

The importance of written security policy for any network connection”

Ladan Kianmehr,
lkianmehr@missouriwestern.edu

Deborah Becker
dbecker@missouriwestern.edu

Ali Kamali
kamali@missouriwestern.edu

Missouri Western State University
Saint Joseph, MO 64507 USA

ABSTRACT

The subject to discuss in this paper is the role of a written network security policy in an organization, the need for writing up a viable policy, and the effects it has on the flow of information in an organization. Policies often look into the relationship between organizations, and the flow of information within an organization (internal departmental and sub-systems information relationship). We defined “security policy” as a written document that determines eligibility in using an organization’s computer system—i.e., the ways in which data, software, and computers are utilized in an organization. Our assumption is that a written security policy acts as a roadmap and is used for network analysis, which identifies possible problems according to its frame. It can verify and suggest what is happening. The policy can act as a guiding principle for talks between the IT and other sections and departments. Hence, we hypothesized that a solid security policy helps to protect an organization’s security systems because any data on the internet is up for grabs. As a result, where security measures are in place, they keep the data confidential (i.e., private); whereas “public data” can be seen by any end users. In examining the above assumptions, we focused on the network system of a small liberal arts institution of higher education in the Midwest in order to propose strategies on: 1) how to magnify the importance of network policy for an organization; and, 2) how to make it easier to write.

Key Words: security policy, network theory, security and assurance, new-active policy

1. INTRODUCTION

Although maintaining networks is the role of computer scientists and technicians, keeping a watchful eye on who is using/misusing a network is a sociological and psychological process because it requires an understanding of the end users’ dispositions and cultural understanding of the system. In the past our primary concerns might have been the highly

trained and intelligent computer professionals and their ability to use/misuse a system. Today through the advent of internet technology and the availability of information on the Internet, anyone using the internet has access to a host of fairly sensitive information with the possibility of using or abusing the information by breaching a network’s security systems. Although abuse in either scenario would mean violating protocols, and widespread access to the Internet reflects

the diversity among the end users, accessibility has created a form of "digital culture" that may in turn reflect the type of persons whose social network and the daring process (or certain immorality) encourage breaching security and misusing the system (Sutherland, 1974). Borrowing from Sutherland (1974), we can easily identify the criminal nature and intents of such behaviors as intrusion. Given this state of mind, it is not surprising that breaching a network's security can easily create a positive image (or social message) and be construed as "cool". Because the general populace is becoming more computer literate, the threat of this type of attack on an organization's networks has become increasing imminent. These threats underscore the need for organizations (universities) to have well written and documented security policies in place.

2. OBJECTIVES OF THE PROJECT AND PROBLEM RECOGNITION

This project was part of a case study on the network and network security issues and policies of a small liberal arts university in the Midwest. The goals were to: 1) research and write a generic document that outlined rules for computer network access within the university system; 2) graphically depict the basic architecture of its computer systems; 3) specify network rules for individuals or groups of individuals throughout the University's system; 4) define a hierarchy of access permissions for the University's network, and 6) make the system available and secure to all users. The final document is a written detailed policy of both inventory and procedures and is part of the university's historical and living documentation.

3. THE THEORETICAL APPROACH

The preponderance of the literature on network analysis and/or IT studies is conducted by computer scientists and system analysts. Derived from these studies, it appears that several theoretical and methodological approaches are relevant to what we have proposed to study in this project. Among them, network analysis (Whitson, 2003), network science (Börner, Sanyal, & Vespignani, 2007), and social network (Knoke & Yang, 2008) seemed most relevant to our purpose in this study. Viewed from these theoretical approaches, a security policy would imply a framework or scaffolding that restrains human behavior within the confinement of its structure.

To avoid this shortfall, we have incorporated Giddens's (1984, p. 16) structuration theory that implies "underlying codes [that can be] inferred from surface manifestation". Simply stated, a network security policy is an amalgamation of rules and regulations that determine appropriate interactions among the end users, and their relationships with the resources. Further review of the current literature reveals an existing ambivalence over incorporating the end users' dispositions, feelings, and other human characteristics in a network security policy. Including this social aspect of the network we propose a hybrid approach, and emphasized the social psychological aspects of the contents of a network security policy.

4. WHAT IS A NETWORK SECURITY POLICY?

Security entails different domains; and there is not an easy way to define [a network security] policy (Whitson, 2003). Maity, Bera1 , Ghosh1 , & Dasgupta (2010) have defined security in terms of access control (RBAC) mechanisms. Policy in any organizational setting reflects a set of rules and regulations. A network security policy is a document for proper management of a network—i.e., a blueprint that grants a user the privilege of utilizing the system - and monitors who enter the system and their purpose for utilizing the system. In recent years, "different network security components, such as *firewalls* and *network intrusion detection systems* (NIDSs), have become the prevailing methods to monitor the security policy in current corporate networks" (Alfaro, Boulahia-Cuppens, & Cuppens, 2008: 103). These hardware and software tools are designed as safeguards to the system.

By definition, "policy" is a collection of rules both written and implied. A policy is normally referred to as either a "procedure" or a "protocol". In network analysis, policies assist the organization in decisions about program and hardware acquisition and spending priorities, etc. (Alfaro et al., 2008). This may seem simple, but there is no easy solution to policy writing or providing a "one size fits all" type of model for policy development. Torjman (2005) elaborated that "policy" can be: 1) substantive and administrative; 2) vertical or horizontal; 3) reactive and proactive; and, 4) current and futuristic. According to Torjman (2005),

"Substantive policy is concerned with the legislation, programs and practices that govern the substantive aspects of community work. The other type of policy focuses largely upon administrative procedures (p. 2).

Vertical policy is what we think of as the normal or traditional way in which policy decisions are made. Horizontal policy-making, by contrast, is developed by two or more organizations, each of which has the ability or mandate how to deal with only one dimension of a given situation" (p. 2).

"Reactive policy emerges in response to a concern or crisis that must be addressed—health emergencies and environmental disasters are two examples. Proactive policies, by contrast, are introduced and pursued through deliberate choice (p. 3).

Some policies are currently on the public agenda, and some are not. Issues already on the public policy agenda (e.g., health care) often have high profile. If an issue is not currently or never has been 'alive' on the public agenda, then there is work to be done in making the case for its importance and raising awareness about the implications of non-response" (p. 3).

Torjman's (2005) classification emphasizes that a successful policy is multifaceted in content and multidisciplinary in scope. The message is very clear: a successful policy must be written in a way that combines the substantive, reactive, and current features of the system. We agree but a comprehensive policy also seeks to eliminate the historical objections users have raised to reactive regulations that constrict the user's access to pertinent information critical the performance of their jobs. Often reactive policies arise from current crises impacting network security administrators. In this regard, to be proactive is to be a step ahead of the game. Keeping current and being proactive is coined in a new term we call "new-active". A "new-active" policy is a constantly evolving policy—allowing a progressive institution to embrace emerging and evolving new technologies.

Clearly, no policy can be complete, and no network can be completely safe. But network analysts concur that a well designed network security policy can prevent major threats (Brandes & Erlebach, 2005). As mentioned

earlier, a network security policy is a set of rules that imply "methodical procedures of social interactions" (Giddens, 1984, p. 18). Hence, we recommend a network security policy that incorporates all resources with a focus on the relationship among the organization's departments and end users.

4. DEVELOPING A NETWORK SECURITY POLICY

There are upwards of fifty departments on a small university campus each interacting at its own level with the computer network and data. Each department has different data needs and different state and governmental regulation restrictions. As the university network grows into the University's social network it is the role of the network security policy to both regulate and provide proper access to system users. Forming an interdisciplinary committee and interviewing department heads and researching current written policies and procedures from the different departments, a basic framework can be constructed which incorporates both the needs and the regulations that govern a university's network policy.

The internet has become a major venue in delivering the university's computer network and network policy. State and governmental internet security and privacy regulations are fluid and ever changing. It would be impossible for one person (the network administrator) to thoroughly understand and implement a balance policy. Government and legal issues provide compelling reasons for a written institutional policy and making the involvement of all departments on a campus critical to a successful policy. Campus-wide involvement also helps educate, disseminate and insure buy-in of the policy from network users.

As systems encounter problems, staff must implement mechanisms that intervene to either redirect or resolve the problems. The network analyst's job is to evaluate and recommend designs, analyze and resolve technical issues, provide documentation on how to maintain the integrity of the system, and strategize short and long-term network protection solutions. This is a simplified task list highlighting the chief responsibilities of a network security officer/administrator. Software can be used to evaluate who is entering the system, who is in the system, and who has just left the system. Policy is written to understand the appropriate use and permissions granted to groups and

users of the system and prescribed remedies for misuse.

Problems encountered by a system occur at computer speed, resolutions must be provided with the same speed. A policy in place enables the system administrators who are overseeing the system to understand the system better. A well written and disseminated policy helps the administrative staff with enforcement and implementation of policy and procedures and insures consistency in network administration during the flow and ebb of personnel.

Incorporating the human factor as an elemental factor in writing a network security policy reflects the interaction between the provider and the end-user. Computer systems are managed, operated, and used by people. Distinguishing between who is safe (legal/legitimate) to enter the system and who is not safe to enter the system is the focus of a network security policy. Managing the vast complexities of the hardware and software of a network is difficult in itself, but the bottom line in network security is managing the social behavior of all users including users who may be intrusive. As a result, one of the most important elements of any network security policy is the human factor for both the gate-keeper and the user.

The interaction between the users and the system is a sociological phenomenon, and requires a set of guidelines for their conduct. For example, a network policy may prevent someone from doing his or her job if the job process is deemed by the network security policy to be intrusive, which in turn affects productivity and output, and may create a sense of uneasiness in the user. Such interactions and mood become part of the user's experience, and explains the relationship between the provider who secures access to the system and the data, the network system that stores and processes the data, and the end user who consumes the data for either productive purposes or intrusive intents. According to Burt (1992), analyzing a network also means analyzing the relationships among people.

Close involvement of all department and department heads can insure that policies both safeguard the systems and provide access to critical data for job completion. Looking at the entire network (hardware, software and users) from this vantage point, we visualize the social psychological characterization of a network

security policy where human interactions and productivity are at stake. Human interactions are primarily guided by their view of each other; therefore, a network security policy should take into account the human element when mapping out the communication structure within and between organization users.

The resulting policy written from our study seeks to validate the social psychological dimension of this process in the communication that occurs within an organization among its members—i.e., stakeholders, employers, and employees, as well as outside players. We emphasize that a good network security policy must address the communication factor based on the needs of the organization in terms of explaining proper use of the system—i.e., computers, the equipment, software, and any other protocol that must be followed.

The process started by developing a master list of users, and then charting their connections—i.e., interactivity and hierarchy. The list was developed based on the structural boundaries of network (device) schematics. In many instances, the reference groups—i.e., those who are referred to for advice—can be plotted as part of a network (see Figure 1 in the appendix). We call this process the "cognitive structuration" because these lists can be developed by physical observation and by thinking through (cognition) the generated data. Without a doubt, mapping out the structural connectivity is a time-consuming, gradual process. Thus, the first lesson in developing a network policy is patience. Viewed from the "cognitive structuration" approach, a network security policy dictates social networking—i.e., permissions and access of users both inside and outside the network.

Using the materials gathered from the physical inventory, the data and regulations contributed by the departments, and following Roger's (2011) proposal for a network security, we looked at the task of developing a network policy in terms of physical security (who has access to the computers and the facility?), network security (who can access data sets?), and authentication (group or individual access and permission based on pass codes?). This type of structuration in our development of a network security policy emphatically magnified the binding of the system, which makes it possible for different actors (especially, the providers, administrators, and the end users) to have

similar practice—usage, but not access—while using the system. This is a systemic approach to the structure of a network security policy.

The project highlighted the need for a network policy that focuses on two adjoining sections 1) inside the campus: all of the institution's buildings, all the users connected with the institution and its subsidiaries; and, 2) outside the campus: other institutions, the Alumni Association, and other non-related clubs and association. From the study, the network system security policy at our institution has kept the following specifications in mind: 1) Clarity of explanation of the reasons for certain policy decisions: involve the end users to aid in understanding and adoption of the protocols. 2) Emphasis on diversity: applying reason and not a cookie-cutter approach to permissions and assess while maintaining the same security levels and protocols. 3) Evaluating the hardware as part of the policy: hardware lifetime and retirement policies. 4) Open access policies: which aspects are restricted to certain end users, which aspects can be left open and free to the public. 5) Threat detection and analysis: explore the ways in which outsiders can have access to the system without permission.

5. CONCLUSION

Modern tendencies towards utilizing information technology—e.g., modes of storing, delivery, and interpreting) are conscious efforts in the 21st century, but have created their own problems and issues.

Utilizing IT is an inevitable choice that does not allow room for falling behind—especially in this technologically dynamic epoch. The structure outline in this paper shows the connections among the cores and their subsidiaries by using lines and dots that bring meaning to the relationships among parts. The drawing helps those who are not literate in computers and software find their way by looking at a graph—hence, our emphasis on developing a linear structure.

In summary, to safely utilize a system, the stakeholders must assume responsibility for its security. Involving all departments in writing a comprehensive security policy insures easier adoption, better regulation compliance and a better educated IT staff. A committee seems a logical choice to be commissioned to conduct a need assessment and make recommendations.

This may work well if such an ad hoc committee is comprised of a multidisciplinary task force, which may well meet the challenge of finding appropriate solutions to their network's security system. An advantage of a multidisciplinary ad hoc committee lies in its variability in perspective and experiences.

6. REFERENCES

- Alfaro, J. G., N. Boulahia-Cuppens, & F.Cuppens. (2008). Complete Analysis of Configuration Rules to Guarantee Reliable Network Security Policies. *International Journal of Information Security*. Vol. 7:103–122
- Brandes, U. & T. Erlebach. (2005). *Network Analysis: Methodological Foundation*.
- Börner, K., S. Sanyal, & A. Vespignani. (2007). *Network Science*. In Blaise Cronin (Ed) *Annual*
- Review of Information Science & Technology, Volume 41. Medford, NJ:
- Burt, R. S. (1992). *Structural Holes: the Social Structure of Competition*. Harvard University Press, Cambridge, MA.
- Giddens, A. (1984). *The Constitution of Society*. University of California Press, San Francisco, CA .
- Knocke, D., & S. Yang. (2008). *Social Network Analysis*. Sage Publications, Inc, Thousand Oak, CA.
- Maity, S., P. Bera, S. K. Ghosh, & P. Dasgupta. (2010). A Formal Verification Framework for Security Policy Management in Mobile IP Based WLAN. *International Journal of Network Security & Its Applications (IJNSA)*, Vol. 2, No. 4, pp. 194-211.
- Rogers, D. (2011). How to Write a Network Security Policy. Retrieved from July 13 from <http://www.network24.co.uk/security>
- Sutherland, E. (1974). *Criminology*. J. B. Lipincott Company, Ney York, NY..
- Torjman, S. (2005). *What is policy? The Caledon Institute of Social Policy*. Ottawa, Ontario, Canada.

Whitson. G. (2003). Computer Security: Theory,
Process and Management. *Journal of*

Computing Sciences in Colleges. Vol. 18.
Issue 6. Pp. 57-66.

