Proceedings of Informing Science & IT Education Conference (InSITE) 2011

Management in a Web 2.0 World: Risks and Counter-Measures

Nicole A. Buzzetto-More
University Maryland Eastern Shore, Princess Anne, MD, USA

nabuzzetto-more@umes.edu

Abstract

Use of personal computers, laptops, mainframes, servers, enterprise computing, electronic data interchange, enterprise-wide systems (e.g. ERP, CRM, SCM), databases, networks (intranet, VPN, internet), are essential resources that are crucial to business practices. Business processes are continuously evolving with the expansion and introduction of new technologies. Contemporary managers must understand the functions of information systems, security threats, and appropriate risk management techniques. Our next generation of management professionals will be/are digital natives, individuals raised in a technologically saturated world who are comfortable with computers, the Internet, and Web 2.0 technologies. This study examined the perceptions of digital natives who are pre or early-career managers with respect to information security risks, the form and frequency of employee misuse, and management responsibilities in risk avoidance and management. According to the participants, information theft is a serious concern to management; employees often misuse information systems; instances of information theft and fraud are common; and management should enforce acceptable use policies, police the internet for corporate identity misuse, monitor employee use of information systems, conduct information security audits, monitor social networking sites, and conduct frequent employee training sessions.

Keywords: employee misuse of information systems, risk management, acceptable use policies, employee monitoring, IT control, management issues

Literature Review

Information systems are crucial in contemporary business practices impacting virtually all aspects of operations and management needs to recognize that the information systems within an organization are a company's most valuable assets (Gawde, 2010). As such, management, accountants, auditors, and academicians must become more knowledgeable and conversant in the design, operation, and control of these systems, which are vulnerable to employee misuse and numerous internal and external threats (Bear & Wen, 2007). According to Gawde (2010, p. 1) "The misuse of Information Systems by employees poses serious challenges to organizations including loss of productivity, loss of revenue, legal liabilities and other workplace issues. Organizations need effective countermeasures to enforce its appropriate usage policies and minimize its losses & increase productivity." In time, the role of management will change to meet these pressures as the responsibility for establishing and maintaining a system of effective internal controls resides with management (Bear & Wen, 2007).

The traditional four functions of management include planning (developing a systematic and comprehensive strategy for reaching pre-determined goals), organizing (bringing together resources, grouping activities, assigning tasks, and delegating), staffing (recruiting, hiring, training, and rewarding talent), and controlling (setting standards and procedures, measuring performance, identifying risks, and initiating corrective or preventative action) (Fayol, 1917). Contemporary managers to plan for the continued use and future integration of technology into business processes, which should involve determining what technologies should, or should not, be incorporated into the organization. Managers need to organize and allocate technological resources as well as properly assign responsibilities and roles, which is enhanced by the staffing of competent individuals and the continued training of existing staffers. Finally, managers must develop an appropriate system of controls to minimize risk.

Information risk, according to Lemiux (2004, p.38) "encompass any threat to business arising from some inadequacy in an organization's records and information. These risks can be many and varied, ranging from those typically addressed by business continuity programs, damage to or loss of records and information arising from disasters or major system faults. In extreme cases, these risks can lead to heavy loss and even corporate failure." Risk avoidance and management can result in an improvement in organizational performance and overall confidence held by customers, employees, and/or stakeholders.

The Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) Computer Crime and Security Survey Report presents the results of a survey of information security and information technology professionals in United States across industries. The 2004 CSI/FBI Computer Crime and Security Survey found that 53% of respondents faced IS security incidents due to the actions of legitimate users, with estimated losses as high as $100,000 per incident and 59% of respondents detected insider abuse of network access (such as downloading pornography, pirating software, and inappropriate use of e-mail) within their organizations, totaling almost $11 million in losses. Further, the percentage of respondents reporting IS security incidents originating from within the organization rose from 37% in 1999 to 52% in 2004.

The 2010 CSI/FBI report was the most comprehensive survey to date representing data collected in 2009. According to the findings:

- Respondents reported significant increases in incidents of password sniffing, financial fraud, and malware infection.
- One-third of respondents' organizations were fraudulently represented as the sender of a phishing message.
- Average losses due to security incidents were up from the 2007 findings
- Most respondents reported that their organization's security awareness training was inadequate.
- Respondents said that regulatory compliance efforts have had a positive effect on their organization's security programs.
- When asked what information security solutions were the most important to their organization, most respondents cited tools that improve log management, security information and event management, security data visualization, security dashboards and the like.

The term Web 2.0 refers to Web-based applications that facilitate information sharing, interoperability, user generated content creation, and collaboration on the World Wide Web (Wikipedia, 2011). Examples of Web 2.0 activities include social networking sites, blogs, wikis, video sharing sites, hosted services, virtual communities and online gaming, mashups and folksonomies.

Following a survey that sampled managers at 1,300 UK companies (Condon, 2009), Websense Inc., found that 37% of respondents admitted that employees at their organization have tried to bypass IT security policies to access Web 2.0 sites. Further, only 43% have tools in place to prevent a company's confidential data from being uploaded onto the Web, and less than 36% have tools that provide real time analysis of website content. The report warned that companies fail to understand the threat posed by the loss of confidential information via social networking sites reporting that most companies are liberal in allowing the use of Webmail, and access to social networking and other Web 2.0 applications.

Employees are commonly engaged in a variety of Web 2.0 activities including online chats, social networking, gambling, shopping, surfing, and other non-business related activities. These activities result in a reduction of productivity, bandwidth drain, legal liabilities, and system vulnerability (Gawde, 2010). As a result, internet abuse is a major concern for contemporary managers forcing organizations to regulate employee internet usage (Young, 2010). Further, internet addiction is a recognized and serious disorder for which organizations may find themselves libel under the Americans with Disabilities Act (Young, 2010).

Gawde (2010) explains that it takes about 150 employees for a company to lose almost a million dollars annually in loss of productivity. Table 1 demonstrates how he estimates loss of productivity converted to actual financial losses suffered by typical organization.

Table 1: Estimated Losses	Number of Employees 200
Hourly pay $25	Number of Internet Abusing Employees 150
Employee Cost Daily Misuse(Hours) 1x$25=$25	Daily Loss Due to Misuse (Hours) $25x150= $3,750
Weekly Loss Per Employee 5x$25=$125	Weekly Loss All Employees 5x$3,750=$18,750
Annual Loss Per Employee 52x$125=$6500	Total Annual Loss 52x$18,750=$975,000
*Based on Gawde (2010)	

Most information systems are insecure because they are designed with user functionality in mind over security concerns (Gawde, 2010). Further, companies often underestimate internal threats posed by both malevolent and well-meaning employees. Overall, improper employee behaviors include: accidental and/or intentional virus download; unauthorized access to important data; security breaches due to a variety of activities including attaching wrong files, typing incorrect email addresses; weak passwords; information leaks; accessing/distributing/downloading pirated information, pornography, copyrighted material, personal information, or other sensitive data; illegal or illicit activities; sexual harassment, virtual harassment, cyber stalking, cyber bullying, and/or other forms of harassment; downloading malware, spyware, viruses or other potentially intrusive and damaging programs; and victimization through phishing scams and social engineering attacks.

Accountants, managers, IT professionals, and anyone working with financial information systems need to be knowledgeable about security threats and appropriate control techniques. Financial Information systems are particular important to protect with potentially severe economic impact on our financial markets and economy as resources are at risk of being embezzled, misappropriated, or diverted (Beard & Wen, 2007). Threats to financial/accounting systems come from a variety of sources. For example, during the data processing phase files can be accessed, deleted, lost, destroyed, altered, corrupted, misused, or stolen. The Sarbanes-Oxley Act of 2002 (SOX, 2002) assigns legal responsibilities to management by requiring reasonable assurance annually regarding the reliability of financial reporting. According to Section 404 of SOX, management is expected to establish, evaluate, monitor, and provide written assessments of internal controls, which include policies and procedures that pertain to the authorization and access, processing, handling, and storage of records and transactions and the detection and timely reporting of unauthorized access to information that can impact financial statements (Bear & Wen, 2007). SOX prohibits auditors from offering information system services to clients; however, SOX requires that all audits include an auditor attestation report relating to the internal control assessments made by management with a requirement that noncompliance be included.

In addition to SOX requirements, the New York Stock Exchange requires all listed companies to maintain an internal audit function that provides assessment of a company's risk management processes (Bear & Wen, 2007). The importance of information systems and risk management is being recognized across the accounting industry and is including on the Certified Public Accountant (CPA), Certified Internal Auditor (CIA), and Certified Management Accountant (CMA) exams. In addition, such certifications as the Certified Information Systems Auditor (CISA) and Certified Information Systems Security Professional (CISSP) indicate the need for certifications related to information technology, systems auditing, and systems security.

Do security policies work? Following a study of 474 employed professionals in the U.S., Darcy (2005) found that respondents considered security policies, security awareness education/training, computer monitoring, and preventative security software effective at deterring employee misuse of IS resources. At the same time, Darcy also found that only 35 percent indicated that they have security awareness programs in place and recommended that organizations should consider allocating a greater portion of their IS security budgets to the development of security policies and ongoing security awareness education and training efforts.

Most of our current management professionals are digital immigrants. The term digital immigrant was introduced by Mark Prensky in 2001. It refers to someone who was not raised in a digital environment but who has come to use and adopt many computer, internet, and World Wide Web usage (Prensky, 2001). On the other hand, a digital native is a person who was born during or after the proliferation of computers. Digital natives (also known as millenials) were born in or after the late 1970's and have been interacting with digital technologies from an early age, generally appreciate the value of technology, are quick to adopt new technologies, seek out opportunities for implementing technological change, and who are comfortable with social media and other Web 2.0 technologies. According to Palfrey and Gasser (2010) digital natives perceive the world differently with differing concepts of privacy, friendship, information ownership, communications, creativity, risk and threat, and productivity than previous generations. Our next generation of management professionals will be/are digital natives and the choices they make regarding the management of IT will likely radically depart from our current standards of practice.

In order to assist business leaders grappling with questions about generational diversity and its impact, the Ethics Resource Center (ERC) mined National Business Ethics Survey to compare the perceptions of baby boomers, gen-xers, and millenials (2010). According to the survey millennials are the most likely to observe misconduct. At the same time, millennial employees are less likely to observe employee privacy breaches than their elder coworkers and more likely to find it acceptable to keep copies of confidential documents, which the ERC explains they can attribute to the differing concept of privacy expressed by digital natives. Millennial employees are more likely to find it acceptable to blog or tweet negatively about their company, but more likely to observe discrimination in the workplace. Finally, the study found that "unlike managers in other age groups and contrary to historical trends, millennial supervisors and managers have more views of their company's ethical culture" (ERC, 2010, p. 12).

In another study, Myers and Sadaghiani (2010) found that the digital generation are especially likely to use incorporate Web 2.0 technologies into the workplace as a means to collaborate as well as interact with organizational members, customers, and suppliers. Further, millenials will lead the use of communicative technologies both intra-organizationally as well as for strategic advantage of organizations. Finally, the authors suggest that digital natives may be the first to notice the potential pitfalls posed by different technologies.

Background

While a number of studies that focus on the opinions of existing management with respect to information technology risks have been, and continue to be, conducted each year (CSI/FBI, 2010; Condon, 2009; Darcy, 2005); the perceptions of management students, and early career professionals is rarely explored. The current generation of management students and early career professionals are digital natives. As explained by Palfrey and Gasser (2010, p. 1), as digital natives come of age "Our economy, our politics, our culture and even the shape of our family life will be forever transformed." They also explain that "Digital Natives will move markets and transform industries, education, and global politics. The changes they bring about as they move into the workforce could have an immensely positive effect on the world we live in" (Palfrey & Gasser, 2010, p. 3).

There several crucial fields such as enterprise computing that are posed to see a huge exodus in the form of retirements over the next 10 years. Digital natives will be filling the gap left by this exodus in the near future. To neglect the perceptions of digital natives from the research is to leave a huge gap in the literature. The study presented in this paper focused on digital natives by examining the perceptions of graduating management students as well as students and recent college graduates enrolled in a enterprise computing management academic and professional program offered in conjunction with IBM Corporation. Within a few short years of this paper being published, many of the participants in this study will be making crucial decisions regarding IT management. This paper provides a snapshot of the opinions of this group with respect to information security risks and management responsibilities in risk avoidance and management.

Methodology

An online questionnaire was developed and distributed to individuals enrolled in an information systems course at a U.S. Mid-Atlantic minority-serving university in the Spring of 2010. A survey was designed and distributed via the online survey tool, Zoomerang. The survey was comprised of a combination of Likert scaled measurement of agreement, dichotomous multiple choice, ranking scaled, and short response questions. There were 319 email invites sent, 145 surveys were taken, and 127 completed and usable surveys were analyzed. The data was analyzed based on descriptive statistics and frequency distribution and the following research questions were explored:

1) Do digital natives perceive there to be significant risks to a company's information systems,

2) Do digital natives believe that behaviors that threaten a company due to the misuse or infringement upon information systems are common?

3) Do digital natives perceive risks differently than contemporary managers?, and

4) Do digital natives support the implementation of counter measures designed to minimize information security threats?

Discussion

Population

Exactly, 60% of the respondents were female while 40% were male. Approximately, 23% of respondents were between the ages of 18-20, 45% were between the ages of 21-24, 14% were between the ages of 25-34, and 18% were over age 35.

Perceived Risks

Participants were asked to respond to the statement "I believe that employees often misuse corporate information" with 64% of respondents saying they agree/strongly agree, 28% reporting neutral/undecided, and 9% in disagreement. The results are depicted in Table 2 and are stronger than what has been reported in the literature which has found that existing management professionals often underestimate both the instances and risks of employee misuse of corporate information systems (Young, 2010; Gawde, 2010) and are consistent with what was reported by the ERC (2010) which found that millenials are more likely to observe employee misconduct.

Table 2: Response to the Statement
"I believe that employees often misuse corporate information systems."

1 Strongly Disagree	1	1%		
2 Disagree	10	8%		
3 Neutral/Undecided	35	28%		
4 Agree	69	55%		
5 Strongly Agree	12	9%		
Total	127	100%		
Mean	**Mode**	**Range**	**Standard Deviation**	**Confidence Interval @ 95%**
3.63	4	4	0.79	[3.49 - 3.76]

The CSI/FBI consistently reports (2004, 2010) the growing frequency of information theft and that the threat of information theft is often unrecognized by contemporary managers (Condon, 2009). As such, respondents in this study were asked to state their agreement to the statement "Information theft is a very real concern in corporate America." A significant majority of respondents (91%) either said they agreed or strongly agreed, 6% were neutral or undecided, and 3% disagreed or strongly disagreed. These results are depicted in Table 3 and indicate that digital natives may be more aware of the information theft threat.

Table 3: Response to the statement
"Information theft is a very real concern in corporate America."

1	Strongly Disagree	2	2%
2	Disagree	1	1%
3	Neutral/Undecided	8	6%
4	Agree	59	47%
5	Strongly Agree	56	44%
Total		126	100%

Mean	Mode	Range	Standard Deviation	Confidence Interval @ 95%
4.32	4	4	0.77	[4.18 - 4.45]

Universally, respondents agreed (99% reporting yes and 1% no) that it is important for an organization to carefully secure their information systems from intrusion; however, perceived risk was not universal. When asked to respond to the statement "management information systems are often vulnerable to attack" 60% or respondents either agreed or strongly agreed, 37% were neutral or undecided, and 3% said that they disagreed or strongly disagreed. The results are depicted in Table 4 and are reminiscent of what was reported by Gawde (2010) who also claimed that companies often underestimate the risk of outright attack.

Table 4: Responses to the statement
"Management information systems are often vulnerable to attack"

1	Strongly Disagree	1	1%
2	Disagree	3	2%
3	Neutral/Undecided	46	37%
4	Agree	58	46%
5	Strongly Agree	18	14%
Total		126	100%

Mean	Mode	Range	Standard Deviation	Confidence Interval @ 95%
3.71	4	4	0.77	[3.57 - 3.84]

Web 2.0 sites such as blogs, wikis, and social networking poses a number of risks to contemporary organizations. Further, the risks posed by Web 2.0 sites (in particular social networking sites) often go under-recognized by managers (Salter & Brydon, 2009). Participants were asked to respond to the statement "There is a lot of unethical activity on social networking sites like Facebook." Contrary to what has been reported in the literature, the respondents included in this study recognized the prevalence of unethical activity on the World's largest social networking site with 71% of respondents reporting agreement. The results are shown in Table 5.

Table 5: responses to the statement "There is a lot of unethical activity on social networking sites like Facebook."

1	Strongly Disagree	0	0%
2	Disagree	5	4%
3	Neutral/Undecided	30	25%
4	Agree	47	39%
5	Strongly Agree	39	32%
Total		121	100%

Mean	Mode	Range	Standard Deviation	Confidence Interval @ 95%
3.99	4	3	0.86	[3.84 - 4.15]

The questions examined in Tables 2-5 were considered with respect to the research question 1 do digital natives perceive there to be significant risks to a company's information systems. Based on the responses given by the participants included in this study one can conclude that the participants do perceive there to be significant risks that threaten a company's information systems. When compared to what has been reported in the literature, the responses were considered with respect to research question 3 do digital natives perceive risks differently than contemporary managers? According to the findings, the responses given by the participants indicated that there is a greater perception of risks that threaten a company's information systems among digital natives.

A series of illicit or risky activities was listed and respondents were asked to report their perceived frequency of these activities based on a four point scale where one equaled very rare and four equaled very often. The results are represented in Table 6, which is sorted based on mean. According to the findings, all of the activities listed are common; however, the most common activities are employees spending time on the internet and/or social networking sites when they should be working, internet/email fraud, phishing scams, internet abuse, abuse of company systems by employees, and the use of technology to steal of misappropriate assets. These findings indicate that the digital natives participating in this study are very aware of the risks that may threaten an organization. Based on what has been reported in the literature, and considered in respect to research question 3, the findings suggest that digital natives are more aware of the specific illicit activities that threaten an organization than earlier generations.

Table 6: Respondents Perception of Commonality of Occurrences

	Mean based on 4pt scale	**Mode**	**Standard Deviation**	**Confidence Interval @ 95%**
Employees spending time on Facebook/the internet when they should be working	3.50	4	0.65	[3.38 - 3.62]
Internet/Email fraud	3.45	4	0.64	[3.34 - 3.57]
Phishing scams	3.27	4	0.8	[3.12 - 3.41]
Email or Internet abuse	3.27	3	0.63	[3.16 - 3.38]
Abuse of company systems by employees	3.11	3	0.63	[3.00 - 3.23]
Use of technology to steal or misappropriate assets	3.03	3	0.69	[2.90 - 3.15]
Ignoring unusual activities occurring on one's information systems	2.98	3	0.62	[2.87 - 3.10]
Use of technology to falsify documents/contracts/invoices etc	2.98	3	0.71	[2.85 - 3.11]
Employees divulging private company info on social networking sites	2.92	3	0.75	[2.79 - 3.06]
Corporate Identity theft (fraudulent use of a company’s identity by another organization/person)	2.88	3	0.71	[2.75 - 3.01]
Abusive behavior over a company's email system	2.83	3	0.75	[2.70 - 2.97]
Employee privacy breach	2.81	3	0.72	[2.68 - 2.94]

Importance of IT Management Education

Students studying management and/or computer science often leave college without coursework or practical experience in the management of information systems and companies frequently fail to provide adequate training that builds the IT security and risk management skills of up in coming managers (Burgess and Mcgrath, 2010). In response to this short fall, a question was included in the survey that asked respondents to comment on the importance of information system management, control, and compliance related education included within higher education management programs with 91% of participants responding that they agreed or strongly agreed that “It is important that students majoring in business receive coursework in IT; information management; risk avoidance; and system security, control and compliance.” The results are presented in Table 7. Additionally, students were asked to respond to a dichotomous yes/no question regarding the marketability of information systems management courses for business graduates. According to the findings, 96% of participants said “yes” when asked “Do you think that taking information systems courses makes a business graduate/student more marketable to potential employers”.

Table 7: Response to the statement
"It is important that students majoring in business receive coursework in IT; information management; risk avoidance; and system security, control and compliance."

1 Strongly Disagree	2	2%		
2 Disagree	1	1%		
3 Neutral/Undecided	7	6%		
4 Agree	61	47%		
5 Strongly Agree	55	44%		
Total	126	100%		
Mean	**Mode**	**Range**	**Standard Deviation**	**Confidence Interval @ 95%**
4.33	4	4	0.76	[4.18 - 4.45]

Control and Counter-Measures

Employee information and technology management programs often include assessment of misuse tendencies during the hiring process, implementation of acceptable use policies, utilization of network filters and other computer security programs, training programs, and dismissal procedures (Young, 2010). The participants in this study were asked to respond to a question that listed a series of activities in which an organization might become engaged and to comment on their perception as to whether management should, or should not, engage in these activities using a five point Likert scale. The findings were considered with respect to research question 4 do digital natives support the implementation of counter measures designed to minimize information security threats. The descriptive statistics are reported in Table 8. The table presents the information sorted based on the mean and indicates that the respondents support the implementation of counter measures designed to minimize information security threats. In particular, the participants were most in agreement that management should enforce a company's acceptable use policy, conduct frequent training sessions, run security audits, police the internet for misuse of their company's image, and monitor employee usage of information systems. These findings are in agreement with the literature (Darcy, 2005; Condon, 2009; CSI/FBI, 2010; Young, 2010; and Bear and Wen, 2010) which have found that risk avoidance training, auditing, threat awareness and other preventative measures are effective at minimizing information security risks.

Table8: Responses to question on management engagement in activities

Management should	Mean	Mode	Standard Deviation	Confidence Interval @ 95%
Enforce a company's technology acceptable use policy	3.44	4	0.6	[3.33 - 3.55]
Conduct frequent training sessions on the acceptable handing of company information	3.35	3	0.59	[3.24 - 3.45]
Conduct technology security audits	3.34	3	0.62	[3.22 - 3.45]
Police the internet for the misappropriation of their corporate identity	3.29	3	0.6	[3.18 - 3.40]
Monitor employee usage of information systems	3.23	3	0.61	[3.11 - 3.34]
Monitor employee use of social networking sites like Facebook	2.89	3	0.75	[2.76 - 3.03]
Monitor social networking sites	2.83	3	0.78	[2.69 - 2.97]
Ban employees from using social networking sites like Facebook while at work	2.81	3	0.76	[2.66 - 2.94]

Limitations

The most significant limitations of this study are the size and limited geographic location of the sample. Additionally, the study did not include a population of working managers so that comparisons can be made across populations. The author hopes to remedy the limitations of this study through expanded research in this area.

Concluding Thoughts and Future Work

Technology has, and continues to alter business practices resulting in the need for new management techniques. New and upcoming managers must understand how emerging technologies can help an organization achieve its goals, recognize the functions of information systems, plan for the use of existing and new technologies, identify threats, and develop and implement appropriate risk management techniques. Digital natives have, and our continuing to, join the workforce and represent the future of management. They are posed to reshape the workforce as well as redefine the way companies do business. This study discussed in this paper examined the perceptions of digital natives with respect to information security risks, the form and frequency of employee misuse, and management responsibilities in risk management. According to the findings, the participants perceived there to be significant risks to company’s information systems and the perception of these risks is similar to what has been reported in studies that have focused on current or late career managers. The findings also suggest that digital natives are aware of the specific illicit activities that threaten an organization and that this awareness is greater than that of their mid-late career management counterparts. Finally, the participants support the introduction of countermeasures designed to minimize risk such as management enforcement of acceptable use policies, policing the internet for corporate identity misuse, monitoring employee use of information systems, conducting information security audits, monitoring social networking sites, and conducting frequent employee training sessions. While this study should be replicated and a wider net cast, the preliminary findings presented suggest that the next generation of management is well prepared to recognize the risks of a Web 2.0 world. Further, and complemented by proper academic preparation, these digital natives will support the implementation of risk avoidance and recognition programs. This line of research will continue to remain relevant as new technologies emerge and new risks develop. This study is currently being expanded to include mid and late career managers as well as to encompass a wider geographic region.

References

Beard, D., & Wen, J. (2007). Reducing the threat levels for accounting information systems: Challenges for management, accountants, auditors, and academicians. *CPA Journal, 77*(5), 34-42.

Burgess, S., & McGrath, G. (2010). Using research techniques to teach management of it concepts to postgraduate business students. *Interdisciplinary Journal of Information and Knowledge Management, 5* 49-59. Retrieved from http://ijikm.org/Volume5/IJIKMv5p049-059Burgess449.pdf

Computer Security Institute. (2010). *CSI computer crime and security survey 2009/2010*. Retrieved 1/10/2010 from http://gocsi.com/survey

Condon, R. (2009). *Companies underestimate Web 2.0, social networking threat, says survey*. Search Security. Retrieved 10/10/10 from http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1359009,00.html

D'Arcy, J. (2005). *Improving information systems security through procedural and technical countermeasures.* Retrieved 1/10/2010 from http://ibit.temple.edu/research/researchreports/issecuritymeasures.pdf

Davinson, N., & Silence, E. (2010). It won't happen to me: Promoting secure behavior among internet users. *Computers in Human Behavior, 26*(6), 1739-1747.

Ethics Resource Center. (2010). *Millennials, Gen X and Baby Boomers: Who's working at your company and what do they think about ethics?* Supplemental Research Brief. Retrieved 2/28/2011 from: http://ethics.org/files/u5/Gen-Diff.pdf

Fayol, H. (1917). *Administration industrielle et générale; prévoyance, organisation, commandement, coordination, controle.* Paris, H. Dunod et E. Pinat, OCLC 40224931

Gawde, V. (2010). *Information systems misuse -Threats & countermeasures.* Retrieved 8/10/2010 from http://infosecwriters.com/text_resources/pdf/information_systems_misuse.pdf

Hearta, T., Maoza, H., & Plinskina, N. (2010). From governance to adaptability: The mediating effect of it executives' managerial capabilities. *Information Systems Management, 27*(1), 42 – 60.

Lemieux, V. (2004). Two approaches to managing information risks. *Information Management Journal, 38*(5), 56-62.

Myers, K., & Sadaghiani, K. (2010). Millenials in the workplace: A communication perspective on millenial's organizational relationships and performance. *Journal of Business Psychology, 25*(2), 225-238.

Palfrey, J., & Gasser, P. (2010). *Born digital*. Retrieved 1/30/11 from: http://borndigitalbook.com/excerpt.php

Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon, 9*(5), 1-6.

Salter, M., & Bryden, C.(2009). I can see you: Harassment and stalking on the Internet*.* *Information & Communications Technology Law, 18*(2), 99-122.

Spears, J., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503-A5

Young, K. (2010). Killer surf issues: Crafting an organizational model to combat employee internet abuse. *Information Management*, 449*(1)*, 34-38.

Biography

Dr. Nicole A. Buzzetto-More is an Associate Professor, Program Coordinator, and the Assurance of Learning and Assessment Chair in the Department of Business at the University of Maryland Eastern Shore. She is also Director of the Maryland State Department of Education Program Affiliate for Business, Management, and Finance. She received doctorate and masters degrees Columbia University and earned a post doctorate from Tulane University. She also earned a masters from the College of New Rochelle and a bachelors from Marist College. Dr. Buzzetto-More is a frequent invited presenter at conferences across the globe; is on the editorial board of several journals; has authored numerous publications; and has been recognized with awards from the American Distance Education Consortium, Global Digital Business Association, InSITE, and the Informing Science Institute. Recently, she was named a Fellow of the Informing Science Institute. She published two books in 2007, Principles of Effective Online Teaching and Advanced Principles of Effective ELearning. In 2010 her third book The E-Portfolio Paradigm: Informing, Educating, Assessing, and Managing with E-Portfolios was published by the Informing Science Press.