Fall 2011

The Insider Threat

Jacinda L. Wunderlich
Regis University

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

Disclaimer

THE INSIDER THREAT

A THESIS

SUBMITTED ON 3 OF OCTOBER, 2011

TO THE DEPARTMENT OF THE SCHOOL OF COMPUTER & INFORMATION TECHNOLOGY

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN SYSTEMS ENGINEERING

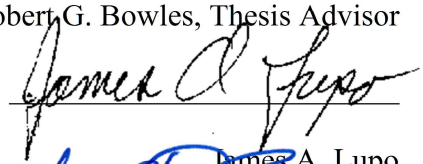
BY

Jacinda L Wunderlich

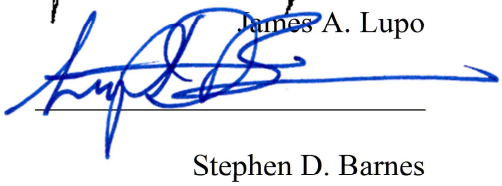
Jacinda L. Wunderlich

APPROVALS

Robert G. Bowles, Thesis Advisor



James A. Lupo



Stephen D. Barnes

Abstract

The Insider threat is defined similarly by experts in the information technology world for businesses, but addressing the threat has not been of great focus for most organizations. Technology and the Internet have grown exponentially over the past decade leading to changes in how business is conducted. Some basic business practices remain the same – protect the organization and its customers from breach of privacy. How data is gathered, stored, and retrieved has changed. Protecting the perimeter is still important, but these changes in technology now open the doors to a new threat – one that is known but not commonly protected against – the insider. Whether intentionally, or accidentally, the insider threat needs to be incorporated into the currently used security architectures and best practices. How should an organization include the insider threat to the current architecture is the question.

Changes need to be made by organizations to the current security architecture. Currently, using technology is not enough, but is still necessary. In order to make it better, considering the employee as a whole and the daily activities necessary to complete a job, as well as working with other business units as a whole needs to be included in the architecture. Behavioral traits can be considered but there are issues in privacy that also need to be considered. Monitoring can be done, but that should not be the only thing considered. Employees lack knowledge as to why actions can have a negative effect on an organization and the way to address this is education. Educating end users is necessary and should be performed regularly to keep not just the technologically inclined up to date. Without education, the current technology used will continue to keep out the intruders, but will not be effective enough to protect against intentional and accidental misuse of the organization and its networks.

Acknowledgements

All my family and friends – especially Darrell, David, and Crystal for putting up with me the past couple of years through this whole process!

Table of Contents

List of Figures

List of Tables

Executive Summary

Many information technology specialists follow general best practices in securing a network – blocking unused ports, requiring passwords, employing encryption, and applying access controls. These practices are most often used to keep out intruders. Intruders can cause a long list of issues for an organization and its customers. Trojans, worms, viruses, malware, and data theft and loss are big concerns that should not be overlooked. With the speed of growth and changes in technology today, federal laws and regulations are required to be followed by organizations. In order to maintain a respectable reputation in the market, professionals agree that protection of a network and its data is essential to maintaining respect and compliance. One debate still remains – what, or who, is the real threat when managing a network and a business? Knowledge of, and protection against, many forms of threats is pertinent in securing a network. Is the real threat still outside the walls, or could the greatest threat be found on the inside?

A renewed focus has come to the attention of the Information Technology security world – the insider threat. Historically, protecting an organization was as simple as keeping cabinets and doors locked and providing access to only those who had a key. Guards, keys, and access badges were once enough to protect sensitive and proprietary information. Changes in technology and business have opened doors to new threats in regards to security measures. Throughout history, securing the perimeter was enough to protect an organization and its customers. China secured itself from northern threats by building the Great Wall. Fur traders across North America built walls and towers to keep enemies and unwanted guests out to protect business. Organizations have used guards, fences, cameras, and locks to stay secure from unwanted access. With the invention of the computer, new security devices (badges, scanners,

etc.) have been created to prevent trespassing. As computer technology progressed networks were protected by blocking ports, requiring passwords, and encrypting data – again, all of these measures were implemented to keep intruders out. The business and communication world has changed drastically with the growth of and usage of the Internet and the globalization of business. Both the Internet and globalization have led to a new threat – those who are on the inside. This has become referred to as the Insider Threat.

There are similar definitions of what is meant by "insider threat." The National Infrastructure Advisory Council (NIAC) has studied and defined an insider threat as "…one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm." (Noonan & Archuleta, 2008, p. 5) Cisco Systems has described the insider as, "…often characterized as an employee performing malicious behavior – through sabotage, stealing data or physical devices, or purposely leaking confidential information." (Cisco, 2008, p. 1) The Cisco study goes on to say, "However, organizations need to be aware that the insider threat is not just the rogue employee, but rather every employee and every device that stores information. Employees are insider threats if they speak loudly about confidential project plans while on the phone at the airport. A lost laptop containing company information can become an insider threat if it is recovered by an outsider with malicious intent." (Cisco, 2008, p. 1) These few examples given by Cisco's report demonstrate how our everyday actions could innocently harm or destroy an organization.

How financially devastating could an innocent action be? With laws and regulations that define punishment, many organizations have suffered. In 2006, Electronic Registry Systems

(ERS) was a victim to theft. With the loss of one desktop and one laptop, 63,000 patients were affected by data loss. Not complying with HIPAA regulations meant a $15.75 million fine plus the cost of credit monitoring for all patients affected. Electronic Registry Systems also suffered from a loss of credibility and reputation. (Kondrup, 2011) UBS PaineWebber was also attacked intentionally by an employee. The employee planted a logic bomb that shut down 2,000 servers. This kept UBS PaineWebber from being able to make trades for weeks. In order to bring the company back online and able again to conduct business cost UBS PaineWebber $3.1 million. Figures were not given in regards to how much business was lost while out of commission. (Linux.com Editorial Staff, 2011) Recently, Bradley Manning successfully breached security with the Department of Defense's Secret Internet Protocol Router Network (SIPRNet) and accessed about 260,000 classified diplomatic cables. This data that Manning was accessed internally was carried out of the building on CD-RWs. This activity was a major failure for the Department of Defense's network and physical security. (Linux.com Editorial Staff, 2011) Whether planned or accidental, an insider can cause a great hardship for many.

With the realization that an insider can pose a greater threat than an outsider, new measures must be taken by organizations to fully protect themselves from insider threats. Best practices for physical and network security should not be ignored. Additional measures should be taken in order to mitigate the risk against the insider threat. An important step to take towards securing an organization is to perform research regarding the levels of awareness of the employees regarding insider threats. Once research is complete, education and awareness will prove to be a huge factor in protection. (Noonan & Archuleta, 2008, p. 38) Recent findings show that currently used security measures by information technology professionals is not enough to

protect information and data from this new threat growing due to changes in technologies and globalization – the insider attack.

Goals and Objectives

1. Define an insider threat.

2. Demonstrate how older forms of security protection are not enough to protect against the now more prominent insider threat.

3. Demonstrate how security awareness training will be beneficial to the future of an organization's success.

4. Present a new approach to Information Technology Security management regarding the insider threat.

5. Discuss the importance of auditing and amending controls put into action to stay on top of the prevention of an insider attack.

6. Demonstrate how important understanding employee's level of security knowledge can impact an organization's success.

7. Identify necessary security controls to enforce, test, and measure against the insider threat

Chapter 1 - Introduction

Many information technology specialists follow general best practices in securing a network – blocking unused ports, requiring passwords, employing encryption and applying access controls. These practices are most often used to keep out intruders. Intruders can cause a long list of issues for an organization and its customers. These practices help defend a network against Trojans, worms, viruses, malware, and data theft and loss. These threats should continue to be addressed and not overlooked. Professionals agree that protection of a network and its data is essential to maintaining respect and compliance. One debate still remains – what, or who, is the real threat when managing a network and an organization? Knowledge of, and protection against, many forms of threats is pertinent in securing a network. Is the real threat still outside the walls, or could the greatest threat be found on the inside?

A renewed focus has come to the attention of the Information Technology security world – the insider threat. Historically, protecting an organization was as simple as keeping cabinets and doors locked, providing access to only those who had a key. Security guards and access badges were once enough to protect sensitive and proprietary information. Changes in technology and business have opened doors to new threats in regards to security measures. Throughout history, securing the perimeter was enough to protect an organization and its customers. China secured itself from threats from the north by building the Great Wall. Forts were built across North America to protect goods and people. Organizations have used guards, fences, cameras, and locks to stay secure from unwanted access. With the invention of the

computer and other similar technologies, new security devices (badges, scanners, etc.) have been created to prevent trespassing. Computer technology continued to progress networks were simply protected by requiring login and passwords, blocking ports, and encrypting data. Again, all of these measures were designed to keep intruders out. The business and communication world has changed drastically with not only the growth of computer technology and the Internet, but this change has also brought on the ability to globalize business. Intentional or not, both technology and globalization have led to a new threat – those who are on the inside, known as the Insider Threat.

Several organizations have defined what is meant by the insider threat. The National Infrastructure Advisory Council (NIAC) has studied and defined an insider threat as, "…one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, service, products, or facilities with the intent to cause harm." (Noonan & Archuleta, 2008 p 5) Cisco Systems has defined the insider as, "…often characterized as an employee performing malicious behavior – through sabotage, stealing data or physical devices, or purposely leaking confidential information." (Cisco, 2008, p 1) The Cisco study goes on to say, "However, organizations need to be aware that the insider threat is not just the rogue employee, but rather every employee and every device that stores information. Employees are insider threats if they speak loudly about confidential project plans while on the phone at the airport. A lost laptop containing company information can become an insider threat if it is recovered by an outsider with malicious intent." (Cisco, 2008, p 1) The insider is not just an employee or partner intentionally planning to harm an organization, but also includes an employee or partner's everyday actions that can innocently harm or destroy an organization.

Innocent misusing a network can have severe effects on an organization. Laws and regulations have been established to protect those who may be compromised. Punishments to an organization can be steep. In 2006, Electronic Registry Systems (ERS) was a victim of data theft. 63,000 patients were affected by the loss of two computers – one laptop and one desktop. This breach of HIPAA regulations meant a $15.75 million fine plus the cost of data and credit monitoring for all patients affected by this loss. A loss of credibility and reputation was also felt by Electronic Registry System. (Kondrop, 2011) UBS PaineWebber was attacked intentionally by an employee. The employee, having access to the internal network, planted a logic bomb that shut down 2,000 servers. This outage kept UBS PaineWebber employees from being able to make trades for weeks – this being a very detrimental shutdown for UBS PaineWebber being a financial institution. In order to bring the company back online and back to business cost UBS PaineWebber $3.1 million. Figures have not been made available as to how much business was lost while out of commission in addition to the $3.1 million repairing server capabilities. (Linux.com Editorial Staff, 2011)

Realizing that with the changes in business and technology, information specialists now agree that an insider can pose as great of a threat to an organization as an outsider, possibly greater. New measures need to be taken in order to mitigate the risk against the insider threat. Many case studies exist showing this to be true. Recent findings show that currently used security measures by information technology professionals is not enough to protect information and data from this new threat growing due to changes in technologies and globalization – the insider attack. An important step to take towards securing an organization is to perform research and know your own insider. Education and awareness will prove to be a huge factor in protection, and just as important is enforcement.

Chapter 2 – The Real Threat

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it is money wasted, because none of these measures address the weakest link in the security chain."

-Kevin Mitnick

"If ignorant of both your enemy and yourself, you are certain to be in peril…"

-Sun Tzu

There is no denying that the insider threat is a real one in the Information Technology field. More and more data has been recorded and many have studied and addressed the issue of the insider and why it should no longer be ignored. The greatest debate remains which threat should be defended against most – from the inside or the outside. Best practices have been created and organizations are required to follow laws and regulations. These laws and regulations focus on protection from the outsider, and fail to address how to protect from the inside. Professionals follow these recommended practices and successfully thwart attacks from outsiders. What happens when the attack comes intentionally, or even accidentally, from an insider's actions? The same penalties apply according to these laws and regulations – as a data breach has occurred. To protect against insider attacks an understanding of best practices is necessary to identify where the strengths and weaknesses are in each organization's security

architectures. Once that knowledge is discovered, a focus needs to be set on including the insider and the threat that comes along with it into the current security architectures.

2.1 - Current Best Practice

Best practices have been used throughout history to protect a business or organization. Most organizations have designated plans on how to protect themselves and their consumers from wrong-doers. The most basic form of security is physical and environmental controls. Physical and environmental security controls include simple acts, such a locking doors and cabinets, and can become complex, involving guards, fences, access control points, as well as temperature controls. Overall, physical security is used successfully as throughout time a main focus was to keep the intruder out. Currently, physical security has been included as a small part of information security. The overall goal of information security is to protect data and information. With the growth of technology and the expansion of business world-wide several organizations have gathered and developed standards of best practices for organizations to follow to help ensure protection levels are the best they can be.

Security professionals follow guidelines outlined in the standard ISO/IEC 27002. This standard was developed in the United States and is maintained by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). Several other countries have also developed similar equivalent standards for their specific country or region. (See Appendix A for a listing of Countries and their standards) Using the CIA triad – confidentiality, integrity, and availability (a model created to provide a basic framework in security policy development), ISO/IEC 27002 makes recommendations regarding controls and how they should be implemented. Made up of eleven main sections, ISO/IEC 27002 focuses on providing guidelines for risk management techniques by remaining neutral regarding which

models to use. Important guidelines to follow include: policy, organizing information security, asset management, human resources security, physical and environmental security, communication and operations, access controls, information systems acquisition/development/maintenance, incident handling, business continuity management, and compliance. ("Cyber-security standards", n.d.)

HIPAA (Health Insurance Portability and Accountability Act) is a standard originally released in 1996 to provide national standards for protecting Americans personal information with the newer electronic record keeping by employers, health care providers, and health care insurance providers. The Gramm-Leach-Bliley Act outlines how financial institutions should report their privacy practices to customers regarding how they are keeping private data safe. The Sarbanes-Oxley Act (SOX) is a federally mandated U.S. law outlining standards for financial reporting to consumers and partners. By complying with SOX, businesses can provide security and confidence to their investors. These laws and regulations in the United States have similar counterparts in other countries (see Appendix A). All of these, in all countries, provide standard guidelines for all organizations to follow in order to provide confidentiality, integrity, and availability to its consumers. These all lead to best practices now followed by organizations.

Many models and fundamentals of information security follow common basic recommended practices. The majority, no matter how detailed, follows risk management and technology based protection methods. Common beliefs encompass policy development, awareness and training, assessment tracking, business continuity and network security tools. Risk assessments are recommended in order to identify assets and data and the threat level each could be subjected to. Policies are created to define threats and vulnerabilities and the responsibilities of organizations in protecting against named threats and vulnerabilities. Most

often, what are relied on to assist policy are tools of network security. These tools are used to help enforce policy. Firewalls are used for perimeter security. Encryption is used to protect data in storage and during transfer over internal and external networks. Anti-virus software is used to stop known attacks that could harm data and the applications used. Remote authentication is used to keep unwanted users out. Organizations are finding that these tools alone are not enough. In the 2010 Annual Cyber Security Watch Survey conducted by CSO magazine, the U.S. Secret Service, the Software Engineering Institute CERT program and Deloitte's Center for Security and Privacy Solutions found that 50% of security breaches were caused by outsiders, 25% were due to insiders and the remainders of breaches (25%) were from undetermined causes. The survey also revealed that 37% of the participants recorded a greater number of security incidents compared to the prior year. Also discovered was that 51% of internal threats led to intrusions. The survey found that 53% of the network incidents were due to attacks from viruses, worms, and malicious code. Unauthorized access accounted for 35% of network attacks, 32% was due to spam and 41% was spyware. 31% of attacks were discovered from server and firewall logs, and 37% were discovered via intrusion detection systems. These network tools, even if kept up to date with current loads and patches, failed to stop attacks. These tools are used to protect the perimeter and log information; sometimes they can stop an attack in its tracks, but being perimeter tools they cannot protect from everything. (Lynn, 2011) These tools are necessary, but these tools fail to address all possibilities when considering where an attack can come from.

2.2 - Where the Best Practices Miss Out

The new world of business involves extensive networks that extend globally. Employees can be located anywhere in the world, and can be accessing an organization's network from

anywhere. Trust has always been inherent in being an employee – trust those you hire and likewise, trust those who hire you. Trust is still important. What happens when those you trust accidentally or unknowingly providing an open door to illegal access to the organization and its data? "What's required is a clear sense that today's battlefield extends deep into our daily routines. From our keyboards we are each on post in the ongoing battles of the cyber age – ready or not. And it is through our individual keyboards that many of these criminals gain access to key intellectual property. So be prepared." (Sloane, 2011, p. 1)

Several information technology organizations are in agreement and make recommendations on how to properly secure the perimeter. Organizations of all sizes follow these recommendations as they are legally required to provide confidentiality, integrity, and availability. A commonly used defense is anti-virus software. In the beginning of the business world using the Internet, anti-virus protection was enough. However, although still a necessary inclusion, it can fail to catch everything. New vulnerabilities lead to issues with policies when the operating systems and PCs are not patched, when applications are not monitored, patched and updated. Zero day threats can cause issues and until the vulnerability is discovered and a resolution is designed, and an OS, PC, or application is updated, a new threat can exist. The attack can occur unknowingly from a single click by an employee. These attacks can be defended against by using technologies such as host intrusion prevention systems (HIPS), but these attacks also have to be set up and kept up to date to prevent an unwanted intrusion. (Metzger & Shaw, 2010)

Employees don't just work at the office anymore. They can work globally and attach to the company network from anywhere – home, hotels, airports, etc. To prevent an external intrusion from occurring firewalls are used. However, when using a computer outside the

network firewall an organization needs to trust that each user connecting from the outside is fully protected, and this may not be so. Technically, there are preventions an organization can and should employ for these types of situations. Requiring laptops to use location-aware firewall software will help – these use HIPS technology to help block suspicious activity. A gateway firewall is still needed on the organization's network being accessed. Again, keeping up to date on Operating Systems patches can keep the operating system and other endpoints on the network safe from possible infections. Keeping PCs patched as well, again, will help protect against undesired infection from the outside. Network Access Control will help keep updates current. Data encryption helps as well in the case that access is successful due to a hole being found, an infected endpoint spreading a worm, or even lost equipment. Application control can be used to keep known vulnerabilities to malware attacks by keeping known applications from being on user's PCs or other endpoints on the network. Some of these applications include instant messaging, social networking sites, voice over IP, games, etc. (Metzger & Shaw, 2010)

These tools, HIPS, NAC, application control, and anti-virus software aren't, and can't, always be at their best recommended settings. Several issues prevent this such as time for updating as well as possible issues with how day to day job functions need to occur on a network. Employees, whether working in the office or outside use the web for work and personal reasons. It is almost impossible to guarantee each and every person connecting via an outside endpoint is updated and using the proper security settings and recommendations that are set for the organization's network. Human error is difficult to prevent. Data encryption can be used to help in instances such as a lost or stolen laptop. Data encryption can keep unwanted access to the data by the wrong hands; however due to laws requiring those who may be at risk to losing sensitive data be notified as soon as possible, can cost an organization thousands of

dollars. The cost, per a 2009 study, included forensics, data breach, lost intellectual property, lost productivity, legal, consulting and regulatory expenses, and averaged $49,246. Dependent upon what is lost the cost could range much higher. (Metzger & Shaw, 2010, p. 6) Another human error often experienced is misdirected email. Mistyping an address or selecting the incorrect address could lead to an accidental loss of confidential data. Again, data encryption can be used, as well as loss prevention software, but the laws and regulations still apply and neither encryption nor software can stop the intentional, or unintentional, loss of confidential data by the employee. Keeping human error in mind, endpoint security is critical in keeping data integrity and confidentiality. Table one provides questions to be considered when designing an organization's security architecture. Many of the questions listed in table 1 could be answered by many information specialists in negative ways.

Table 1

Evaluating endpoint protection: Seven questions to ask

- How do you protect users from malicious websites when they are out of the office and surfing the internet?
- How does your current solution protect you against unknown threats not covered by the latest protection update?
- How concerned are you about the lag between updates from your security vendor?
- How do you mange updating protection across your organization?
- How many of your users have installed unauthorized applications such as VoIP, IM, P2P or games?
- How do you ensure employees aren't saving confidential information to removable storage devices?
- Are you able to check that all computers that connect to your network have their anti-virus and firewall turned on and Windows Update enabled?

Note. From Eight threats your anti-virus won't stop (Metzger & Shaw, 2010)

Questions five through seven are pertinent when considering your security against the insider. These three questions are difficult to prevent using many current intrusion detection and prevention methods used by specialists today. Without these methods an organization would be non-compliant and susceptible to large amounts of damages. However, these methods miss out

on some important aspects of data and information security. Knowing it is impossible to prevent all losses and intrusions could more be done with the current best practices to better secure the information? When employing security practices, and knowing the changes in business operations and technological advances today, a user, any user, can be your weakest link.

Understanding threats is the first step. The lengths an organization should go to are dependent on the criticalness of the location to the organization's overall physical security. Using the internet the next point of security considered is controlling access to the Internet. Keeping control of who has access to the internal network from inside and out, and who has access to the external network from the inside is considered. Firewalls are commonly used for this purpose. Firewalls are employed at several points in the network – from the main access point to individual workstations. Also commonly used to control access are usernames and passwords. Employees are very familiar with having to use them and organizations can place password requirements such as password length and character usage, and password expiration timeframes. These requirements do not always ensure the users will steer clear of using obvious information in order to help keep passwords remembered easily. It also does not keep users from sharing password information with others. In addition to usernames and passwords, access control lists are also used as another defense in keeping unwanted users out.

When access is attempted how does an organization keep unwanted users out? Authentication and encryption are used in addition to access control lists (ACLs) and usernames and passwords. Authentication is used when controlling access to network devices. Access via authentication can be completed by considering who has access, and at what level can this access be granted. Can the user access at all, at a read-only level, or does the user have full rights to access, read, and change the data accessed? The types of authentication methods used are

dependent on the organization and the number of devices and users involved. In addition to username and passwords, some protocols commonly used by organizations for authentications purposes include: CHAP, RADIUS, TACACS+, and Kerberos. These protocols not only assist in authentication, but provide encryption methods as well. Encryption is an important consideration as if unexpectedly accessed encrypted data is not readily readable. Cipher text methods (DES, 3DES, AES, RC4) and Hash methods (MD5 and SHA) are employed to keep data safe from unwanted access. All of these methods, overall, protect an organization's perimeter. (Leidigh, 2005)

In the end, no matter the method and protocols chosen by an organization, policies should also be designed to enforce the proper usage of these tools. "The following would typically be part of an enterprise network security policy:

- Firewalls at all public-private network transit points.
- Version controlled and centrally deployed firewall rule sets.
- External resources placed in dual firewall, DMZ protected networks.
- All network hosts lock down unneeded network ports, turn off unneeded services.
- All network hosts include centrally managed anti-virus software.
- All network hosts utilize central security updates.
- Secure central authentication such as RADIUS, Windows/Kerberos/Active Directory.
- Centrally managed user management with password policy (i.e. must change every 3 months and must be a "secure password").
- Proactive network scanning for new hosts, or out of date systems
- Network monitoring for suspicious behavior

- Incident response mechanisms (policies, manual, automated, etc.)" (Leidigh, 2005, p. 13)

Keeping in mind the above mentioned policy inclusions, depending on an organizations current policy set, the size of the organization, risk analysis and cost impacts are necessary considerations to creating a successful security policy. Completing a system analysis and documenting the critical and non-critical systems involved is a good starting point, even if only for review.

How many employees truly understand the ramifications of their actions? Many may, but is security always in the back of an employee's mind during daily work activities? Many employees trust that the organization's information security team has fully protected the network and there is nothing to be concerned with. A survey was performed by the research firm InsightExpress on behalf of Cisco to identify the concerns organizations should consider about the insider threat. Cisco chose to survey to show that, "…despite the security policies, procedures, and tools currently in place, employees around the world are engaging in risky behaviors that put corporate and personal data at risk. Employee behaviors included:

- Unauthorized application use: 70% of IT professionals believe the use of unauthorized programs resulted in as many as half of their company's data loss incidents.
- Misuse of corporate computers: 44% of employees share work devices with others without supervision.
- Unauthorized physical and network access: 39% of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility.

- Remote worker security: 46% of employees admitted to transferring files between work and personal computers when working from home.
- Misuse of passwords: 18% of employees share passwords with co-workers. That rate jumps to 25% in China, India, and Italy."

(Cisco, 2008, p. 1)

This survey was conducted in ten countries selected because of differences in social and business cultures. Surveys were collected from 2,000 respondents made up of 100 end users and 100 IT professionals in each country. (Cisco, 2008, p. 2) This survey, although considering the population of the global business world is a good representation of how the new business world is facing this new threat – the insider attack.

Being a global business world, employees communicate and work together from many different points on the globe. Technologies such as wireless devices have provided an advantage in this way to organizations and employees alike. Data being stored on a network is now more at risk as this makes it more accessible than ever. (Cisco, 2008) This data is moved and shared at significant rates, leading to greater risks of compromised data. Policies are designed to help prevent this; however employee behavior can now open doors to additional risks and vulnerabilities. This survey demonstrates how behavior needs to be integrated into the security culture.

Organizations that operate globally should consider that not all users' behavior will reflect equally. Not only do employees in different positions hold different information technology knowledge, but also different parts of the world hold different cultural and ethical beliefs. A successful security policy needs to make room for these differences. The survey conducted by InsightExpress identified and demonstrated this factor.

- China has such a high level of information technology abuse that IT decision makers audit computers for unauthorized content.
- In Japan, 65 percent of end users do not adhere to the corporate IT policy all of the time and the research indicate that end-user abuse of information technology is increasing.
- End users in India tend to use email and instant messaging for personal use and change IT security settings on business computers so they can view unauthorized websites.
- Employees in Brazil use business computers for personal communications and for activities such as downloading music.
- End users in France have the lowest rate of IT policy compliance of all the countries surveyed, with only 16 percent of employees claiming that they adhere to security policies all the time. (Cisco, 2008, p. 2)

Employee behavior should be considered as well as management awareness. "In China, IT managers confront employees directly for not adhering to security policies. IT professionals in India have a low awareness of the extent to which security is being compromised by employees, with less than half believing that end users are using non-IT programs and applications on their company computers. Brazil showed the greatest alignment between employee abuse of IT and IT decision-maker perceptions of employee behavior, with IT decision makers evaluating and updating corporate policies more frequently than any of the other countries surveyed." (Cisco, 2008, p. 2)

The survey revealed how organizations need to understand employee behavior globally in order to impact the effectiveness of policy design and enforcement considerations. Several

"risky" behaviors were revealed including unauthorized application use, misuse of corporate computers, unauthorized physical and network access, remote worker security, and misuse of username/passwords and login/logout procedures. The following table provides details regarding what the study found with unauthorized application usage by employees. "These applications pose a high risk for data loss by an employee or data theft by a hacker because they are often unmonitored and do not use corporate security standards. Employees also risk infection from malicious sites." (Cisco, 2008, p. 3) The unauthorized application uses listed in table 2 lead to the misuse of corporate computers.

Table 2:

Unauthorized application use

- 78 percent of employees accessed personal email from business computers. This number is approximately double the level of authorized use.
- 63 percent of employees admit to using a work computer for personal use every day, and 83 percent admit to using a work computer for personal use at least sometimes.
- 70 percent of IT professionals believe the use of unauthorized programs resulted in as many as half of their companies' data loss incidents. This belief was most common in the United States (74 percent), Brazil (75 percent), and India (79 percent).

Note. From Cisco: Data leakage worldwide (Cisco, 2008, p. 3)

Employees alter security settings and share devices and sensitive information as well in order to, "…download music, shop online, pay bills, and in some cases, engage in online gambling and pornography." (Cisco, 2008, p. 3) Sensitive information was shared with friends, family, or even strangers by 25% of the employees surveyed. Half of the employees surveyed shared work devices with people outside the company. Table 3 provides findings from the Cisco study regarding global unauthorized usage habits of employees.

Table 3

Unauthorized use:

• Bypass corporate policy and IT security settings

– China: 42 percent

– Brazil: 26 percent

– India: 20 percent

• Share sensitive corporate information outside the company

– Brazil: 47 percent

– India: 27 percent

– The United Kingdom: 26 percent

– Italy: 22 percent

– Germany: 24 percent

• Share work devices with non-employees without supervision

– China: 43 percent

– India: 28 percent

Overall: 44 percent (32 percent of respondents shared work devices with co-workers, and 19 percent shared work devices with non-employee family and friends)

Note. From Cisco: Data leakage worldwide. (Cisco, 2008, p. 4)

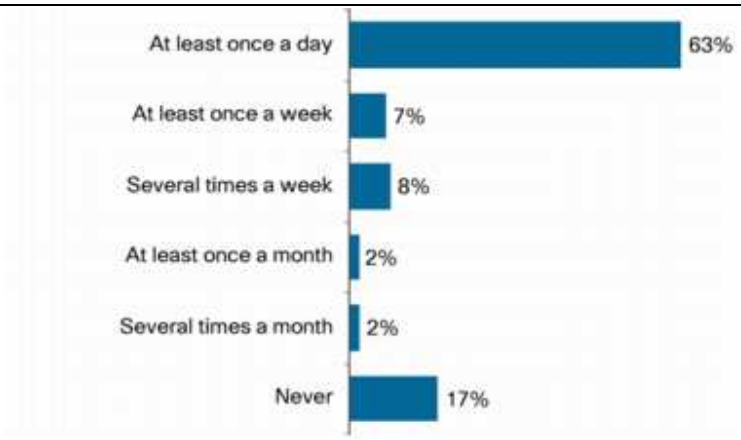


Figure 1: Frequency of Personal Use

(Cisco, 2008, p. 4)

The findings regarding remote worker security and the misuse of passwords and login/logout procedures are showing in table 4.

Table 4

Remote worker security

• 46 percent of employees admitted to transferring files between work and personal computers when working from home.

• More than 75 percent of employees do not use a privacy guard when working remotely in a public place. This number is much higher in Brazil, China, and India-countries that have the most reckless behavior.

• 68 percent of people do not think about speaking softly on the phone when they are in public places outside of the office.

• 13 percent of those who work from home admit that they cannot connect to their corporate networks, so they send business email to customers, partners, and co-workers via their personal email.

Note. From Cisco: Data leakage worldwide (Cisco, 2008, p. 6)

The research performed by Cisco also found the following misuse of passwords and login/logout procedures and this is shared in Table 5.

Table 5

Misuse of password/login/logout procedures

• 28 percent of employees in China store login and password information for personal financial accounts on their work devices.

• 18 percent of employees share passwords with co-workers, and that rate jumps to 25 percent in China, India, and Italy.

• 10 percent of employees in India, the United Kingdom, and Italy keep written notes of login information and passwords on their desk at work, leaving sensitive data accessible if the machine is stolen even if the computer is logged off.

• 5 percent of employees in the United Kingdom and France leave passwords to personal and financial accounts printed on their desks at work, so their information can be stolen with any other computer even if their work computer is safeguarded.

Note. From Cisco: Data leakage worldwide. (Cisco, 2008, p. 6)

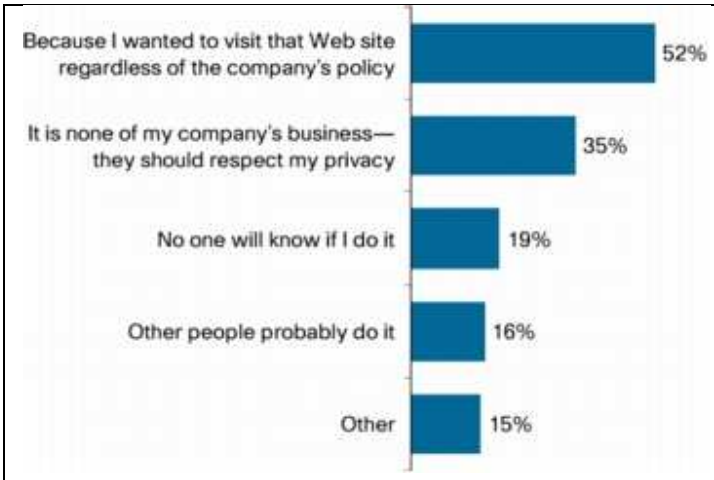


Figure 2: Reasons for altering security settings

Note: From Cisco: Data Leakage Worldwide (Cisco, 2008, p. 7)

The survey conducted by Cisco went beyond demonstrating misuse and also demonstrated why employees fail to comply with policy and fail to help keep security practices secure. Reasons given by employees were many. With the stress of today's business world, 44% replied that they, "…needed to bounce ideas off of people." 30% replied that they, "…needed to vent," and 29% responded, "…didn't see anything wrong with it." Some other reasons and responses are in figure 2.

Policies are created and technology is purchased and employed to protect critical data and information. The old standards of inputting rules and regulations into the latest technology will not successfully defend against all newly evolving threats. Recently, Sophos published the Security Threat Report Mid-Year 2011. In this report, Sophos reports seeing 150,000 malware samples every day – a 60% increase comparatively to 2010. Also noted, is 19,000 new malicious URLs each day in the first half of 2011 – 80% of those URLS being legitimate websites that were hacked or compromised. (Sophos, 2011) Some more findings by Sophos:

- 59% decline in email uses among 12 -17 year olds and a 34% decline for 25-34 year olds. The reason, Facebook, texting, and tweeting are now preferred communication methods for these age groups.
- The FBI estimates that nearly a million people were tricked into purchasing fraudulent software. The price ranges from $50 to $130 netting this cybergang $72,000,000.
- 89% of organizations have established an acceptable use policy, but only 69% of these organizations have specific policies for company-owned mobile device users.
- A click jacking scam has infiltrated social websites. Known as "Chocolate Rain," 68,593,657 people viewed this on YouTube – if receiving this link via a social site such as Facebook, a person may have been compromised.

(Sophos, 2011)

Malware is a giant threat to today's networks. This quickly growing threat is spread via links on the web, via operating systems, and software used on desktops and laptops, and via emails and attachments. Many Internet users today don't realize that visiting legitimate websites has the potential of spreading infection. Also growing is fake anti-virus security software, known as rogue ware or scare ware. How many want to believe that the advertised software is actually an attack? Sophos released where this malware is often found infecting systems and is shared in table 6.

Table 6

Top 10 countries hosting malware (via infected pages) January 1- June 22, 2011

- Russian Federation 13.06%
- Germany 7.88%
- France 7.06%
- China 4.63%
- Poland 2.91%
- United States 37.9%
- United Kingdom 2.67%
- Ukraine 2.61%
- Netherlands 2.4%
- Czech Republic 1.74%
- TOTAL: 82.86%
- Other 17.14%

Note. From Sophos security threat report mid-year 2011

(Sophos, 2011, p. 7)

These attacks are successful due to their social engineering abilities. Search engines are gaining popularity by users and cybercriminals. Knowing how search engines are relied on by all Internet users, search engines such as Google, Bing, and Yahoo are often compromised to draw in victims. Of course, the traditional Trojan, worm and virus continue to be a threat. To prevent these intrusions it is recommended to screen web use with protection technology, monitoring tools, antivirus software, check web browser settings, and keep up on patches and fixes. Also recommended is to educate those who may be tempted against protection about the value of the protection. (Sophos, 2011)

Mobile devices are proving to be a real threat to the organization's network – a threat that has not, historically, been included in many organization's acceptable use policies. Mobile devices have become, "PCs in your pocket…because they run operating system software that provides access to the web." (Sophos, 2011) As reported, 85% of organizations have established acceptable use policies, but only 69% of those have policies regarding company-owned mobile devices, and only 31% address acceptable use regarding employee-owned mobile devices. Mobile devices are used for the same purposes as the desktop PC or laptop – access to the Internet. From these mobile devices, as well as from company provided PCs and laptops, users are also accessing social networking sites such as Facebook, Twitter, and Google+. Through these social networking sites attackers are able to continue with the popular social engineering attacks. Many organizations have established acceptable use policies, but these policies usually allow personal use of the Internet whether throughout the day and/or during breaks. Accessing these sites via an employer provided connection opens up the organization's network to potentially harmful actions. In some cases, if not protected properly on the perimeter, an organization could face an attack via a user connected remotely.

Common, older vulnerabilities still exist even in the midst of the growth of social networking sites. Email is still in use and attachments are sent from network to network. Spam and spear phishing are still popular scams used to transport malware and steal sensitive information. Organizations can use anti-spam software to protect against some of the threat, but the vulnerabilities still exist due to social engineering techniques. No matter where an employee is located, spam can reach them, it's a global threat. Table 7 shows an example of this international threat. (Sophos, 2011)

Table 7

Spam by Continent January- June 2011

- Asia 39.79%
- Europe 28.90%
- North America 16.30%
- South America 11.83%
- Africa 2.50%
- Oceania 0.69%
- Antarctica 0.00%

Note. From Sophos security threat report mid-year 2011 (Sophos, 2011)

All of these threats are mitigated using common techniques. Anti-virus software can be used, monitoring for malware at the gateway level, using web filtering, anti-spam software, encryption, patching, vulnerability monitoring and testing, and rules regarding devices and network control all help an organization protect the inside from the outside. A common factor still remains – the insider.

2.3 - Why to protect on the Inside and the Effectiveness of Current Security Architecture

The study conducted by InsightExpress also opened up the door and showed how, "In the hands of uninformed, careless, or disgruntled employees, every device that accesses the network or stores data is a potential risk to intellectual property or sensitive customer data." (Cisco, 2008,

p. 1) IT professionals have focused on spending time and money on protecting reactively via technological methods. Of the IT professionals surveyed globally:

- -33% were most concerned about data being lost or stolen through USB devices.
- -39% were more concerned about the threat from their own employees than the threat from outside hackers.
- -27% admitted they did not know the trends of data loss incidents over the past few years. (Cisco, 2008, p. 1)

The threat from the outside is still very much real. Employee behavior internally on a network mixed with technology is also proving to be damaging and can open doors to the insider for an outsider. Educating IT professionals on the seriousness of this new threat and educating employees on how their behavior could negatively impact an organization or its customers can only help strengthen the overall security structure.

The "insider" is defined differently depending on how an organization may want to address the issue. There are two basic opinions on who the insider is. Some organizations believe the insider to be an employee intent on maliciously attacking the organization. This is an older version of who the insider historically was. With recent technological and business changes, IT professionals should consider a second angle regarding who the insider truly is. The insider is, "…not just the rogue employee, but rather every employee and every device that stores information." (Cisco, 2008, p. 1) The malicious employee is dangerous but the accidental behavior is more commonly harmful. The malicious employee sets out to cause harm for many reasons, all reasons ultimately being a personal reason. When considering confidentiality, integrity, and accountability, IT professionals should consider the "accidental" insiders and

whether or not the organization's culture supports this negligent behavior or whether it proactively helps prevent negligent behavior.

Do employees truly understand the possible consequences of their actions on the network? Most all employees have heard of the dangers, but how many believe it couldn't happen to, or because of, them? The InsightExpress study found that, "…a lack of awareness, a lack of diligence, and defiance within company ranks pose a significant insider threat to data." (Cisco, 2008, p. 2) A common assumption among IT professionals is that employees truly understand how a computer and a network work and what appropriate activity is as opposed to inappropriate activity. Many employees use computers and the Internet at home, not just in the workplace. Neither having a PC or laptop for daily job functions and/or a PC or laptop at home for personal use, guarantees an employee is aware of threats and vulnerabilities. Of the IT professionals surveyed, 43% said they are not educating employees well enough and 19% said they have not communicated the security policy to employees well enough. (Cisco, 2008, p. 2) Expecting professionalism and common sense cannot be relied on. Many times people are overheard sharing sensitive information about themselves, their employer, or even a customer. How many actually lock up or log off of their PC or laptop when walking away? Passwords are used several times a day to access sensitive data – how many people still record these passwords and leave them in an easily targeted location? Many employees today carry a laptop and use mobile phone to complete daily job functions. How many laptops and mobile devices have been lost or stolen?

- Nine percent of employees reported that they have lost or had their corporate device stolen.
- Of those employees who reported loss or theft of a corporate device, 26 percent experienced more than one incident in the past year.

- The top concern among IT professionals regarding data leakage was the use of USB devices, with 33 percent sharing this concern globally. The number-two concern was email; 24 percent of global IT respondents shared this view.
- When asked why their employees are less diligent in safeguarding intellectual property, 48 percent of IT professionals responded that employees are dealing with more information than ever before, and 43 percent listed a growing apathy toward security stemming from the quickening pace of employees' jobs.

(Cisco, 2008, p. 3)

Why this lack of awareness by users and how their activity could be potentially harmful, and why this lack of awareness by IT professionals as to the actual level of knowledge by employees? The perimeter has always been the focus, but now there are new doors and windows discovered everyday by hackers. The time has come to, "…contemplate the role of existing norms in influencing what should be moving forward…to include how, for example, political, cultural, and economic systems shape and interact with technical systems and what this suggests for information assurance and security ethics." In the book, Information Assurance and Security Ethics in Complex Systems, several technology specialists included articles regarding ethics, culture, and the need to change because of the changes information technology has brought in to the world. The idea portrayed by the authors is that ethics are learned and built by those in society. Ethics and laws are a required part of having a secure and productive organization. "Being ethical is not just a matter of what one (individual or organization) does, but who or what they are. This "take" is a sense of the cultures and values that guide them. It emerges from the people in the organization and what they sense of the culture and values that guide them." (Dark, 2011, p. 47) The overall theme is that ethics are cultural (organizationally and by country) as

well as created and learned by the society that creates the ethics followed. There are the ethical standards of an organization and the ethical standards of the world. These standards have reached a point where inspection and reinvention are needed. "Organizations crossing boundaries must not only be sensitive to local laws, but must institute policies that will allow them to successfully interface with local populations…organizations will be able to better formulate information security polices given enhanced understanding of differences in cultural norms specific to information security." (Dark, 2011, p. 56) This same article goes on to discuss how there are guidelines and templates made available to organizations by groups such as the SANS Institute and ISO 27002 – but neither of these addresses the differences global employment brings to organizational culture. One strongly held belief is that organizational culture can influence, positively or negatively, the ethical behavior of employees. Other factors to consider regarding ethical behavior include economic and political climates. It is suggested that, "as researchers investigate the effectiveness of information security policy, [look] at the many factors that can influence a person's interpretation, including user expectations, user experiences, and culture." (Dark, 2011, p. 73)

Distributing user acceptance policies to employees has been a standard amongst the business community. The ideology now is that it is time be become proactive. Currently used technological tools are primarily reactive. A firewall is used to control incoming and outgoing traffic, as well as routers. Switches can be used to isolate specific areas of access from those who should not have access. Intrusion Detection Systems can be put in place to monitor the network and report suspicious activity. Intrusion Protection Systems can help monitor the network and control access to the network. These, however, are mostly reactive. Each device needs to be programmed to look for specific information. Once the information is received the

task is then to identify the perpetrator. Could this perpetrator have been identified before the attack?

An insider could have intentionally behaved maliciously, or could have taken actions that led to an accidental intrusion. The debate is whether or not an insider could be identified prior to an incident. Since there are essentially two types of insiders (the malicious insider and the accidental insider) considerations in security need to be addressed from two different angles. The malicious insider is the insider thought of most often. "Employees with a spiteful agenda and a profit motive can use their insider status to engage in activities that cause even greater financial loss than external threats." (Cisco, 2008, p. 3) Also referred to as disgruntled employees, the malicious insider has an advantage – already being on the inside. Knowing the internal organizational network structure, and depending on what access levels this employee may have, changes could be made in favor of the malicious insider allowing damage to be done. In the 2008 Cisco study performed by InsightExpress, 20% of the IT professionals surveyed said, "…disgruntled employees were their biggest concern in the insider threat arenas." (Cisco, 2008, p. 3) Access controls are the most commonly used control in regards to insider access levels, but this is proving to no longer be enough. "What stops someone who has legitimate access to a file from emailing it to someone who should not have access? Not only do you have to strictly control access, you must also monitor it." (Cole, 2011, p. 4)

The accidental insider is any employee who, as discussed, accidentally opens a door for attack via social engineering, malware, or a lack of understanding the reasons behind specific security policies that have been set. The fact that the insider is now as great a threat as the outsider, IT professionals believe this threat needs attention and addressing. Current security architectures do a good job of protecting organizations data from the outsider. An employee

does not need to be a technical expert to cause damage. The information is available to anyone, and with a minimal amount of privileges and/or the knowledge of someone with necessary privileges, could provide a large enough crack in the foundation for an insider to squeeze through. Too much permission or too much freedom or the network could allow the accidental insider to create a crack big enough for the latest adware, malware, virus, work, or Trojan to find its way in. Research has been done to demonstrate indicators of an insider. This information can be used to add to the current practices used to develop a new strategy.

The accidental insider is easier to identify and address than the malicious insider. The accidental insider can be any employee, anywhere, at any time. The malicious insider takes more monitoring to identify. Both types of insider threats can be addressed with educating the entire organization regarding both, how to be safe, what to look for, and how to handle an insider threat if suspected. There is an inherent trust between employer and employee, and between co-workers and peers. Educating that trust is still pertinent but also educating to keep an eye out for suspicious activity can lead to a change in the organizational culture. Being a part of a global business world also leaves desire for educating all employees about each other culturally and ethically. Once understood, the organizational culture needs to be a part of daily business life for all employees no matter what region the employee works from. Current practices need to be better, and then enhanced with additional educational measures.

Many professionals have written and recommended new actions to follow to protect against the insider. One common theme for all recommendations is education. In his book, "Enemy at the Water Cooler," Brian T. Contos begins chapter 3 by saying, "There is no piece of technology that once deployed will solve all of an organization's security problems. Security encompasses people, process, and technology. By finding the right combination of these, an

organization can successfully reduce risk." This point is true – technology is not the only factor to be considered – policy should be strengthened and people's actions, morals, and beliefs need to be addressed. Enterprise Security Management is a complex venture that should be taken in today's business climate. Contos shares that security management should still encompass current recommended practices (event collection, asset relevance, active and watch lists, data content, anomaly detection, false-positive reduction, real-time analysis, forensic analysis, and remediation, just to name a few, as well as reducing risk, reducing response time, better data and reporting, and actionable information, repeatable and measurable incident management, remaining compliant and detecting and responding to attacks as a Return on Security Investments (ROSI). This can all be done by the organization itself, outsourced, or even co-sourced. (Contos, 2006, p. 97) There are known holes in making the route chosen to work successfully. Recent research has found that, "…a common factor in insider espionage is that in most cases damage could have been prevented by timely and effective action to address the anger, pain anxiety, or psychological impairment of perpetrators, who exhibited signs of vulnerability or risk well in advance of the crime of abuse." (Dark, 2011, p. 135) This remains one focus of research – how to identify attack related behaviors before the attack occurs.

Another focus in research has pointed to the reasons current practices are no longer as effective as in the past regarding the average employee – overall, the focus has become one of policy effectiveness. Cisco's survey conducted by InsightExpress demonstrated that the greatest concern is, "…the importance of a comprehensive security policy approach that includes education and accountability," (Cisco Systems, 2008, p. 2) and without a renewed focus on education and accountability the current architectures of security will continue to fail regarding the insider threat. The methods currently used fail to appropriately communicate security

policies to employees. Keeping in mind that many large organizations now employ globally, the global environment should be considered in developing and communicating security policies. In the Cisco study, 75% of the companies surveyed had security policies. Of the employees surveyed 40% did not know the policies existed and 20% of the IT professionals were unaware of the existing policies.

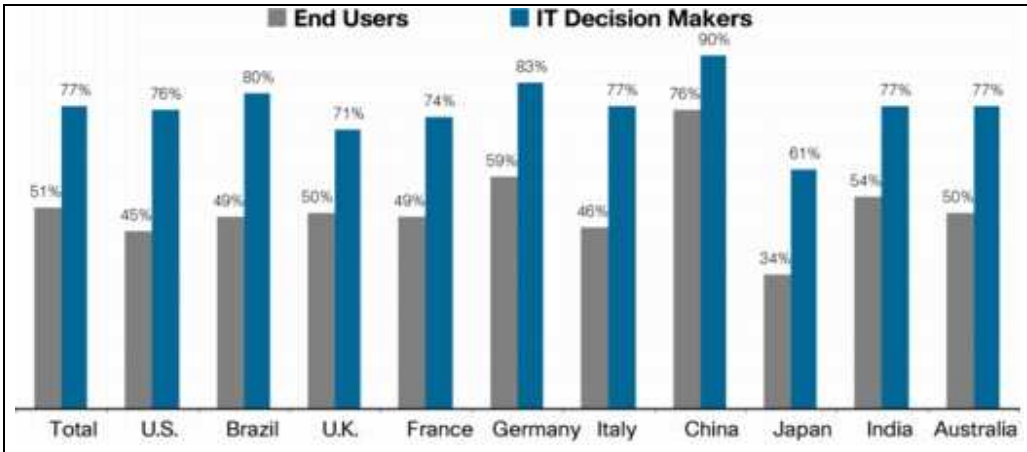


Figure 3 Disconnect Between End User and IT Security Policy Awareness

Note. From Cisco Data leakage worldwide (Cisco Systems, 2008, p. 3)

Figure 3 demonstrates that there is a major disconnect between policy makers and the employees who are to follow policy. The study found reasons for this disconnect is due to a lack of communication:

- 11 percent of employees say that security policies were never communicated to them or that they were never educated about the policy.
- Europe had the highest prevalence of this belief, where the United Kingdome (25 percent) and France (20 percent) far exceed the global average.

- Germany also has a high percentage of employees who claim that IT never communicates security policies to them (16 percent).

(Cisco Systems, 2008, p. 3)

This lack of communication occurs in several instances:

- 56 percent of IT professionals report that security policies are communicated to new hires during orientation, yet only 32 percent of employees say they were educated.
- In Japan, 66 percent of IT professionals claim they communicate security policies to every new hire, but only 35 percent of employees say they received that information.
- The United States had an even larger gap (42 percent) with 70 percent of IT professionals claiming that security policies are communicated to new hires and only 28 percent of the American employees saying they received these briefings.

(Cisco Systems, 2008, p. 3)

Why such a large report of lack of communication was also revealed. It was found that updated security policies are often shared via email. The receipt of these emails was confirmed by 59% of employees and 68% of IT professionals, but the potential for missing or deleting this message is high due to the amount of email communication, sent and received daily. Another factor mentioned, emails don't always communicate the importance and that delivery in person is often more effective. A third finding points to a lack of compliance or enforcement of the policies. "…More than half of the employees surveyed admitted that they do not abide by their company's security policies. France featured the highest percentage (14%) of employees who admitted they adhere to policy sometimes, hardly at all, or never. India wasn't far behind, with 11% admitting that they hardly ever or never abide by corporate policies." (Cisco Systems, 2008, p. 4) Only a portion of countries have been included in table 8. The results demonstrate

the beliefs between IT professionals and employees about the current Security culture in organizations.

- Only 22 percent of IT professionals believe that security education needs to be improved. A greater number of IT professionals believe that employees are wayward because they don't understand the risks of their behavior, because security is not a top-of-mind priority, or because they simply don't care. When asked why they altered security settings on computers to view unauthorized sites, for example 52 percent simply replied that they wanted to view the site – regardless of its conflict with corporate policy.
- IT's perception of employee apathy is highest in France (57 percent), which parallels the French employee acknowledgement that they often ignore company policies.
- In China, 77 percent of IT professionals said security is not a tip-of-mind concern for employees.
- Many IT professionals (41 percent) believe that employees are willing to engage in these risky behaviors because they think that IT will solve any problems that arise as a result or that no one will know.
- The most common reason given why employees do not adhere to corporate security policies is a lack of alignment between job activities that are perceived as necessary and policy constraints. Forty-two percent of employees worldwide knowingly disregard security policies because they believe that the policies limit their ability to perform their work effectively. China (62 percent) and the United Kingdom (55 percent) featured the highest percentages of employees expressing this frustration.
- Despite the fact that employees often violate security policies, IT professionals do not confront employees very often. About three out of four respondents say they deal with

> employees who violate their company's IT policy a few times a year or less frequently. In Australia, only 10 percent of IT respondents say they confront employees once a month or more often.
>
> (Cisco Systems, 2008, p. 5-6)

Table 8

Reasons for Violating Corporate IT Policy

Reasons	Total (n=776)	US (n=76)	BRA (n=85)	FRA (n=75)	CHN (n=92)	JPN (n=61)	IND (n=77)
They do not think there is enough risk to be concerned	47%	51%	44%	41%	59%	49%	51%
They think IT is there to protect them if something goes wrong	41%	39%	36%	33%	47%	38%	52%
Security is just not top-of-mind for them	39%	34%	29%	31%	77%	25%	38%
They do not care	38%	38%	21%	57%	34%	49%	39%
They do not know about or understand the policy	34%	30%	35%	43%	45%	41%	35%
They do not know that security is a concern for IT	33%	28%	22%	24%	59%	30%	36%
They are in a hurry	25%	29%	24%	27%	17%	13%	38%
We need to create or improve our employee education and training programs	22%	21%	27%	5%	40%	30%	44%
Other	2%	1%	0%	1%	1%	2%	0%
Don't know/not sure	2%	4%	1%	3%	0%	0%	0%

Note. From Cisco: Data leakage worldwide (Cisco Systems, 2008, p. 5)

Employees will not adhere to policy when they feel it interferes with their daily work functions, or when they simply felt they had the right for personal reasons. This behavior can lead to an accidental attack mostly due to the misunderstanding of why the policy is set as it is. The insider may behave maliciously in this manner for personal reasons, many times due to anger or frustration with a co-worker or manager. IT professionals responded to the survey that they rarely confront those who may be intentionally or unintentionally breaking policy. (Cisco Systems, 2008, p. 6) Overall, the Cisco survey identified that a change in enforcement of security policies needs to change. Policies that work should be created, consequences to

violations need to be enforced, employees need to be educated as to what the policies are and the consequences of violating them, and in the end, and these consequences need to be enforced. This change will require a change in current security culture's and leadership. All of this will require time and attention by leadership.

Several Information Technology specialists have recommended models on how to incorporate the insider threat into the current best practices. In 1999, Dorothy E. Denning wrote about the growing threat of information warfare in her book titled, "Information Warfare and Security." A small section is devoted to security awareness and training discussing that a major vulnerability is people and a major point of warfare is education. Denning writes, "Security awareness and training programs can serve to inform employees about their organizations information security policy, to sensitize them to risks and potential losses, and to train them in the use of security practices and technologies…Employees can be made aware of social engineering tactics and how to detect and avoid them. System administrators can be trained in information security so that they can properly configure and monitor systems. They and other staff members can be instructed in their responsibilities regarding information security practices and incidents." (Denning, 1999, p. 382) In 1999, several practices were already in place to educate computer users. Universities were initiating programs. The University of Delaware required students to pass a test about its computer-use policy before receiving a password to access the University's network. Cornell University requires students to complete a course on the use of campus computers before receiving access to the network. Penn State University sends students caught misusing the network to a similar class about the appropriate use of computers on the University network. The University of Michigan made use of posters around campus warning students about things to be wary of using the network. Students, however, felt

the tests and campaign strategies were not enough. It was reported that much of the information was obvious and felt like a waste of time. What students felt was most effective was learning about Information Warfare. These courses taught users/students how vulnerabilities were exposed. "The lesson to be learned here is that it is not enough to tell users how to behave – they must understand and appreciate the reason behind the rules." (Denning, 1999, p. 383) Similar programs have been offered to consumers including the Australian Competition and Consumer Commission website to inform Internet users how to identify scams. The Federal Trade Commission in the United States also offers a program to educate consumers about web scams. (Denning, 1999, p. 384) However, neither of these programs is required, and it is up to the user to be motivated to use these programs for educational purposes. Most of her book addresses technological approaches to security – encryption, analysis, monitoring, cryptography, intrusion detection, and access controls. Though discussed in 1999 by Denning, the recent study performed by Cisco via InsightExpress reveals that there is still a lack of education regarding why a user's behavior could negatively impact an organization.

Another study performed in the United Kingdom by the Network Research Group also demonstrates the lack of end-user concern regarding security policy. Two questionnaires were distributed to 58 companies willing to participate. The questionnaires were distributed to gather knowledge of the IT team's belief of the infrastructure and a second to identify the user's awareness to the access to systems, company security and personal opinions. Some common IT infrastructure uses were found – all respondents used anti-virus software, maintained backups, and required the use of passwords. Only five of none administrators that completed the questionnaire claimed to have formal policies in place, and only 44% of the IT respondents had a strategy for dealing with an external attack. Only 2/3 of the companies surveyed educated

employees about security issues and this was rated by all as low priority. The results of the survey also showed that the administrators considered employee actions more of an issue than technical security issues – however, as previously stated, education and awareness were low on the list of priorities. The main reason reported by the administrators for the lack of attention was budgetary. Two-thirds of the respondents reported less than 1% of the annual budget was used for security, and no respondent claimed more than five percent of the budget allocated for security. The greatest belief of administrators as to why such a small amount was allocated to security is a lack of support from senior management- by 45% of the respondents. (Finch, Furnell, & Dowland, 2003)

The end user questionnaire revealed more details regarding password usage, 42% admitted to using personal information to create a password, but only 4 out of 50 end users admitted that they realized this made password guessing easier, while the rest felt this was not of concern. Twenty-two percent of the end user respondents admitted they would open an email attachment even if the sender was unknown. This is a large enough number to be concerned with the potentiality of an attack by infection. Both of these topics demonstrate a lack of knowledge by end users on the company's networks. Security policy was also addressed in the end user questionnaire. The questionnaire addressed whether end users were required to sign a security policy, keeping in mind that four of the surveyed companies didn't even have a security policy. Of the thirty four respondents that could have signed one that was in existence, a total of thirty-four, only six reported having signed one. Of the fifty users surveyed total, only six had actually reported being required to sign a security policy, and of those 6 only 3 referred to the policy on a regular basis. "This clearly indicates that merely having a policy and getting users to sign up to it is an inadequate means of ensuring that it will actually mean anything to them. Organizations

need to take more proactive steps, such as education and training (which the earlier administrator results acknowledged was lacking) in order to improve understanding." (Finch et al., 2003, p. 8) In this same survey, administrators and end-users were asked to rank a list of threats in order of perceived danger. A disconnect is demonstrated between administrators and end-users when considering risks in table 9.

Table 9

Comparison of administrator and user views

Threat	Admin Rank	User Rank
Employee errors in computer software/hardware use	1	4
Viruses	2	1
Employee actions that are intentionally harmful	2	2
Physical Theft (e.g. notebook theft)	4	6
Internet and Intranet connection	5	5
Harmful Intrusion from outside	6	3

Note. From Assessing IT security culture: System administrator and end-user perspectives (Finch et al., 2003, p. 9)

Administrators were more concerned about employee errors than the users, demonstrating that the users were less aware of the risks their actions could have on the network. These results demonstrate a need for awareness education. "The most significant point is that a company cannot rely on the security message to spread itself…there was clear scope for improvement of security, and associated awareness, within all of the respondent companies promoting security amongst end-users goes beyond simply having a security policy (although this is a necessary starting point). Ongoing reinforcements of the issue need to be given more attention." (Finch et al., 2003, p. 9)

2.4 - Suggestions on How to Address the Insider Threat

Professionals have focused attention on the fact that education and awareness are lacking when it comes to computer and network security just as many professionals have offered their versions of a good model to follow. Many still only offer technical solutions. A proper way to include education has not completely been included. Recommendations have been made by many, but in order to successfully implement a model, a deeper understanding of where an organization is regarding security policy and awareness is necessary. Before jumping into any specific model a holistic approach should be made by each organization to determine areas of strengths and weaknesses in the current architecture used. With the intrinsic need to rethink business security architecture, a baseline approach may need to be taken by many organizations.

In a white paper published by IDC, and sponsored by RSA, the security division of EMC, the belief that, "…organizations should look at insider risk as a holistic problem that requires a holistic solution… to identify the framework of policies, procedures, and best practices needed to effectively address the problem." (Burke & Christiansen, 2009, p. 1) This study by IDC and RSA revealed that the numbers of unintentional damaging actions are on the rise and now more threatening than those that are intentional. Research showed that organizations experienced an average of 14.4 incidents of unintentional data loss due to employee negligence over the span of twelve months – this averages at least one incident per month. Allowing users personal use of the Internet raises the vulnerability of malware and spyware attacks. Eighty percent of legitimate websites now contain malware. URL filtering can no longer keep up with this growing phenomenon. In 2009, Microsoft reported an estimate of more than one million websites being compromised each month. The global economy is also proving to impact insider threats demonstrated by the increase in internal fraud. (Burke & Christiansen, 2009, p. 1-2) See

appendix B for figures on reported internal incidents per year and incidents by country. Appendix B also includes findings of the IDC and RSA regarding the financial impact per region of the insider risks. In Table 10, the research found that the overall greatest risk to organizations is the insider also includes contractors and temporary staff, as well as internal IT administrators and technical staff.

Table 10

Insider Risks: Accidental versus Deliberate (% of Respondents)

Insider Risks: Accidental Versus Deliberate (% of Respondents)

	Total	Predominantly Deliberate	Predominately Accidental	Equal	Not sure
Contractors and temporary staff	19.5	13.3	23.3	16.7	27.3
Permanent employees	12.7	13.3	13.2	12.3	
Management/executive team	9.1	8.4	9.3	7.9	18.2
Technical staff, including IT administrators	14.1	22.9	9.3	17.5	9.1
Line-of-business staff (nontechnical)	9.1	14.5	7.9	6.1	27.3
Remote employees	13.2	8.4	13.7	17.5	
Business partners	7.7	8.4	6.2	10.5	9.1
Outsourcers	13.2	10.8	15	10.5	9.1
Other	1.4		2.2	0.9	
Valid n =	440	83	227	114	11

Note. From Insider risk management: A framework approach to internal security (Burke & Christiansen, 2009, p. 1-2)

The IDC and the RSA, after performing this current research recommends the following Framework is followed:

1. Risk assessment should be the first priority. Organizations must understand the scope of the problems and prioritize remediation through policy and procedure and identify key security controls around network, access, data, applications, and audit.

2. Review and update information security policy on an annualized basis. For the sake of auditors and regulators, thoroughly document any changes and underlying reasoning; ensure the policy clearly demonstrates enforcement of security controls, such as data and access controls, as well as monitoring and reporting capabilities; and an update the policy to include new threats such as spyware, malware, social networking, etc.

3. Educate employees on policy changes. Consider making security education a required element in annual performance reviews. Automate employee notification of violations, reiterate policy, and log all incidents.

4. Define insider threats by determining the value of customer accounts, intellectual property, confidential financial information, employee data, executive communications and other confidential information to the firm. Calculate the cost of this data and the impact if it is exposed, leaked to competitors, and/or corrupted.

5. Classify and search for all high-risk data, determine where the data is and if it is secure in its current location, and determine which individuals are accessing it and if their access is appropriate. With full consideration for avoiding disruptions to critical business practices, consider data loss prevention and other data controls to protect and enforce policy on the data itself (such as quarantining data from being emailed, deleting data from endpoints, encrypting) and not just protecting the location (e.g. laptops, PDAs, databases, file servers).

6. Audit all active internal user accounts — employees, contractors, partners, customers and other legitimate account holders. Expunge the dead accounts (up to 50-60% of accounts in poorly managed environments) and, in some cases for contractors and other semi regular workers, freeze inactive accounts.

7. Provide strong security controls for *all* your internal users (not just remote users) to access network and critical information in order to ensure that only legitimate users are accessing corporate resources. This also provides audit ability for any investigation or remediation activity following a breach.

8. Identify high-risk internal users, such as system administrators, users with access to critical business applications or customer data, job leavers, users turned down for promotion, etc., monitor and review their activity on a regular basis, such as log-in attempts, and correlate that activity. Develop and test an incident/event management plan for prompt remediation.

9. Reconcile the access privileges of all users, starting with high-risk users, for their current role and job description, and immediately revoke excessive privileges. This is especially important for contractors and temporary staff who are generally given the same access rights as permanent employees when they don't need it.

10. Implement regulatory reporting on compliance with a focus on internal security policy and meeting key performance metrics.

11. Make all these steps a continuous process with regular reports on any exceptions sent to IT, compliance officers, risk officers, HR, and senior management (Burke & Christiansen, 2009, p. 16)

IDC writes, "…organizations should adopt a framework of technologies that manage internal risks across the entire infrastructures (such as endpoints, networks, applications, databases, storage, etc). Technologies include encryption, information classification and discovery, identity management and assurance, data loss prevention, and security and event information management." (Burke & Christiansen, 2009, p. 18) Most of the recommended actions by the

IDC include best practices already in place, but an important step was added – educate employees.

Another approach suggested is a predictive model framework. This approach involves surveillance of employees to help predict an insider threat. This model addresses the insider and, "…members of an organization authorized to access its information system, data, or network with a degree of trust by the organization and who accepts a commensurate level of scrutiny by the organization to deter possible abuse of these privileges." (Greitzer et al., 2009, p. 6) Predictive modeling addresses behavior modeling and how it can be used to predict insider activity as an actual threat. The idea is that even though it is difficult to predict who will actually perform intentionally malicious acts, it can help in the monitoring and discovery of malicious and non-malicious activity. Studies have identified twelve psychosocial indicators of insider threat. (See Appendix B) This method relies on observational/management reporting relying on personnel data and judgments that are likely to be available from management and human resources staff. (Dark, 2011, p. 151) Several points are emphasized regarding this model:

- The indicators need to be empirically tested or vetted with larger samples of HR experts and managers to assess their validity, at least at a subjective level.
- The judgments based on observations will necessarily always be subjective – there is no expectation that an objective test instrument will emerge from this research.
- Nevertheless, we believe that with appropriate training, management and HR personnel would better understand the nature of the threat and the likely precursors or threat indicators that may be usefully reported to cyber security officers.
- Most importantly, the approach in predictive modeling is to proved "leads" for cyber security officers to pursue in advance of actual crimes, without which they would likely

have little or no insight with which to select higher-risk 'persons of interest" on which to focus analyses.

"For security analysis purposes, only cases where a manager is 'highly concerned' about such factors or combinations of factors would be advanced in the predictive model to raise the level of concern or risk. As the risk level increases, so too would the level of monitoring and analysis on an individual increase." (Dark, 2011, p. 150-151)

Should behavioral warning signs be addressed proactively to prevent harm to the organization? Would the collection of psychosocial data violate employee trust or legal guidelines? If behavioral data are to be monitored, what type of data should be acquired? Considering the devastating effect of a false accusation on an employee, what are the implications of the predictive approach? Due to the social and ethical issues this model brings to the surface further research and development is necessary, but the underlying ideology that an informed and enlightened organization requires some new approaches by human resources and management in order to properly maintain awareness of worker satisfaction and well-being – often a precursor to malicious behavior. (Greitzer et al., 2009, p. 17)

Others have offered suggestions on preventing and reacting to an insider attack. A model addressed, A Systems Dynamic Model, based on the malicious insider using the Tim Lloyd/Omega Case. This model is based on the idea that insider attacks occur when the insider perceives the system as being extremely vulnerable. (Melara, Sarriegui, Gonzalez, Sawicka, & Cooke, 2003, p. 8) Per the research into this model, security should not be based on implementing technical methods, formal controls also need to be in place and enforced. These technical and formal controls need to be supported with educational and training programs to help the employee understand:

- How the system works (or should work),
- The kind of risks that are posed to the information system,
- The three different aspects security must cover,
- The role that each employee plays in securing the system,
- The legislative sanctions to intentional misuse of information systems and enterprise-owned data (it is usually a good deterrent of insider attacks), and
- The security tools or measures employees and managers should put in place at any time, especially when becoming aware of a specific risk. (Melara et al., 2003, p. 18)

MITRE Corporation has also performed research to help, "…characterize and create analysis methods to counter sophisticated malicious insiders in the United States Intelligence Community." (Maybury et al., 2005, p. 1) In this study, six months were spent studying prototype techniques developed to provide early warnings of insider activity.

Several mechanisms are already in use to help predict insider attacks. Many organizations track employee access, utilize camera systems, and monitoring email usage, signature based detection monitors for known types of attacks. Monitoring for anomalies and misuse is another set of methods used. In addition to these, policies are also set up. Role Based Access Control controls access to areas of the network based on roles of the organization. Simulators have been designed to help gain real time activity to detect anomalies and misuse. Simulators, however, are another form of technology that can't always be used to identify an insider. (Nellikar, 2010)

Another set of theories used to discuss information security and the effects of organizational, environmental, and behavioral factors on information security success include the protection-motivation theory, deterrence theory, and again, organizational behaviors. Tejaswini

Heratch and H. Raghav Rao used these theories to investigate and demonstrate how organizational culture will positively or negatively affect the success of security policy. These theories address the ideologies behind threats affecting individuals and organizations and the effect of deterrence on compliance. "Security-related behaviors may be connected to an individual's motivation to protect organizational information assets due to awareness and fear of the outside environment, as well as his/her closeness to the organization…employee commitment to organizational well-being." (Herath & Rao, 2009, p. 109) To test several hypotheses regarding employee behavior and compliance with security policy, research was performed to demonstrate importance in behavior and information security. "Our results indicate the employees' understanding of the severity of the threat significantly affects their concern regarding security breaches…that on average, employee perceived security breach certainty perceptions are low…that if employees believe that complying with policies is a hindrance to their day-to-day job activity, they are less likely to have favorable views towards security policies…that if employees perceive that their compliance behaviors have a favorable impact on the organization or benefit the organization, they are more likely to have more positive attitudes toward the security policies." (Herath & Rao, 2009, p. 117) Another finding in the study was that social influences are important in positively affecting employee behaviors. "This suggests that beliefs regarding the expectations of superiors, peers, and IT personnel seem to have the most impact on employee security behaviors. Not only the expectations of others, but also the perceived behavior of similar others, was found to be a significant contributor in employee intentions to comply with the policies." (Herath & Rao, 2009, p. 118) A third factor found in research was that if employees know there is likelihood that there will be consequences imposed with non-compliance they will behave more positively. (Herath & Rao, 2009) These factors

come from the organizational culture – how an employee has knowledge of organizational policies and perceives the importance of compliance to the organization.

Organizations worldwide concur that with the globally expanding world of business via the use of the Internet and mobile devices a better approach to security architecture is needed. Research has proven that this changing environment now has a greater threat than previously thought – the insider. IT professionals and end-users worldwide each holds different knowledge bases and understanding of security threats to an organization's network. The conclusion by professionals is that awareness and training in security policy about why the policy is in place to better control end-user behavior. Without attention to policy, and the lack of importance placed on end-user behavior will only lead to greater incidents of security breaches due to insider activity. Organizational policy and culture needs to change along with the changing business world in order to continue to provide the all important confidentiality, integrity, and availability expected of organizations today by consumers.

Chapter 3 – Project History and Methodology

While engaged in a discussion with managers, the topic about best practices in security came up. A question posed regarded whether or not employees truly understood the reasoning behind security policy. The managers seemed to feel that, yes, most employees understood and knew the difference between right and wrong when using company property such as desktops and PCs connected to the network, and how to appropriately act when using them. The reasons behind security are common sense, right? Knowing the behaviors of co-workers with the company network, some question the degree of understanding and whether the employee should be considered more of a threat. Many larger corporations have security policies in place, but it seems the employees and partners are not all fully aware of the policies and/or reasoning behind it. Daily, co-workers abuse security policy and corporate ethics. New network based storage tools are being created to use the corporate network to store proprietary company information and customer information. Being network based, this allows employees based around the world to work using the same software, storage networks and databases, as well as also allowing business partners around the world access to these same databases. This architecture is great in being able to guarantee data that is used by anyone associated with the company, whether a direct employee or a partner, be the most accurate it can be, hence providing integrity as a business for its consumer. This architecture also opens doors to new security issues concerning confidentiality and availability. Would the currently used security policies protect against the insider? Does the insider truly know right from wrong, especially with employees and partners being located around the world? How much consideration has management teams taken in

regards to the insider? If considered, how would an organization properly address the insider threat?

In order to investigate the true threat of the insider to organizations, a grounded theory, qualitative approach was chosen. The first question that needed to be answered was regarding how much research had already been done regarding the true threat of the insider. Based on the prior research done further observations could be recommended based on the already available data. In the beginning the idea of surveying current employees of several organizations globally would help identify whether the insider should be considered a true threat. Another topic to consider regarded how these same employees felt about the corporate security culture and how the policies are enforced. It was discovered that many surveys similar to this had already been conducted by several trustworthy organizations such as the NIST, CERT, and even corporations such as Cisco. When comparing data these organizations had already published, it was decided that another survey was not necessary and that the already collected data, being current and similar in results, could be used to answer the questions posed about the insider threat.

A collection of research, studies, and previously published thesis reports was gathered from sources such as CERT, the NIST, the ACM, and the IEEE. Also researched were writings published by information technology and security experts via journals, textbooks, technology magazines, and blogs. The consensus for years seems to be that the insider is a true threat. There were common definitions of what the insider threat truly is, but not all were the same. A disconnect between whether the insider should be considered in only malicious situations or whether the insider could also be anyone who unintentionally caused damage was noted. The first question found that a good definition of what an insider is would help confirm the direction an organization needs to take in security.

After reviewing published literature and data, a comparison was made as to what each organization and researcher found considering the true threat posed by the insider. Much of the information discovered similar information, whether based on small or large subject groups. There is a true threat from the insider in this global corporate internetworking culture. Research also demonstrated the reasons employees shared for not complying with security policy no matter the region. Some regions held a general malaise regarding confidentiality, integrity, and availability making it important for organizations to make considerations regarding this malaise and the vulnerabilities that could arise because of it.

The final step was to compare information from the collected data and research. Once compared disconnects was found including current security policies and enforcement. Much of the techniques used were still technological. Using the technologies available to secure a network follow many of the currently followed best practices recommended for organizations to protect the networks involved and to comply with laws and regulations designed to protect the consumer. The commonly found missing factor in security policy is that the insider threat is not fully addressed but should be. Enforcement of policy is also lacking. This led back to my original thought – that employees have a lack of understanding of how their actions could negatively affect the organization's network. Current best practices can help in protection against the insider only minimally. Best practices need to be revamped to include education and enforcement.

Chapter 4 – Project Analysis

"The big lie of computer security is that security improves by imposing complex passwords on users. In real life, people write down anything they can't remember. Security is increased by designing for the way humans actually behave."

-Jakob Nielson

"The greatest danger in times of turbulence is not the turbulence; it is to act with yesterday's logic."

-Peter Drucker

The insider threat is no longer a threat to be ignored. Current best practices are not enough to tackle all the vulnerabilities opened up to an organization by the insider. Common ground exists amongst organizations on many levels regarding the importance of protecting a network from the dangers the Internet has brought to the business world. The business world is now a global culture. This global influence has created environments that now exist internally to an organization, but also outside the perimeter. The historical walls of security that existed have been torn down making the world of security a different reality. When a world or environment changes the old ways of the community also change. Keeping the current security architecture based on best practices will help keep an organization secure, but no longer is the organization secure enough.

Change is never easy. In the information technology world it has been clearly demonstrated and recognized that a change is necessary, but this change has not occurred. Many reasons will keep an organization from making change. Time and cost are just a couple reasons

mentioned by organizations for the lack of change. Data continues to be captured, however, that the insider threat is growing as quickly as the technology that opens up the windows of opportunity to the insider, but the business world is not keeping up. A formal review of current best practices needs to be made, and weaknesses regarding the insider need to be addressed.

Current literature demonstrates how current technology is not enough to defend against the insider. Large barriers exist in coming up with ways to defend against the insider. Current technological practices cost time and money, but so does an attack. Organizations have invested time and money in protection technologies based on common risk management techniques. Once in place, however, budgets are not set to continually support necessary changes, and if not supported changes aren't made. There is a comfort in the current ways used by organizations to guarantee confidentiality, integrity, and availability to customers and regulators. Current expectations and regulations protect well against an outside attack, but what happens when insider attacks begin to outnumber attacks from the outside? Being proactive can only help against future vulnerabilities and threats. No longer can security remain as passive as it has historically.

Sun Tzu wrote hundreds of years ago to, "know your enemy." Information technologists have known the enemy and documented changes in attack. The attack has normally come from the outsider, but research and documentation has been performed and demonstrates how attacks from the inside are taking the lead. A holistic approach to information security should be adopted. Business and technology remain the focus of the chosen weapons, but the battle is changing. The focus no longer should remain on just technology but also the human aspect. This will involve several organizations working together – upper management teams, human resources, etc.

Every organization functions differently so each organization faces different risks dependant on the business conducted. Tools have been created that can be used by all, and these tools will still continue to work, but the question is posed whether they can be used in different ways in order to provide even better protection? The best preventative actions to take include currently followed best practices as well as combining these with behavior and culture. Currently provided data demonstrates that behaviors by all employees, whether intentionally malicious or not, affect how easily an insider could infiltrate and inflict damage. When assessing risks, organizations need to include the insider.

In 2009, CERT Software Engineering Institute published new and updated recommendations to best practices regarding the insider threat. The 3rd Edition of "Common Sense Guide to Prevention and Detection of Insider Threats" was funded by CyLab and published in 2009. The research performed involved analysis of insider threat cases logged between the years 2003 and 2007. Focusing on cases involving theft and fraud, CERT set out to identify behaviors and conditions that would identify the possibility of a malicious act occurring by an individual or groups of individuals. Using the newer view towards insider crimes this information was used to provide information and recommendations to organizations on how to recognize and address the insider. The changes recommended in CERT's publication addresses how current practices can be adjusted to include the insider. Referring to the recommendations made by CERT, and similar recommendations made by other professionals, I am recommending the use of current practices and adding education to help an organization defend against the insider. (Cappelli, Moore, Trzeciak, & Shimeall, 2009)

4.1 - Recommendations

Education is the key to successfully creating change. Based on research performed employees stated several reasons for not following policy. The time has come to reassess current policies and practices. CERT's research into the success of malicious insiders identifies reasons the insider was successful. Most of the insider activity occurred while the person was still currently employed. Only five of the seventy-seven analyzed cases involved were not currently employed. The gender split was equal – half were male and half were female. The majority held non-technical positions with the company. The pattern identified was one of financial gain. Several situations existed. Some cases involved a single insider, some involved collusion between the insider and someone else inside the company, and some cases included collusion between just insiders. Insiders were paid by outsiders to collect or modify data for them; others committed the acts internally by abusing access and processes of the organization. 95% of the users stole or modified data during normal business hours, and over 75% used authorized access. Only sixteen percent of the crimes were initially designed using technical knowledge, 85% used their own password and 10% compromised someone else's account by accessing via an unattended computer, using customer accounts, or social engineering schemes. (Cappelli et al., 2009, p. 18-19) Detection was not able to be used to stop the insider prior to attack as this isn't the common way to identify an issue. CERT found that over 50% of the cases were detected internally by non-IT people, 26% by clients or customers of the organization, approximately 10% by customers, and 5% by competitors…in most cases system logs were used to identify the insider." (Cappelli et al., 2009, p. 20)

CERT's "Common Sense Guide to Prevention and Detection of Insider Threats" summarizes sixteen best practices to follow:

- Practice #1: Consider threats from insiders and business partners in enterprise-wide risk assessments.
- Practice #2: Clearly document and consistently enforce policies and controls.
- Practice #3: Institute periodic security awareness training for all employees.
- Practice #4: Monitor and respond to suspicious or disruption behavior, beginning with the hiring process.
- Practice #5: Anticipate and manage negative workplace issues.
- Practice #6: Track and secure the physical environment
- Practice #7: Implement strict password and account management policies and practices.
- Practice #8: Enforce separation of duties and least privilege.
- Practice #9: Consider insider threats in the software development life cycle.
- Practice #10: Use extra caution with system administrators and technical or privileged users.
- Practice #11: Implement system change controls.
- Practice #12: Log, monitor, and audit employee online actions
- Practice #13: Use layered defense against remote attacks.
- Practice #14: Deactivate computer access following termination.
- Practice #15: Implement secure backup and recovery processes.
- Practice #16: Develop an insider incident response plan.

(Cappelli et al., 2009)

Practice one, *considering threats from insiders and business partners in enterprise risk assessments*, and practice three, *instituting periodic security awareness training for all employees*, are two practices that are currently not focused on by organizations. Practice two has also been demonstrated in studies, *document and consistently enforce policies and controls*. These three practices work together and it is necessary to continually examine practices and re-examine to make necessary changes.

To begin, threats from insiders need to be included so re-examining current risks will be necessary to make adjustments. In many organizations it may be necessary to convince top level management of this necessity. Education may need to begin here in order to gain the support needed to be successful. Most current policies will not need to be adjusted tremendously, but adjustments will need to be made making it necessary for a budget to include this time for adjustments. Overall, the first step to successfully make changes will be to gain upper level approval and agreement, without this, current practices are unlikely to change. Educational meetings may need to be held to persuade upper levels to the importance of the need. Current practices will need to be explained in a way to demonstrate how the insider threat is growing and should now be added to security architecture. Demonstrating how organizations similar to the one being addressed have been affected could help, along with presenting data to upper level management the data already gathered over the past several years regarding the growing threat. Once this is understood, the greatest data to present would be data on how the insider has affected the organization being addressed. This will be the single most difficult task in addressing the insider threat. It will take time and a group of employees to gather logs and statistics regarding the effects of the insider on the current organizational network security architecture. In Chapter 2, literature on research conducted in the information security field has

been done to demonstrate that the culture of organizations does not fully support the insider threat, if at all. Money and time have already been spent to develop currently followed practices that are working against the outsider – relevant data will be needed to convince upper levels of this change.

Education needs to be used to change organizational culture. Many organizations, being global now, will need to tackle several legal, ethical, and cultural issues to accomplish this. While educating users about the new company culture they can also educate about ways to protect themselves and the organization. Chapter 2 also demonstrated that employees do not comply with security policy. Over time, the new community culture should change as all employees learn of the risk of the insider and the ways the insider can infiltrate the system. Education should not be focused on just non-technical employees – ALL employees at ALL levels should be required to receive training. The management team is important when considering the organizational culture. A factor in the successful organizational cultures is referred to as, "the tone at the top" by the writer's of "Embedding Information Security into the Organization." (Johnson & Goetz, 2007, p. 17) This article addresses the many challenges known by the Information Security community in managing and changing the culture of an organization regarding security. It is believed that senior management involvement is essential, but the awareness needs to span all levels of the organization. Knowing the importance of the information security to the organization is important, but it must also relay the importance of individual responsibility. Another study performed in 2007 discusses how findings show that, "To ensure positive social pressure, top management, immediate supervisors and IS security staff should clearly and explicitly note the importance of complying with IS security policies."

(Pahnila, Siponen, & Mahmood, 2007, p. 8) All managers must be involved in the understanding and acceptance of the cultural change.

The type of training offered will also make a difference. Practice two states that organizations should clearly document and enforce policies and controls. Investigations into why users don't comply to policy has shown that many employees believe that nothing will happen to them as these policies are not enforced. Enforcement cannot strictly rely on training – something needs to come out of suspected bad behavior or it will continue as the policy will not be taken seriously. The success of the policy will depend on employee acceptance. "Individuals are influenced both by messages about expectations and the observed behavior of others." Sometimes people consult the behavior of those around them to find out what to do." (Herath & Rao, 2009, p. 113) This study on protection motivation and deterrence found that, "… if an employee believes that his/her colleagues follow the organizational security polices, she/he is more likely to have positive intentions to follow them as well…studies have examined employees' perceptions of the expectations of superiors, managers, and peers in relevant IS departments…and believes that the managers, IT personnel, or peers expect information security policy compliance, she/he is more likely to intent to comply."(Herath & Rao, 2009, p. 113) This is all part of the organizational culture – if the importance of information security isn't enforced, all the policies in the world won't persuade users from non-compliance.

Most employees will respond to minimal attention if suspected of non-compliance. Monitoring employees may depend on the role of each employee in the organization. How this is done depends on the organization but several teams need to be put together to construct the proper enforcement policy. This involves managers of teams, human resources, and legal teams. Issues come up regarding individual rights and policies, but organizational requirements for

compliance to protect business and its customers – at what point do the organization's policies override rights of individuals? This is one decision that needs to be made by several levels of the organization, and then shared with the organization's population. Just as between a child and parent, the technique chosen may be different, but without enforcement the child will not follow the rules because these rules, then, essentially do not really exist. Enforcement policies can be reviewed periodically, but still requires enforcement. Discussing the policy twice a year with employees is not enough. When suspicious activity occurs it needs to be investigated and addressed.

Employees also need continuous reinforcement and training in security awareness considering how quickly the techniques used change. New methods are discovered daily by hackers, but the average employee does not keep up on this information as it is released. A minimum of once per year employees globally and at all levels, should be trained on what to watch for. Who the organization considers to be the insider should be discussed. Behavior traits should be shared with employees – the insider is not always who you may expect him/her to be. Also understanding personal individual behavior inside and outside the office is important. CERT has listed some behaviors to consider in Table 11.

Table 11

Behaviors to look for

- Threats against the organization or bragging about the damage one could do to the organization,
- Association with known criminals or suspicious people outside of the workplace,
- Large downloads close to resignation,
- Use of organization resources for a side business, or discussions regarding starting a competing business with coworkers,
- Attempts to gain employees' passwords or to obtain access through trickery or exploitation of a trusted relationship (often called "social engineering")(Cappelli et al., 2009, p. 39)

Note. From CERT's Common sense guide to prevention and detection of insider threats

Social networking and social engineering techniques need to be shared with employees to help all employees realize if it may be happening to them or someone they know. A better understanding of responsibilities regarding personal usage of company and personal property on the network, such as password protection and Internet usage will only help. Employees also need to be trained on the proper ways to report suspicious activity. Training should inform employees on how system activity is monitored in order for employees to fully understand the entire security process. (Cappelli et al., 2009) Reinforcement methods include measures such as emails with updates and reminders of security policy and compliance, seminars and training sessions for review, posters and articles distributed among employees can also help. The idea is to keep the importance of security and compliance in the regular day to day activities of each employee.

In addition to re-examining and re-vamping policies to address the insider threat and then educating the employees, continuous auditing needs to take place. Organizations need to keep up with recent changes in the insider attack methods and examine current policy to make sure it continues to protect the organization properly. Keeping in mind, "…how do you know if security initiatives and awareness are making a difference? How should metrics cascade throughout the organization? How can risk and security metrics be more closely tied to tactical and strategic decision making?" (Johnson & Goetz, 2007, p. 21) When measuring, a couple other questions need to be kept in mind, "Are the metrics really helping to reduce the risk? Will they help save money next year? Will they add business value?" (Johnson & Goetz, 2007, p. 21) What measurements are used are dependent on the organizations need for monitoring – how has it been done in the past and is the measurement still appropriate to the organization's needs? Just as adjustments need to be made to IDS and IPS to protect the perimeter, patches and updates are

performed on systems and applications, so should adjustments be made to training and reinforcements. Employees need to be continuously updated to the threats, changes made to policy, and changes to employee responsibility. With proper training, the employee can become a great weapon against the insider threat.

Chapter 5 – Conclusion

"The search for static security – in the law and elsewhere – is misguided. The fact is security can only be achieved through constant change, adapting old ideas that have outlived their usefulness to current facts."

-William Osler

Canadian physician, 1849-1919

Information security in the business world can no longer rely on tools. The way business works today is more social than it ever has been before. The Internet has allowed globalization to grow at tremendous speeds and business is now conducted around the world. Businesses now keep pertinent and private information on computer systems rather than on paper. These systems are accessed via networks interconnected via the Internet. Business has made the world smaller than it has ever been. New ways to communicate exist, as do new ways to steal and exploit information. In some ways, theft and exploitation are now more powerful as it can occur from anywhere around the world at any point in time. Physical and environmental security is no longer enough. Communities hear every day from each other how someone or something has been exploited by an unknown attacker. Many times, these attacks are successful because of unintentional, accidental actions taken by the unsuspecting victim. Every person performing regular daily day to day activities could now open doors for an attack on anyone without even knowing it. Educating users about these social changes can help protect businesses.

Cultural changes are the greatest concern in order to make education work. Policies can be created but without education and enforcement the policies will prove to be a waste of time. "Will the new tools and laws we've described here put an end to all privacy invasions, unfair

misuse of personal information, copyright infringement, and identity theft? No, perfect compliance is not the proper standard by which to judge laws or systems that help enforce them. Rather we should ask how to build systems that encourage compliance and maximize the possibility of accountability for violations." (Weitzner et al., 2008, p. 87) Security is never 100%, but current protections are not going to be enough. Organizational culture needs changes through education and enforcement. For years this information has been discussed in management. Studies have been done on what is missing in current practices and why it no longer is enough. Being an organizational force, no longer are small policy group and technological tools going to be enough. An article in the Journal of Organizational Change Management addressed this thought. "Additionally, wisdom must be transferred throughout the organization. This will not happen unless:

- The concept of organizational wisdom is understood and valued throughout the organization; and
- Organizational leadership, culture and structure are specifically focused toward facilitating its development and transfer."(Bierly III, Kessler, & Christensen, 2000, p. 613)

The need for change exists and that has been demonstrated for years. The ability to change will depend on all parts of an organization. No longer can groups of an organization function separately, the involvement of all groups to combine and work together will be the key to successful change. Gaining and maintaining the compliance of employees will involve education and reinforcement. Without compliance the work done to change will not be worth the time.

Change will take time and will not occur overnight. Without considering several factors, including cultural influences by region, internal cultural influences, and employees' personal traits, changes will not be effective. "…70 percent of change programs fail because of lack of strategy and vision, lack of communication and trust, lack of top management commitment, lack of resources, lack of change management skills, resistance to change, etc. Research dealing with organizational change has mainly focused on organizational factors neglecting the person-oriented issues." (Vakola, Tsaousis, & Nikolaou, 2004, p. 88) Current best practices should not be neglected, but should now include social and psychological considerations. All employees from the top down should be involved. Educating users on security issues will help empower all end-users in protecting sensitive information. The outsider now has a new way inside, via mistakes made by those who are already inside. The disgruntled employee is one to keep an eye on, but all employees need to change the way they know and protect from the inside out.

References

Bierly III, P. E., Kessler, E. H., & Christensen, E. W. (2000). Organizational learning, knowledge and wisdom. *Journal of Organizational Change Management*, *13*(6), 595-618. Retrieved from http://www.deepdyve.com/lp/emerald-publishing/organizational-learning-knowledge-and-wisdom-OsNgiBp0xu

Burke, B. E., & Christiansen, C. A. (2009, August). *Insider risk management: A framework approach to internal security* (White Paper 219015). Retrieved from RSA, The Security Division of EMC: www.rsa.com/document.asp?doc_id=10388

Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. (2009). *Common sense guide to prevention and detection of insider threats* (CERT Software Engineering Institute). Retrieved from CERT: www.cert.org/archive/pdf/CSG-V3.pdf

Cisco. (2008). *Data leakage worldwide: The high cost of Insider threats* (White Paper). Retrieved from Cisco Systems, Inc.: www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.html

Cisco. (2008). *Data leakage worldwide: The effectiveness of security policies* (White Paper). Retrieved from Cisco Systems: http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.html

Cole, E. (2011). *Address the insider threat of privileged users* (White Paper). Retrieved from NetIQ: http://www.idgconnect.com/view_abstract/5674/address-insider-threat-privileged-users

Contos, B. T. (2006). Enterprise security management (ESM). In *Enemy at the water cooler* (pp. 69-98). Rockland, MA: Syngress Publishing, Inc.

Cyber security standards. (n.d.). In Cyber security standards. Retrieved August 24, 2011, from http://en.wikipedia.org/wiki/Cyber_security_standards

Dark, M. J. (2011). Information security and security ethics in complex systems. In *Information assurance and security ethics in complex systems: Interdisciplinary perspectives*. Hershey, PA: IGI Global.

Denning, D. E. (1999). *Information warfare and security*. Reading, MA: ACM Press.

Finch, J., Furnell, S., & Dowland, P. (2003). *Assessing IT security culture: System administrator and end-user perspectives* (White Paper). Plymouth, United Kingdom: University of Plymouth.

Greitzer, F. L., Paulson, P. R., Kangas, L. J., Franklin, L. R., Edgar, T. W., & Frinke, D. A. (2009). *Predictive modeling for insider threat mitigation* (U.S. Department of Energy PNNL-SA-65204). Retrieved from Pacific Northwest National Laboratory: www.pnl.gov/cogInformatics/media/pdf/TR-PACMAN-65204.pdf

Herath, T., & Rao, H. R. (2009, February 23). Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*(2), 106-125. Retrieved from www.palgrave-journals.com/ejis/journal/v18/n2/abs/ejis20096a.html

ISO/IEC 27002. (2011). In ISO/IEC 27002. Retrieved August 24, 2011, from http://en.wikipedia.org/wiki/ISO/IEC_27002

Johnson, M. E., & Goetz, E. (2007, May/June). Embedding information security into the organization. *IEEE Security & Privacy*, 16-24. doi: 10.1109

Kondrup, D. A. (2011, January 11). *Cyber security threats: Incident response and management*. Paper presented at the Cyber Security and Business Continuity, Berlin, CT.

Leidigh, C. (2005). *Fundamental principles of network security* (White Paper 101). Retrieved from American Power Conversion: www.apcmedia.com/salestools/SADE-5TNRPG_R1_EN.pdf

Linux.com Editorial Staff. (2011). *Top five insider attacks of the decade*. Retrieved from http://www.linux.com/news/technology-feature/security/397143-top-five-insider-attacks-of-the-decade

Lynn, G. (2011). *Network Security Best Practices*. Retrieved from http://www.faulkner.com.dml.regis.edu/products/securitymgt/feb2011

Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., ... Lewandowski, S. (2005). *Analysis and detection of malicious insiders*. Retrieved from Mitre Corporation: nrrc.mitre.org/NRRC/ana_det_malicious_insiders.htm

Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A., & Cooke, D. L. (2003). *A System dynamics model of an insider attack on an information system*. Retrieved from CERT.org: www.cert.org/research/sdmis/insider-threat-desc.pdf

Metzger, J., & Shaw, J. (2010). *Eight threats your anti-virus won't stop*. Retrieved from http://www.sophos.com/en-us/security-news-trends/security-trends/why-endpoint-security.aspx

Nellikar, S. (2010). *Insider threat simulation and performance analysis of insider detection algorithms with role based models* (Master's thesis, University of Illinois at Urbana-Champaign). Retrieved from www.scribd.com/doc/51868949/Insider-Threat-Analysis-of-Case-Based-System-Dynamics

Noonan, T., & Archuleta, E. (2008, April 8). *The National Infrastructure Advisory Council's final report and recommendations on the insider threat to critical infrastructures* (Final Report). Retrieved from DHS: www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. . doi: 10.1.1.106.7038

Sloane, S. (2011). *Let's stop the billions lost to cyber thieves* [Peer commentary on the journal article "" by]. *Washington Technology*, Retrieved from http://washingtontechnology.com/Articles/2011/07/21/Stan_Sloane-cy...

Vakola, M., Tsaousis, I., & Nikolaou, I. (2004). The role of emotional intelligence and personality variables on attitudes toward organizational change. *Journal of Managerial Psychology*, *19*(2), 88-110. doi: 10.1108/02683940410526082

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008, June). Information accountability. *Communications of the ACM*, *51*(6), 82-87. Retrieved from http://dig.csail.mit.edu/2008/06/info-accountability-cacm-weitzner.pdf

Appendix A National Equivalent Standards to the United States ISO 27002

Countries	Equivalent Standard
Australia New Zealand	AS/NZS ISO/IEC 27002:2006
Brazil	ISO/IEC NBR 17799/2007 – 27002
Chile	NCH2777 ISO/IEC 17799/2000
China	GB/T 22081-2008
Czech Republic	ČSN ISO/IEC 27002:2006
Denmark	DS484:2005
Estonia	EVS-ISO/IEC 17799:2003, 2005 version in translation
Japan	JIS Q 27002
Lithuania	LST ISO/IEC 27002:2009 (adopted ISO/IEC 27002:2005, ISO/IEC 17799:2005)
Netherlands	NEN-ISO/IEC 27002:2005
Peru	NTP-ISO/IEC 17799:2007
Poland	PN-ISO/IEC 17799:2007, based on ISO/IEC 17799:2005
Russia	ГОСТ/Р ИСО МЭК 17799-2005
South Africa	SANS 17799:2005
Spain	UNE 71501
Sweden	SS 627799
Turkey	TS ISO/IEC 27002
Ukraine	СОУ Н НБУ 65.1 СУІБ 2.0:2010
United Kingdom	BS ISO/IEC 27002:2005
Uruguay	UNIT/ISO 17799:2005

– National Equivalent Standards ("ISO/IEC 27002", 2011)

Appendix B - Indicators that determine the relative "risk level" of an individual

1. **Accepting Feedback** – the employee is observed to have a difficult time accepting criticism, tends to take criticism personally or becomes defensive when message is delivered. Employee has been observed being unwilling to acknowledge errors; or admitting to mistakes; may attempt to cover up errors through lying or deceit.
2. **Anger management** – the employee often allows anger to get pent up inside; employee has trouble managing lingering emotional feelings of anger or rage. Holds strong grudges.
3. **Disengagement** – the employee keeps to self, is detached, withdrawn and tends not to interact with individuals or groups.
4. **Disregards authority** - the employee disregards rules, authority or policies. Employee feels above the rules or that they only apply to others.
5. **Performance** - the staff member has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance.
6. **Stress** - the employee appears to be under physical, mental, or emotional strain or tension that he/she has difficulty handling.
7. **Confrontational** - employee exhibits argumentative or aggressive behavior or is involved in bullying or intimidation.
8. **Personal issues** - staff member has difficulty keeping personal issues separate from work and these issues interfere with work.

9. **Self-centered** - the staff member disregards needs or wishes of others, concerned primarily with own interests and welfare.
10. **Dependability** - employee is unable to keep commitments/promises; unworthy of trust.
11. **Absenteeism** - staff member has received a disciplinary action (verbal warning, written reprimand, suspension, termination) for excessive time away from work.

(Greitzer et al., 2009, p. 9)