Global Information Assurance Certification Paper

SANS – GIAC Certification – Security Essentials
Information Security/User Policies

Steven W. Tursi
November 10, 2003

TABLE OF CONTENTS

A. Abstract

B. Policy Development

C. Policy Implementation

D. Policy Training

E. Policy Enforcement

F. Conclusion

G. References

A. Abstract

Information technology continues to evolve at an incredible pace as does the threat to public and private organizations. The threat is real and repeatedly demonstrated through high profile attacks against major business and government institutions. The internal threat is also profound; employees with no specific guidance will, intentionally or not, continue to cause extensive and in some cases irreparable damage to organizational infrastructures. Poor security practices and policies and a lack of employee training and guidance significantly contribute to the threat.

Security breaches are costly. Forty one companies said they lost $170.8 million last year from the theft of proprietary information, according to the 2002 Computer Security Institute/FBI Computer Crime and Security Survey; up from $33.5 million in losses reported by 20 companies in 1998.

Organizations have responded to the threat by upgrading their information technology security infrastructure and have realized a truly effective posture begins with internal and effective security polices. Effective policies are crucial to protecting sensitive data, intellectual property and the overall organizational operation. Information security specialists in companies throughout the world have been and will continue to be tasked to develop sound and enforceable policies to protect against disaster.

Many articles and research have been done regarding the proper preparation and documentation of adequate security polices but most agree that a policy must be documented, distributed and communicated, must clearly define areas of responsibility, be implement able and enforceable (Peikari and Fogie, 2003).

This paper will discuss security policy development, implementation, training and enforcement.

B. Policy Development

Most organizations, private and public, require the use of information technology to operate in the world today. Information technology is quickly becoming the mainstay of effective business. In an effort to protect proprietary information and other critical assets, organizations are developing security policies in an attempt to reduce the internal/external threat while providing users the ability to meet their goals and objectives.

According to an article in the Cyber Crime Fighter, June 2003, there are several reasons why organizations fail to understand that the threat is real. They often fail to realize current employees have increased skills and possess the ability to inflict crippling damage to an organization. The Cyber Crime fighter points to another reason: incompetent security professionals who fall short of having not only the proper training

but also the proper motivation to develop staff and employ proper adequate policies and procedures.

The development of security policies is the first step of setting up an adequate fortress to protect an organization. It is not just a matter of writing down what employees should or should not do or what hardware or software should be used; but a larger project of determining the entire security posture of the organization. The policy must be a strategic document defining the depth and scope of security required by the organization. Policy development should initially discuss security issues in broad terms using statements of goals, missions, objectives and purpose then refined to address specific issues. Policies should define why the security issue is important, why assets need to be protected and to what extent security should reach (Stewart, 2002)

Information security managers tasked with developing security policies must ensure they are a functional part of the organization. This means having a clear understanding of the organizational structure, short and long term goals and the mission. To the dismay of many administrators and IT managers, a good security policy is not a simple plug and play component. For a policy to show any return on investment, it must be integrated into the processes and procedures of the business and with the support of the people who are expected to follow it (Peikari and Fogie, 2003). Policy development is completed around the function of the organization; meaning there must be an understanding of the business and its processes. Key elements of the business must be identified and policies tailored to allow employees access; without compromising security. To the integrated IT manager, this means sitting down with senior management as well as mid-level mangers and workers to determine their needs and requirements. Employees should have an active role, if possible, in the development of policies because they, more than anyone, understand the organizational structure and can provide insight as to how the policy will affect the big picture. If employees have an active part in the development, they are more likely to accept and adhere to the requirements. Along those same lines, an information security manager has to be integrated and aware of organizational proprietary information as well as the competition to the organization. This is accomplished through the security manager talking to senior management, production managers and finance managers and determining what is most important to the company and where is it located. Critical to the level and implementation of the security policy is an understanding of the significance of what the policy is designed to protect.

An assessment of the network structure must also be completed prior to any policy being written. It would seem only obvious that the security manager in conjunction with his/her IT staff would have a handle on the topology of the organizational network. Unfortunately, the exact opposite it often true. There is a significant lack of knowledge regarding the structure of the network leaving it and the data on it susceptible to theft or destruction. Security managers must identify the location of all systems, servers, back up servers and firewalls. They must have a clear understanding of how the network is connected and through whom as well as the ability

to identify potential weak points. Grasping the organizational information technology infrastructure is crucial to the development of security policies.

The last step before the actual developing of policy, and probably the most crucial and difficult is commitment. "Fundamentally important to any security programs success is the senior management's high level statement of commitment to the information security policy process, and a senior managements understanding of how important security controls and protections are to the enterprises continuity. Senior management must be aware of the importance of security implementation to preserve the organizations viability and must publicly support the process (Krutz and Vines, 2001).

There is no limit to the number of articles to be found regarding the development of organizational security polices. The Government Accounting Office (GAO), the auditing arm of Congress stated in a report released in October 2002 that it had identified common elements that should be included in an organizational information security policies. These policies were formulated after the GAO reviewed literature and conducted research in the public and private sector. The GAO interviewed privacy experts from universities and researchers from national business organizations, officials from the Department of Labor and the National Labor Relations Board. The GAO also conducted extensive interviews with fourteen Fortune 1000 private sector companies from industry. The GAO produced the "Key Elements of a Computer Use Policy"

Policy Element/Type of Statement:

Monitoring use of proprietary assets: The policy enforces that company computing systems are provided as tools for business and all information created, accessed or stored using these systems are property of the company and subject to monitoring, auditing and review

Establishing no expectation of Privacy: The policy should emphasize the limitations on privacy protections for employee use of email , the Internet and computer files

Improper Employee Use: Policy should enforce that some uses of company computers are inappropriate, including specific notices banning offensive material such as pornography, racial slurs and other offensive content.

Allowable employee uses: Policy describing the proper and acceptable uses of the company systems, including whether or not personal use is permitted.

Protecting Company Sensitive Information: Policy should be clear as to the handling of proprietary information on company systems.

Disciplinary Action: Policies should reinforce that disciplinary action will be taken and the penalties involved for violations of usage policies.

Employee Acknowledgement Policy: Making employees sign a statement indicating they understand the company policy and acknowledge their responsibility to adhere to it (Holmes, Judy, Ph.D.)

A second source providing insight regarding security policies was derived from Michael Overly, Author of "e-policy, How to Develop Computer, Email and Internet Guidelines to Protect Your Company and Its Assets" (1999), there are six essentials. First, the computer belongs to the business. The policy should make it clear that the computer and the email systems belong to the business and are only to be used for authorized purposes. Second: expectations of privacy. The policy needs to explicitly define what privacy rights, if any, employees have in the material they create or receive on the computer. In most cases, the policy will state that the employee has no expectation of privacy in anything they create, send receive or store on the computer. Third is monitoring. If an employer intends to monitor, employees should be made aware that monitoring could occur at any time. Fourth is ensuring employees take care in messages sent from their computers. Employees must understand for example, the unique nature of email and that anything they send can be sent again and that the content represents the company. Fifth; employees need to be informed to avoid inappropriate content. More importantly, employees need to be clearly trained in what is considered inappropriate and that even the appearance of unacceptable content could subject them to disciplinary action. Lastly, employees need to sign off. In an effort to make employees take the policies seriously, they should be required to sign a form indicating they do understand and that there are serious potential ramifications for failure to comply

Once the framework is completed and the IT manager has the commitment of management and an understanding of the organization they must conduct a risk assessment. As mentioned above, many companies still incorrectly believe a security incident could not happen to their company. Senior management need to remember that they are susceptible to damage by both internal and external threats. The security manager developing organizational policies needs to understand the risk to the organization and be able to articulate that risk not only to senior management but also to employees. Risk is the potential for harm or loss. Risk Analysis represents the process of analyzing a target environment and the relationships of its risk related attributes. The analysis should identify threat vulnerabilities, associate these vulnerabilities with affected assets and identify the potential for and natures of undesirable results and evaluate risk reducing countermeasures (Tipton and Krause 2000). Risk Assessment represents the assignments of value to the assets, threat frequency and consequence. Finally, there is risk management; characterizing the overall process including assigning priorities to, budgeting for and implementing and maintaining appropriate risk reducing measures. Like policy management, risk management is a continuous process.

Whatever the content of your security policy; Internet use or antivirus updates, the policy should be drafted with implementation in mind. Security policies should be designed to make the security managers' job easier instead of harder. Are the policy statements short? It is difficult enough to get employees to pay attention to security. It would be counter-productive to ask an employee to read through 200 pages of security

issues and expect them to remember and adhere to the rules. Each policy should be no more that two to three paragraphs long. Short policies like these can be put up in the coffee room and on bulletin boards and will get the attention of employees. Is the policy clear? The policy should be clear and concise, for example, "No employee will download MP3's onto any company computer" or "No employee will operate a company computer without Anti-Virus protection". The last check is to determine if the policy is practical. Can the policy actually implemented and enforces, if not, is should be re-written (Scheier, 2003).

Research indicates that there are many ways to develop policies that work. Some experts still want to do the stubby pencil development while others want to use integrated software like SOS Information Security Policies (www.security.kirion.net/securitypolicy). Regardless, the policies need to be developed with the organizational needs in mind and be adaptable and expandable to meet the overall goals.

C. Implementation:

The policies have been developed and support the organizational mission. Security managers are often at a loss for the proper way in which to ensure the policies are implemented. Many security managers are faced with the dilemma of split based operations; being responsible for multiple networks dispersed over a large geographic area with large amounts of employees and no ability for enterprise management. They are also burdened with employees who may not understand or be resistant to change or restrictions on their ability to function. There are several avenues to "get the word out" to employees. First, as part of the new hiring procedure, employees should be required to read and certify they understand not only the policy but the ramifications of not adhering to them. The organization should make the policies available in public areas for everyone to see. For example, in areas frequented by employees such as break areas, smoking areas and locker rooms, signs or posters should be evident indicating the need for all employees to adhere to security policies. Since the events of 9/11, all employees should be concerned about security issues and should make it their first priority. The corporate Intranet is also a good avenue to post security policies as well as sending periodic emails to all employees with the policy document attached. At a minimum, the policy document should be sent to all employees whenever changes are made (Andress, 2001). Senior management must support the implementation of the security policies and employees should not be surprised by the security policies. The implementation or change in a particular policy needs adequate notification to the organizational staff. Policies requiring action or activity by the employee should be clear and concise and defined as to when they will be implemented or when the change will take effect.

Policies are implemented through the use of security tools must be closely evaluated to determine their effects on the current infrastructure. As mentioned during the policy development phase, time must be spent determining the current infrastructure as how new policy tools will be incorporated. If part of a new policy includes monitoring and software is now installed on the network to collect data, part of the implementation

must include the location of the data storage, a determination of how long it will be stored and the capabilities of the organization to review what is collected.

D. Training

Training, not only for security policies but for the entire mission is crucial to any organizational success. Continued training in all areas gives employees the feeling they are part of the organization and that the leadership is concerned. Policy training is crucial to the success of the organization, from the Chief Executive officer to the forklift operator. Ernst and Young, a United Kingdom based company surveyed 1400 large companies. The survey revealed 83 % of respondents ranked investment in technology as the top information security spending priority; however, only 29 % considered information security training for their own employees to be a priority. Employees during their daily routine have a million things to accomplish; chances are they do not pay attention to material about computer security. A good first step in educating employees about security policies is to figure out which policies effects which employees. Distributing germane policies to the proper employees is only the first step. Companies need to test employees to verify the policies. There are web based systems available to quiz and verify employee knowledge of policies. Employers must educate staff about security policies (Hurley, 2002). In addition to making sure employees know the policies, there must be some type of structure in place in which employees can report violations of security. Information must be able to flow up and down the organizational structure. Hurley points out that if an employee understands policies and the importance of security, they can act as the eyes and ears of the information security department.

An article in Information Week (www.InformationWeek.com) reflects the still apathetic attitude of surrounding training of Information Security Polices. The author, George Hulme, “Security Training Still a Business Afterthought (2002) points to several statistics. Though many small companies, those with annual revenue up to $50 million, have focused their spending on deploying security applications, only 18% say they've invested in security training. Midsize companies, with annual revenue of $50 million up to $500 million, fare slightly better, at 26%. Large companies, with revenue of $500 million or more, do better still, with 35%. "This shows that most companies still view security as something you buy, such as firewalls and antivirus, and forget about," says Lloyd Hession, chief security officer at Radianz, which runs a network for the financial-services industry. The numbers support Hession's observation: 82% of companies have bought antivirus software and 78% network firewalls, but only 22% of companies have an employee security-awareness campaign and only 13% have user security training classes. There may be better news ahead: 67% of U.S. companies say raising user awareness, and 55% say training staff about security are both key organizational priorities in the next 12 months.

There are a myriad of ways to develop and distribute training and if handled correctly, security and policy training can be a rewarding experience for the employees. Though it cannot be repeated enough, management must support the training and abide

by the policies they signed off on. If the employees clearly see management support, they will in turn have a positive attitude toward the policies. Several factors exist to make training effective. A designated representative needs to be clearly defined as the person responsible for training. This should be an employee with knowledge of the policies and in the best scenario one of the authors. The organizational training representative must be motivated and have the personality traits consistent with public speaking; being able to deliver an energetic training program emphasizing the importance of the training for the company. Training should be scheduled in the long and short term. Long term training should project the organizational training requirement 6-12 months in the future and focus on the structure of the organization in the future. If there will be an anticipated change in the infrastructure of the organization, employees should know as soon as possible to prepare for the change. Short term training should include training the current policies and short fuse changes. All employees training should be scheduled and coordinated through the entire organization. Training that is haphazard is not effective and a waste of employee time and resources. To counter this, again with the support of management, the trainer needs to coordinate with the immediate supervisors of the employees to be trained to ensure there will be no scheduling conflict. Training should be conducted during business hours and to be effective it must be interesting, detailed, well planned and hold the attention of the audience. The trainer should know the audience beforehand and gear the training appropriately. Some type of multi-media, for example, PowerPoint, must be employed and used an effective training aide. The employees should be provided either copies of the slides or other media to take with them from the training as a reminder of the security policy requirements. An effective training program need not be expensive as long as imagination and initiative is applied and the atmosphere of the organization supports it. Additionally, the training representative should take the opportunity to train first level supervisors emphasizing their responsibility to enforce security policies. Organizational training must include information for employees to report potential security violations and issues which they perceive to be a security risk. Examples of this could include another employee brining in external software and installing it in contrast to the security policy stating that no privately owned software is authorized.

Establishing company security policy is relatively straightforward; ensuring they are adhered to is another issue. Employees that are trained on a continuous basis are more likely to know what the policies are as well as adhere to them. The best policy in the world is worthless unless trained, understood and adhered to by employees. More than technology is needed, a proactive training and awareness program is crucial to success.

E. Enforcement:

As an Information Security practitioner, it is inevitable that you will have to deal with questionable practices by employees and outright violations of established policies. The information security representative, along with the training representative will have the daunting task of advising management on policy infringements. Twenty-two percent of companies have fired an employee over improper e-mail use, up from 17 percent in

2001, according to a survey of 1,100 companies conducted by The e-Policy Institute, the American Management Association and Clearswift, maker of software to manage and secure electronic communications (www.marketwatch.com/news/story). Even if the policies are well developed, fit the organization, are implemented and trained to employees, there will always be those who fail to adhere to the policies.

"A security policy is really just a piece of paper unless you can enforce its provisions" says Jerry Harold, CISSP and co-founder of NetSec, a managed security services company. (www.scmagazine.com). Security experts have two schools of thought when it comes to the ability to enforce organizational security polices. John de Santis, CEO Sygate Technologies believes that it is generally accepted that education is a component of an overall enforcement plan; it is often "not the one you can count on". Therefore, most companies who have actually written an adequate security policy would be better off enforcing it with tools rather than relying on employee awareness and their ability to pay attention in training classes. The opposing view is that though technology is critical to policy enforcement, in practice it is extremely challenging. Security tools may not integrate well with the current infrastructure and may actually create extraordinary amounts of data which someone in the organization will have to review. Finding the right security products requires planning research and time (Armstrong, 2003). Companies need to find the best of both worlds; policies that are understandable, rational and acceptable backed up by security tools which are usable and support the organizational mission.

Many factors are important to deciding what action to take against an employee(s) who violate security polices. The legality of the policy, its intent, clarity and method of training could all be called into question. Enforcing the policy will bring into light the time spent developing it. Security policies should be reviewed by legal personnel to ensure they are enforceable and without question, should be enforced with a standard across the spectrum of the organization. Failure to take action against an employee for a security violation reduces the credibility of the organization and may lead employees to believe the policies are useless and unenforceable. Intended actions resulting from policy violations should be discussed prior to the incident. Security professionals should have already had meetings with management as to how they (management) will handle situations and this information should have been conveyed to employees during their training. There should be no surprise to any employee caught downloading pornography when they are terminated if there is clear policy prohibiting such actions.

F. Conclusions:

Organizational information security polices are "living documents" and must be able to be adjusted with the evolutionary threats to information technology continue to rapidly change. The goal of the Information Technology security manager must be integrated into the organization and be supported by management. He/she must developed policies that are clear and concise and support the priorities of the organization. Security policies should be adapted as necessary and in an organized fashion, trained to employees as often as possible. Policies must be enforceable and

employees must realize that a violation of a security policy will have ramifications. Though it is generally understood that it is impossible to protect from a network from every threat, it is possible to develop effective policies that when properly implemented, training and enforced, can mitigate the threat to acceptable levels.

References:

American Management Association (URL: www.marketwatch.com/news/story)

Aikisensei, "Zombies, Trojans Worms and More – A Top Hacker's Security Advice to Business and Law enforcement" Cyber Crime Fighter, 2003

Andress, Mandy, Effective Security Starts with Policies" InfoWorld (URL: www.infoworld.com)

Armstrong, Illena, "Policy that lives – Enforcing security policies in spite of users", Policy Management Compliance, July, 2003 (URL: www.scmagazine.com)

Hulme, George, "Security Training Still a Business Afterthought, Information Week, 2003 (URL: www.informationweek.com)

Hurley, Edward "Employers must educate staff about security policies" Security Search.com (URL: www.securitysearch.com)

Krutz, Ronald and Vines, Russell ' The CISSP Prep Guide – Mastering the Ten Domains of Computer Security" Wiley Publishing, 2001

Overly, Michael, "e-policy – How to Develop computer, email and Internet Guidelines" 1999 SciTech Publishing Inc

Peikari, Cyrus and Fogie, Seth, "Writing a Security Policy" Security Search (2003)

Power, Richard, "2001 CSI/FBI Computer Crime and Security Survey" Computer Security Institute, 2000 (URL: www.gocsi.com)

Scheier, Robert L, "A reality checklist for an effective security policy" Search Security, (2003)

Stewart, Michael, "Elements of a formalized security infrastructure" Search Security (2002)

Tipton, Harold and Krause, Micki, "Information Security Management – 4th Edition"Auerbach Publications, 2000

Last Updated: September 22nd, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive