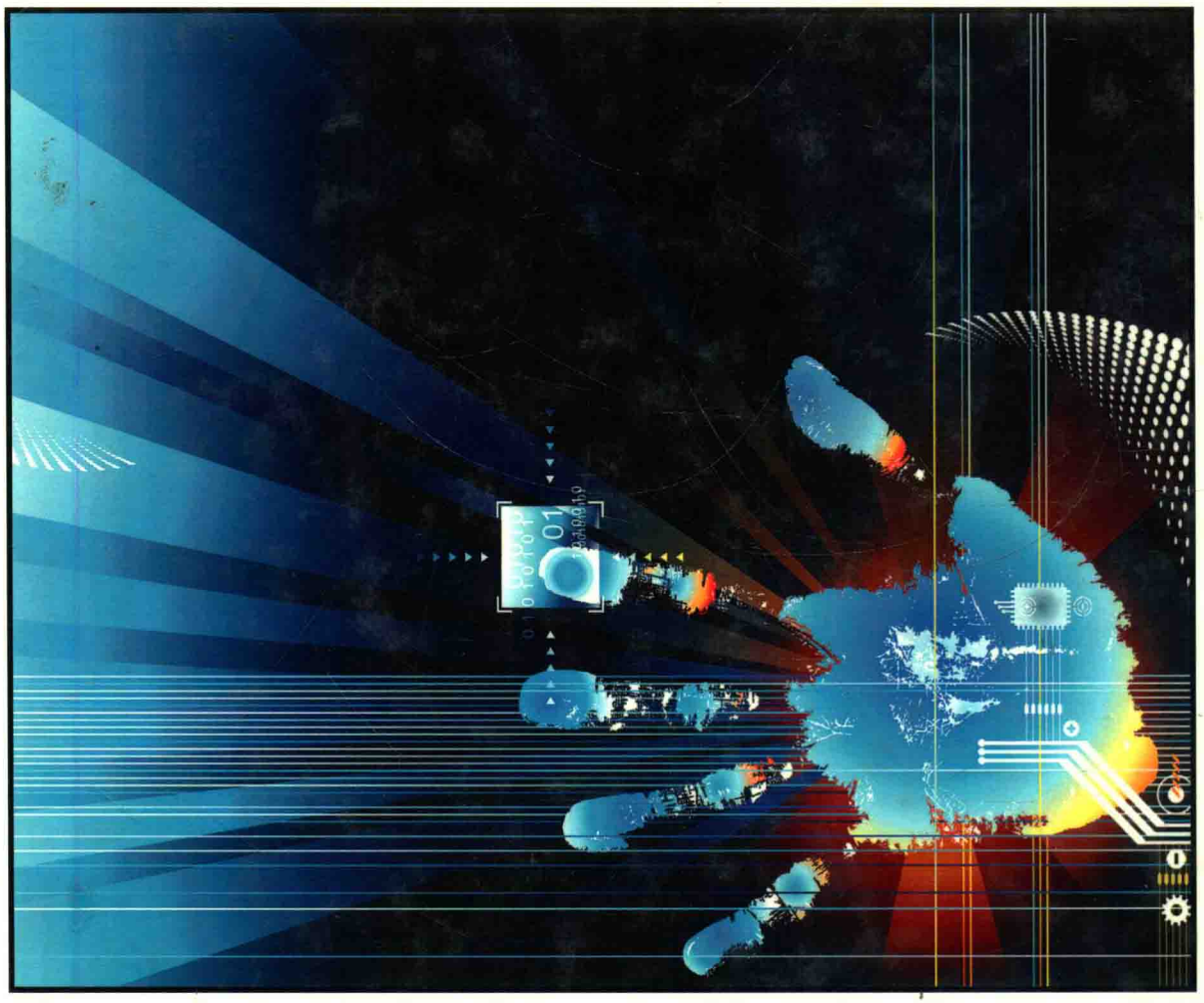
PREMIER REFERENCE SOURCE

Security and Privacy Assurance in Advancing Technologies

New Developments



Security and Privacy Assurance in Advancing Technologies:

New Developments

Hamid R. Nemati
The University of North Carolina, USA

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Book Publications: Julia Mosemann
Acquisitions Editor: Lindsay Johnston
Development Editor: Myla Harty
Publishing Assistant: Natalie Pronio
Typesetter: Natalie Pronio
Production Editor: Jamie Snavely
Cover Design: Lisa Tosheff

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Security and privacy assurance in advancing technologies : new developments / Hamid R. Nemati, editor.
p. cm.
Includes bibliographical references and index.
Summary: "This book provides a comprehensive collection of knowledge from experts within the field of information security and privacy and explores the changing roles of information technology and how this change will impact information security and privacy"--Provided by publisher.
ISBN 978-1-60960-200-0 (hardcover) -- ISBN 978-1-60960-202-4 (ebook) 1. Information technology--Security measures. 2. Management--Technological innovations. I. Nemati, Hamid R., 1958-
HD30.2.S437 2011
005.8--dc22

2010046637

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

This book is dedicated to my beloved parents. I love you guys.

Preface

It is unmistakably apparent that we in the midst of a "technological revolution" that has profound implications for all aspects of our lives. This revolution has transformed our lives in way unimaginable in less than a decade. We are able to communicate more freely and effortlessly with one another, make more informed decisions, and have a higher standard of living, all, resulting from advances in Information Technologies (IT). More people are employed generating, collecting, handling, processing and distributing information than any other profession and in any other time (Mason 1986). IT has made us more productive in our workplaces, has brought us closer, transformed our lives and has helped in redefining who we are as humans. Its impacts can be felt in the ways in which we relate, interact, and communicate not just with one another but also the way we interact with the technology itself. To some extent, information technologies have become "information appliances". Yet, we are only at the threshold of what is to come and many experts believe that we have only seen the tip of the iceberg. The dizzying pace of advances in information technology that characterize this revolution promises to transform our lives even more drastically than what we can conceive. Technology has redefined our relationships with businesses we interact with and governmental agencies representing us. Our world has been altered so irrevocably that we are no longer able to conduct our lives without it. But perhaps the most sweeping aspect of this revolution can be found in how we perceive and identify ourselves as individuals and eventually in how we will interact with one another. Consequently, we are on the verge of the biggest societal transformation in the history of mankind traced directly to advances in the information technology. This transformation will most likely create new opportunities and challenges we have yet to fathom. Information defines us. It defines the age we live in and the societies we inhibit. Information is the output of our human intellectual endeavors which inherently defines who we are as humans and how we conduct our lives. New technologies make possible what was not possible before. This alters our old value clusters whose hierarchies were determined by range of possibilities open to us at the time. By making available new options, new technologies can and will lead to a restructuring of the hierarchy of values (Mesthene, 1968). Mason (1986) claims that unique challenges facing our modern societies are the result of the evolving nature of information itself. This evolving nature of information requires us to rethink the way we interact with one another. Although this technological revolution has brought us closer and has made our lives easier and more productive, paradoxically, it has also made us more capable of harming one another and more vulnerable to be harmed by each other. Our vulnerabilities are the consequence of our capabilities. Mason argues that in this age of information, a new form of social contract is needed in order to deal with the potential threats to the information which defines us. Mason (1986) states "Our moral imperative is clear. We must insure that information technology, and the information it handles, are used to enhance the dignity of mankind. To achieve these goals we much formulate a new social contract, one that insures everyone the right to fulfill his or her own human

potential." (Mason, 1986, p 26). This new social contract has profound implications for the way our society views information and the technologies that support them. For technology to enhance the "human dignity", it should assist humans in exercising their intellects ethically. But is it possible to achieve this without assuring the trustworthiness of information and the integrity of the technologies we are using? Without security that guarantees the trustworthiness of information and the integrity of our technologies, ethical uses of the information cannot be realized. This implies that securing information and ensuring its privacy are inherently intertwined and should be viewed synergistically. In order for us to take full advantage of the possibilities offered by this new interconnectedness, organizations, governmental agencies, and individuals must find ways to address the associated security and privacy implications. As we move forward, new security and privacy challenges will likely to emerge. It is essential that we are prepared for these challenges in order to take full advantage of the opportunities. With the emergence of the new paradigm in information technology, the role of information security and privacy will evolve. Therefore, whilst advances in information technology have made it possible for generation, collection, storage, processing and transmission of data at a staggering rate from various sources by government, organizations and other groups for a variety of purposes, concerns over security of what is collected and the potential harm from personal privacy violations resulting from their unethical uses have also skyrocketed. Therefore, understanding of pertinent issues in information security and privacy vis-à-vis technical, theoretical, managerial and regulatory aspects of generation, collection, storage, processing, transmission and ultimately use of information have never been more important to researchers and industry practitioners alike. Understanding and studying salient issues of Information security and privacy is a complex and multifaceted undertaking. As a result, it has received considerable attention from researchers, developers and practitioners from a verity of different perspectives and backgrounds. Information security and privacy have been viewed as one of the foremost areas of concern and interest by academic researchers and industry practitioners from diverse fields such as engineering, computer science, information systems, psychology, sociology, the law and management. In this preface, we will consider how advances in information technologies have ushered an unprecedented explosion in data that define us and discuss why understanding of the security and privacy issues relating to this data is essential in any meaningful examination the role of technology in our lives. To achieve this, we will define information security and privacy and will discuss important defining issues currently dominating each. We will conclude by looking ahead in an attempt to seek clues as how this technological revolution will impact this field.

An Ocean of Data

A byproduct of pervasiveness of Information Technology in our daily lives is the amazingly large amount of data currently being generated. According to IBM, worldwide data volumes are currently doubling every two years (IDC, 2010). Data experts estimate that in 2002 the world generated 5 exabytes of data. This amount of data is more than all the words ever spoken by human beings. The rate of growth is just as staggering – the amount of data produced in 2002 was up 68% from just two years earlier. The size of the typical business database has grown a hundred-fold during the past five years as a result of internet commerce, ever-expanding computer systems and mandated recordkeeping by government regulations. The rate of growth in data has not slowed. International Data Corporation (IDC) estimates that the amount of data generated in 2009 was 1.2 million Petabytes (IDC, 2010). (A Petabyte is a million gigabytes.) (IDC Report, 2010). Although this seems to be an astonishingly large amount of data,

it is paled in compression to what IDC estimates that amount to be in 2020. IDC estimates that the amount of data generated in 2010 will 44 times as much as this year to an incomprehensible amount of 35 Zettabytes (A Zettabyte is 1 trillion gigabytes). IDC reports that by 2020, we will generate 35 trillion gigabytes of data. Moreover, that amount probably doubles every two years (Hardy, 2004). This astonishingly large growth in data, according a survey by US Department of Commerce, can be traced to the ever increasing number of Americans who are online on daily basis and are engaged in several activities, including engaging in online purchases and e-commerce, conducting banking online, learning, entertaining each other and being entertained by others and above all interacting socially. According the Neilson (Neilson 2010), Americans spend almost 25% of their time online on social networking sites and blogs, up 43 percent from one year earlier and they spend a third their online time (36 percent) communicating and networking across social networks, blogs, personal email and instant messaging (Lawson, 2010). A recent Neilson study (Nielson 2010) revealed that activities that generate larger and more private data are on the rise. Table 1 summarizes the findings.

Almost everything that we do in our daily lives can generate a digital footprint. Whether we are using credit cards, surfing the Internet or viewing a YouTube video, we are generating data. IDC senior vice president, John Gantz states: "About half of your digital footprint is related to your individual actions—taking pictures, sending e-mails, or making digital voice calls. The other half is what we call the 'digital shadow'—information about you—names in financial records, names on mailing lists, web surfing histories or images taken of you by security cameras in airports or urban centers. For the first time your digital shadow is larger than the digital information you actively create about yourself." Our digital shadow, the sum of all the digital information generated about us on a daily basis, now exceeds the amount of digital information we actively create ourselves (IDC, 2010). This digital footprint including

Table 1. Top 10 Sectors by share of U.S. Internet time

Top 10 Sectors by Share of U.S. Internet Time				
RANK	**Category**	**Share of Time June 2010**	**Share of Time June 2009**	**% Change in Share of Time**
1	Social Networks	22.7%	15.8%	43%
2	Online Games	10.2%	9.3%	10%
3	E-mail	8.3%	11.5%	-28%
4	Portals	4.4%	5.5%	-19%
5	Instant Messaging	4.0%	4.7%	-15%
6	Videos/Movies	3.9%	3.5%	12%
7	Search	3.5%	3.4%	1%
8	Software Manufacturers	3.3%	3.3%	0%
9	Multi-category Entertainment	2.8%	3.0%	-7%
10	Classifieds/Auctions	2.7%	2.7%	-2%
11	Other	34.3%	37.3%	-8%

Source (http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity/)

our digital shadow represents us, as humans, it represents who we are, and how we conduct our lives. It needs to be secured, protected, and managed appropriately.

The growth in Internet usage has offered businesses and governmental agencies the opportunity to collect and analyze information in ways never previously imagined. "Enormous amounts of consumer data have long been available through offline sources such as credit card transactions, phone orders, warranty cards, applications and a host of other traditional methods. What the digital revolution has done is increase the efficiency and effectiveness with which such information can be collected and put to use" (Adkinson, Eisenach, & Lenard, 2002).

The proclamation about data volume growth is no longer surprising, but continues to amaze even the experts. For businesses, more data isn't always better. Organizations must assess what data they need to collect and how to best leverage it. Collecting, storing and managing business data and associated databases can be costly, and expending scarce resources to acquire and manage extraneous data fuels inefficiency and hinders optimal performance. The generation and management of business data also loses much of its potential organizational value unless important conclusions can be extracted from it quickly enough to influence decision making while the business opportunity is still present. Managers must rapidly and thoroughly understand the factors driving their business in order to sustain a competitive advantage. Organizational speed and agility supported by fact-based decision making are critical to ensure that an organization remains at least one step ahead of its competitors. According to Kakalik and Wright (1997), a normal consumer is on more than 100 mailing lists and at least 50 databases. A survey of 10,000 Web users conducted by Georgia Institute of Technology concludes that "Privacy now overshadows censorship as the No. 1 most important issue facing the Internet" (Machlis 1997). A UCLA study released on February 2003, reported that 88.8% of the respondents said that they were somewhat or extremely concerned when purchasing online.

The gathering of data for data mining purposes was initially an attempt by companies to learn as much as possible about their customers so that they could provide customized or personable service and increase sales. The development and use of computer/data technology helped speed this process as it made the gathering and analyzing process easier. However, recent developments have caused the individual to lose control over that data about them. As technology advanced, the tools became more invasive, thorough and accuracy increased. It is possible that this data, available to anyone (individuals, businesses, governments) can be manipulated in such a way as to produce an in-depth profile of an individual or group.

Concerns have arisen regarding the use of data mining, as an individual has to interpret the results and data or knowledge gained can be taken out of context. For example, the US government utilizes some very powerful surveillance tools to gather data about its citizens. There are legitimate concerns regarding accuracy of data and privacy of the material these tools produce. The use of data mining technologies to make sense of this fata can provide limited and inaccurate results. What is the cost of a mistake? Is it a type one or type two error? What if you wrongly accuse an innocent person or allow a guilty person to go free? What percentage of accurate results is acceptable? Is an 85% accuracy rate good? If you are sending out a flyer or picking a stock then yes it is. If you are deciding if a person should be questioned and possibly detained by the police is that percentage still acceptable? What if you are one of the 15% wrongly accused? What are the implications? (Under the Patriot Act, if the accused is an immigrant they may be detained indefinitely). These are questions that must be seriously considered. The end-users of the technology must understand these concerns and the limitation of the technology they employ.

Information Security

Until recently, information security was exclusively discussed in terms of mitigating risks associated with data and the organizational and technical infrastructure that supported it. A common motivation for corporations to invest in information security is to safeguard their confidential data. This motivation is based on the erroneous view of information security as a risk mitigation activity rather than a strategic business enabler. No longer should information security be viewed solely as a measure to reduce risk to organizational information and electronic assets, it should be viewed as way the business needs to be conducted. To achieve success in information security goals, an organization's information security program should support the mission of the organization. Information security is concerned with the identification of an organization's electronic information assets and the development and implementation of tools, techniques, policies, standards, procedures and guidelines to ensure the confidentiality, integrity and availability of these assets. Although Information Security can be defined in a number of ways, the most salient definition is set forth by the U.S. government. The National Institute of Standards and Technology (NIST) defines Information Security based on the 44 United States Code Section 3542(b)(2), which states "Information Security is protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability." (NIST, 2003, p3). The Federal Information Security Management Act (FISMA, P.L. 107-296, Title X, 44 U.S.C. 3532) defines Information Security as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" and goes on to further define Information Security activities as those "carried out in order to identify and address the vulnerabilities of computer system, or computer network" (17 U.S.C. 1201(e), 1202(d)). The United States' National Information Assurance Training and Education Center (NIATEC) defines information security as "a system of administrative policies and procedures for identifying, controlling and protecting information against unauthorized access to or modification, whether in storage, processing or transit" (NIATEC, 2006). The overall goal of information security should be to enable an organization to meet all of its mission critical business objectives by implementing systems, policies and procedures to mitigate IT-related risks to the organization, its partners and customers (NIST, 2003). The Federal Information Processing Standards Publication 199 issued by the National Institute of Standards and Technology (NIST, 2004) defines three broad information security objectives: "Confidentiality", "Integrity" and "Availability". This trio of objectives sometimes is referred to as the "CIA Triad".

The Information Systems Security Association (ISSA) has been developing a set of Generally Accepted Information Security Principles (GAISP). GAISP include a number of information security practices, including the need for involvement of top management, the need for customized information security solutions, the need for periodic reassessment, the need for an evolving security strategy and the need for a privacy strategy. This implies that information security should be viewed as an integral part of the organizational strategic mission and therefore, requires a comprehensive and integrated approach. It should be viewed as an element of sound management in which cost-effectiveness is not the only driver of the project. Management should realize that information security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of security-related losses. Information security requires a comprehensive approach that extends throughout the entire information life cycle. The management needs to understand that without a physical security, information security would be impossible. As a result, it should take into considerations a variety of issues, both technical and managerial and from within and outside of the organization. The management needs to realize that

this comprehensive approach requires that the managerial, legal, organizational policies, operational, and technical controls work together synergistically. This requires that senior managers be actively involved in establishing information security governance.

Effective information security controls often depend upon the proper functioning of other controls, but responsibilities must be assigned and carried out by appropriate functional disciplines. These interdependencies often require a new understanding of the tradeoffs that may exist, which means achieving one may actually undermine another. The management must insist that information security responsibilities and accountability be made explicit and the system owners have responsibilities that may exist outside their own functional domains. An individual or work group should be designated to take the lead role in the information security as a broad organization wide process. This requires that security policies be established and documented, and the awareness among all employees be increased through employee training and other incentives. This requires that information security priorities be communicated to all stakeholders, including customers, and employees at all levels within the organization to ensure a successful implementation. The management should insist that information security activities be integrated into all management activities, including strategic planning, capital planning. Management should also insist that an assessment of needs and weaknesses should be initiated and security measures and policies should be monitored and evaluated continuously. Information security professionals are charged with protecting organizations against their information security vulnerabilities. Given the importance of securing information to an organization, this is an important position with considerable responsibility. It is the responsibility of information security professionals and management to create an environment where the technology is used in an ethical manner. Therefore, one cannot discuss information security without discussing the ethical issues fundamental in the development and use of the technology. According to a report by the European Commission (EC, 1999, p. 7) "Information Technologies can be and are being used for perpetrating and facilitating various criminal activities. In the hands of persons acting with bad faith, malice, or grave negligence, these technologies may become tools for activities that endanger or injure the life, property or dignity of individuals or damage the public interest." Information technology operates in a dynamic environment. Considerations of dynamic factors, such as advances in new technologies, the dynamic nature of the user, the information latency and value, systems' ownerships, the emergence of a new threat and new vulnerabilities, dynamics of external networks, changes in the environment, the changing regulatory landscape, should be viewed as important. Therefore the management should insist on an agile, comprehensive, integrated approach to information security.

Information is a critical asset that supports the mission of an organization. Protecting this asset is critical to survivability and longevity of any organization. Maintaining and improving information security is critical to the operations, reputation, and ultimately the success and longevity of any organization. However, information and the systems that support it are vulnerable to many threats that can inflict serious damage to an organization resulting in significant losses. The concerns over information security risks can originate from a number of different security threats. They can come from hacking and unauthorized attempts to access private information, fraud, sabotage, theft and other malicious acts or they can originate from more innocuous sources, but no less harmful, such as natural disasters or even user errors.

David Mackey, IBM's Director of security intelligence estimates that IBM recorded more than 1 billion suspicious computer security events in 2005. The damage from these "security events" can range from loss of integrity of the information to total physical destruction or corruption of entire infrastructure that support it. Damages can stem from the actions of a variety of sources, such as disgruntled employees defrauding a system, careless errors committed by trusted employees, to hackers gaining access to the

system from outside of the organization. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid negative publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system. Broadly speaking, the main purpose of information security is to protect an organization's valuable resources, such as information, hardware, and software. Any information security initiative aims to minimize risk by reducing or eliminating threats to vulnerable organizational information assets. The National Institute of Standards and Technology (NIST, 2003, p. 7) defines risk as "...a combination of: (i) the likelihood that a particular vulnerability in an agency information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability, and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on agency operations (including mission, functions, and public confidence in the agency), an agency's assets, or individuals (including privacy) should there be a threat exploitation of information system vulnerabilities,". "Risks are often characterized qualitatively as high, medium, or low" (NIST, 2003, p 8). The same publication defines threat as "...any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability," and vulnerability as "...a flaw or weakness in the design or implementation of an information system (including security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an agency's operations (including missions, functions, and public confidence in the agency), an agency's assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability" (NIST, 2003, 9). NetIQ (2004) discusses five different types of vulnerabilities that have direct impact on the governance of information security practices. They are: exposed user accounts or defaults, dangerous user behavior, configuration flaws, missing patches and dangerous or unnecessary service. An effective management of these vulnerabilities is critical for three basic reasons. First, an effective vulnerability management helps reducing the severity and growth of incidents. Second, it helps in regulatory compliance. And third and the most important reason can be summed by simply saying, it is a "good business practice" to be proactive in managing the vulnerabilities rather than be reactive by trying to control the damage from an incident.

The importance of securing our information infrastructure also applies to the government of the United States. The U.S. Department of Homeland Security (DHS) identifies a Critical Infrastructure (CI) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." According a recent report by the DHS titled The National Strategy for Homeland Security, which identified thirteen CI's, disruption in any component of a CI can have catastrophic economic, social and national security impacts. Information Security is identified as a major area of concern for the majority of the thirteen identified CI's. For example, many government and private-sector databases contain sensitive information which can include personally identifiable data such as medical records, financial information such as credit card numbers, and other sensitive proprietary business information or classified security-related data. Securing these databases, which form the back bone of a number of CI's, is of paramount importance.

Losses due to electronic theft of information and other forms of cybercrime against such databases can amount to tens of millions of dollars annually. In addition to specific costs can be incurred as the result of malicious activities such as identity theft as a result of data breaches (such as theft of hardware or system break ins, or virus attacks or denial of service attacks), one of the major consequences of

dealing with a security attacks is the decrease in customer and investor confidence in the company. This is an area of major concern for the management. According to an event-study analysis using market valuations to assess the impact of security breaches on the market value of breached firms, announcing a security breach is negatively associated with the market value of the announcing firm. The breached firms in the sample lost, on an average, 2.1 percent of their market value within two days of the announcement – an average loss in market capitalization of $1.65 billion per breach. The study suggests that the cost of poor security is very high for investors and bad for business. Financial consequences may range from fines levied by regulatory authorities to brand erosion. As a result, organizations are spending a larger portion of their IT budget in information security. A study by the Forrester Research Group estimated that in 2007 businesses across North America and Europe will spend almost 13% of their IT budgets on security related activities. The same report shows the share of security expenditure was around 7% in 2006.

It is obvious that information security is a priority for the management, as it should be. Regardless of the source, the impact on organization can be severe ranging from interruption in delivery of services and goods, loss of physical and other assets, loss of customer good will and confidence in the organization to disclosure of sensitive data. Such sensitive data breaches can be very costly to the organization. However, recent research shows that investing and upgrading information security infrastructure is a smart business practice. By doing so, an organization can reduce the frequency and severity of losses resulting from security breaches in computer systems and information technology infrastructure. Information Security is not just a technology issue. It encompasses all aspects of business from people to processes to technology. Bruce Schneier founder and editor of Schneier.com states that "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." Information Security involves consideration of many interrelated fundamental issues to consider. Among them are technological, developmental and design, and managerial considerations. The technology component of information security is perhaps the easiest to develop and implement. The technological component of information security and privacy is concerned with the development, acquisition, and implementation of hardware and software needed to achieve information security. The developmental and design component of information security deals with issues related techniques and methodologies used to proactively design and develop systems that are secure. The managerial and personnel component focuses on the complex issues of dealing with the human elements in information security and privacy. It deals with policies, procedures and assessments required for the management of the operation of security activities. Undoubtedly, this is the hardest part of the information security to achieve since it requires a clear commitment to security by an organization's leadership, assignment of appropriate roles and responsibilities, implementation of physical and personnel security measures to control and monitor access, training that is appropriate for the level of access and responsibility, and accountability.

Information Privacy

Privacy is defined as "the state of being free from unsanctioned intrusion" (Dictionary.com, 2010). Westin (Westin, 1967) defined the right to privacy as "the right of the individuals… to determine for themselves when, how, and to what extent information about them is communicated to others." The Fourth Amendment to the U.S. Constitution's Bill of Rights states that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not

be violated." This belief carries back through history in such expressions from England, at least circa 1603, "Every man's house is his castle." The Supreme Court has since ruled that "We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts." Thus, because the Amendment "protects people, not places," the requirement of actual physical trespass is dispensed with and electronic surveillance was made subject to the Amendment's requirements (Findlaw.com, 2010). Generally the definitions of privacy in regards to business are quite clear. On the Internet, however, privacy raises greater concerns as consumers realize how much information can be collected without their knowledge. Companies are facing an increasingly competitive business environment which forces them to collect vast amounts of customer data in order to customize their offerings. Eventually, as consumers become aware of these technologies, new privacy concerns will arise, and these concerns will gain a higher level of importance. The security of personal data and subsequent misuse or wrongful use without prior permission of an individual raise privacy concerns and often end up in questioning the intent behind collecting private information in the first place (Dhillon & Moores, 2001). Privacy information holds the key to power over an individual. When privacy information is held by organizations, which have collected the information without the knowledge or permission of the individual, the rights of the individual are at risk. By 1997, consumer privacy had become a prominent issue in the United States (Dyson, 1998). In practice, information privacy deals with an individual's ability to control and release personal information. The individual is in control of the release process: to whom information is released, how much information is released and for what purpose the information is to be used. "If a person considers the type and amount of information known about them to be inappropriate, then their perceived privacy is at risk" (Roddick & Wahlstrom, 2001). Consumers are likely to lose confidence in the online marketplace because of these privacy concerns. Businesses must understand consumers' concern about these issues and aim to build consumer trust. It is important to note that knowledge about data collection can have a negative influence on a customer's trust and confidence level in online businesses.

Privacy concerns are real and have profound and undeniable implications on people's attitude and behavior (Sullivan, 2002). The importance of preserving customers' privacy becomes evident when we study the following information: In its 1998 report, the World Trade Organization projected that worldwide Electronic Commerce would reach a staggering $220 billion. A year later, Wharton Forum on E-commerce revised that WTO projection down to $133 billion. What accounted for this unkept promise of phenomenal growth? Census Bureau, in its February 2004 report states that "Consumer privacy apprehensions continue to plague the Web and hinder its growth." In a report by Forrester Research, it is stated that privacy fears will hold back roughly $15 billion in e-commerce revenue. In May 2005, Jupiter Research reported that privacy and security concerns could cost online sellers almost $25 billion by 2006. Whether justifiable or not, consumers have concerns about their privacy and these concerns have been reflected in their behavior. The Chief Privacy Officer of Royal Bank of Canada said "Our research shows that 80% of our customers would walk away if we mishandled their personal information." Privacy considerations will become more and more important to customers interacting electronically with businesses. As a result, privacy will become an import business driver. People (Customers) feel "violated" when their privacy is invaded. They respond to it differently, despite the intensity of their feelings. Given this divergent and varied reaction to privacy violations, a lot of companies still do not appreciate the depth of consumer feelings and the need to revamp their information practices, as well as their infrastructure for dealing with privacy. Privacy is no longer about just staying within the letter of the latest law or regulation. Sweeping changes in attitudes of people regarding their privacy will fuel an intense political

debate and put once-routine business and corporate practices under the microscope. Two components of this revolution will concern businesses the most, rising consumer fears and a growing patchwork of regulations. Both are already underway. Regulatory complexity will grow as privacy concerns surface in scattered pieces of legislation. Companies need to respond quickly and comprehensively. They must recognize that privacy should be a core business issue. Privacy policies and procedures that cover all operations must be enacted. Privacy Preserving Identity Management should be viewed as a business issue, not a compliance issue.

Information Security and Privacy Issues

Information security and privacy will be everyone's business, not just IT's. This change in the way companies view and approach information security and privacy will be driven primarily due to consumer demand. Consumers will demand more security for information about them and will insist on better ethical uses of that information. This demand will drive business profitability measures and will ultimately manifest itself as pressure on the government and other regulatory agencies to pass tougher and more intrusive legislation and regulations, resulting in greater pressure on the business organizations to comply and to demonstrate a commitment to information security and privacy. Therefore to be successful, organizations need to focus on information security not just as an IT issue rather as a business imperative. They need to develop business processes that align business, IT and security operations. For example, information security considerations will play more of a prominent role while considering offshoring, collaborations and outsourcing agreements. In the same vein, business partners must prove that their processes, databases and networks are secure. This will also have an important implication for the outsourcing/offshoring agreements and collaborations. The need for more vigilant and improved policies and practices in monitoring insiders who may be leaking or stealing confidential information will become more apparent. The black hat will become the norm. Hacking will be increasingly become a criminal profession and will no longer be the domain of hobbyists. Attacks will be more targeted, organized and will have a criminal intent meant to steal information for profit.

Regulatory and compliance requirements will continue to plague organizations. Regulations and laws will have direct impact on IT implementations and practices. Management teams will be held accountable. Civil and criminal penalties may apply for non-compliance. Security audits will become more widespread as companies are forced to comply with new regulations and laws. The regulatory agencies and law enforcement will become more vigilant in enforcing existing laws such as HIPAA, Sarbanes-Oxley Act, etc.

Identity management will continue to be the sore spot of information security. The use of identity federations will increase. With advances in technology and the need for more secure and accurate identity management, biometrics will become mainstream and widely used. Additionally, the use of "federated identity management systems" will become more widespread. In a federated identity management environment, users will be able to link identity information between accounts without centrally storing personal information. The user can control when and how their accounts and attributes are linked and shared between domains and service providers, allowing for greater control over their personal data.

Advanced technical security measures, such as data-at-rest encryption, granular auditing, vulnerability assessment, and intrusion detection to protect private personally identifiable data will become more wide spread. Database security continues to be a major concern for developers, vendor and customers. Organizations demand more secure code and vendors and developers will try to accommodate

that demand. In addition to more secure code, the demand for an explicit focus on unified application security architecture will force vendors and developers to seek further interoperability. This is the direct result of increase in sophistication of malware. Malware will morph and become more sophisticated than ever. The new breed of malware will be able to take advantage of operating systems and browsers' vulnerabilities to infect end user computers with malicious codes for key logging that monitor and track end users' behaviors such as web surfing habits and other behaviors. Malware sophistication will include vulnerability assessment tools for scanning and penetrating corporate network defenses to look for weaknesses. Phishing will grow in frequency and sophistication and phishing techniques will morph and become more advanced. Phishing is defined as a method where private information such as social security numbers, usernames, and passwords are collected from users under false pretenses by criminals masquerading as legitimate organizations. Malicious websites that are intended to violate end users' privacy by intentionally modifying end users' configurations such as browser settings, bookmarks, homepage, and startup files without their consent will gain popularity among the hacker community. Sophisticated malware code can infect the users' computers simply by users visiting these sites. These infections can range from installing adware and spyware on a user's computers, installing dialers, keyloggers and Trojan horses on a user's machine. Keyloggers have the ability to be installed remotely by bypassing firewalls and email scanners and in most cases may not be detected by antivirus software. The most sophisticated keyloggers will be able to capture all keystrokes, screenshots, passwords encrypt them and send these information to remote sites undetected. Malicious code such as BOTs will be a growing problem for network administrators. BOT applications are used to capture users' computers and transform them into BOT networks (botnets). These BOT networks can then be used for illegal network uses such as SPAM relay, generic traffic proxies, Distributed Denial of Service (DDoS) attacks, and hosting phishing (and other malicious code) websites.

The proliferation of Internet use will accelerate. People, companies, governments will conduct more and more of their daily business on the Internet. Not only will the Internet be used for more, but it will also be used for more complex and previously unimagined purposes. This will be partly fueled by advances in the Internet technologies that will be more complex and far reaching. However, the pace of advances in security technology will be able to keep pace with the Internet's growth and complexity. As social computing networks such Peer-to-Peer, Instant Messaging, and Chat gain more popularity and continued adoption of these technologies, organizations will be exposed to new and more disruptive threats. These social computing networks will drain more and more of the corporate bandwidth and will require additional technologies to combat. For example, it was estimated that in 2007, Instant Messaging would surpass e-mails as the most dominate form of electronic communication. Yet, Instant Messaging is not regulated in most companies and is not subject to the same level of scrutiny as the e-mail systems are. Similarly, individuals are not as vigilant when using Instant Messaging tools. Therefore, these social computing technologies are fast becoming very popular with attackers. According to a recent study, the most popular malicious use of Instant Messaging is to send the user a link to a malicious, phishing or fraudulent website which then installs and runs a malicious application on the user's computer in order to steal confidential information.

There are serious concerns that current technology and technology being developed, will allow governments extraordinary ability to monitor their citizens. There is a legitimate concern that "Big Brother" has arrived. Proper oversight and usage is essential to limit abuses. Concerns about surveillance tools were abundant prior to 9/11, since then they have lessened with the understanding that the technology will be used for national security. However the new legislation increasing law enforcement

and governmental powers are not limited solely to terrorism. In our rush to protect ourselves we must be certain not to trample on individual rights in such a way that we regret it in the future. The balance between individual rights vs. national security should be carefully weighed. Those mining data obtained by business or governmental surveillance tools need to consider how the data is obtained, its accuracy and the limitations of the tools. They must be especially aware of the potential use of their analysis. Reliance on inaccurate results could have profound effects on individuals or our society as a whole.

Yet Another Security and Privacy Concern: Medical Data

Another area of concern is the growth in the use of information technology for medical purposes. Confidentiality is sacrosanct in any physician-patient relationship and rules governing this relationship going back millennia are meant to protect patient's privacy. Confidentiality, a major component of information security, is a significant mechanism by which a patient's right to privacy is maintained and respected. However, in the era of Electronic Medical Record (EMR), it is hard to achieve. Although the use of information technologies for medical purposes shows potential for substantial benefits, it is fraught with concern related to security and privacy. Since there are so many points along the EMR life cycle where security and or privacy of medical data can be compromised, wide spread use of EMR is not possible without a thorough understanding and resolution of such issues (Hunt, et. al, 1998; Johnston, et. al, 1994).

One of the most far reaching laws with privacy implication impacting electronic medical data research and practitioner communities is Health Insurance Portability and Accountability Act of 1996. It provides a standard for electronic health care transactions over the Internet. As the integrity and confidentiality of patient information is critical, this requires being able to uniquely identify and authenticate an individual. Health information is subject to HIPPA. The original legislation went into effect in 2001 and the final modifications took effect in April, 2003. A core aspect of HIPAA is to appropriately secure electronic medical records. The act applies to health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses. The Office for Civil Rights (OCR) is responsible for implementing and enforcing the HIPPA privacy regulation. HIPAA has strict guidelines on how healthcare organizations can manage private health information. This includes: Authentication: A unique identification for individuals using the health care system; Access control: Manage accounts and restrict access to health information; Password management: Centrally define and enforce a global password policy; Auditing: Centralize activity logs related to the access of health information. The act sets standards to protect privacy in regards to individuals' medical information. The act provides individuals access to their medical records, giving them more control over how their protected health information is used and disclosed, and providing a clear avenue of recourse if their medical privacy is compromised (Anonymous, 2006). Improper use or disclosure of protected health information has the potential for both criminal and civil sanctions. For example, fines up to $25,000 for multiple violations of a single privacy standard in a calendar year and the penalties for intentional or willful violations of the privacy rule are much more severe with fines up to $250,000 and/or imprisonment up to 10 years for knowing misuse of personal health data. There are more immediate risks of private lawsuits relying on the HIPAA standard of care. Security and privacy of electronic medical records constitute major regulatory compliance issues. Security must be in compliance with the "security rule" of the Health Insurance Portability and Accountability Act (HIPAA). There are five guiding principles of HIPPA's security rule: scalability, comprehensives, technological neutrality, and consideration of both external and internal security threats, and risk analysis (HIPPA, 2010). Scalability ensures that compliance with security does not depend on the size or scope of the medical entity and

requires that covered entities (CE), regardless of their size, must comply with rules. Comprehensiveness requires for a CE to develop a "comprehensive" approach to all aspects of electronic medical records' security. Neutrality of the technology provides flexibility to a CE in determining the most appropriate technology and the onus is on the CE to justify the technology that is used. The CE is required to protect its data from both internal and external security threats, to regularly conduct security risk analysis and to provide appropriate documentation. In addition, the security rule requires the CE to be in full compliance; partial compliance is not acceptable. There are a number of other key concepts to assure the security of medical records. One requirement is the establishment and formal documentation of security processes, policies, and procedures. Another is the "reasonableness" requirement. Reasonableness requires the CE to certify and document that reasonable measures have been taken to protect electronic medical records. Lastly, CEs must provide regular security training, awareness to its workforce and revise its security policies and procedures as needed. These compliance security challenges stem from the fact that patient data sets are large, complex, heterogeneous, hierarchical, time series, nontraditional, and originate from a verity of sources with differing levels of quality and format. Further, data sources may have incomplete, inaccurate and missing elements, some may be erroneous due to human and equipment error and lastly, the data may lack canonical consistencies within and between sources (Ciosa, et al, 2002). Patient data are voluminous and are collected from various sources including medical images, patient interviews, laboratory data, and the physicians' observations and interpretations of patients' symptoms, and behavior (Ciosa, et al, 2002). Securing such diverse and voluminous type of data housed on multiple heterogeneous systems with diverse data stewardship is not a trivial task and requires a whole set of different and difficult considerations. For example, medical data lack the underlying data structures needed for mathematically based data encryption techniques. Unlike data collected using other processes, medical data consists of word descriptions by physician and nurses, with very few formal constraints on the vocabulary, medical images, hand written charts and others. Additionally, medical data also lack a canonical form that encapsulates all equivalent forms of the same concept and is the preferred notation used in most encryption algorithms. For example, all the following are medically equivalent: Colon adenocarcinoma, metastatic to liver; Colonic adenocarcinoma, metastatic to liver; Large bowel adenocarcinoma, metastatic to liver. (Ciosa, et al, 2002). Lastly, medical data are time sensitive and may have been collected at different times using different data collection methodologies. As a result, they may reside on heterogeneous systems with differing representation and stewardship. Massive quantities of patient data are generated as patients undergo different medical and health care processes and procedures. As a result, these large patient databases may contain large quantity of useful information about patients and their medical conditions, possible diagnoses, prognosis and treatments. A major challenge in using these large patient databases is the ability to properly secure and anonyomize the data.

Another security and privacy issue deals with data mining of medical data. Careful and systematic mining of patient databases may reveal and lead to the discovery of useful trends, relationships and patterns that could significantly enhance the understanding of disease progression and management. This process is referred to as Data mining (DM). DM is an exciting new facet of decision support systems. Data mining derived from the disciplines of artificial intelligence and statistical analysis and covers a wide array of technologies. Using data mining, it is possible to go beyond the data explicitly stored in a database to find nontrivial relationships and information that would not have been discovered by way of standard analysis methods. Medical Data Mining (MDM) is data mining applied to patient data and has been shown to provide benefits in many areas of medical diagnosis, prognosis and treatment (Lavrac, 1999). By identifying patterns within the large patient databases, medical data mining can be used to