2010

Security practices: A Mixed approach

Sourabh Dass

2010

Security Practices

A mixed approach

- Thesis Documentation

Name:

Sourabh Dass

Chair Professor:

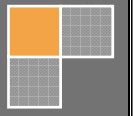
Prof. Charlie Border

Committee Member:

Prof. Luther Troell

Prof . Pete Lutz

Sourabh Dass
Rochester Institute of Technology
6/30/2010



Contents:

Rochester Institute of Technology
B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in Networking and System Administration

Student Name: **SOURABH DASS**

Thesis Title: **SECURITY PRACTICES – A Mixed Approach**

Thesis Committee

Professor Charlie border

Chair

Professor Luther Troell

Committee Member

Professor Pete Lutz

Committee Member

I. Introduction:

Consistency of information is ideally maintained by adhering to the best practices and policies that have evolved around it. Be it maneuvering information from a single source to a single destination or just harnessing the power of information by either its usage or storage, large organizations have developed innumerable policies and procedures to protect the information from unauthorized manipulation. Yet with the passage of every year there is a marked increase in the incidence and severity of data theft and fraud which is a result of misuse of information and identity theft. According to CSI Computer Crime Security Survey [16] incidences of malware infection rose at an alarming rate of 64.3% in 2008 compared to 50% the previous year. Denial of service attacks were recorded at 29.2%, a sharp increase from 21% in the same time frame. Despite our best efforts, data breaches occur with significant consequences, resulting in potential loss of business and revenue for organizations. High profile social websites such as Face book and Twitter also have faced f data and identity theft in the past year. The above illustrates that even though organizations have invested substantial amounts of time and effort in the development of policies and procedures regarding information security governance, there may be scope for improvement in their implementation. The process of Information security governance forms an integral part of business today by lending them an edge in the competitive global market. Security Governance adds value to business processes, harnesses the growth of information technology while at the same time mitigating the risks associated with it. However, fraud and identity theft incidences

continue to occur. Terabytes of data are facing a constant threat from a wide range of evolving attack vectors which surpass our best security policies and practices. Nimda, CodeRed, Subseven are just a few exploits that have penetrates our systems and annually affect nearly 94 million people worldwide [14]. These statistics point to the need for improvement in our implementation of security policies for countering attack vectors. This research paper identifies the potential problems that may arise between policies and their implementation in practice which often form the basis of information security governance. This paper adopts a mixed methods approach of qualitative analysis followed by a quantitative survey, which was most appropriate to gather information about difficulties faced by system administrators in the implementation process. The methodology is organized in two primary sections: first, it gathers in depth knowledge regarding the design and implementation of various security policies through discussions with security/system administrators. Second, with the information gathered, a survey is conducted on a larger group of end users from various domains identifying end user problems in adhering to security policies. Being a system administrator, it is essential to me that implementation of security principles and practices in my production environment is apt and usable for my end users and causes minimal interference with their work and applications. It is an extremely difficult task to maintain the best practices and ensure their proper implementation.

2. Literature Review:

Security of information has been one of the prime concerns when evaluating the increased reliance on information technology. From investing in devices that thwart a hacker's movement beyond the firewall, to creating access rules and including modifications in application configurations, we have made numerous changes to make our environment secure. Yet, there are incidences of data breaches resulting in loss of information. Lack of proper implementation of security policies is often the cause of these incidences. According to Willert [14] most data comprises, thefts, and corporate hacks occur from within the perimeter of a firewalled environment. Overall this type of exploit accounts for two-third of the total exploits. While some insider attacks are deliberate, while others are not the variety of insider attacks provides a unique outlook on security, which means a corporate environment is threatened more by its own employees as by outside hacker. Insider based attacks cannot be negated by the mere installation of devices or application of policies since most insiders are unwilling to change their approach despite the consequences arising from their actions and handling of information. Even though insiders often understand the ideas around information security, they do not follow the policies and procedures designed to maintain information security and instead claim to be over burdened with excessive and confusing security policies. The author points to various security installations which form a layered approach, that an organization may consider using in their security structure to distribute responsibilities for maintaining security architecture. This approach enables an organization to counter attack vectors from more than one avenue and also acts as a

backup approach in the event the front line of defense fails. Layered approach often thwarts and disheartens attackers where layers in security are complicated and time consuming [2]. However, from the users' perspective, too many layers of security while blocking an attack may adversely impact workers' productivity. It may also provide them incentives to circumvent security policies while attempting to enhance their perceived productivity.

These situations give rise to another critical piece of the puzzle in the security field. Often employees become slack in their implementation of security policy, since they perceive the policies as being too difficult to follow or they do not share the same enthusiasm for security as their employers. Siponen et.al [11] have pointed out a similar situation where employees give rise to potential threat situations when they fail to follow security guidelines. Employees often perceive security policies and procedures as being confusing and cumbersome and they do not see any productivity for their invested time and effort in following procedures. This can result in information theft or data breaches, which can cause damage to organizations, in terms of the company's reputation or even force them to close their doors or go bankrupt. In a study conducted by Hinde [5] he found that 91 percent of the organizations' own employees are unable to follow simple security procedures, giving rise to these attacks. Siponen et.al delved into deeper analysis of the psychological aspect of why following a security policy is difficult for employees. In their survey they had a response rate of only 29.4 percent which further emphasizes the lack of enthusiasm of the employees for security. They found that a lack of education in and knowledge of security policy were the primary reason why implementation of security has so many critical failure points. Their findings suggest that

positive social pressure and also visibility in security principles and practices improve the implementation of security principles. The need to promote the importance of data and information security and the consequences of data breaches are also highlighted. Organizations need to find various avenues such as television broadcasts, newspaper or corporate magazines to make their employees more aware of their environment and the potential threat of critical data breaches that arise from their handling of information in their daily work. Managers and supervisors need to get their teams together in formal or informal discussions depicting practical data breach incidents and identifying measures that are appropriate to counter security threats within the organization.

The third paper that I would like to reference is by Murray, [9]. To emphasize the importance of security one has to delve much deeper into a corporate security practice and start from the ground up which leads me to review the methodology for security implementation regarding personal laptops or user workstations. Murray advocates that like most of our belongings such as a house or property, a laptop or a workstation also needs to be protected from malicious activities. It is imperative especially in the case[s] of laptops and workstations where the value of the device increases exponentially with the content and information stored on them. The value of the information stored on the device is probably much higher than the value of the device and could potentially cause much greater harm if it falls into inappropriate hands. Often advice regarding the encryption of a laptop or hard drive filled with critical information is not followed. It is not that users underestimate the value of the contents of their devices but as Whitten and Tygar [1] observed, most users are not comfortable with navigating through an encryption package. While Murray successfully identifies two basic principles to

facilitate the protection of property and the data itself, we also have to understand that the reason why users fail to adhere to security practices involving protection of their devices.

The concept of security is more than just simple adherence to security policies and procedures, rational implementation within the end user environment is also critical in this whole puzzle. End User Security Management [EUSM] holds the key to successful security. The paper challenges the previous belief that end users are the weak link in information security. The paper [3] surveys employees and end users from production environments who are responsible for information exchange and emphasizes two critical aspects of security. First, end users are not heedless about their security needs but are more likely unsure of the appropriate action or are frustrated by the complicated corporate policy and structures. Second, it is the general inadequacy of the usability engineering [EU] that leads users to poorly implement otherwise valid security policies. To challenge the overall concept of the end user being a weak link and constantly falling prey to social engineering attacks the paper includes a brief review of Human computer interaction and a field survey of end users who at various levels of organizations are responsible for handling of sensitive information. The paper stands out in that, even though most security papers have embraced a top down approach where the notion of security is depicted as a policy driven organizational paradigm, security actually can be treated as a bottom up approach directed towards the individuals that make up an organization. The other consideration of the problem regarding the implementation of security practices that we need to pay attention to is that the users' time that is consumed in following security procedures is not an infinite resource. Herley [4]

provides evidence as to why we need to consider the cost to users regarding implementation of security policies as part of the policy itself. Often users perform an implicit cost /benefit calculation when they implement or try to follow a security directive. In most cases the cost of security implementation adds a direct overhead cost to users but provides little in terms of direct benefits. Moreover the benefits are almost always targeted at a very small percentage of users who may actually fall victim to vulnerabilities and exploits whereas the cost to follow the directive applies to the entire population of users. Even the directives designed to avoid problems are based on worst case scenarios and not practical situations where the consequences of a missed directive are not as grave. While devising our security principles we often take users time for granted and with policies and procedures being upgraded so often the over head increases and eats at users' productivity.

The final reference comes from the paper on IT governance by Michael Tarn et al. [20]. This paper provides the fundamental reason for delving deep into the complications of implementing a good policy via adequate procedures and the need for a good security framework. With the increased dependence of organizations on information systems and Information technology it makes proper business sense to envision a robust IT governance structure guided by good information security policies and backed up by valid procedures. IT governance is a not a separate entity within an organization but an extension of the corporate governance structure and includes policies and procedures that ensure realization of business goals and objectives while mitigating risks. IT governance adds value to business by generating capital for businesses and attracting more investments from various sectors and also mitigates risks associated with

adoption of information technology to enhance productivity. The paper also points out that organizations have made substantial progress in revenue earnings and achieved operational excellence by creating good security governance procedures. They have also been able to develop optimal risk management schemes through security governance. Hence it is critical from a business standpoint to understand the underlying conflict that may exist between a good policy and a viable procedure.

3. Purpose Statement:

This thesis paper identifies various points of failure that arise out of improper implementation of a good policy through procedures. It is designed to help system administrators to implement security policies and procedures which will provide better information security to organizations. The primary research conducted is an extension of previous work on Human computer interaction [3] with a focus on delivering basic guidelines for implementation of usable security policies.

4. Methodology:

In order to gain an enhanced knowledge of why organizations falter in the implementation of valid security policies, this thesis research followed a mixed methods approach. Because there exists a gap between what we as system administrators perceive as ideal security measure and the reality of implementation of those policies there is a need to both analyze our security policies and procedures as well as the after effects of implementations. Pursuing a single research design on either a qualitative or a quantitative analysis was inadequate in this scenario. A mixed methods approach

which employed research mechanisms combining the collection and analysis of quantitative and qualitative data helped in the better understanding of our present day security problems. This research provides a deeper understanding of the problems we face in implementation of a good security policy that resists it from becoming a valid security practice. The Research was initially focused on conducting interviews with appropriate personnel, such as security administrators and system administrators from five different organizations who encounter problems in implementing various security measures in tandem with the organizations' policies. Interviews with these personnel revealed their take on security, difficulties they encountered in ensuring the safe transit of data and also their perception of user behavior towards acceptance and adherence of policies. These in-depth qualitative interviews revealed the difficulties in implementations of security policies faced by security administrators.

The subsequent part of the research employed a more quantitative approach targeting a broader mass of end users to verify the notions of security obtained from above and also focused more on end user problems adhering to security policies. The research method analyzed security components at an individual level, reminiscent of a bottom up approach. The survey was conducted with the knowledge acquired from the responses of the earlier respondents for at least 300 employees who are directly or indirectly involved in security practices or are part of a security policy. The research gathered information on how they perceive security in their organization and the difficulties they face while trying to adhere to organizational security policies. It also tried to answer the question of the impact information security policies actually have on personal productivity. This allowed me to evaluate our present situation, existing policies and

procedures and their usability and feasibility within production environments. This research provided a unique opportunity to gather valuable information regarding the effectiveness of our present security policies and their failure that arise due to improper implementation.

5. The Interviews:

The first phase of this research was conducted with candid interviews with five System administrators/security managers to discuss the issues they encounter while designing and implementing an information security policy into a practice. To gauge their notion of importance of information security and who they thought critical to successful IT governance, I asked them who in their opinion was responsible for security in their respective organizations. Most respondents emphasized that primary responsibility lies with the security administrators or managers who design the organization's security. However, a couple of them responded that along with system administrators, end users were equally responsible, since the real IT governance occurs from adherence to security principles by them. They felt sometimes the security administrators are limited in their scope in that they are only responsible for designing and implementing.

In order to have usable information security policies it is important that the right people be involved in the policy formulation. When asked if they consider themselves along with other system administrators as active participants in the process, most of the respondents felt even though there exists a central authority who governs information security policies and principles, they too are involved. The central authority formulates and prescribes principles based on the work environment and business needs as well

as the risks that exist during that time in the environment. One of them did feel that at times the governing authority decides and formulates policies without involving system administrators which could have been improved as they could provide valuable insights.

When there are numerous branch locations within an organization, policies sometimes need to be site specific and there may be requirements to tweak the parent policies. When asked if branch system administrators voice their thoughts and provide suggestions while policies are being formulated most of them felt IT is not separate from the corporate entity and they do voice their opinions. However, some of them felt site specific tweaking of policies is rare and sometimes nonexistent. If however there is a specific need, policies do get customized as per requirement but only after approval from central governing authority. In most cases there is very minimal scope for site specific policies since they are almost always governed by best practices.

Even though most policies are derived from the best security practices, sometimes it becomes difficult to implement them, even when they are essential. I asked system administrators if they have faced any such situations before in their organizations. Most respondents have faced similar situations at one time or the other. The most common issue they had encountered was the one with ‘Password Change’. System administrators felt that most users have difficulty following this policy for a number of reasons. They sometimes get comfortable using the same password or they feel it is easy to remember. One of the respondents believed that end user’s often do not consider the corporate domain as their own and are not always eager to adhere to policies. Hence it falls to them to make those policy changes at the systems end and not give users a choice. He also believed that to resolve this problem there needs to be a

culture change and since most difficult aspect in policy implementation is compliance it takes a while before users get it. He felt repetition should be the key. The other problem faced by system administrators occurred when security policies were used to automate installations of some Microsoft product. However, since polices were very strict it was difficult to work with them.

When asked how they would go about resolving similar issues, they replied that they would have to log exceptions with the product vendors for its resolution. However even with their repeated efforts there has been little to no solution to mitigate these risks.

Some organizations have multiple branch locations including some abroad. Maintaining a consistent level of security can be difficult in a widespread network so I asked system administrators if they have encountered problems maintaining security in remote locations or even when negotiating with a third party or other alliances to further business. Most respondents replied that they are concerned only when there are differences in information security policies at offshore branch locations or with outsourced companies. In most situations they are satisfied with the level of information security policy that prevails across their network. However, in situations where there are differences in security policies and procedures across outsourced companies they try to keep proprietary information confidential. Some even remarked that if they are concerned with the level of security policies and procedures of the other organization, they try to mutually agree upon a common standard and ensure that it is followed. Most of them felt when there is a need to outsource information to other companies even with varied levels of security and it cannot be ignored since it is primarily driven by a

business need. In those situations they work on a mutually agreed upon standards to suffice their need.

Even though most of the times we have best information security polices, our security practices often fail to live up to the desired standard. This generally is a direct result of users not being able to follow polices in the manner desired. To understand why users in an organization sometimes do not follow polices or are reluctant to adhere to security principles I asked system administrators why they thought that end users are not enthusiastic about following policies or if they just do the bare minimum. Most of the time respondents found that there are certain policies or situations when users fail to adhere. The most common one across organizations was the password changing policy. Most users were unenthusiastic about this policy and often times just performed the bare minimum there by defeating the spirit of the security policy. They felt users at times put convenience before policies during their daily work.

As outlined before in this research paper true IT security governance comes from the users who are responsible for adhering to it, it is imperative to understand the cause for this reluctance in following policies by end users. I asked system administrators what they thought of as reasons for the noncompliance and why end users perceive security policies as a hurdle in their daily operations. System administrators pointed towards numerous reasons for this behavior by end users. Some believed that end users initially get overwhelmed and fail to see true benefits of a security policy. Some of them felt that noncompliance or reluctance in compliance arises within less computer savvy people. In their opinion less knowledgeable users do not understand the risks presented by not

following security procedures and at times act callously. Noncompliance often happens because a user is unable to comprehend the importance of a security policy.

So why do users not like security policies? The respondents had a variety of thoughts in this regard. Some felt, users often misinterpret or do not understand what policies are intended for and hence they do not follow them. Most of the respondents agreed that users perceived certain policies as more of an inconvenience as they interfere with their daily work habits. They felt that implementing a policy required a work-culture change; when users get used to a certain way of work it is difficult to persuade them to change their work habits to accommodate newer policies. Even though users should treat their work domain as their own and be proactive in adherence of security principles and polices, it seldom happens.

Given this rift in outlook of some end users the question arises if improvements in user culture are required to bridge this gap and better the notion of security among them, and what possible measures can be conceived? Most respondents felt educating a user about the importance of security and the threats that exist outside as well as internal to an organization are crucial to success of a policy. Education in the form of emails or flyers or company magazines, were needed to educate users about policy changes. They felt that it can also serve as reminders that security should be everyone's concern. They felt that this is one area that could be improved with increased communications from their end allowing users to grasp the importance of security. Some mentioned that while formulating policies, education of end users should be made a requirement of the policy itself. They believed that most people who fail to adhere to security policies do not understand the magnitude of threats that exist. They are unaware of the extent of

damage it can cause when there is a failure in following policies. Users often feel that the ill consequences of noncompliance are not real. However, despite repetitive corporate and IT measures there are situations where users fail to comply with the security policies of an organization. In those cases some respondents felt that since security is a primary concern for the well-being of their organization there have been situations when they were forced to terminate employees who failed to adhere to policies. Since noncompliance with policies is not limited to end users but can also be found at the management level, some system administrators felt that it is better at times to refrain from forcing a policy on those users.

Education of users and enhanced awareness of security information provided at every juncture may raise another issue where a user feels overwhelmed by the sheer volume of information. System administrators were asked how much information they felt was adequate to educate a user that serves the purpose without having adverse effects in their production. Most of them felt that it is necessary to inform users about major changes in objectives and policies in an organization. However, almost all of them believed that too much information will eventually interfere with the daily work of users and they should refrain from doing so. Users should be notified only of critical changes or changes pertaining to their specific production environment. Asked if they would prefer to make situations like global virus attacks or phishing attacks relevant to the security of an organization public and warn them of consequences, most respondents felt that in case there are valid worms or Internet viruses that have potential to harm corporate environment or corrupt information, they would want to make users aware of risk situations and warn them of consequences if they do not follow mandated

procedures. However, most of them felt that most security risks should be analyzed and handled by security administrators for most part since it is their primary job function and not overwhelm end users. They should be the ones responsible in mitigating security threats at the perimeter rather than passing on all information to end users.

In the light of new policies being introduced, user adherence, conflicts and education of end users, it is important to understand how system administrators themselves view their organization's security. Are they satisfied or do they see scope for improvements? To this question most of the respondents answered that they were happy with the level of security they have attained but almost all of them believed that the situation could be improved. System administrators believed that one can never be satisfied with the information security structure since policies and practices need to be updated with the constant changes in environment. They were satisfied with their present level of control over users and processes but were looking to improve on it. For all future purposes, everyone I interviewed wanted constant update of policies in tandem with changing technology. They considered lack of update of policies as one of the primary factors why users were reluctant to follow them. One of the respondents believed that to have a more robust security structure and increase adherence to security policies and thereby making it a successful practice four primary components need to occur in tandem. Firstly, there should be continuous updating of policies to reflect the current work environment. Secondly, there needs to be better implementation at the user level. Thirdly, education for users' needs to be included within policies for better adherence, and finally, there is a need to adopt newer technology and modify policies accordingly to enhance the process. This was of the opinion that all of these functions needed to

happen simultaneously and should be in equilibrium. The policies which are required should be made more usable since one cannot have a good policy with bad implementation or vice versa. It is also not conducive to security governance if one has good policies and implementation but non cooperative users or even bad technology. In a distributed environment it is essential to consider all of these aspects to achieve a secured environment.

Sometimes system administrators are required to make exceptions to security policies and procedures to accommodate business needs. Is that a good practice? Respondents felt in most situations that they do not allow exceptions to occur because that results in direct conflicts with information security procedures. However, they did encounter rare instances where they had to allow conditional access to prohibited sites or to relax a policy to accommodate a business need for short periods of time. Respondents mentioned that those situations can be a potential threat and thus they are more careful while administering those exceptions. A respondent from a law firm cited an example in this regard where the general rule in the firm stated that all websites which do not relate to business needs be prohibited. However, certain attorneys in the firm had business requirements to navigate to certain gambling sites or sites which were vulgar in nature to investigate client claims. In those situations even though primary IT governance and security policies did not allow for such access, exceptions were made. A couple of respondents however declined to present exact specifics of customized policies since they considered it part of their confidentiality agreement.

I also asked respondents how they felt about changes, an Act like Sarbanes and Oxley brings to an organization. I referred to a situation where organizations were forced to

make changes as per Sarbanes and Oxley to prohibit instant messaging or IMs within their network. This inconvenienced a lot of users who were by then used to the feature and in some organizations the change was brought about without informing users. I asked system administrators if this type of situation creates a trust deficit between a system administrator and the end users burdened with adherence to security policies. Most of them felt situations like this do create a rift between users and administrators implementing a policy but if an Act like Sarbanes and Oxley exists there is little they can do but to conform to it. Some of them also felt that removal of such popular services in the wake of risk containment, though essential, creates inconvenience to users but the decision is always made with the best interest of the organization in mind. Some of them felt that the trust deficit is a constant factor as they believed that it occurred both ways. They observed that users deemed information security policies as non-essential components and were not keen on adherence and also in the same token system administrators too, implement policies such as Microsoft best practices [mentioned before in page 14] before evaluating the effects on the work environment. For the question, if they felt it was necessary to make users aware of policy changes and maintain a certain level of communication during changes, most of them believed it was necessary and not necessarily depending on the users' population. They felt if the job functions of users are more of an administrative nature, the changes should be communicated, where as if users have limited operational functions, it will be better to communicate only changes pertaining to their job. Almost all of them shared the view that excess information about changes in policy and information security will adversely affect their production.

Finally to wrap up the interviews I encouraged respondents to share their views on how they perceived a good policy on paper could be transformed into a good practice. Most of the respondents wanted a good policy that they are required to implement be equally feasible to implement. They wanted policy makers to take note of the production environments the policy will be subjected to as well the customer needs for the business and also user's experience. Policies good on paper, will in their opinion be good practices only if they satisfy both the conditions. Usability was their primary concern along with modifications of the same in the face of newer technologies and business needs.

6. Survey Details:

The next phase of this research project focused on gathering information from the end users, on their take on security policies of their organization and their perception of information security. The survey was designed to collect data on end users' perception of various IT governance policies and how they enhance or interfere with their daily work. The survey was conducted on at least 300 people with a response rate of 20%. They were presented with 27 information security related situations and were asked to provide their opinion on them. They were also encouraged to provide additional notes in form of comments. The survey included several information security related facts encouraging them to participate and making them more aware of the risks in their online activities.

The survey gathered demographic information from respondents to observe (if any) trends in users' behavior and their tendency to adhere to information security policies depending on their demographic background.

Age was chosen as one of the criterion to gauge the level of comfort respondents had interacting with information systems and if it is justified to relate certain trends in user's behavior in regards to adherence and compliance based on age groups. There was a need to identify if people older or younger than a certain age group had a tendency to adhere more to policies and if advancement of technologies and implementation of complex policies interfere with their work culture. The survey respondents comprised a fairly young group where most users [81.36%] ranged from 20 - 30 years of age. Hence

the response received can be a fair indication of how our present generations of users perceive security.

The next parameter chosen for the demographics purposes was gender. The numbers in this section reflected a fairly balanced ratio of male and female users [55.93 % to 49.07%] who chose to participate in the survey. The results and conclusions that can be drawn from the responses of the survey thus will not bear any male/female bias and can be used to comprehend responses in a neutral manner.

The next question dealt on how much time each user spent with computers in their day to day life. This was required for a more generic insight of user behavior outside work environments to gauge their ease with computer systems. This was a required parameter to distinguish between a novice user and a more computer savvy professional. The figures in this section indicated that most respondents spent at least 8 hours or more with computer systems which is a fair indication that they had acquired a fair knowledge of how computer systems work and they are should be aware of the risk presented by usage of such technology.

The final question in the demographic segment enquired about their nature of work and if they were supervisors or managers. This section was required to analyze the nature of responsibility they share and if they were end users subject to policies or they had further requirements of managing a group of people and also maintain a standard security within their environment. System administrators in the interviews conducted mentioned that they felt more confident in sharing details on risks associated with

information technology with managers and supervisors than end users. The ratio was approximately 80/20 in favor of end-users who were not subject to a supervising responsibility.

The next sections of questions dealt more specifically with information security and the theme of this research project, on making information security polices into better, sustainable, pragmatic and applicable practices. The first question I asked users was if they felt information security is essential to their day to day work. It was critical to understand if a user perceived the risks associated with using computer system and if they were comfortable with the notion of information security. Every respondent answered in agreement indicating that they understand the need for security policies and perceive them as a basic requirement in production environments.

The following question enquired if users felt information security policies are valuable to an organization. Business goals of an organization are almost always reflected in their corporate governance polices and more so within IT governance framework. As mentioned before in previous research our enhanced dependence on technology requires us to mitigate risks which are associated with proper governance of IT security principles and policies. Most respondents [92.59%] acknowledged this fact while a few were undecided on the matter.

The basic requirement for an organization to be successful lies in the unhindered operational ability to conduct business and create an environment where there is minimal hindrance for its employees. Previous conversations with system administrators revealed *inconvenience* as a potential factor which often renders good security policies

on paper impractical for use. Hence my following question asked users if they felt information security policies actually enhance productivity as employees within an organization? Even though most respondents [59.26] supported the motion, a fair population [24.07%] did not share the same views or were undecided [16.67%].

Good information security policies often do not yield expected results because they are confusing to users. Sometimes it is the nature of technology or the mode they are presented in or even the method of documentation that forces polices to lose their objective for users. Good policies which could have enhanced productivity thus get bypassed at user level. Respondents when asked if they felt information security policies are often times confusing and hence get overlooked were almost equally divided in their opinions. While 39.62% respondents felt policies to be not as confusing, a substantial 30.19% felt otherwise and an equal number of them were undecided.

Every policy which turns into a practice in a corporate environment has a lifecycle during which it ensures enhancements in productivity while mitigating risks for a particular technology or application. However, an information system itself is a dynamic environment and requires policies that relate to it to be up to date. Organizations who fail to address this issue regularly, are often faced with higher instances of noncompliance from users. In order to understand the work culture of the respondents and how active their work environment correlates to changing technological advancements, people were asked if they believed information security policies in their organization are up to date or required modification. Even though around 40 % of respondents felt their policies were up-to-date, a substantial number [23.08%] wanted some modifications and 36.54 % of them were unsure.

The primary objective of any policy either corporate or the ones which govern IT security framework, is to enhance productivity while mitigating. IT governance policies are meant to enhance business productivity through secure use of technology. Respondents were asked if they felt security policies create a more secure corporate environment and almost 89% believed it to be true. The remaining respondents were unsure.

Policies are often formulated based on industry best practices and are meant to provide guidance on how to conduct business that is beneficial to the organization and is less of a hindrance to users. However, some policies fail to take into account the diversity of environments and users and often fail to yield the desired outcome. In order to understand if our present policies are as usable as they were meant to be, respondents were asked if they thought information security policies are designed to help them work more efficiently. Most of the respondents [62.26%] felt that guidelines provided by policies actually increased their productivity while a lesser 16.98% felt otherwise and 20.75% of respondents were unsure.

During conversations with various system administrators in the first phase of this research, I found many system administrators felt they should be part of policy making and not just be included at the implementation end. This is also true in the case of end users who are responsible for the real governance of policies. User recommendations, their difficulties and suggestions should be obtained at times in order to make Information security policies more adaptable and usable by users. Asked if users wanted to provide suggestions regarding their organization’s information security

policies, the respondents were divided in their opinion. While 39.61% declined from that responsibility, 33.96% wanted to voice their opinion and 26.42% were undecided.

Information technology is a dynamic environment and information security policy changes occur with adaptation of newer technology, government mandates, and vendor suggestions and also with evolving global risks. Often the changes in information security policies are implemented but are not conveyed to users. This situation has in the past triggered a trust deficit between a policymaker and the user community and has led to poor adherence to information security policies. In the survey respondents were asked if they wanted notifications for every change with information security policies governing their organization. Most respondents [61.11%] welcomed the idea of notifications for policy changes while 25.93% preferred not to and a lesser 12.96% were undecided.

Earlier conversation with system administrators revealed that providing notifications about every change in information security policies put an additional burden on end users and deteriorates their productivity. Most of them believed that users should be notified of changes only pertaining to their domain that specifically affects them. Asked if users wanted to be notified of the changes which were specific to their daily work, there was slight increase in response for people who favored being notified. The number rose from 61.11% for all notifications in the previous question to 68.52% for specific notifications. Respondents who declined notifications and also who were undecided were recorded at 27.78% and 3.70% respectively. Respondents who were undecided on whether they wanted notifications for the entire volume of information security policy

changes were more sure when they were presented with the option for specific changes pertaining to their domain.

One of the respondents during my interviews had mentioned that certain Microsoft practices which were referenced by information security policies were extremely difficult to implement in their environment and most of the times were unusable or unsuitable for their users. In my opinion, it is of utmost importance that policy makers and system administrators who are responsible for designing and implementing policies give more priority to their production environments and business needs and not just follow best practices. Users who are subject to policies are often a great resource to gather valuable information from about feasibility of new policies and their requirements from newer technology before implementation. Respondents were asked if they wanted their system administrators should talk to them more before implementation of information security policies. Most of the respondents [87.22%] wanted their system administrators to interact with them more often before implementation of new policies so that they can suggest appropriate requirements and expectations from the same.

Recording the after effects of a new policy is equally important than its designing and initial implementation. Sometimes the spirit of new information security policies which were introduced gets defeated due to bare minimum adherence by users. Compatibility issues, feasibility issues or even conflict of objectives with policies and business needs sometimes causes more inconvenience than provide guidance to users. Respondents were asked if they wanted their security administrators to review a policy with them after it has been introduced to evaluate the after effects on users and business. A majority [88.89%] preferred to provide suggestions while a few of them were left undecided. The

response rate in favor was slightly better than the previous one which indicates that users felt it is more important to provide their suggestions after implementation of policies.

Some respondents during the interviews raised concerns about some end users' being non computer savvy or even not enthusiastic about information security. They felt users at times underestimate the pertinent danger of not following policies or information security best practices. Since better information security governance demands more focus on individual users being abreast with information security rather than a top down approach, users were asked if they preferred to learn more about information security at their organization. A substantial number [68.89%] of respondents expressed their eagerness to acquire more knowledge while the remaining respondents were either unsure or felt otherwise.

Respondents during interviews mentioned that providing excess information to users can often have adverse effects on their productivity. They felt that providing information about every threat that exists, will over burden and interfere with the daily work of the end users. They preferred to provide limited information to users about critical threats which were consistent with their organization. Survey participants were asked the same question and most [73.33%] of them were eager to learn more about current Internet viruses and worms and their practical implications on their daily work. A lesser 15.56% were unsure and 11.11 % were not keen on receiving those information.

In order to manage business effectively organizations often have numerous information security policies but there are times when a user feels confused or feels governing

policies provide inadequate guidance in handling critical situations. Respondents when asked if their organization's information security policies answer almost all of their security or work related questions were divided in their opinion. Even though most [42.22%] of them felt information security policies suffice their needs, a critical 37.78% were undecided and 20% felt they were inadequate.

System administrators always felt information security policies can better even when they were satisfied with their present level of control over information security at their organization. Reform and update of policies with newer technologies and business needs are critical to adherence and creates more acceptances amongst users. Respondents of the survey were asked if they felt their organization's information security policies can be better. Even though 54.55% of respondents felt strongly about it and a substantial 43.18% were undecided.

Existing policies often times do not reflect changes in business objectives or corrections per change in production environment. Even when system administrators attributed numerous reasons for lack of adherence to policies amongst users, outdated policies not reflecting true business objective was a critical one. Some policies derived from industry standard approaches may be good on paper but are often found wanting when it comes to implementation in certain environments. The inability to tweak policies often renders them being generic and not specific to certain work situations. Respondents were asked if they felt their organization's information security policies were too generic and lacked focus on specific business objective of their organization. Of them, 52.27% believed the policies they are subject to at work are adequate and specific to their

environment whereas approximately 30% of them were unsure and around 18% felt they lacked focus on specific business objective.

Sometimes the language or the literature or the sheer length of a policy can prevent it from being a good practice. In order to accommodate several attributes and address multiple issues, policies are often constructed as being very lengthy. This can throw a user off-balance and obfuscate the true objective of a policy. Respondents of the survey were asked if they felt that polices they are subjected to at their organization are lengthy and hence confusing. Responses were almost equally divided with 42.22% saying they felt it was lengthy and 35.56% feeling otherwise. The remaining respondents were unsure.

To gauge the perception of users as to who they think are responsible for information security at their organization they were asked if only system administrators should handle information security. Information security is a process which requires involvement at every stage to become successful. Adherence to policies by a user is equally important as the designing of good policies by security administrators. However, most respondents around 62% felt it should be handled by system administrators whereas around 27% felt otherwise.

The final question in this section of the survey was centered on the construction and presentation processes of a policy. Good policies on paper fail to yield desired results because users cannot fully comprehend the objective of a policy or a policy addresses multiple issues and there by steals focus from one particular situation. Survey participants were asked if they preferred information security policies to be simpler.

Most [68.18%] of them acknowledged that policies could be simpler while the remaining respondents either felt otherwise or were undecided.

The section of the survey was designed to gain a further fine grained knowledge on users' take information security, it issues and in responses to check for consistency in responses. Some questions were constructed to understand the computer proficiency levels of respondents and also requested them to provide additional responses if any which the survey did not include. This section employed a liquored scale to evaluate responses in order to make detailed observations in user reactions.

To obtain a fair understanding of responses, to check for the integrity and also consistency of the survey it was critical to analyze the computer proficiency level of respondents. A simple question was constructed, enquiring about their preference, their comfort level in using computers, their preference in using it often or if they use it only due to job requirements. Most users felt they preferred using computers most of the time and only a few indicated that it was part of their job requirements.

The liquored scale provided a unique opportunity to gauge varied levels of user reactions rather than a generic binary answer and also evaluated the degree of acceptances and disappointments within users for specific enquiries. Respondents were asked to rate how they felt about information security practices and policies at their organizations from level of dissatisfaction to being extremely satisfied. Of them approximately 65% of them were either satisfied or extremely satisfied where as 22% felt neutral about it. Around 9% of the respondents felt things should be improved.

Following up on a question from the previous section on how and if information security policies influence their work, respondents were asked if they felt policies improved their productivity in their daily work. Almost 57% of respondents felt it actually helped them to follow policies and become more productive whereas approximately 16% disagreed with the statement. Few [approximately 27%] of them were undecided.

Advancements in information technology have been often attributed for the recent successes in the production and work environments however; the advancements have also brought about an increased growth in the number of Internet worms, viruses, malwares and many more that hinder our progress. It is a users' responsibility to administer caution when they interact with information technology whether at work or at home to protect their identity and data. To review the notion of such responsibility amongst users on how they perceive this nature of threat and it resolution, respondents were asked on how concerned they were when they encounter Internet worms and viruses. The survey revealed that most participants [65.91%] were concerned about these threats but only a fraction 36.36% of them felt adherence to information security policies might help resist these situations. A worrying section of them [15.91%] felt it was not their responsibility and someone else will handle those situations for them in an event of such attacks.

A primary reason voiced by most respondents as to why good information security policies fail to be transformed into good practices was convenience. Convenience in terms of their usage, the interference with their productivity and also the time consumed in their adherence, often discouraged users to follow policies. Respondents in the survey were asked if they felt they were inconvenienced with adherence to security

policies. A majority [43.18%] of them were undecided if policies actually helped them or interfered with their work habits. The remaining respondents who had an opinion were divided in either agreement or disagreement that policies hindered their productivity. Participants who perceived policies to interfere with their daily work were recorded at 31.82% while the rest either disagreed or strongly disagreed [total of 25%].

Most respondents were eager to learn more about information security policies and wanted to gain further knowledge about relevant threats as evidenced in a previous question in the survey. Hence it was also critical to know if they felt supporting materials to aid this process in their organization was effective or adequate. Even though most respondents were of neutral opinion to this question, approximately 36% respondents felt the materials available serve the primary purpose. However 20.45% of them also felt that it can better and were not satisfied with the present availability of materials.

In the final wrap-up to the survey, respondents were also encouraged to provide additional opinions which were not covered in the questionnaire but were relevant. A few of them who responded to this question believed policies could be simpler or felt present situation is robust enough to handle adverse effects of information technology. Some of them also felt it is the job of respective system administrators to handle the same or specific opinions about their present work related problems.

7. Results:

The premise of this research relates to the concept of the importance of information governance in a corporation. Before presenting my findings and concepts on information security policies and practices, and its points of failures, success, and improvements, I would like emphasize the need for governance in general. Governance [18] has often been described as the act of governing activities, granting permissions, and verifying performance of entities that constitute an integral part of an organization. The need for governance transpires from the requirements in obtaining a transparent yet cohesive act of management through policies and decision making that enhance the productivity and business objective of the organization. Information security governance extends from the primary corporate governance needs to embracing newer technologies in the field of computer and information systems. IT Governance is a subset of basic governance processes that have a specific need to manage, improve, and mitigate risks associated with integrating information sciences within a business process. The structure of the information security governance process includes the concept of management of assets through policies and the adherence to laws and legislation prescribed by the government or those established by the corporate body itself. This structure is designed to reflect the basic organizational structure and further the objectives of the corporation by reaping benefits of improvements in information sciences. The business, comprising directors, executives, and stakeholders and all physical and intellectual assets are aligned in balance within the governance process to provide a stable and robust risk management environment, maximizing productivity.

Large corporations such as Arthur Anderson, Tyco, and Enron are just a few examples where the lack of proper governance and execution of uncontrolled business processes have rendered organizations extinct [19]. Even though many research papers and management may contradict the fact that employees are more valuable than information and intellectual property pertaining to an organization, it is beyond doubt that information and credible management of the same holds the key to the success of a business. IT governance, as mentioned before, has two potential benefits. One, it adds value to a business or corporation, harnessing the growth in information technology, and increases its capital revenue or inviting more business. It also helps in mitigating risks which exists with advancements in information technology. The policies and procedures defined in the risk management guidelines form the backbone of the management and governance structure. They are derived from several industry best practices standards, both federal and state laws, and also from the primary need for the business. However, studies conducted before have indicated that the mere existence of information security governance does not relate proportionately to the progress of an organization. Companies with above average governance procedures have generated 20% higher profits than their counterparts with below par management with similar strategies. The need for this research study stems from the very fact that there exist fundamental differences between better information security governance and an average one. The paper identifies various points of failure in implementations of security policies which look robust and fool proof but fail to deliver the desired results.

Based on the data collected during the research, through interviews with security/system administrators and the users subject to the policies, it can be

determined that there is a need to regard policies and procedures of information security governance as a process. It has a life cycle of its own, from its inception following a business need, to its formulation into a feasible and usable guideline, to implementation within users, and to being replaced with newer procedures. Information technology is a dynamic environment and policies relevant today may not be suitable for the future. The notable differences between a policy which transforms itself into a good practice and the one which fails have been recorded below as observed in the research study:

a) Ownership of responsibility: Information security policies set by management and security administrators offer guidelines for increased productivity in a risk free or risk managed environment. However, it has been observed during discussions with several system administrators and even CEOs of organizations that true governance lies with users who adhere to them to make it a practice. Administrators are often limited in their scope in either designing or implementing newer policies which further business objectives, but the guidelines need to be followed by users. The burden of responsibility in managing a secured environment in production thus falls on every person who comprises the network. From users to security administrators to system administrators, everyone has an integral part to play in making a policy a good practice. Alienation of users from that responsibility will encourage them to treat their own production network as a third party environment where security of information systems is not their concern. Organizations that have often obscured business objectives and importance of information security, and only have mandated policies to be followed by users have faltered more often in the long run.

b) Involvement of appropriate personnel: During the course of the interviews, many system administrators expressed their limitations with their involvement during policy formulations. Participation of people responsible for policy implementation is as important as design of the policy itself. The need to know an environment and the nature of business before executing industry best practices often determine the success and failure of such business strategies. The industry best practices are often defined on assumptions of a standard production environment with preconfigured parameters and may or may not suit all business needs. To ensure the progress of business and to obtain the desired results from business strategies, it is critical to involve personnel who are responsible for their implementation. Their insight on previous implementation fallouts, their knowledge of the complexity or simplicity of their production environment, users' behavior and limitations of resource availability, all account for a policy becoming a success. Moreover, when an organization exerts its global presence with multiple office locations, it is more crucial to gauge the notion of corporate culture, user behavior, and the environment of those remote locations before implementation of core policies. Strategies and policies defined by management without the involvement of people responsible for its implementation have often rendered policies meaningless in corporate environments. The adverse effects of such actions have hindered the growth and progress of businesses and have contributed to discontent amongst users.

c) Implementation failures: Success and failures of policies have often been determined by the effects that a new policy brings to a corporate environment. Administrators have often ignored or bypassed the need to assess networks after

policies take effect. Interaction with users, their take on new policies, changes in the production environment, the amount of tolerable user discomfort in their work activities, all are factored into success or failure of policies. When a change in policy occurs and users are required to accustom themselves to the new procedures there always lies a time period when an administrator needs to encourage a user to adopt the newer procedures and the user accepts the same. This time period is crucial to gauge the effectiveness of the policy, feasibility of its use in the network, and also to determine whether or not it actually forwards the business objective without adversely affecting a user's performance. Policy implementation failures arise from the lack of feedback from the production network after its implementation. There have been situations where minor tweaking or making conditional exceptions to policies have helped system administrators to effectively implement policies better. Rigid adherence to policies even when they are extracted from industry best practices can sometimes cause conflict of interest within a business and result in its failure.

d) Need for education: The growing trend in our present industry prescribes separation of information or its conditional access for users. System administrators interviewed believe that excess information to users will exert additional overhead and interfere with their productivity. Transfer of information related to security should be controlled and allowed only when there is need. However, data collected during the survey indicate that younger generation of users who spend more than 8 hours with computer systems often look to participate more actively in the information security governance and desire access to more information. In several questions asked during the survey, a majority of users preferred being updated not only to changes pertaining

to their daily work, but the information security for the organization as a whole. Even though it is true that making all information security related information available to users might pose a threat to the confidentiality of the business, it is also critical to find the right balance where users feel more involved in the security framework. System administrators often tend to feel that when more information is divulged to users it poses a security risk to the environment in addition to adversely affecting their productivity. However, in order to make users more responsible and aware of existing threats in information technology, it is critical to educate willing users with appropriate resources. Use of newsletters, corporate magazines, and email notifications regarding information security threats should be more readily available since the present generation of users are more knowledgeable and are at ease using computer systems. System administrators need to develop more controlled trust and faith in users' ability to handle information systems and the risks associated with it. Education should be made an integral part of policies so as to make them more acceptable and usable amongst users.

e) Limitations of policy: Information systems security is a dynamic environment which has seen a tremendous amount of change in the past decade and half following exceptional growth in technology. Organizations which have harnessed these advancements in technology have increased their productivity manifold. However, users are often faced with strategies and policies that do not reflect the present advancements. Our present information security policies have often lacked the reform necessary with technological advancements or changes in business objectives. Management and administrators responsible for designing and implementing policies have often left older strategies linger within the production environment which adds little

to no value to the productivity of a user. Hence users often perceive policies as an unnecessary interference in their day to day work rather than easing it. Policies need to be updated regularly and management and administrators are responsible for making them more usable and useful to end users and customers.

f) Simplicity: Inconvenience has often times cited by users and administrators for which a policy which is good on paper fails to become a good practice. This inconvenience sometimes stems from the complexity in the language or definition of a policy or its length which leads common end users to lose focus from its core objective. In order to help users comprehend the need for such policies and adhere to them to further business strategies, policies need to simpler. Focus should be on helping users visualize the business need for such a process and how it can enhance their productivity.

g) Culture Change: Information security governance often reflects the general organizational structure. The policies and strategies determined at the helm by management and administrators are often pushed down to users in a top down manner. This approach often limits the scope, accountability of users, who form an integral part of our security governance and also discourages their participation. This behavior forces users to treat their production environment as an alien work place rather than their own domain. In order to establish a better security governance framework, one might consider a more bottom up approach which focuses on sharing of appropriate information with users, paying heed to users' needs and recommendations, and devising of policies which are more feasible and usable by users. Security

administrators and management responsible for policy making often assume the users' scope as being limited to their specific work, and try to define best practices on their behalf. This situation at times is inappropriate as mentioned earlier in the analysis, as policies for the production environment often requires critical user input to make them more acceptable. Users on the other hand often doubt the effectiveness of policies installed. They feel alienated from previous situations where policy changes were made by management without citing reasons. There are also situations when they could not comprehend need for specific policies because they are unaware of the threats associated with information technology. They fail to visualize their production environment as their own domain and hence refrained from sharing responsibility critical for the creation of secured work environments. A culture change is essential in our present situation where we counter multiple attack vectors, and responsibility needs to be shared across all personnel who comprise a secured corporate network.

8. Recommendations:

Based on the interviews conducted and data collected in the survey during this research project I would like to draw a few basic guidelines that may help system/security administrators evaluate and benefit from a better information security governance structure.

a) Bottom-up approach: At times it may be relevant for administrators to adopt a bottom up approach with focus not only on business needs but also user needs when a new policy is introduced. It will help them gauge needs and issues pertaining to their specific production environment before policies are applied.

b) Culture change:_Sharing responsibility amongst users and allowing controlled access to information pertaining to security policies and adoption of newer technology will make users more knowledgeable and responsible in their daily interaction with information systems. Explaining the need to update/modify or change policies to counter newer threats will make policies more acceptable.

c) Feasible usable policies: Administrators may keep an open mind while designing policies based on industry best practices and customize it accordingly to fit their production environment better to yield desired results. The critical changes will make information security policies more usable in their environments.

d) Involvement of appropriate personnel: System administrators responsible for implementation of policies at specific locations should be consulted by management who define information security policies for better understanding of work environments.

e) Simplicity: Policies should be compiled using simple language and restricted to a limited length so that users do not lose focus on the objective of the policy.

f) Feedback: System administrators should interact more with users after a new policy is put in place to gauge its after effects. This is critical for the success and acceptance of a policy amongst users. This will often help administrators to evaluate if a policy delivers the desired results and furthers business objectives.

g) Update: The success of a policy lies in its relevance to business objectives and newer technologies. Policies should be updated and reformed with dynamic changes in technology to maintain relevance in production environments. Older policies which add little or no value should be discarded to maintain a simple security governance structure.

h) Education: Our present day users spend more than 8 hours with computer systems and feel the need to learn more about information security to improve their handling of information systems. Organizations should make use of corporate newsletters, magazines, email notifications, or even hold quarterly meetings to educate users about the relevance of information security and persistent threats. It should also be made part of new policies whenever appropriate.

i) Repetition: Rejection of policies often occurs because users get used to a certain mode of operation and fail to change their work habits when new policies are introduced. When a policy is relevant, repetitive use of the policy amongst users will eventually pave the way for the policy being accepted.

j) Firm implementation: System administrators may at times encounter situations when certain sections of users fail to adhere to policies even after repetitive implementation. In those situations one may use peer pressure to influence unwilling users and encourage them to adhere to policies. In an event where lack of adherence to relevant policies creates security risks to corporate environments, fear of drastic measures can also be used as a tool for motivation.

9. Future work:

As per the 19th American Institute of Certified Public Accountants' Annual Top technology Initiatives survey for 2008, Information technology governance ranks second as one of the more pursued initiatives. It comes second only to Information Security management which is also essential in the governance framework. In our present times IT governance with its use of policies and procedures harnesses the growth in information technology while mitigating risks associated with it. It is a critical component that often defines the success or failure of businesses. IT adds value to business as well as encourages key stake holders such as board level executives, department heads, and managers with limited technical knowledge to make appropriate decisions which are in the best interest of the business. With advancements of technology and increased rates of threats being detected on a global landscape, improvements in our existing IT governance structure will be imperative. Further research should be conducted on how to make information security policies better reflect business objectives and yet remain feasible and usable to users. Improvements in the implementation of policies and making them more users friendly and acceptable without lowering the standards of business will be a challenge for the future.

10. Conclusion:

Information security governance, with its policies and procedures, furthers business objectives of a corporation providing it a competitive edge in the global market. Today, when every organization is trying to harness advancements in technology to increase productivity, it is highly imperative to evaluate the existing information security procedures that mitigate risks associated with it. As evidenced throughout this research project, organizations who have successfully established robust security procedures have benefitted much more than its counterparts that possess an average IT governance structure. Effectiveness of information security policies and procedures, and their feasibility and usability within a production environment often determines if it can transformed into a good practice, and hence provide acceptable security for information. Many parameters factored into the success or failures of policies include culture change, adaptation to newer technologies, and even sharing of responsibility amongst users and policy makers. Our present generation of users is more knowledgeable and their potential should be fully realized in creating a secure environment.

II. References:

[1] Dhamija, Rachna, J D Tygar, and Marti Hearst. *Why Phishing Works*. http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf (accessed July 7, 2010).

[2] gladiatortechnology. http://www.gladiatortechnology.com/press/BFITSRDec09.pdf (accessed July 7, 2010).

[3] Gross, Joshua B, and Mary Beth Rosson. *Looking for Trouble: Understanding End-User Security Management*. http://www.cc.gatech.edu/classes/AY2008/cs4235b_fall/Group1/UnderstandingEndUserSecurityMgt.pdf (accessed July 7, 2010).

[4] Herley, Cormac. *So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users*. http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf (accessed July 7, 2010).

[5] Hinde, Stephen. "Security surveys spring crop." *Computers & Security* 21, no. 0167-404 (2002): 310 - 321. doi:10.1016/S0167-4048(02)00404-2. http://www.sciencedirect.com/science/article/B6V8G-46692F5-4/2/aef02bbe7ed912eab7824c7264ed5f61 (accessed July 7, 2010).

[6] identitytheft. http://www.identitytheft.info/breaches09.aspx (accessed July 7, 2010).

[7] Kern, Axel, and Claudia Walhorn. "Rule support for role-based access control." In *SACMAT '05: Proceedings of the tenth ACM symposium on Access control models and technologies*, 120 - 138. Stockholm, Sweden: ACM, 2005. doi:http://doi.acm.org/10.1145/1063979.1064002 (accessed July 7, 2010).

[8] Mannan, Mohammad, and P C Van Oorschot. "Security and usability: the gap in real-world online banking." In *NSPW '07: Proceedings of the 2007 Workshop on New Security Paradigms*, 1 - 14. New Hampshire: ACM, 2008. doi:http://doi.acm.org/10.1145/1600176.1600178. http://portal.acm.org/citation.cfm?doid=1600176.1600178# (accessed July 7, 2010).

[9] Murray, William. "Good security practice for personal computers." 1986. In *PCS '86: Proceedings of the Northeast ACM symposium on Personal computer security*, 1 -12. Waltham, Massachusetts: ACM, 1986. doi:http://doi.acm.org/10.1145/318772.318775 (accessed July 7, 2010).

[10] searchsecurity. http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1256995,00.html (accessed July 7, 2010).

[11] Siponen, Miko, Seppo Pahnila, and M Adam Mahmood. *Are Employees Putting Your Company At Risk By Not Following Information Security Policies?* http://doi.acm.org/10.1145/1610252.1610289 (accessed July 7, 2010).

[12] Tsiakis, Theodosios. "Information Security Expenditures: a Techno-Economic Analysis." *International Journal of Computer Science and Network Security* 10, no. 4 (April 2010): 1 - 5. http://paper.ijcsns.org/07_book/201004/20100402.pdf (accessed July 7, 2010).

[13] wellsfargo. https://www.wellsfargo.com/privacy_security/online/guarantee (accessed July 7, 2010).

[14] Willert, Jon. "Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters." *sans.org*, October 22, 2001, 1 -15. http://www.sans.org/reading_room/whitepapers/hsoffice/computer-security-practices-home-home-office-small-business-telecommuters_616 (accessed July 7, 2010).

[15] Write Down Your Password. http://www.schneier.com/blog/

[16] Collins, Hilton. Govtech. http://www.govtech.com/gt/736410 (accessed July 8, 2010).

[17] Zurko, Mary Ellen. *User-Centered Security: Stepping Up to the Grand Challenge*. http://www.acsac.org/2005/papers/Zurko.pdf (accessed July 7, 2010).

[18] "Governance." *Wikipedia*. N.p., 9 Aug. 2010. Web. 18 Aug. 2010. http://en.wikipedia.org/wiki/Governance.

[19] **:**Poore, Ralph Spencer. "Information Security Governance." *EDPACS* Nov. 2005, Volume XXXIII ed.: 1 - 8. Web. 19 July 2010. http://www.informaworld.com/smpp/content~db=all~content=a768432841

[20] Tarn Michael J, Raymond Heath, Razi Mohammad, Han Bernard T. Exploring information security compliance in corporate IT governance. http://iospress.metapress.com/content/330280271432078j/ (accessed July 7, 2010).

12. Appendix:

[A] Interviews:

Interview 1 Respondent 1

Who do you think is responsible for security in your organization?

The whole population of the organization because people who design security and implement security they are limited to designing or implementation. The real governance is by the people following the policy.

Can you provide a couple of instances, in your experience, where you find it difficult to implement a policy that might not be practical but is essential?

I think one of the difficult policies to put into practice is the password changing policy which occurs at regular intervals for end users. In normal circumstances every individual differs and when you have a policy for instance where a user needs to change a password every 3 to 6 months, a user should consider it their own domain and should adhere to it. However, this does not happen normally because people get comfortable using the same password since it is easy to remember. It is a grey area where there is a need to push it out even though it is difficult and force people to adhere to it by not giving the option and changing it through the backend system.

It also requires a culture change and it takes time but eventually people do get it.

Do you consider yourself and other system administrators to be active participants in policy formulation?

Yes. The policy is governed by a main central body which is in NY and people who are part of the governance body they are ones who are responsible for designing the policy. They design policy based on the risk out there and at the same time the branch policy

primarily inherits the main policy but for business reason they might have to tweak some policy or sub policy. However this has to be approved by the head or the policy officer.

Does the central body make active considerations of different system administrators from various branches?

Yes, all the different operations including the IT or the non IT would be in consideration. Any security policy just does not govern IT but the business as a whole and the components involved in it.

If you have a system administrator in a branch location, which has problems in implementation of a policy, does that make a difference in formulation of policy by the central body?

It does not make much difference when we form or develop a policy because all policies are governed by best practices and standards.

In situations when you have to custom make policies do you tweak your policies to suit your need?

No. The main policy has to be followed and if there is an issue that needs to be resolved through the base policy there is amendment to the policy or there is an exception granted for a short duration but everybody has to follow the base policy.

Do you outsource information to different countries?

Generally we do not outsource information to different countries but if we need to, we have a policy in place.

Will you be concerned in a situation where you have to do business with a different country and when their security policies are not as good as your organization?

Yes if they do not have the same standard I will be concerned. Their policies have to meet our standard and if it is not we need to mutually agree to a common standard and check if it is worth it.

If the security policy of the other organization is not at par with ours then it is a concern. Having said that there are exceptions when a policy may be weaker but there is a business need, then each of those policies needs to be evaluated for the risks and then a decision has to be made.

Do you find users to do bare minimum when it comes to adhering to security policies for instance password policies?

Any policy that is made takes into account what an end user can and cannot do or what they are allowed or not allowed to do, based on that, password policy is a difficult one to implement.

In your opinion does the end user see adherence to policy as a hurdle to their day to day operations?

Initially, they may be overwhelmed but once they get used to it, it is not a hurdle. At the end of the implementation cycle a user sees the benefit of adherence to a policy. Initially when a user does not see benefit in following a policy, it is necessary to educate a user as to why it is necessary and why it is done and what are the end goals and once they start following it they would see the benefit out of it.

For example as we talked about the password change it is beneficial to the user itself so they are the ones who are responsible for their act. If their passwords get compromised their identity gets lost and also can cause damage to the company.

When certain users do not feel the need to adhere to security policies initially, do you have procedures to educate them or encourage them to follow these policies?

With policies we also have training materials which are send out timely as messages. It is also included in a policy that training is necessary.

Can you provide couple of examples as to how you will go about educating users in this regard?

We send out flyers or emails with the forth coming changes or with the reminder that security is everyone’s concern and they have strictly follow the policies.

In situations where there is global virus attack or phishing attack do you feel the need to let users know about them?

If there is a known error message then a message goes out that certain worms or certain email hacks are happening, be careful do not click on it, a notification goes out primarily as an email. However, that is only pertaining to a virus, at the same time we don't notify every single incidences that occur in a security paradigm to the end users cause they will not be able to understand.

In your opinion why do you think people do not like policies?

Sometimes it is not clear to them what the policy is intended for. Secondly, till they are used to a policy, it is worry for their day to day work. However, once they are used to it that overhead goes away. Thirdly, implementing a policy requires a culture change because users gets used to a certain way and then with implementation of policy we ask them to do it in another way.

Are you satisfied with security at your organization?

I am satisfied but there is still room to grow. It is not a static environment and keeps changing and one can never be satisfied. You can be satisfied with what you have and what the controls are but there is always room to grow and fix issues that you may have. So I will never say *I* am completely satisfied because the dynamics of security policy keeps changing but I am satisfied with the controls and procedures that we have.

Do you have a unique policy that is specific to your organization the way you do business or people you interact with?

Yes we do and it is confidential.

In your opinion in order to gain further fine grained control over your security procedures do you think you need to tweak/change your policies or change your implementation

methods? It is a combination of actually four things. First is the change in the policy. And then there is the implementation and also educating end users and change in the technologies. The more you give users control, the more risks you have, not that the users won't know but they may be unaware of the risks.

If you could pick one of these four things which will it be? Where do you see the big change coming in?

It is a very open ended question, but if I were to pick one it will be in *implementation*. However, all of the four changes are required and are in equilibrium. You cannot have a good implementation and a bad policy and a good policy and a bad implementation. You also cannot have both good policies and implementation but bad users and also you can have all three but poor technology. We cannot concentrate only on a few of them and ignore the rest. In a distributed environment it is essential to consider all of these four things to achieve a good secure environment.

Back in 2005 Sarbanes Oxley was very popular and every company was adhering to it. One of the auditing policy encouraged companies to stop using IMs in their environment to make it more secure. Many companies removed IMs without notifying the users. Do you think companies should have communicated with users since they were used to IMs in their daily communication? Does this create a trust deficit between the policy maker and the end user who is responsible for following it?

In some instances it may, and again, they are all related to the risks they are trying to contain. In our example IMs have been taken out in many cases and the risk of running an IM based on Sarbanes Oxley is higher. Yes it affects users in their day to day jobs but each of these policies or changes to these policies in certain magnitude that occur in accordance with government law are outside their control and you have to implement it. Security administrators have to evaluate each of those rules and impact of those rules and what are you trying to protect. It is the job of the security administrator to protect the organization as a whole. Hence in some cases there might be a rift between end users and security administrators or system administrators. In most of the cases when there is a BAU kind of process there is not rift.

Do you think it is necessary to let users know of the current situation so they are aware as to why it is necessary?

It depends on the user population. If the users have limited access and their operations are not affected they do not need to know all details, as providing them all the details will cause more confusion and will affect negatively. If however, users comprise system administrators then you need to tell them.

Moving forward in your opinion what would you recommend making a good policy on paper into a good practice?

My recommendation will be any policy on paper has to be practical enough to implement. You cannot have a policy which is very good on paper but not practical to implement it. So one has to look at the environment, the requirements and come up with a policy that satisfies both sides of the world, the security paradigm and also the customers and users experience. The four fundamentals of any policy to be successful will be the ones I mentioned before.

Interview 2 Respondent 2

1. How do you perceive security at your organization? Do you feel Comfortable with the security that's already present?

   It is good security. As we exchange more information and store and manage more, awareness of security increases and the attention we pay to implementing best practices and adhering to standards stays in pace with that also.

2. What are the difficulties you face in implementing policies into practices? Couple of instances.

Our inclination and our preference from a pure security perspective will be to block everything outside of HB. We will not allow people to access anything on the web or use the Internet at all. Obviously that will cripple the business so as we blocked and filtered and tried to control that, we have gotten feedback from user s, “we need access to that site”, either from an administrative person saying that attorney I work with asked me to go this site to download something or may be attorney saying to us I am doing a research about gambling for example, I have to able to get to this gambling site and you block them all. We had to create special policies for different types of situations.

Person by person or PC by PC we grant access.

3. Do you have a dedicated Security Team?

We have security Policy and we have educated people so everybody has some sense of security. Both, the other respondent & I have our CISSP certification and others in IT have gone through some security training.
Shorter answer to your question to ‘do we have dedicated people who do only security?’ No.

4. Do some people specifically manage security?

Yes

5. Are you guys involved in deciding which policies are best for your company?

We participate with attorney and other administrative staffs during the creation of policies.

6. Do they take your and other system administrators’ opinion who works along with you?

Oh sure they ask for it.

7. Do you also get to participate during the formulation of policy rather than just at the implementation end?

   Start to finish.

8. Do you outsource your work to other nationalities such as BPOs?

   No.

9. In your experience have you seen users to do bare minimum to adhere to the practice?

   Password Policy - the bare minimum.

   Respondent A: Depends on the individual. There are individuals who understand. There is a need is more based on business needs and who their clients are. Some people may be working as matrimonial attorney and may not be up to speed with corporate attorney because they have very different business needs.

10. Do you see there is a need to encourage people who are lesser inclined to adhering to policy?

    It will be a nice thing to do but sometimes they are the owners of the business so it is kind of difficult. Pick and choose your battles, I would not choose that as long as they are complying.

11. Do you think you can improve the situation by bringing changes to policies to better fit your needs or encouraging more people to indulge in security policies?

    Education is probably the biggest one.

12. How do you educate your users?

We include some information in our internal semi monthly newsletter. We send email messages when appropriate to let people know of certain things for e.g. maybe it's a phishing email that is going around. We also have started a series of educational presentation about security specifically. We did our first one in May of this year and we may do other live or we may record them and put them on our internal website so that people can watch video and more and more share with other people. We also have written communications like an email about certain security policies and practices.

13. Do you see that trend as a threat to your company?

As long as anyone is using a computer there is a threat, but the password convention is the commonly accepted convention with different types of characters with upper case and lower case and certain number of characters and certain minimum.

14. Do you perceive that users do not envision following policy as part of their work but as a hurdle they need to cross to get to their real job?

There is an interesting mix of people understanding the need for security and wanting to comply and really trying to comply but also trying to other things.

15. Do you think people are more confused when they want to comply with security procedures? For example external hard drive encryption.

I don't know if they are confused as much as they are so busy and are trying to satisfy the attorneys and clients that if they haven't been in the situation as you described before [sending a hard drive out] they may not know what to do? They almost certainly

have some understanding to do something so they will ask another administrator; they may ask an attorney, they may call HR; they may call the help desk [IT].

16. Are there any reasons in your opinion as why users might not follow security policy?

It's get in the way of work and life. Inconvenience.

17. In one word you do take security very seriously, it is very essential?

Oh Yes! Without confidentiality of security we are out of business.

18. You also make it a point to push it down to end users?

Yes, but it is a long process and takes multiple repetitions of any one thing but we work at it pretty hard.

19. What is one of your most unusual policies that are very typical to Harris Beach?

The need to give certain individuals/attorneys specifically access to sites that we don't give anybody else whether it is gambling or sex, social networking, we block all of that stuff. Very small number of attorneys has the legitimate need to access those sites in representation of clients. They need to do the research.

20. Since there is a gap between a policy and practice what is in your opinion is the best way forward?

Refresh, keep on top of the policies
Update as necessary.
Keep it at the forefront because things have a tendency to get buried.

Interview 3 Respondent 3

Who do you think in your organization is responsible for security? Is just the system administrator or the users?

The ultimate responsibility for security is for the security administrators. We have specific people whose job is to be in charge of security.

Can you provide me couple of instances, in your experience, where you find it difficult to implement a policy that might not be practical but is essential?

A specific instance is when there are security policies such as the one which automates the installations of a Microsoft product for installations on computers. Sometimes the security policies they have are strict and not suitable to adhere to them because the applications won't work if you adhere to the security policies.

So in those situations what would you do?

Usually we try to log exceptions and check if in a policy if they will allow for exceptions. However, often they are not well documented it comes up again and again. They asked us over and over again to implement a policy which we told them over and over again we can't.

So often time we run into the policy that doesn't make sense, which are not applicable to or are not able to apply to work situations.

When a central body gives out a policy and different system administrators from different branch locations have to implement them, do they come up with their own individual modifications which are specific to their work space, does the central body take that into consideration in subsequent formulation of policies?

Usually the people who develop the security policies they sit by themselves and decide what they are going to do and they do not pay attention what happened before.

They paid attention to the environment when they developed them.

In your experience have you found it difficult to maintain a certain standard of security in different branches or different offices?

Yes.

Are they implementation issues, comprehension issues or are they something else?

Two things, firstly, the policy isn't made with an open mind focusing on different needs of different departments. Secondly, the end users also do not want to do it.

But as far as the different departments are concerned they cooperate with each other. We usually work together to try and implement policies as best we can.

Do you outsource information to different offices and organizations?

Yes to multiple companies.

Do you see that as a threat, where the standards of security might differ regarding policies.

No. Even though we deal with other companies, as much as possible proprietary information is kept proprietary.

Can you provide an example where you find end users to do the bare minimum to comply with security policies?

Most noncompliance comes from non-computer savvy people. Most people either comply or they care not to comply with security policies. I have not seen them in between.

Do you feel there is a reason why certain people do not comply with security policies?

There are those people who just do not understand due to lack of computer knowledge and there are people who do not care. They feel they are exceptions and security does not matter for them.

Do you feel there is scope for improvement as to how a policy is constructed or implemented to encourage non complying users?

Yes I think there can be improvements with explaining a policy to users as to why policy and security is important. We do not communicate that enough at times.

What are your recommendations in this situation?

I think the best thing to do is to try to explain to people the reality of the threat. I do not think people understand how big the threat is for the amount of damage that can happen through their computers. That is one of the biggest thing we can do. If people understand their threat, I think they would do a better job of following the policies.

If you notice a threat on the web for e.g. phishing attacks, do you make users aware of the situation?

I think that kind of thing overloads them and they stop paying attention to it. I think the information that you give them has to be something they get often enough but also seldom enough that they will listen. Because otherwise after a while they will stop paying attention to what is said.

If there is a significant attack on a company we should tell people not the specifics because that can cause danger but that something happened or could have happened if it was successful.

Do you feel users do not see proper cost benefit leverage in following policies where cost is users' time and benefit is security?

I do not think they understand the benefit because partly they do not understand the threat.

Can you recall one most unusual policy that you have seen that is relevant to work place but may be not others?

Password policy- believe it or not, we are restricted to simple passwords because some of the people implementing the password policy do not understand the technology. For e.g. there are cases where we use 8 character user names and also when they do not allow you to use special characters in a password because old technology did not allow it. They are stuck will old policies.

Is there scope to update policies to new technology?

Yes. There is a need to update the security policies because security policies are often times in regard to technology.

I personally use very complex passwords for many different things but I have to use simpler password than I want because the policy won't allow it.

As a system administrator if you were to make a recommendation to improve our security structure, where do see the most change coming in?

I think that the consequences of not following a policy have to be more real. Few companies have real consequences. To rephrase, for people not following policies intentionally there should be real consequences.

Do you think updating a policy is also important? For instance certificate errors are almost 99.9% false positives and in that situation should a user follow the policy or use common sense to overlook that particular policy?

To be honest I do not know, never thought about that. Yes that is a problem because often times you get so many certificate errors and also you are tired of saying *yes* time and time again when you know it is bogus.

Back in 2005 Sarbanes Oxley was very popular and every company was adhering to it. One of the auditing policy encouraged companies to stop using IMs in their environment to make it more secure. Many companies removed IMs without notifying the users. Do you think companies should have communicated with users since they were used to

IMs in their daily communication? Does this create a trust deficit between the policy maker and the end user who is responsible for following it?

I think there is trust deficit both ways. I think there is trust deficit with end users because they tend to think that lots of these policies are not needed and hence they do not follow them. In the same token there is a trust deficit from the policy makers side in that often times they just get a general policy from Microsoft best practices for instance which they just do not evaluate before they put it in place. They sometimes institute it without evaluating what impact it has on the customer and end users who have to work. It is on both sides. They do not trust end users to know what tools they really need and what tools are just fun. The end users too do not understand the policy and do not agree with it and hence do not follow it.

Interview 4 Respondent 4

Who do you think is responsible for security in your organization?

As a System Administrator, I along with other IT support engineers feel responsible for security in the organization. But from a security perspective, we make sure that all users have been educated on the aspects of maintaining a secure IT environment.

Can you provide a couple of instances, in your experience, where you find it difficult to implement a policy that might not be practical but is essential?

There have been few policies which may not have been practical, but not following them might have worsened the situation. IT staff and non-IT staff often have divergent views when it comes to the ownership of intellectual property. Complying with IT policies has been difficult for some non-IT staff. Non-IT staff has not always found the idea of having computer security policies applied to their desktops or workstations acceptable. But these policies are needed for data security and web security.

Do you consider yourself and other system administrators to be active participants in policy formulation?

Yes, since we as system administrator are responsible for maintaining a secure IT environment, we have been regularly participating in the policy formulation and any upgrades to those policies, as necessary.

Does the central body make active considerations of different system administrators from various branches?

We do not have multiple locations but since there are multiple engineers at one location, all of them have equal responsibilities towards the security plan.

If you have a system administrator in a branch location, which has problems in implementation of a policy, does that make a difference in formulation of policy by the central body?

Again since we do not have multiple locations, this question would not apply but by experience, I can say that I have observed that there is usually a centralized plan but if there are issues which are location-specific, central body does tend to bend rules to accommodate exceptions which would suit that location but would not risk IT security for other locations.

In situations when you have to custom make policies do you tweak your policies to suit your need?

Yes, I have done so to meet the needs of the organization but keeping in mind the IT security policy.

Do you outsource information to different countries?

No.

Will you be concerned in a situation where you have to do business with a different country and when their security policies are not as good as your organization?

Yes, if there is a need to outsource, I would make sure that security practices at the other organization is equally good and acceptable

.

Do you find users to do bare minimum when it comes to adhering to security policies for instance, password policies?

Most of the times, I have noticed that users are not very enthusiastic when it comes adhering to security policies and so as a system administrator, I have forced policies like having users change passwords every 90 days and/or creating secure passwords with minimum required nomenclature.

In your opinion does the end user see adherence to policy as a hurdle to their day to day operations?

For about 98% of the time, end user would not complain about following the security practices. There are instance like content filtering or regular password changes or e-mail management, where the end user would voice their opinions against. But again, not so much as to the fact that policies like these are hurdles to their day-to-day operations.

When certain users do not feel the need to adhere to security policies initially, do you have procedures to educate them or encourage them to follow these policies?

Yes, all the users are educated on the need for following the security policies even though they may feel that such policies should not apply to them. This takes some persuasion at our end and understanding on theirs.

Can you provide couple of examples as to how you will go about educating users in this regard?

We provide documentations to end users regarding policies and procedures. Any changes to policies are also notified to the users through email or during status

meetings. I personally have not encountered any end user who would not eventually adhere to the policies after some training.

In situations where there is global virus attack or phishing attack do you feel the need to let users know about them?

Absolutely yes, I as a system administrator, make sure that if there is any outbreak that is reported, all end users are notified so that security practices are followed strictly to avoid any infection to the workstations and importantly the network.

In your opinion why do you think people do not like policies?

End users always want to have freedom when they want to access Internet at work but that is not possible. Spending time buying stocks or shopping or playing games affects productivity and also from the network point of view utilizes bandwidth.

Are you satisfied with security at your organization?

Yes, I am satisfied with the current security plan at my organization. However, I feel there is always place for improvement.

Do you have a unique policy that is specific to your organization the way you do business or people you interact with?

I would say that the security practice at my organization is similar to any other business-oriented organization keeping in mind the end users' and company's productivity.

In your opinion in order to gain further fine grained control over your security procedures do you think you need to tweak/change your policies or change your implementation methods?

Like I said before, there is always place for improvement and yes if I need to, I am open to tweaking policies so that security practices are implemented correctly and followed by all. But as now, I do not see any need to do so.

Back in 2005 Sarbanes Oxley was very popular and every company was adhering to it. One of the auditing policy encouraged companies to stop using IMs in their environment to make it more secure. Many companies removed IMs without notifying the users. Do you think companies should have communicated with users since they were used to IMs in their daily communication? Does this create a trust deficit between the policy maker and the end user who is responsible for following it?

I have been in organizations where in one case using IM tool was a daily practice and encouraged and in other case, IM was a banned as it seemed that usage was affecting organization's productivity. End users did complain about the ban by saying that using IM was their way to communicate internally as well and apparently there were cases, wherein user had asked me to make exception and said that I could keep a tab on his activities to make sure that he was using IM for internal communication only. So that's where I felt that user doubting my trust towards his internet activities.

Do you think it is necessary to let users know of the current situation so they are aware as to why it is necessary?

Yes. Users have the right to information as to why the policy is being implemented so that they are able to understand the usage and consequences that might result from it.

Moving forward in your opinion what would you recommend to transform a good policy on paper into a good practice?

I would be looking forward to following objectives:

– Actively promote good practice in information security and ensure that it is applied effectively across the organization.

– Ensure business and IT managers, users and others with access to the information and systems of the organization understand the key elements of security, why it is needed and their personal responsibilities.

– Maintain a high-level of awareness of information security among users of the application. Users should be aware of a high-level information security policy, and comply with it.

– Ensure that computers used by staff workers in remote locations operate as intended, remain available and do not compromise the security of any facilities to which they can be connected.

– Ensure that electronic mail services are available when required; the confidentiality and integrity of messages is protected in transit; and the risk of misuse is minimized. Mail servers should be configured to protect the availability of electronic mail (e-mail) systems, by limiting the size of messages / user mailboxes, restricting the use of large distribution lists and preventing e-mail 'loops'.

Interview 5 Respondent 5

Who do you think is responsible for security in your organization?

In my opinion everyone in our organization is responsible for security, however it is our duty as system admins to maintain security. We as admins are much more accountable for security lapses.

Can you provide a couple of instances, in your experience, where you find it difficult to implement a policy that might not be practical but is essential?

Policy I found difficult was one with the content filtering. It blocked out all websites not pertaining to our business which made a lot of users unhappy. They could not access Facebook, twitter and other social sites. I would not say it was not practical because we

were getting lots of virus hits due to access to those sites but it definitely was a difficult implementation.

Do you consider yourself and other system administrators to be active participants in policy formulation?

Yes and no. There are times when management wants us to make IT related decisions and there are situations which are driven by business needs where the management or the policy maker makes decision which is best for the business. In those situations we system admins do not participate actively.

Does the central body make active considerations of different system administrators from various branches?

Again, yes and no. Like I mentioned before primary decision making occurs with the management and even though we participate with the core IT related processes the final decision comes from them. If some off site location has specific needs they might want to know about it but most times it does not affect decision making with policies. Industry best practices are generally followed.

If you have a system administrator in a branch location, which has problems in implementation of a policy, does that make a difference in formulation of policy by the central body?

Not always.

In situations when you have to custom make policies do you tweak your policies to suit your need?

We try to follow whatever is prescribed and offered by the management. There is little scope for customization. However, when there is a pressing business need we occasionally consider exceptions to policies. Again this has to be approved by the management. Generally we follow policies very strictly.

Do you outsource information to different countries?

No.

Will you be concerned in a situation where you have to do business with a different country and when their security policies are not as good as your organization?

Hypothetically yes of course. When a certain standard is not maintained in security, I will be definitely concerned. Security of Information is very critical to our business.

Do you find users to do bare minimum when it comes to adhering to security policies for instance password policies?

It is not so much as bare minimum as inconvenience to them. But they follow whatever the policy restrictions regarding passwords are so I am happy. They do not have the options of going below a set standard.

In your opinion does the end user see adherence to policy as a hurdle to their day to day operations?

It does cause inconvenience to them for some policies. But most times it is essential to our business. We try to make policies as user friendly as possible but there are times when there is no other way but adhere to policies even when they are difficult.

When certain users do not feel the need to adhere to security policies initially, do you have procedures to educate them or encourage them to follow these policies?

Yes we try to explain to all users the need for new policies or why we made certain changes to policies. We do send them notifications about our security concerns. Generally email notifications are sent.

Can you provide couple of examples as to how you will go about educating users in this regard?

Like I said, emails are frequently used to inform users of changes. However, SharePoint sites are slowly being introduced to post general notifications for users too.

In situations where there is global virus attack or phishing attack do you feel the need to let users know about them?

When there is a specific virus or security breach we are concerned about, or if there is something specific to our business we generally let users know about those risks. We provide guidance on how to handle those situations as well. Most of the time we as system admins take care of potential threat situations before it reaches users.

In your opinion why do you think people do not like policies?

First reason is, it causes inconvenience. Secondly, users prefer to work in a certain way and a policy change causes them to behave differently. People mostly try to resist changes because they are used to in a certain way. If you have given them certain privileges before it is difficult for them to accept when you take it back due to security concerns.

Are you satisfied with security at your organization?

Yes, I am satisfied but there is scope for improvement as is always the case.

Do you have a unique policy that is specific to your organization the way you do business or people you interact with?

Yes like I mentioned before blocking Facebook was a difficult policy to implement. To allow users conditional access to sites like Facebook I had to create a different VLAN in our network with select work stations where users might access Facebook and other sites during lunch hours. The VLAN was kept separate from production environment.

In your opinion in order to gain further fine grained control over your security procedures do you think you need to tweak/change your policies or change your implementation methods?

Present control that we have on our processes is satisfying, however I would like to improve implementation procedures.

Back in 2005 Sarbanes Oxley was very popular and every company was adhering to it. One of the auditing policy encouraged companies to stop using IMs in their environment to make it more secure. Many companies removed IMs without notifying the users. Do you think companies should have communicated with users since they were used to IMs in their daily communication? Does this create a trust deficit between the policy maker and the end user who is responsible for following it?

Yes it does at times. But when changes like these are made, most times these are directed from management or government we have every little options as system admins but to implement it. Users most often will not like it but there is no option.

Do you think it is necessary to let users know of the current situation so they are aware as to why it is necessary?

Users are generally informed the reason for critical changes in policies. However, most of the changes related to security are only informed to people who are concerned with it like managers and admins. We do not want to overwhelm users with too much information.

Moving forward in your opinion what would you recommend making a good policy on paper into a good practice?

Couple of things:

- Implementation improvements are crucial.
- Policy should be updated regularly.

.

The Survey

Page 1. About YOU!

Page 2. Basic Information for Demographic Purposes

1. How old are you?	% of Respondents	Number of Respondents
20 - 30	81.36%	48
31 - 40	10.17%	6
41 - 50	5.08%	3
51 - 60	1.69%	1
61 - 70	1.69%	1
71 - 80	0.00%	0
Number of respondents		59
Number of respondents who skipped this question		6

2. Are you Male or Female?	% of Respondents	Number of Respondents
Male	55.93%	33
Female	44.07%	26
Number of respondents		59
Number of respondents who skipped this question		6

3. How many hours do you spend every day using a computer?	% of Respondents	Number of Respondents
Less than 1	0.00%	0
1 - 3 hours	5.08%	3
3 - 5 hours	5.08%	3
5 - 7 hours	6.78%	4
8 hours or more	83.05%	49
Number of respondents		59
Number of respondents who skipped this question		6

4. Are you a Supervisor?	% of Respondents	Number of Respondents
Yes	20.34%	12
No	79.66%	47
Number of respondents		59
Number of respondents who skipped this question		6

Page 3. Did you know?

Page 4. Pick your Choice

5. Do you feel Information security is important?	% of Respondents	Number of Respondents
Yes	100.00%	54
No	0.00%	0
Maybe	0.00%	0
Number of respondents		54
Number of respondents who skipped this question		11

6. Do you feel most information security policies are valuable to your organization?	% of Respondents	Number of Respondents
Yes	92.59%	50
No	1.85%	1
Maybe	5.56%	3
Number of respondents		54
Number of respondents who skipped this question		11

7. Do you feel information security policies make you more productive as an employee?	% of Respondents	Number of Respondents
Yes	59.26%	32
No	24.07%	13
Maybe	16.67%	9
Number of respondents		54
Number of respondents who skipped this question		11

8. Do you feel most information security policies are confusing and hence difficult to follow?	% of Respondents	Number of Respondents
Yes	30.19%	16
No	39.62%	21
Maybe	30.19%	16
Number of respondents		53
Number of respondents who skipped this question		12

9. Do you feel information security policies at your organization are outdated or need modification?	% of Respondents	Number of Respondents
Yes	23.08%	12
No	40.38%	21
Maybe	36.54%	19
Number of respondents		52
Number of respondents who skipped this question		13

10. Do you feel information security policies create more secure corporate environments?	% of Respondents	Number of Respondents
Yes	88.46%	46
No	0.00%	0
Maybe	11.54%	6
Number of respondents		52
Number of respondents who skipped this question		13

11. Do you feel information security policies are designed to help you work more efficiently?	% of Respondents	Number of Respondents
Yes	62.26%	33
No	16.98%	9
Maybe	20.75%	11
Number of respondents		53
Number of respondents who skipped this question		12

12. Do you want to voice your opinion in your organizations' policy making regarding information security?	% of Respondents	Number of Respondents
Yes	33.96%	18
No	39.62%	21
Maybe	26.42%	14
Number of respondents		53
Number of respondents who skipped this question		12

13. Do you want to be notified with every change in information security policies of your organization?	% of Respondents	Number of Respondents
Yes	61.11%	33
No	25.93%	14
Maybe	12.96%	7
Number of respondents		54
Number of respondents who skipped this question		11

14. Do you want to be notified with only the change in information security policy that affects your daily work?	% of Respondents	Number of Respondents
Yes	68.52%	37
No	27.78%	15
Maybe	3.70%	2
Number of respondents		54
Number of respondents who skipped this question		11

Page 5. Did you know?

Page 6. Pick your Choice - Continued

15. Do you feel a system/security administrators should talk to you about your work requirements before a information security policy is put into practice?	% of Respondents	Number of Respondents
Yes	82.22%	37
No	6.67%	3
Maybe	11.11%	5
Number of respondents		45
Number of respondents who skipped this question		20

16. After a new policy has been introduced, do you feel a system/security administrator should speak with your regarding the problems or suggestions you might have?	% of Respondents	Number of Respondents
Yes	88.89%	40
No	4.44%	2
Maybe	6.67%	3
Number of respondents		45
Number of respondents who skipped this question		20

17. Do you want to learn more about information security at your organization?	% of Respondents	Number of Respondents
Yes	68.89%	31
No	15.56%	7
Maybe	15.56%	7
Number of respondents		45
Number of respondents who skipped this question		20

18. Do you want to receive security notifications regarding present Internet worms, viruses, and malwares that have practical implications in your organization?	% of Respondents	Number of Respondents
Yes	73.33%	33
No	11.11%	5
Maybe	15.56%	7
Number of respondents		45
Number of respondents who skipped this question		20

19. Do you feel your organization's security policy answers almost all of your security/work related questions?	% of Respondents	Number of Respondents
Yes	42.22%	19
No	20.00%	9
Maybe	37.78%	17
Number of respondents		45
Number of respondents who skipped this question		20

20. Do you believe information security policies in your organization can be better?	% of Respondents	Number of Respondents
Yes	54.55%	24
No	2.27%	1
Maybe	43.18%	19
Number of respondents		44
Number of respondents who skipped this question		21

21. Do you believe information security policies that you are subject to in your organization are generic and do not relate to your work?	% of Respondents	Number of Respondents
Yes	18.18%	8
No	52.27%	23
Maybe	29.55%	13
Number of respondents		44
Number of respondents who skipped this question		21

22. Do you feel information security policies are too lengthy?	% of Respondents	Number of Respondents
Yes	42.22%	19
No	35.56%	16
Maybe	22.22%	10
Number of respondents		45
Number of respondents who skipped this question		20

23. Do you believe information security should be handled only by System and Security administrators?	% of Respondents	Number of Respondents
Yes	62.22%	28
No	26.67%	12
Maybe	11.11%	5
Number of respondents		45
Number of respondents who skipped this question		20

24. Do you want Information Security Policies to be simpler?	% of Respondents	Number of Respondents
Yes	68.18%	30
No	18.18%	8
Maybe	13.64%	6
Number of respondents		44
Number of respondents who skipped this question		21

Page 7. Did you know?

Page 8. A few more Details

25. How comfortable are you with computers?	% of Respondents	Number of Respondents
I never use it.	0.00%	0
I rarely use it.	0.00%	0
I use it occasionally.	0.00%	0
I have to use it. It is part of my job.	18.18%	8
I am always on computers/laptops.	79.55%	35
Details Other (Specify)	2.27%	1
Number of respondents		44
Number of respondents who skipped this question		21

26. How do you rate Information Security Policies and Practices at your organization?	% of Respondents	Number of Respondents
Very Dissatisfied	0.00%	0
Not Satisfied	9.09%	4
Neutral	22.73%	10
Satisfied	54.55%	24
Very Satisfied	11.36%	5
Details Oth (Specif	2.27%	1
Number of respondents		44
Number of respondents who skipped this question		21

27. Do you feel Information Security policies make you more productive?	% of Respondents	Number of Respondents
Strongly Disagree	2.27%	1
Disagree	13.64%	6
Undecided	27.27%	12
Agree	47.73%	21
Strongly Agree	9.09%	4
Number of respondents		44
Number of respondents who skipped this question		21

28. How concerned are you when you encounter Internet worms, viruses or Trojans?	% of Respondents	Number of Respondents
It happens every day, information security policies cannot stop it.	0.00%	0
omeone will fix it for me.	15.91%	7
never had a virus/Internet worm/Trojan attack.	15.91%	7
I am worried.	29.55%	13
Very Concerned. Should always follow polices.	36.36%	16
Details Oth (Specif	2.27%	1
Number of respondents		44
Number of respondents who skipped this question		21

29. It is difficult to work if you follow every information security principle?	% of Respondents	Number of Respondents
Strongly Disagree	4.55%	2
Disagree	20.45%	9
Undecided	43.18%	19
Agree	31.82%	14
Strongly Agree	0.00%	0
Number of respondents		44
Number of respondents who skipped this question		21

30. Do you feel that the support materials available in your organization to learn about Information Security is adequate?	% of Respondents	Number of Respondents
Very Dissatisfied	0.00%	0
Not Satisfied	20.45%	9
Neutral	43.18%	19
Satisfied	25.00%	11
Very Satisfied	11.36%	5
Number of respondents		44
Number of respondents who skipped this question		21

31. Do you have any comments for your system/security administrator to help improve information security in your organization?	% of Respondents	Number of Respondents
Details Oth (Specif	100.00%	10
Number of respondents		10
Number of respondents who skipped this question		55

Page 9. Thank You!