Running head: INFORMATION SECURITY POLICY

Information Security Policy

for Small Business

Bruce D. Waugh

ICTN 6823 Information Security Management

July 2008

Abstract

Information security policy, while being one of the most important steps in helping to secure an information system, is also one of the most frequently overlooked and misunderstood in small businesses. Performing the steps necessary to create strong, effective, and more importantly, enforceable policy are usually perceived to be beyond the resources of most small businesses. Yet with the pervasiveness of small business, these information systems can become unwitting tools for attackers and provide a stepping stone for larger attacks on enterprise networks.

By understanding the pertinent issues in creating and maintaining effective policy, small businesses can create workable rules by first understanding the psychology of their workers, the Information landscape in which they operate, and the value of the information being protected.

Introduction

First, definitions are in order to clarify our target; Information Security Policy (or simply "Policy") is used to describe a documented collection of rules and allowed or disallowed behavior for an information system and its assets. There are three types of policy that are generally agreed upon, namely Enterprise-level policy, or policy that applies to general behavior within the information system and is generally strategic in nature; Issue-specific security policy, by far the most prolific and extensive for small business, describing how technology can be used in the organization, and finally System-specific security policy, more akin to specific instructions on how to use individual technologies including preferred settings and installations. All three areas will be addressed, but Issue specific policy is usually the most difficult for small business. Consider that while large organizations use technology to further their mission, small organizations may use the exact same technology and

require that these same issues be addressed without access to the necessary resources or controls. Frequently, the only control choice for small business may be policy.

'Small business' is defined many different ways in the literatures, but we shall use it to refer to an information system with less than 100 employees. Some organizations try and further sub-divide businesses into more specific niches; unfortunately, very little research or material is available that addresses these sub-divisions.

As stated above, creating effective and enforceable policy requires the understanding of assets, risks and resources available for risk management; before you can dictate how to protect something, you first must know what you have to protect and what to protect it from. Flailing about in the Information security landscape is expensive, and uninformed buyers are prime targets for malfeasance and inadequate safeguards. But asset valuation, followed by risk assessment, usually requires substantial investment is both personnel and time, both perceived to be beyond the scope of most small businesses. (Kadel 2004, Morgan) Most documented methodologies are targeted to enterprise-level audiences, with departments, consultants, or staff member teams that can be tasked to perform these projects. Further, since most small businesses are more niche-focused than most large organizations, the pool of necessary security knowledge is limited and sometimes non-existent. (Piero 2005)

Changes to the regulatory environment have also highlighted he need for comprehensive policy design at nearly every level of enterprise. Rules such as HIPAA and others sometimes make little distinctions in requirements between large and small business and can severely impact continuity and success. Outsourcing can control much of the risk, but again, may be beyond the resources of small business (Colson 2003).

Further, we encounter problems when technical-minded staff are asked to perform what is essentially a people-oriented mission in whatever the size of the organization; telling employees what they can and cannot do with the organizations' information system. (Stanton et al 2004)

Within the past few years there has been a paradigm shift in thinking about where information security fits into an organization. Previously an outgrowth of the IT department, information security professionals required above-average skills to perform their jobs. In the past few years however, there has been a gradual shift away from IT and towards independence within the organization as security practitioners and industry leaders found themselves serving the mission of their organization more directly, and not limiting themselves to simple IT concerns (Guzman 2004). In other words, emphasis began shifting from pure technology to the information system itself, and began dealing more directly with issues of human nature and behavior. Unfortunately, this is still a gradual shift and many technology-oriented staffers lack an understanding of social skills, psychology, and sometimes even basic human nature (Kabay 2000). Training in these areas is often lax or non-existent; those who succeed are usually straddling the worlds of business acumen and technical savvy, with expertise in neither. Large businesses compensate for this lack by creating project teams that take this into account, mixing technical staffers with sales, business, and human resources professionals. This way, if communications between these communities of interest is reasonably good, policy decisions are usually more successful. Small business lacks the resources to create this type of gestalt and therefore suffers.

Methodology

However, by using the same principles of Security Project Management and applying them to small business, strong policies can be created that are within the means of most small business with the foresight to implement them.

Endless descriptions of how to create policy for an information system exist, and most authors agree that it is one of the basic requirements for securing an information system. Unfortunately, these same authors often fail to acknowledge that there is a substantial difference between enterprise-level organizations and the average small business. Principles may carry across these organizations, but methodology must be significantly different. Further, understanding how users react to policy is extremely useful in forming that policy. Most texts agree that the various communities of interest must be part of the policy process, but with modern societal, cultural, and economic changes, it becomes harder to define those various communities. Small business often defies descriptors that apply to larger organizations; frequently there can be one individual representing several 'officially' defined communities, further muddying the waters.

Creating taxonomy for discussion is not my intent here. Most authors agree on the basic steps in creating policy. Some changes will be made to address specifics for small business. RFC 2196 or the "Site Security Handbook" describes these steps:

> One generally accepted approach to follow is suggested by Fites, et. al. [Fites 1989] and includes the following steps:
>
> (1) Identify what you are trying to protect.
> (2) Determine what you are trying to protect it from.
> (3) Determine how likely the threats are.
> (4) Implement measures which will protect your assets in a cost-effective manner.
> (5) Review the process continuously and make improvements each time a weakness is found.

For the purposes of this paper, four basic steps in policy making will be discussed as they apply to small business. While neither comprehensive or complete, these general principles carry over to essentially all organizations; 1)Asset Valuation or What do you have that might need protecting? 2) Risk Analysis or What bad things can happen to those assets? 3) Risk Management or What can be

done to reduce or remove those risks? Specifically, what kind or rules need to be in place to ensure that your business continues operating? And 4) Who are your policies addressed to?

Overall strategies

First, the individual tasked with beginning the policy process must have a reasonable grounding in the technology and processes of the information system. Detailed knowledge of the technology is usually not essential; of more value is the ability to communicate and gather information. To say that knowledge of 'human nature' is required does no sufficiently describe the situation. Even those who deal regularly with the public or employees frequently find that they cannot quantify the skills necessary for successful social interaction. Finding information that describes behavioral practices in IT related functions can be invaluable. Stanton et al (July 2004) describe findings related to common security related behaviors based on the type of organization, the information that is processed and demographic factors of users:

> …Third, as the taxonomy of end user security related behaviors would suggest, several mechanisms may help to move end user behaviors from the naive mistakes category to the basic hygiene category. More specifically, training, awareness, knowledge of monitoring, and rewards exhibited positive associations with changing passwords more frequently and choosing better passwords. Unfortunately, improvements in these areas also seemed to associate with a greater likelihood of writing down one's password. In addition, training, awareness, knowledge of monitoring, and rewards appeared to lack relations with password sharing behaviors, an issue that deserves further research.

Business owners must be brought into this process from the beginning; they must first understand the need for good policy within their organization (Piero et al 2005). Enterprise-level projects usually stipulate upper management sponsorship for all policy creation processes; the difficulty here is that many small business owners are the only upper level management and must distribute their efforts across a wider range of responsibility within the organization. Those tasked with beginning this process must not assume that the small business owner understands and accepts the need for policy—many organizations at this level have very little written policy and use their familiarity with their staff to determine policy. This very familiarity can be helpful in a small organization, but eventually will impede growth and change. Policies written to address the skill sets and/or weaknesses of individual workers become useless when that employee either leaves orchanges their functions within the organization.

Asset valuation

Often the most difficult and counter-intuitive process for small business owners, determining what they actually need to protect is essential to starting the policy process. Clear definitions of the organizational mission, along with the environment, personnel, and tools necessary to accomplish that mission are essential and must be exhaustively comprehensive. In communicating this to business owners, the Security professional must understand the social makeup of the organization, as well as the technical. Interviewing the business owner and all employees involved in the information system may provide the needed material, but in a small business environment, formal interviews may diminish return—most small businesses operate with a very informal table of organization. Identifying personnel assets can be easier with small business simply due to the number of employees. Frequently, however, the importance of one employee can be misunderstood or under-estimated, even

by the business owner. Responsibilities for routine maintenance, recovery and backup, and interfacing with vendors and specific technologies may devolve on one individual. Depending on the nature of the business and the technical savvy of the owner this may be invisible, and therefore of prime importance to address in policy and procedure. Asking employees to informally note what their responsibilities are and observing them in their daily or weekly routine can assist the policy maker greatly.

Risk Assessment

Once the assets of the information system are known and prioritized, it is necessary to determine what risk there exists to those assets. In a large organization this can be a daunting process, taking hundreds of work-hours; and even small organizations with the availability of advanced technology can accumulate information assets out of proportion to the size of the organization. Luckily, many of the risks to large organizations are the same for small business that work in similar fields and share some common missions.

Risk management

Risk appetite must be addressed once a business owner understands what his assets and risks are. Luckily, most small business owners are familiar with this concept and with very little coaching can proceed. Keeping this process as informal as possible helps maintain owner buy-in and support. Security Professionals must constantly remind themselves of the overall goal and the limited resources available. Over-thinking and analysis often kills the process at this point—controls are often too expensive, and commercial products and software often target either the home user or the large enterprise, making control choices for small business difficult. Often, some creativity and disregard for marketing labels can aid this process; understanding the needs of the organization and the makeup

of the current technology environment can lead to sometimes unconventional choices that better serve the organization. Policy is no different; it must be tailored to fit the needs of the business.

Many organizations such as The SANS Institute offer ready- made templates for different policies that are carefully and thoroughly worded for effectiveness (The SANS Security Policy Project). Unfortunately, many small businesses encounter these policy templates, and without understanding the language, dismiss them as inappropriate or unnecessary. Asking an employee to read and sign multiple pages of cryptically worded sets of rules is counter-productive and may case more problems than it solves. If employees feel that they are untrusted or under suspicion, even the best employees' performance may suffer. A punitive approach will almost certainly develop hostility and increase resistance to change, as well as enhancing the likelihood of insider attacks. Frank discussion at all levels of this process is essential for all involved, constantly keeping in mind both the goal of the organization and the interpersonal environment within the business.

The security professional must first provide a bridge that links the needs of the organization with the final product provided by these types of templates. Use of terminology familiar to the communities of interest is essential. Creating a series of informal documents that outline the intent of the policies based on the needs as they apply to the individual business is very useful and usually overcomes the reticence of most small business owners to put their rules on paper. This document then can act as the bridge to the formalized wording necessary to make policy binding and effective.

Gathering learning resources for management must be carefully thought out—most business owners do not want to devote extra time to 'homework'. Evaluating the business owner's ability to use and understand technology is essential to this process. Publications such as those available from the ISAlliance, Microsoft and large security vendors such as Symantec and MacAfee can be extremely useful in communicating the need for protections and the methodology for adoption.

Another difficulty for small business is keeping the policy flexible enough to successfully keep up with the needs and mission of the organization. Small businesses can experience sudden phenomenal growth based on a single transaction or client aquisition; creating policy that will grow with the organization is challenging and requires clear commitment from all members of the information system.

Understanding the Communities of interest

As stated earlier one of the biggest challenges for Information security professionals is often understanding those impacted by policy. Policy written without regard to these concerns is both ineffective and unenforceable. Larger more impersonal enterprises have experience with policy enforcement, while small business may have no provisions at all for disciplinary action or procedures for termination. Further, impact from policy enforcement can be greater for small business—termination of one employee in a ten-person staff is at least a 10% loss in productivity. Impacts to the bottom line like this are usually unacceptable to small business owners unless under extreme circumstances such as proven intentional malfeasance or vandalism.

Studies by Stanton et al (2004) (2003) have described organizational behavior as regards information security practices and found correlations between security behaviors and the individuals financial level, job history and education level; Using security-related behaviors such as revealing passwords, writing down passwords, attitudes toward password training, personal web surfing, personal email, personal gaming, acceptable use training, discussing acceptable use policies, and abiding by acceptable use policies as indicators,

> … tests showing that greater organizational commitment, fewer negative emotional events, more technical knowledge, and more management

> responsibilities associated positively with productive security-related behaviors and negatively with counterproductive security-related behaviors…. Taken together, the two studies did suggest that security-related end user behaviors relate to a combination of relevant situational and personal factors. We believe that these findings support our essential belief that examining the motivational antecedents of information security behavior may prove productive in improving information security within organizations. The potential seems to exist for a variety of practitioner interventions that could influence the enactment of security-related behaviors

Conclusion

It is essential that those responsible for creating policy within a small business environment understand the need for using un-conventional and non-technical methods to make policy effective and enforceable. Tools available such as Microsoft's Small Business Center, Internet Security Alliance's Common Sense Guides, SANS Security Policy Project can provide valuable guidance

As part of the Cyber Trust initiative funded by the National Science Foundation, (NSF 08-521**)** research is ongoing into better ways to create and enforce security policy

> …The dominant contemporary approach to securing information technology in organizations is based on risk analysis, policy development, and enforcement. The paradigm is at serious risk, though, when it comes into conflict with economics or with individual and social psychology. The cost of security – both direct and indirect costs – may be either too high or too low, often simply because the resulting policy is not flexible and adaptive. And security rules may be thwarted by individuals, even friendly ones, for a

> variety of reasons: they are making what they believe are responsible tradeoffs on the organization's behalf (and they may be right), they are not entirely aligned with the organization's goals or don't understand exactly how they relate to a particular security related behavior (and it may be cognitively unreasonable to expect them to), or they are responding to basic social norms or fundamental cognitive limits. A techno-social system that suffers from misalignment between the security aspects of its technology and the behavior of its people is intrinsically weaker both economically and against malicious attackers.

It is the responsibility of practitioners, educators and administrators to acknowledge and address these issues. Security threats continue to grow and continually outpace user education. The world of information security changes and becomes more complex daily; it is up to each of us to prepare organizations and information systems to successfully navigate the shifting landscape. Acknowledgement that our current practices may leave significant portions of our workplaces essentially unprotected is no longer acceptable. Just as flexibility is a requirement for successful policy, so too is it a requirement for its designers.

Citations

CISSP Forum and ISO27K Implementers Forum, Top Information Security Risks for 2008 December 31, 2007
http://www.iso27001security.com/Top_information_security_risks_for_2008.pdf

Colson, R. E. "HIPAA and Outsourcing: The Impact of Business Associate Rules Under the Final Privacy and Security Standards" Haynes and Boone, LLP September 2003

Cyber Security Tip ST04-0003, National Cyber Alert System (www.us-cert.gov/cas/tips/ST04-003.html)

Federal Register / Vol. 68, No. 34 *Health Insurance Reform: Security Standards* February 20, 2003 / Rules and Regulations

Fites, Johnson, and Kratz, 1992] Fites, Johnson, and Kratz, "The Computer Virus Crisis", Van Hostrand Reinhold, 2nd edition, 1992

Guzman, I. R., Kaarst-Brown, M.L. (2004). "Organizational Survival and Alignment: Insights into Conflicting Perspectives on the Role of the Information Technology Professional". ACM - Special Interest Group on Management Information Systems - Computer Personnel Research Conference. Tucson, Arizona. April, 2004.

ISAlliance "Common Sense Guide for Senior Managers" (www.isalliance.org)
http://www.nam.org/s_nam/bin.asp?CID=163&DID=231351&DOC=FILE.PDF

Kabay, M.E. "Psychosocial factors in the implementation of security policy" Network World Security Newsletter, 02/16/00 http://www.networkworld.com/newsletters/sec/0214sec2.html

Kadel, L., "DESIGNING AND IMPLEMENTING AN EFFECTIVE INFORMATION SECURITY PROGRAM: PROTECTING THE DATA ASSETS OF INDIVIDUALS, SMALL AND LARGE BUSINESSES" SANS Institute 2004, As part of the Information Security Reading Room

Keeling, J. E. "Social Engineering for the Good Guys" July 2001 As part of the Information Security Reading Room.

Lafrance, Y. "Psychology: A precious security tool" SANS Institute (2004), As part of the Information Security Reading Room.
http://www.sans.org/rr/whitepapers/engineering/1409.phpey fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Microsoft's Small Business Center
http://www.microsoft.com/smallbusiness/support/checklist/default.mspx

Morgan, R. "Information Security for Small Businesses" http://www.infosecwriters.com/text_resources/pdf/Information_Security_for_Small_Businesses.pdf

Odlyzko, A, "Economics, Psychology, and Sociology of Security" (2003) Digital Technology Center, University of Minnesota http://www.dtc.umn.edu/~odlyzko/doc/econ.psych.security.pdf

Partida, A., Eight Critical Success Actions for Information Security The SANS Technology Institute Leadership Laboratory July 11th, 2007 http://www.sans.edu/resources/leadershiplab/partida_infosec.php

* Partida, A., Ezingeard, J. "CRITICAL SUCCESS FACTORS AND REQUIREMENTS FOR ACHIEVING BUSINESS BENEFITS FROM INFORMATION SECURITY" Proceedings of European and Mediterranean Conference on Information Systems 2007 (EMCIS2007) June 24-26 2007, Polytechnic University of Valencia, Spain

Peiro, A. Cook, P.; Beydoun, H. "Small Business Information Security Readiness" Small Business Technology Institute in association with Symantec July 2005

* RFC 2196 "Site Security Handbook" Network Working Group, B. Fraser Editor September 1997

SANS Security Policy Project, SANS Institute http://www.sans.org/resources/policies/#template

Sicker D.C., Caccamise, D., Lewis C., Lookabaugh T., CyberTrust: Models for Security Behavior and Dynamic Security Policy University of Colorado, Boulder

* Stanton, J. M, Mastrangelo, P. R., Stam, K.R., Jolton, J. (2004 August) "Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices" Proceedings of the Tenth Americas Conference on Information Systems, New York, New York, August 2004

Stanton, J. M, Mastrangelo, P. R., Stam, K.R., Jolton, J. "Analysis of end user security behaviors" July 2004 a4-125 Center for Science and Technology, School of Information Studies, Syracuse University, Genesee Survey Services

* Stanton, J. M., Stam, K. R., Guzman, I. R., & Caldera, C. (2003, October). "Examining the linkage between organizational commitment and information security." Proceedings of the IEEE Systems, Man, and Cybernetics Conference, Washington, DC.

Swanson, M., Guttman, B. (September 1996) National Institute of Standards and Technology 800-14 "Generally Accepted Principles and Practices for Securing Information Technology Systems "

Swanson, M., Hash, J. Bowen P. (February 2006) National Institute of Standards and Technology Special Publication 800-18 "Guide for Developing Security Plans for Federal Information Systems"

Woody C, Clinton L. Common Sense Guide to Cyber Security for Small Businesses Recommended Actions for Information Security 1st Edition – March 2004