

Regis University

ePublications at Regis University

Regis University Student Publications
(comprehensive collection)

Regis University Student Publications

Summer 2011

Computer Security Policy: Preventing Vulnerabilities and the Impact of Selective Enforcement On an Organization

LaTrice D. Parker-Stewart
Regis University

Follow this and additional works at: <https://epublications.regis.edu/theses>



Part of the [Computer Sciences Commons](#)

Recommended Citation

Parker-Stewart, LaTrice D., "Computer Security Policy: Preventing Vulnerabilities and the Impact of Selective Enforcement On an Organization" (2011). *Regis University Student Publications (comprehensive collection)*. 480.

<https://epublications.regis.edu/theses/480>

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

**COMPUTER SECURITY POLICY: PREVENTING VULNERABILITIES AND THE
IMPACT OF SELECTIVE ENFORCEMENT ON AN ORGANIZATION**

A THESIS

SUBMITTED ON THE 23RD OF JULY, 2011

TO THE DEPARTMENT OF INFORMATION TECHNOLOGY
OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES
OF REGIS UNIVERSITY

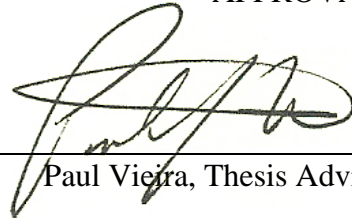
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN
INFORMATION ASSURANCE

BY

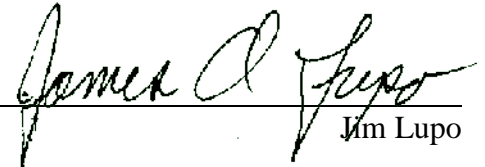


LaTrice D. Parker-Stewart

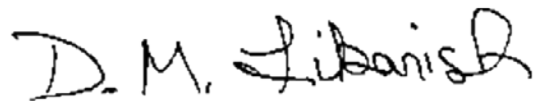
APPROVALS



Paul Vieira, Thesis Advisor



Jim Lupo



Daniel Likarish

Abstract

This project focuses on the importance of a computer security policy as a whole. It also looks at how security policies assist in preventing vulnerabilities that may be instigated by employees. Moreover, the project views how the concept of selective enforcement can affect and impact an organization. This project delves into actual cases of employee misconduct in various organizations. It explains how policies were violated and the repercussions of these various misdeeds. Finally the project discusses different items that a good security policy should have and how important it is for policies to be enforced. It is vital that an organization inform its employees of what is appropriate and who is responsible for the use of technology in the workplace. This project finds that the protection of a company's and an employee's privacy is important and what most individuals are concerned with. The exploitation of an employee's trust and ignorance is what a policy can prevent.

Acknowledgements

First I would like to thank my thesis advisor, Mr. Paul Vieira, for his support and outstanding guidance and leadership. He gave me the push I needed to keep going with this program. I would like to thank the staff and my other professors at Regis University who provided a great learning environment, and imparted their knowledge to me.

I would also like to thank my family, who helped me grow and let me complete this project and program. Last but not least, I would like to thank my husband, Jason, who always believed in me and has been my rock, my editor, and my cheerleader from the very beginning. I could not have done this without you.

Table of Contents

Abstract.....	ii
Acknowledgements.....	iii
Table of Contents.....	iv
List of Figures.....	v
Chapter 1-Introduction.....	1
Chapter 2-Review of Literature.....	3
Chapter 3-Methodology.....	12
Chapter 4-Analysis/Results.....	14
Chapter 5-Conclusion.....	29
Reference.....	31

List of Figures

Figure 1- List of available types of software employers may use to monitor their employees	Page 5
Figure 2-A framework for insider threats	Page 10
Figure 3-McGraw-Hill Companies Code of Ethics for CEO and SFOs	Page 17
Figure 4-McGraw-Hill Companies Code of Ethics continued	Page 18
Figure 5-Steps in the development of a security policy	Page 22
Figure 6- West Virginia's DHHS Computer Use Policy	Page 24
Figure 7-West Virginia's DHHS Enforcement Authority	Page 25
Figure 8-West Virginia's DHHS Violation Policy	Page 25

Chapter 1 – Introduction

Organizations utilize security policies to “inform all users of the goals of and constraints on using a system” (C. Pfleeger & S. Pfleeger, 2007 p. 547). In most organizations there are telecommunication, organizational, and security policies that govern specific actions day to day. The potential for policies to be ignored or forgotten is a problem that any company can face with regards to its employees. So how does one ensure that employees are consistently following the policy, that employers are constantly enforcing the policy, and that there is education being provided that teaches employees about vulnerabilities that may occur when policy is disregarded? There must be an enforceable policy in place. Whitman, Townsend, and Aalberts (1999) surmise that “the overall premise for having a policy is to provide a common basis of understanding of exactly what the employee can and cannot use the technology for” (p. 104). If employees do not know what they are allowed or forbidden to do, then there is no recourse of action if they fail to follow assumed guidelines and damage company assets via an attack.

This project examines factors that make a good security policy and how organizations can be affected by ignoring their policy. It also briefly explores how vulnerable an organization is when policy is not employed. Plus this project looks at selective enforcement and how dangerously unethical and unreasonable it is for an organization that has policies in place. For example, if employees of an organization are knowingly violating its security policy, what happens if there are no consequences – or inconsistent consequences – for these violations? Question further: If the individuals breaking the policy are the managers, what happens? Do they receive the same reprimand as an employee that is not a manager? Selective enforcement divides a company more than it already may be. There is always a clear division between executives, managers, and a standard employee. It is more pronounced when an employee gets

into trouble for breaking policy and their manager, who does the same thing, does not.

Moreover, it is evident when a manager gets penalized for something one of their underlings has done. Chapter 4 addresses these issues in detail.

Chapter 2 – Review of Literature and Research

The following chapter is a discussion regarding the review of relevant literature acquired from scholarly journals accessed from research databases and from general Internet research. First it provides a general overview of IT computer security policy; followed by a discussion regarding the importance of security policy, and then a small review of selective enforcement, due to the lack of an abundant amount of literature found that dealt with law enforcement and not computer security. Lastly this section explores the influence of a security policy on insider threats.

There are many reasons for an organization to have a computer security policy. An organization develops security policies to aid them in keeping their trade secrets safe and to keep vulnerabilities at bay. Security policies also protect computer equipment from being ravaged by viruses, by informing employees what is acceptable use of the company's belongings. Aalberts, Townsend, and Whitman (1999), authors of *Considerations for an Effective Telecommunications-Use Policy*, feel that a sound security policy "codifies system controls and reporting authorities... reinforces the organization's expectations about how systems should be used... and it serves to indemnify the organization against liability for an employee's inappropriate or illegal system use". (p.101) They further assert that a published policy "serves a legally binding agreement between parties...and shows that the organization has made a good faith effort to ensure that its telecommunication systems are not used in an illegal manner". (p.102)

The importance of this study is to show the significance of having a telecommunications and information technology (IT) security policy that directs and outlines proper technology usage and that it is vital companies enforce it. "Any information security policy should address

systems security, product security, community security and corporate information security.”

(Aalberts, Townsend, & Whitman, 1999, p. 102) The use of computers and telecommunication equipment in organizations has been a necessity; however, the expansion of our telecommunication dependency has gone global and the method (Internet, virtual private networks [VPN], or cellular) has become vital. Now with companies being exposed to the same medium that anyone with a computer has access to, it is critical to keep all organizational information safe. A good security policy is one that affects the entire organization, so it should be written with the organization in mind as well as the users. Policies should answer any questions an employee may have regarding their usage of computer/telecommunication equipment.

However, while we ensure security do we risk privacy? Introna (2000) also states “Technology has created the potential to build surveillance into the very fabric of organizational processes”. (p. 38). This described, ten years ago, what is all too true today. Information technology is completely intertwined with business; an organization’s telecommunications policies are there to guide employees in the use, capabilities and limitations of technological equipment. Herbert claims (2008) “Electronic technology has enabled the growing decentralization of the workplace, with some employees integrating their personal computer equipment with their employer's equipment” (p. 50)

Most individuals working today feel very strongly about their “right to privacy” or “protection of privacy”. They expect some level of trust to exist between the company and the employee. They assume that the company is reading all of their emails or counting keystrokes (which most people know nothing about) or having an information technology guru ghosting

their computers, watching or keeping screenshots of everything they do. A list of surveillance capabilities are listed in Figure 1.

The workplace end user types any keystroke in any window on his/her remote PC, that text appears on the network administrator's screen in real time or archived to a corporate server.
Typed text that is monitored may include email messages, online chat conversations, documents, passwords and all other keystrokes.
The network administrator can view the actual screen of the workplace desktops being monitored.
Internet usage can be monitored in real time and a log file recording of all Internet activity can be made.
A spy module can see and list software running on the remote PC and can view in real time the software applications and run executions.
A record and activity log for all workstations on the local or shared network location can be produced.
Monitoring software provides the ability to take snapshots of a remote PC screen or active window in specified time intervals and save them on the local or shared network location.
The workplace user's system can be turned off, restarted, and actually logged completely off the network.
The network administrator can run programs and execute commands on remote computers, open Web pages or documents, send instant messages for remote users, and terminate remote processes.
Files can be readily copied including logs and screenshots from the desktop computers. The administrator can have the same file access permissions, as a current user has on the workplace computer.
Multiple employee computers can simultaneously be monitored from a single workstation in the LAN.
Workplace surveillance software that runs on monitored computers is hidden and difficult for an employee to locate or even know that the software is present and monitoring their every keystroke. The monitoring software usually cannot be terminated without the network administrator's permission.

Figure 1. A descriptive list of available types of software employers may use to monitor their employees. (Nord, Nord, & McCubbins, 2006, p. 75)

Unfortunately none of this falls under the United States federal government legislation. Our constitutional right to privacy is usually inferred through the U.S. Constitution's Fourth Amendment's right to freedom from unreasonable search and seizure. This does not protect us in the private or public sector of employment. Nord, Nord, and McCubbins (2006) proposed that the Electronic Communications Privacy Act (ECPA) is the only piece of federal legislation that shows any interest in employee privacy. (p. 74) However, they also list that there are three

exceptions that may “effectively eliminate any substantial expectations of privacy an employee might have with respect to his/her employer.” (p. 75)

- First is the “provider” exception- If the employer owns or is providing the telephone, email, or Internet services to the employee, then the employer is protected from any possible claims.
- Second is the “ordinary course of business” exception- This exception gives the proverbial “green light” to employers to “monitor employee communications to ensure such legitimate business objectives as assuring quality control, preventing sexual harassment, and preventing unauthorized use of equipment”. (Nord, Nord, & McCubbins, 2006, p. 75)
- Third is the “consent” exception- Nord et al. (2006) explains this exception as, “if at least one party to the communication is either the party who intercepts the communication or gives consent to the interception then the ECPA has not been violated”. (p. 75)

Having a clear and an effective security policy in place can render employee claims moot. As previously stated, security policies should answer any questions an employee may have, and tell an employee exactly what he or she can or cannot do; furthermore, these policies also give the organization a clear and precise level of protection.

Lucas Introna (2000) states that an employer can “...monitor all aspects of work and communications...as long as the employer explicitly communicates policy that monitoring can take place and that the employer can justify it for a valid business purpose.” (p. 35) The Washington Post reported on April 23, 2010 that the Securities and Exchange Commission (SEC) did not fire thirty-three employees who were found to have used SEC-issued computers to view obscene material. (McElhatton, April 29, 2010) Many of these employees held senior

positions, earning approximately \$99,000 to \$220,000 annually. (O’Keefe, 2010) Another article regarding this situation from the Washington Times tells us that only eight were given the option to resign before termination, five contractors were relieved of their contracts, and all the others were suspended and returned to work.

These articles, of course, do not list why each employee decided to view these obscene materials during work time, or why they chose to use their work equipment. However, this matter is a perfect example of how not enforcing security policy will lead an organization to public scrutiny and shame. The Washington Post reported that “a senior attorney at SEC headquarters in Washington admitted he sometimes spent as much as eight hours viewing pornography from his office computer.” (O’Keefe, 2010) The article listed several other examples of this kind of conduct.

With regards to this case concerning these employees at this particular government agency, we see a media-induced portrayal of selective enforcement. We are led to believe that the SEC would presumably fire a regular (non-management/contract) employee for violating policy, however, since these are upper level (management/executive) employees they are let off with warnings or mild forms of punishment. Alternatively, if they were to be fired, they were given the opportunity to resign. Selective enforcement can bring about feelings of division in a workplace. It may make some people feel that they are “outside of the law” and better than everyone else. One may go so far as to describe selective enforcement as a mild form of tyranny. Selective enforcement of a policy is unethical, unjust, shows signs of favoritism and possibly leads to extortion if the employee is malicious. Why have rules or a policy in place if it holds no weight because of your position?

Security policies specific to this project are created to manage the security risk of cyber attacks. These policies are put in place to help employees as well as to protect them. Johnson and Goetz (2007) pointed out that "...senior management isn't the biggest hindrance to better security. Rather middle management might represent one of the largest challenges because they impact the organization daily." (p. 17) They also point out that proper teaching of the organizational policy is a key ingredient to employees understanding security policy, and that it must start at the top. All levels in an organization must be aware of the importance of security. Johnson and Goetz (2007) further discuss an important fact: Despite middle management being a challenge, it is the duty of the executives and the senior staff to set the tone of following the policy. They surmise "executives and senior level management need to be aware of, engage in, and supportive of security issues, strategies, and policies that address them." (p. 22)

When we think of insider threats, the first thing that may come to mind is a vindictive and vengeful ex-employee trying to sabotage the company's computer network by utilizing denial of service attacks or installing viruses. Or possibly a soon to be ex-employee may create a back door in the network so they can access information after they are terminated, or even steal some customer information or trade secrets to advance his or her career for a competitive organization. In the article, *Are Employees Putting Your Company at Risk by not Following Information Security Policies*, (2009) by Mikko Siponen, M. Adam Mahmood, and Seppo Pahlila the definition of an insider threat can be narrowed down to **any** employee. Careless, lazy, irresponsible and ignorant employees comprise a large portion of the "insider threat" to an organization, not malevolent employees. The authors of this article state that "information security breaches...can cause harm irreparably by shutting down computers forcing business to lose potential revenues or by leaking corporate confidential information and customer data

possibly making corporations vulnerable to legal and regulatory problems...” (Mahmood, Pahnla & Siponen, 2009, p. 145) The article goes further into detail explaining some ways for companies or “practitioners” of a security policy to assist the employee in adhering to policy. The Results portion of this project discusses this issue further.

In Bulford, Hunker & Predd’s (2008) article *Insiders Behaving Badly*, they study an organization’s logically misappropriated attentions only to outside attacks and not insider threats. Why do we not pay close attention to employees that have legitimate access to systems? Insiders also have the means to put business and data systems at risk with risky behavior. The article lists numerous examples of real life situations where a current employee performed an action that put his or her company in harm’s way. For example, there is the naïve user, who would take a piece of computer equipment home to finish up some work that is due the next day and although there was no security policy forbidding removal of the computer equipment, said computer would have all the organization’s customer information on it, thereby jeopardizing consumer privacy and all or access to all of the organization’s financial information. A further example of an insider threat is one that can happen to any one of us at any given time; the ordinary employee usage or mistake. What if you worked for a big company and you needed to send an email to individuals in your group and instead of accessing the group address you hit “reply all” to the global address book and everyone in your company got a copy of your email? What would you do? Since the email server is not able to withstand the amount of replies that it was a mistake or angry outbursts thinking it was a joke, you have unwittingly caused a denial-of-service (DoS) attack on your own company. Lastly they list the malicious insider who would purposely try to steal information from their company for personal gain. (p. 67)

An organization's telecommunications and information technology security policy would help in all these examples. It is an organization's responsibility to play a role in its own protection. First Bulford et al. (2008) states that an organization "defines legitimate access and decides to whom it should grant that access". (p. 68) Next they explain how an organization should set the policy and use it to assist in comparing behaviors. They state, "Organizations must distinguish official organizational policy (the *de jure* policy) from the organizational policy as members actually implement or understand it (the *de facto* policy)". (Bulford et al., 2008, p. 68) Figure 2 offers a framework for insider threats that "lets technologists and managers classify a complete range of insider actions and develop strategies to address each one". (Bulford et al., 2008, p. 69)

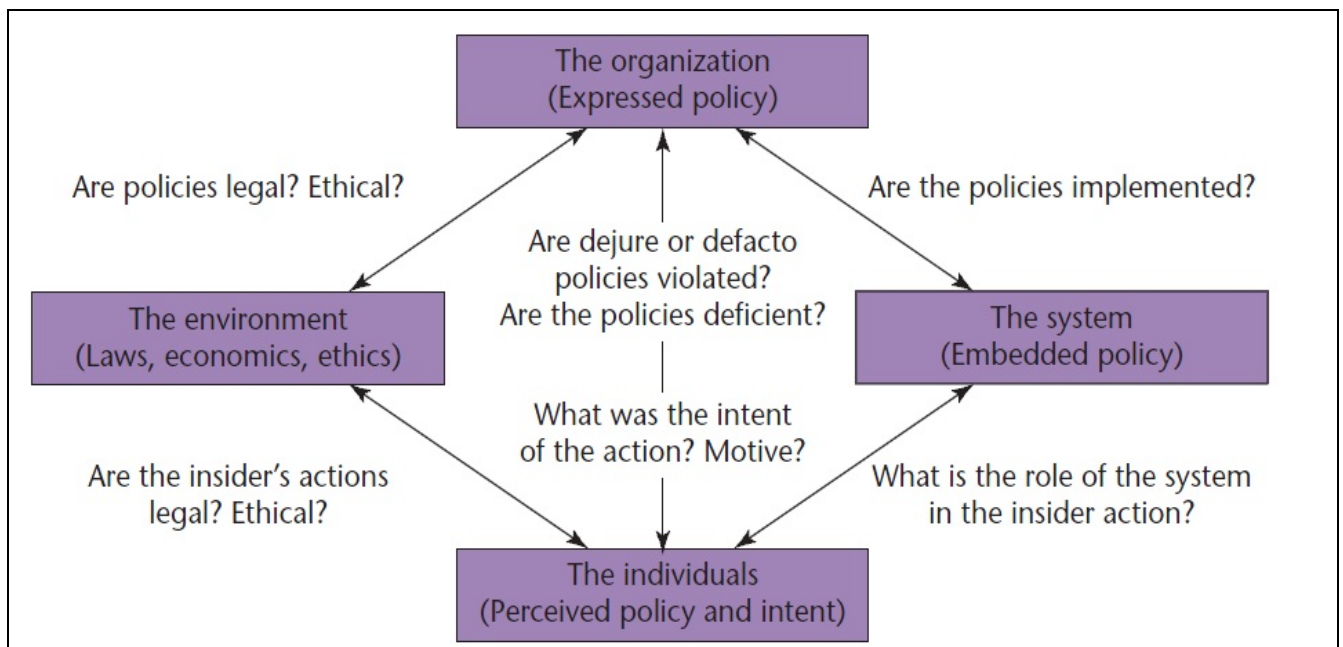


Figure 2. A framework for insider threats. (Bulford et al., 2008, p. 69)

And lastly the article explains that it is the organization's responsibility to "set the culture" which will demonstrate and illustrate how employees should properly behave regarding security policy. These articles relate to and explain telecommunications/IT security policy and the importance therein. It is my goal for this project to utilize this and additional research to further explain the importance of computer security policy.

Chapter 3 – Methodology

This project seeks to assert that telecommunications and information technology security policy is a subject that is vital to any organization that employs any form of electronic communication in their arsenal. A qualitative methodology with a constructivism epistemology was utilized for this project. These concepts allow the reader to experience and explore the human side of this topic. We as researchers have the opportunity to describe views and relationships that amalgamate telecommunications/IT security policies and organizations.

The Internet and my college resource databases were the main sources of literature collection. Using keyword searches such as “security AND policy”, “security policy”, “telecommunication policy”, “selective enforcement”, “information technology security and policy”, “example of security policies”, “government security policy”, “organizational policy”, and “organizational security policy” all garnered numerous results, except for selective enforcement. Selective enforcement retrieved results that mainly dealt with law enforcement and racial profiling.

During the initial research, the articles found illustrated and fully supported the idea that telecommunication and information technology security policies are vital to the operation of an organization and the disregarding of a policy will undoubtedly bring vulnerabilities and adversity. In fact, the only real dispute was regarding who was responsible for enforcing policy, i.e., whether it was middle management or executives. As it happens, the information uncovered in the articles found was sufficient enough to proceed with the project analysis.

In analyzing the data attempts were made to shy away from the percentages and numbers. It was important to look at security policies as a concept that affected the people of an organization instead of just a document. The questions listed and answered in the “Results”

section of the project are a restatement of the questions asked in the “Introduction”. They were developed as the means to analyze the information and a way to articulate the objective of the project. The questions became a conduit for channeling the relevant information gleaned from research into the points that this project conveys.

Moreover, past experiences of being under a telecommunications/IT security policy while employed as an officer and a supervisor at a local county jail also proved useful. This afforded the opportunity to view this project from an employee’s perspective as well as that of a policy writer.

Chapter 4 –Analysis/Results

It is important that the notion of an IT security policy is relevant in organizations today. The telecommunication/ IT security policy itself makes a difference in the productivity from employees in any corporation or organization. It is important for all members of an organization to observe IT security policies and consistently impose consequences on individuals that violate said policies. Failure to do so could leave the company or organization vulnerable to threats and cost a company millions in lost trade or services and lost time that an employee has wasted.

- What happens when employees get complacent and they knowingly break the rules?
- What if the individuals breaking the policy are the managers?
- Is selective enforcement really unreasonable and unethical?
- Is a company at risk when a telecommunications/information technology security policy is ignored?
- What items should be in a good security policy?
- Is there an example of a comprehensive security policy?
- What can be done to ensure consistent practice of telecommunication/IT security policy across the board, for a fair and equal workplace?
- So how do we ensure that employees are consistently following the policy, and that employers are constantly enforcing the policy?

Let us look at, answer and discuss these questions.

What happens when employees get complacent and they knowingly break the rules?

Complacency happens to many workers in every area of the workforce, whether the employee has worked at a job for a considerable number of years, or if the person has to do the same repetitious occupation all day, every day (for example: a factory worker). Complacency, especially somewhere like a factory, can be extremely dangerous. For a police officer, for example, it could mean life or death. Hopefully in the information technology or business arena, it is not life or death; however, complacency is a significant issue that can cost a company millions of dollars. Bringing into play the SEC once again, the report *SEC workers investigated for porn-surfing* (February 2, 2010) by Jim McElhatton begins with the statement “The work computer of one regional supervisor for the U.S. Securities and Exchange Commission showed more than 1,800 attempts to look up pornography in a 17-day span” (¶ 1). This example shows a worker who was so very comfortable in his/her job, in what he/she does everyday, that he/she allowed his/her desire for viewing pornography to overrule his/her common sense involving his/her work ethics.

The complacent attitude of these employees of the SEC put their agency at risk. The employees must “realize that these threats can cause serious negative consequences to their organization”. (Mahmood et al, 2009) Employees of any organization must realize that security is much less effective when handled by a complacent mindset. Laura Corriss (2010) is of the opinion that, “Just as we would never want to treat security as an add-on application in the software or hardware world, we need to make security integral to the organizational culture”. (p. 35) This statement reiterates that potential workers tend to treat security (IT and telecommunication) and their policies as if they are no more important than the superfluous

software that is downloaded on a computer system. Quite the contrary, the security policy of an organization is fundamentally important to the employee as well as the organization.

What if the individuals breaking the policy are the managers?

The individuals who preside over day-to-day work activities in an organization are placed in that position for various reasons. Whether it is education, tenure, or experience, the person that maintains this standing is set to a higher level of responsibility by their superiors and their subordinates. Again using the SEC as an example, the majority of the individuals accused, reprimanded, or released, were employees in a managerial type position or higher. Ed O'Keefe (2010) writes that "a regional office staff accountant admitted to viewing pornography on his office computer and on his SEC-issued laptop while on official government travel" (§ 2). The article also noted that

"a senior attorney at SEC headquarters in Washington admitted he sometimes spent as much as eight hours viewing pornography from his office computer...[and] the attorney's computer ran out of space for the downloaded images so he started storing them on [compact discs] CDs and [digital video discs] DVDs that he stored in his office" (O'Keefe, 2010 § 3).

O'Keefe's (2010) article also lists another senior accountant for the SEC, a senior executive at the National Science Foundation (NSF), a chief judge of the U.S. 9th Circuit Court of Appeals, and a National Park Service employee as all being caught either chatting with nude models or downloading, viewing, or posting explicit photographs on or from their work computers (§ 5).

Many employees may feel that if their superiors get caught breaking the rules they should be even more harshly dealt with simply because they should know better. McGraw-Hill

Companies has a Code of Ethics for its Chief Executive Officer (CEO) and Senior Financial Officers listed on the Internet. It clearly states who it affects, and what the protocol is for a violation of duties listed below in Figure 3 and 4.

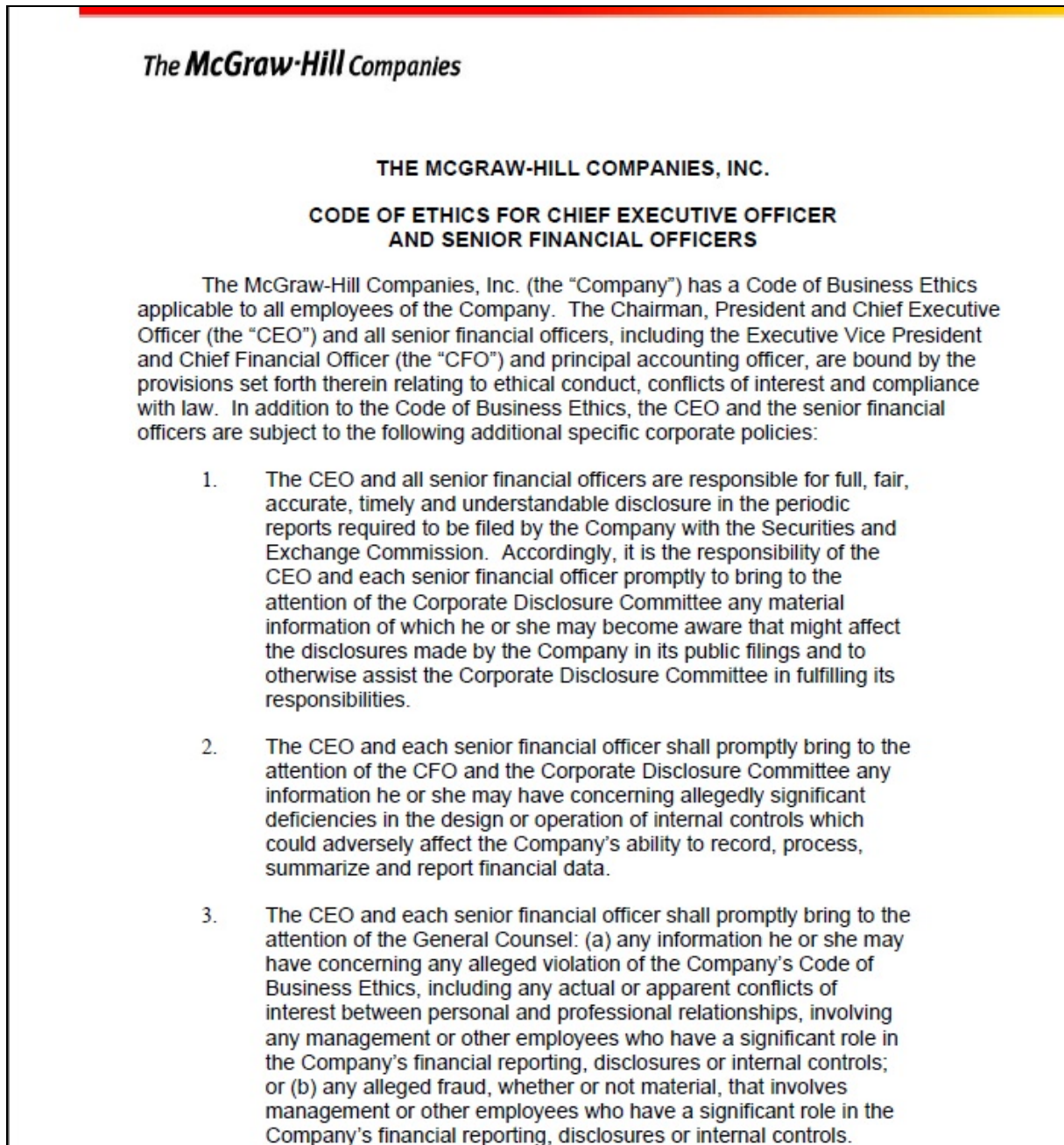


Figure 3. McGraw-Hill Companies Code of Ethics for CEO and SFOs <http://investor.mcgraw-hill.com/phoenix.zhtml?c=96562&p=irol-govconduct>

4. The CEO and each senior financial officer shall promptly bring to the attention of the General Counsel any information he or she may have concerning alleged evidence of a material violation of the securities or other laws, rules or regulations applicable to the Company and the operation of its business, by the Company or any agent thereof, or of a material violation of the Code of Business Ethics or of these additional procedures.
5. The General Counsel may in the General Counsel's discretion refer the matters set forth above in paragraphs 3 and 4 to the CEO, the CFO, the Corporate Disclosure Committee, the Corporate Audit Department and/or the Audit Committee of the Board of Directors.
6. The CEO shall determine, or designate appropriate persons to determine, appropriate actions to be taken in the event of violations of the Code of Business Ethics or of these additional procedures by the Company's senior financial officers. Such actions shall be reasonably designed to deter wrongdoing and to promote accountability for adherence to the Code of Business Ethics and to these additional procedures. In determining what action is appropriate in a particular case, the CEO or such designee shall take into account all relevant information, including the nature and severity of the violation, whether the violation was a single occurrence or repeated occurrences, whether the violation appears to have been intentional or inadvertent, whether the individual in question had been advised prior to the violation as to the proper course of action and whether or not the individual in question had committed other violations in the past.
7. The Board of Directors shall determine, or designate appropriate persons to determine, appropriate actions to be taken in the event of alleged violations of the Code of Business Ethics or of these additional procedures by the CEO.

Figure 4. McGraw-Hill Companies Code of Ethics continued <http://investor.mcgraw-hill.com/phoenix.zhtml?c=96562&p=irol-govconduct>

The last code listed is the most profound, because it allows all the employees to see that their highest superior is subject to discipline by the Board of Directors if he or she violates any rules. However, while this provision looks good on paper, will the corporation stand by its written policy? It is certain that the Security and Exchange Commission has some type of policy in play for the members of their staff. They do not promote the inappropriate usage of the government's

equipment. In fact, Jim McElhatton (April, 2010) mentions that the Chairman of the SEC, Mary Schapiro, sent out an agency-wide email reminding employees of the rules regarding unsuitable Internet usage. This proves that there are clear guidelines set; however, there may be a glitch in auditing and reporting, because if they can count the years that someone has been accessing Internet pornography, the relaying of the information shows fault within the information technology department as well as with the offender.

Is selective enforcement really unreasonable and unethical?

In short, yes. Selective enforcement breeds ill will amongst employees of an organization. If a worker's superior does something erroneous or iniquitous and receives a "slap on the wrist" it will become known by others, even though most disciplinary hearings and their conclusions are to be kept secret. Furthermore, if it circulates that another employee in a lower position did the same wrongdoing, violating the same policy agreement, and that person is fired, it will create sense of irrevocable disquiet among the non-managerial staff. It then, in turn, may give the managerial staff a feeling of being supreme or untouchable.

The unethical nature of selective enforcement is apparent even in its name. *Enforcement* meaning "compelling obedience to a law, regulation or command" and *Selective* meaning "not universal or applying to some but not others" (Encarta Dictionary, Microsoft Word 2003), blatantly showing that a person, group, or organization guilty of selective enforcement chooses who can get away with breaking the regulations of a company.

It is an understatement to say that selective enforcement is unreasonable. Selective enforcement is hypocritical in nature to the fundamentals of policies in any arena. It allows one

to question “Why have a policy prepared, and have everyone employed sign for it, but only punish some of those who may violate it”? One author states:

“Consider politics, the criminal justice system, professional sports, and economic trade as examples of competitions confused for games... That means awful as it sounds that there will be tolerance for some measure of opacity, intentional ambiguity and yes some lying, cheating and free riding to keep games as games.”

(Schaefer, 2009 p. 31)

This quote merely brings it back to reality by stating there will be murkiness dealing with policies and how people enforce and interpret them. Moreover, it will be a part of organizational politics to determine who gets fired and who gets to stay, because it may be easier to fire and hire a non-managerial employee versus someone who has the education and experience required for a managerial or an executive level job.

Is a company at risk when a telecommunications/information technology security policy is ignored?

Every employee that ignores their organization’s telecommunications/information technology security policy is putting their company in extreme jeopardy. The policies are outlined to protect the company, its assets, and its employees. The probability for an attack on an organization’s network is higher the moment someone ignores the rules. Research suggests that employees (especially the uneducated computer user) may truly be ignorant to the risks associated with violating policy. In other words, “...if employees realize how vulnerable their organization is to security threats and the severity of those threats, they are likely to have a strong intention to comply with information security policies”. (Mahmood, et al, 2009, p. 145)

The employees who helped write the policy, or those that are intentionally violating the policy, are the employees that have the potential to cause the most damage. Most employers fear that it will be the disgruntled employee who gets fired from their position, and may want to retaliate and cause harm to the network and company. It is more likely for an active employee to make an error and trigger a network malfunction or bring about an attack than for an ex-worker to purposely attack an organization.

Employees violating policy by viewing pornography or visiting inappropriate websites, or even regular websites, are putting their company at risk. The risks of tracking cookies, viruses, hackers, crackers, and back doors being created and opened are far more likely to occur if an employee chooses to visit company restricted websites. Companies that allow web searching try to have an airtight antivirus protection program covering their network. It is up to you as a representative of your company to have the desire to do right by the company. Staying away from inappropriate websites is good for the company, good for the network, and good for your career.

What items should be in a good security policy?

A good security policy should be precise, all-encompassing, comprehensive, and most of all, flexible. Technology is ever changing, so an IT security policy should change with the times. A telecommunications security policy from the government in 2000 should not be the same as it is today. There are emerging markets of technology that didn't even exist 11 years ago. Virtual private networks (VPN) are a good example for the utilization of our smartphones (iPhone®, Palm®, Blackberry®) and tablets (iPad®, Galaxy Tab®, Folio®).

The figure below shows steps that can be taken while developing a security policy. The items listed are the foundation of the security policy which represents a strategy to meet security requirements (Halfmann & Kühnhauser, 1999).

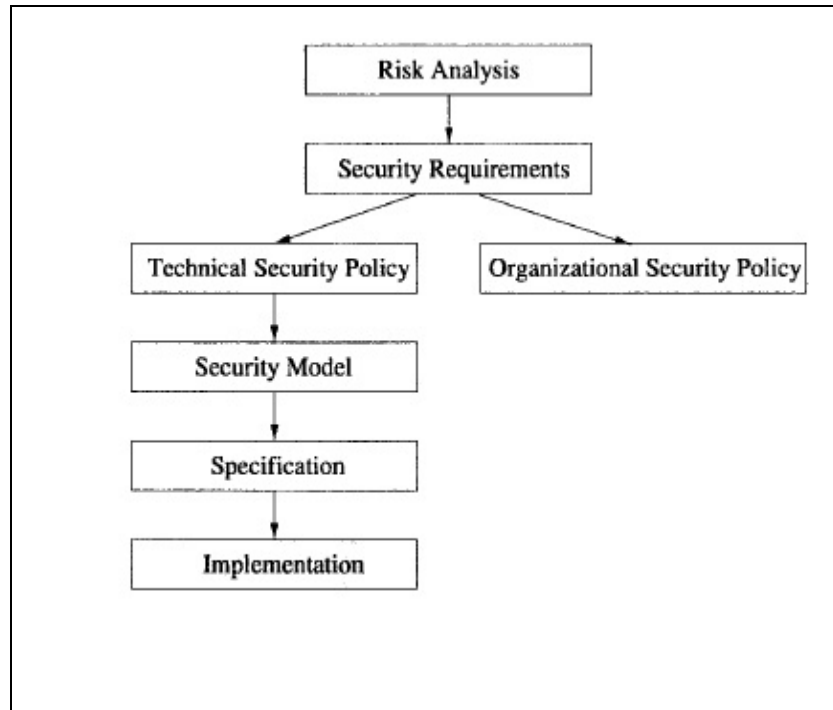


Figure 5. Steps in the development of a security policy. (Halfmann & Kühnhauser, 1999)

The culture of an organization is good place to start when writing a computer security policy,

“given that an organization’s overall security is the result of each individual’s actions”.

(Johnson, et al, 2007) Some questions you can ask, while in the development stage, are; what kind of tone have we set for the policy? Where are the roles the executives will play with regards to information security? A listing of some individual items that should be taken into account when creating a policy is:

- Scope and applicability
 - Define your technologies (all of them)
 - List the responsibilities for all levels in the organization
 - User access
 - Protection of privacy (list the employee's rights)
 - What is fair and acceptable usage of the technologies
 - What is improper use of equipment
 - Define criminal usage
 - Define what is harassing and offensive material
 - Clearly explain the concept of "trade secrets" and company property and resulting responsibility of employee
 - Explain the importance of copyrights and intellectual property
 - Explain and list how information is managed and stored
 - Clearly identify who is monitoring and how the employer monitors the system
 - Explain the physical aspects of security for the equipment as well as viral protection
 - Identify what can cause breaches in the security of the network
 - Clearly define the consequences of violation of the policy
 - Limitations of liability
 - Clarify how often the policy is reviewed and updated
 - Enlighten the workers so they know that when policy is updated so are the employees
- (Aalberts, et al, 1999)

Is there an example of a comprehensive security policy?

Most policies are written with the intention of being comprehensive. Each organization does its level best attempting to include all aspects that are important to them and incorporating that into their policies. Listed below are three snippets of a computer security policy found from the West Virginia's Department of Health and Human Services (DHHS).

4.1	Employee Responsibilities
4.1.1	Employees must use portable computers and mobile devices for business purposes only.
4.1.1.1	All rules regarding the acceptable use of IT Resources within the DHHR apply to the utilization of mobile equipment. (See policy IT-0501, <i>Use of IT Resources</i>)
4.1.2	Each portable computer and mobile device must receive program updates, security patches, and anti-virus updates at designated intervals. (See OP-19 – <i>Security for DHHR Portable Computers and Mobile Devices</i>)
4.1.2.1	In order to receive updates, each portable computer and mobile device must be connected and logged-on to the DHHR network.
4.1.2.2	OMIS reserves the right to disable computer accounts for any device not connected to the network or updated at the time of the designated interval.

Figure 6. West Virginia's DHHS Computer Use Policy

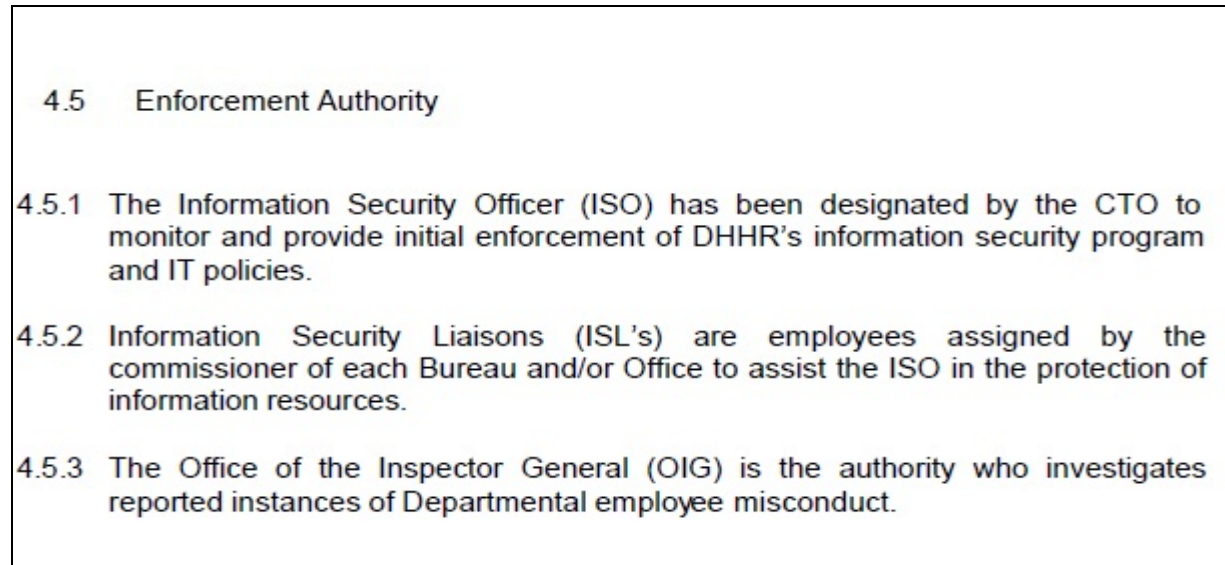


Figure 7. West Virginia's DHHS Enforcement Authority

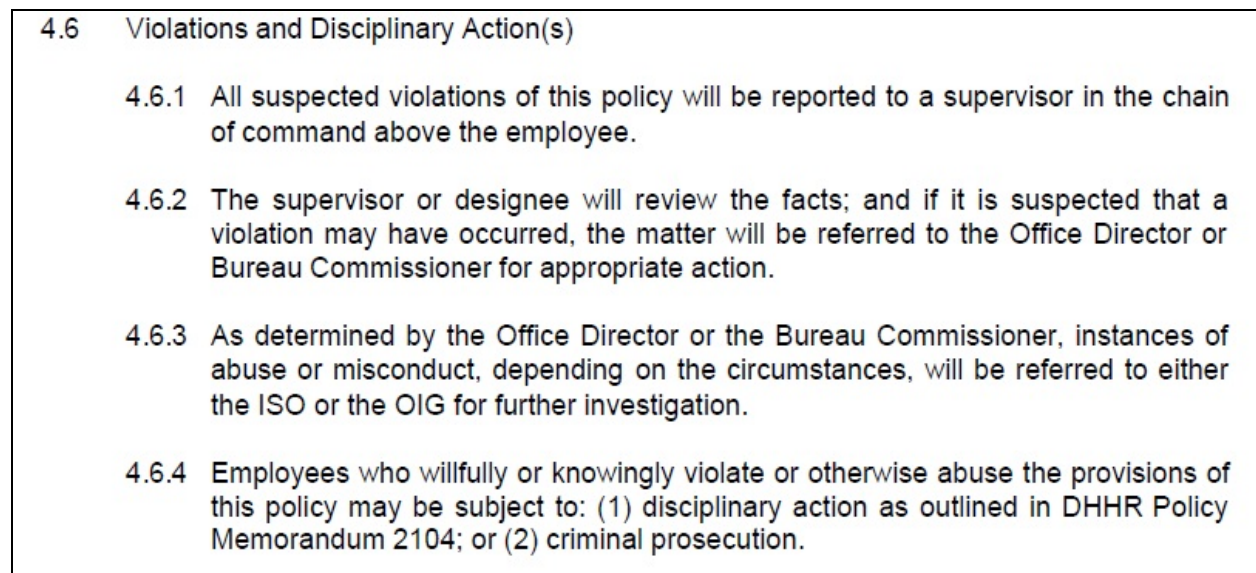


Figure 8. West Virginia's DHHS Violation Policy

In Figure 6, the first directive listed states that employees must utilize the equipment given to them by that agency for business purposes only. Some may feel that it is silly to make a redundant statement such as that; however, most people do not feel that the checking of their personal email accounts or updating their Facebook© status is such a big deal. But according to this organization's computer policy, an employee doing that is in clear violation. Figure 8 lists some repercussions if one were to violate the policy. It also illustrates the chain of command for the organization in Figure 7.

What can be done to ensure consistent practice of telecommunication/IT security policy across the board, for a fair and equal workplace?

The first thing that can be done to ensure consistent practice is to train and educate regularly. There is a widely known cliché that says “ignorance is bliss”; however, that can not be the case when dealing with policy and procedures. If employees do not know the rules, then how can they be expected to follow them? Most employers want to treat adults like adults and expect them to read and understand the rules of their workplace. It also helps when an employee's superiors and peers are showing that they are following the rules and they are striving to show that they take their workplace policy earnestly. One article agrees with the previous statement and states that “the behavior of managers, information security staff, and peers should be persuasive enough for employees to take compliance with information security policies seriously”. (Mahmood, et al, 2009, p. 146)

Mahmood, et al (2009) also stated that they “found that perceived vulnerability and perceived severity have a direct effect on employees' intention to comply with information security policies”. (p. 146) If employees never see or hear about anyone getting terminated or

suspended because of inappropriate usage, then they may feel that they too are “untouchable” when perusing various websites. Moreover, if employees never hear about the impact a virus had on the organization’s network due to inappropriate use, then they will never understand the vulnerability of the network.

So how do we ensure that employees are consistently following the policy, and that employers are constantly enforcing the policy?

Awareness is every organization’s first step to consistency. Be aware of the policy. Be aware that your organization may have policy issues. Be aware that front-line employees, managers, or even executives may be abusing their position or title and desecrating the very essence of an organization’s mission statement, because a company’s “mission statement is created based on the core values...[which] spell out the organization’s basic beliefs and passions”. (Corriss, 2010) After an organization becomes aware, the next thing to do is to educate, and educate regularly. Education of an entity’s inner working is a good thing. It conveys simple reminders, and lets the workers know that there may have been changes to the policy that they were not aware of. Laura Corriss (2010) elucidates “if we want employees to know and to internalize what is critically important to an organization, these values must be explicitly stated”. (p. 37)

A radical way to help an organization to impart consistency between all levels of employees is to,

“Have line managers...take personal responsibility for security and involve company auditors to help enforce security levels. This creates a different level of awareness among line managers; it also helps integrate security into the corporate

culture, making it a crucial part of the business process”. (Johnson & Goetz, 2007)

One final thought concerning consistency: Be fair. The golden rule may be ancient, but it applies to a lot in life, even if it does not apply to the concept of business. An employer wants the best employees and wants the employees to give their best. It only makes sense for an employer to give its employees the best -- the best working environment, the best organizational culture that will allow an employee to grow as an individual, which should in turn help an organization to grow. There should be no room for favoritism, selective punishment, selective praise or abuse of any kind. Behavioral guidelines should exist for all categories of employees in a business. No one person, policy or piece of equipment does it all, and that makes everyone and everything that is connected to an organization important, especially the people.

Chapter 5 – Conclusions

This project illustrates that security policies help organizations. It shows that an enforced policy is beneficial to an organization as a whole. Telecommunications and IT security policies are designed to keep intruders out by educating employees on what to do on the inside. Proper education, training, and knowledge of what the policy is, not what the employee believes it says, will help organizations protect their assets; because if you do not educate and reinforce policy then you cannot assume your employees know to properly employ said policy.

An organizational security policy should include a fundamental philosophy of the company. It should contain information that will protect the company as well as its employee. It should be comprehensive and always changing to keep up with the fluctuating influx of technology. Most organizations are a globalized concoction of software, hardware, people and experience. Security is one of the most important factors in an organization whether executives realize it now or not. The need for keeping trade secrets, meeting government regulations and maintaining financial privacy is vital. It will all trickle down to the need for a good and comprehensive telecommunication and information technology security policy.

Furthermore, when an organization fails to consistently enforce its security policies, it places the company at risk for vulnerabilities and instills an atmosphere of discord. Selective enforcement is one notion that has no business being in business. This concept leads to shameful publicity if it ever reaches the eyes and ears of the public and also sends the employee morale into a downward spiral. Having a good security policy in place takes the guesswork out of what is proper and acceptable behavior. Taking time to place all information that a company requires of its employees in its security policy makes it most effective and easiest to enforce. Fairness and consistency in enforcing the policy will ensure that personnel are aware of the consequences

for violation and can create a greater sense of well-being and security for the organization as a whole.

References

- Aalberts, R. J., Townsend, A. M., Whitman, M. E. (1999). Considerations for an effective telecommunications-use policy. *Communications of the ACM*, 42(6). doi: 10.1145/303849.303868
- Bulford, C., Hunker, J., Pfleeger, S. L., Predd, J. (2008). Insiders behaving badly. *IEEE Security & Privacy*, 6(4), 66-70. doi: 10.1109/MSP.2008.87
- Corriss, L. (2010). Information security governance: Integrating security into the organizational culture. *GTIP '10 Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies*. doi: 10.1145/1920320.1920326
- Enforcement. (n.d.). In Encarta Dictionary. Microsoft Word 2003 Application.
- Halfmann, U., Kühnhauser, W. (1999). Embedding security policies into a distributed computing environment. *ACM SIGOPS Operating Systems Review*, 33(2), 53
- Introna, L. (2000). Workplace Surveillance, privacy and distributive justice. *Computers and Society* 30(4), 33-39. doi: 10.1145/572260.572267
- Johnson, M. E., Goetz, E., (2007). Embedding information security into the organization. *IEEE Security & Privacy*, 5(3), 16-24. doi: 10.1109/MSP.2007.59
- Mahmood, M. A., Pahnla, S., Siponen, M. (2009). Technical Opinion: Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, 52(12), 145-147. doi: 10.1145/1610252.1610289
- McElhatton, J. (2010, February 2). SEC workers investigated for porn-surfing. *The Washington Times Online Edition*. Retrieved from <http://www.washingtontimes.com/news/2010/feb/2/sec-workers-investigated-for-viewing-porn-at-work/print/>

McElhatton, J. (2010, April 29). Porn peepers still working at SEC. *The Washington Times*

Online Edition. Retrieved from

<http://www.washingtontimes.com/news/2010/apr/29/porn-peepers-still-working-at-sec/>

McCubbins, T. F., Nord, G. D., Nord, J. H. (2006). E-Monitoring in the workplace: Privacy, legislation, and surveillance software. *Communications of the ACM*, 49(8). doi:

10.1145/1145287.1145290

McGraw-Hill Companies, Inc. (2004, January 28). *Code of Ethics for Chief Executive Officer and Senior Financial Officers*. Retrieved from [http://media.corporate-](http://media.corporate-ir.net/media_files/nys/mhp/corpgov1/seniorofficers.pdf)

[ir.net/media_files/nys/mhp/corpgov1/seniorofficers.pdf](http://media.corporate-ir.net/media_files/nys/mhp/corpgov1/seniorofficers.pdf)

O'Keefe, E. (2010, April 23). SEC porn investigation nets dozens. *The Washington Post*.

Retrieved from [http://voices.washingtonpost.com/federal-](http://voices.washingtonpost.com/federal-eye/2010/04/eye_opener_porn_and_federal_wo.html)

[eye/2010/04/eye_opener_porn_and_federal_wo.html](http://voices.washingtonpost.com/federal-eye/2010/04/eye_opener_porn_and_federal_wo.html)

Selective. (n.d.). In Encarta Dictionary. Microsoft Word 2003 Application.

Schaefer, R. (2009). Software maturity: Design as dark art. *ACM SIGSOFT Software*

Engineering Notes, 34(1), 31. doi: 10.1145/1457516.1457528

West Virginia Department of Health and Human Services (2006). Policy: Acceptable use for portable computers and mobile devices. Retrieved from

<http://www.wvdhhr.org/mis/IT/IT0515.pdf>