December 2006

Ethnocentric Strategies in Information Security Management

Richard Taylor
University of Houston

Ethnocentric Strategies in Information Security Management

Richard G. Taylor
University of Houston
rgtaylor@uh.edu

ABSTRACT

The strategic approach used to develop organizational security is strongly influenced by management's perception of risks. These perceptions often result in management focusing on technology-based solutions to keep their data safe from outsiders. However, research has shown that more severe threats to information security come from organizational insiders. A case study [in process] uses intergroup bias theory to investigate the current strategies to protect organizational information, arguing that current strategies focus on attempts to keep data safe from outsiders, yet these strategies neglect the threats from insiders. This study suggests that this is influenced by ingroup-trust and outgroup-distrust.

Keywords

Information security, ethnocentrism, intergroup bias

INTRODUCTION

Evidence suggests that organizations have often been victims of serious incidents which have put their information at risk (Hoffer & Straub, 1989). A yearly report conducted by the Computer Security Institute/Federal Bureau of Investigation (Richardson, 2003) revealed that 90 percent of organizations they surveyed detected computer security breaches. Eighty percent of those organizations actually incurred financial losses due to the security breaches. These numbers convincingly validate that organizational information continues to be at risk. To address the issue of information security, organizations must change their current perspective on information security and adopt a new view.

The current view of information security still remains very technology oriented (Dhillon, 2001), resulting in organizations spending heavily on technology solutions to protect organizational information. These technology solutions consist of firewalls for perimeter security, anti-virus software to prevent viruses and worms, and intrusion detection systems to discover potential abusers. Properly installed and maintained these hardware and software solutions do create a solid foundation for effective information security. However, these technology-based solutions are primarily intended to prevent outsiders from gaining access to organizational information and are thus inadequate to prevent all security breaches. This can ultimately create a false sense of security for an organization (Frolick, 2003). Along with these technology-based solutions, organizations must also adopt a human-based approach to address the information security risks introduced by the social and cultural aspects of the human element (Frolick, 2003). Dhillon and Backhouse (2000) stressed the importance of focusing on human-based risks created by organizational insiders:

> *"…evidence suggests that the violation of safeguards by trusted personnel of an organization is emerging as a primary reason for information security concerns*" (p. 13).

By understanding that information security is a social issue, it becomes necessary to investigate behavioral issues that may affect information security. While these issues may be numerous, this paper will only investigate trust, and attempt to answer the following research question:

How do internal trust and external distrust affect an organization's information security strategy?

TRUST

Understanding why people trust and how trust shapes social relations has been a focus for psychologists (Deutsch, 1962), sociologists (Gambetta, 1988), and organizational behavior researchers (Kramer & Tyler, 1996). The role of trust in organizational environments is also getting increased attention from managers and management researchers (Mayer, Davis, & Schoormann, 1995). It is believed that trust is important and useful in many organizational activities, including team work, leadership, goal setting, performance appraisal, development of labor relations, and negotiation (Mayer et al., 1995). However, there is also growing concern about distrust and the violation and/or abuse of trust within organizations (Sitkin & Roth, 1993). Researchers have observed that the potentially greatest threat to modern organizations is not external agencies but the betrayal of trust by organizational insiders (Hogan & Hogan, 1994). To better understand the trust relationships among organizational insiders one can look at literature related to intergroup bias. This literature explains the relationship between ingroups and outgroups.

ETHNOCENTRISM

Intergroup bias refers to the tendency to evaluate members of one's own group (ingroup) more favorably than non-members (outgroup) (Hewstone, Rubin, & Willis, 2002). This group-serving tendency involves favoring the ingroup and/or derogating the outgroup. The term "bias" implies that this favoring and/or derogation involves an interpretive judgment than may be unfair and unjustifiable (Brewer & Brown, 1998).

Throughout history societies have formed group relationships for the purpose of survival, thus creating ingroups. Those not associated with one's ingroup were considered the outgroup. Sumner (1906) coined the term 'ethnocentrism' to refer to positive sentiments toward one's ingroup– pride, loyalty, and perceived superiority. These psychological expectations of ingroup members result in a high level of interpersonal trust among ingroup members.

> *"… ingroups can be defined as bounded communities of mutual trust and obligation that delimit mutual interdependence and cooperation. An important aspect of this mutual trust is that it is depersonalized, extended to any member of the ingroup whether personally related or not. Psychologically, expectations of cooperation and security promote positive attraction toward other ingroup members and motivate adherence to ingroup norms of appearance and behavior that assure that one will be recognized as a good or legitimate ingroup member"* (Brewer, 1999, p. 433).

Being attached to an ingroup does not necessarily mean there is hostility toward the outgroup (Allport, 1954); it may simply represent a preference for one's ingroup.

> *"…members of a group share a common outcome that is distinct from the outcome shared by members of the other group. Such a co-occurrence of group boundaries and common fate is one of the criteria for perceived "entitivity" of social groupings"* (Brewer, 1979, p. 308).

However, hostility toward the outgroup is not uncommon. Derogation of an outgroup is often associated with fear of the outgroup members. If outgroup members are perceived as posing a threat, strong intergroup bias will exist (Stephen & Stephen, 2000). Threats can involve the ingroup's social identity, values, or goals, and may or may not be realistic (Esses, Jackson, & Armstrong, 1998).

Research in this area has also established the concepts of ingroup-trust and outgroup-distrust (Allport, 1954; Brewer, 1979; 1999). These concepts explain how groups of people will blindly trust members of their ingroup, while outgroup members are shrouded by suspicion, distrust, and hate, even when little is known about the actual members of the outgroup (Insko, Schopler, Hoyle, Dardis & Graetz, 1990). Ingroup-trust and outgroup-distrust can also be attributed to the "homogenous effect" (Judd & Park, 1988). Members of an ingroup are seen as homogeneous with behavioral expectations based on a positive exemplar (often oneself), while members of the outgroup are also seen as homogeneous; however behavioral expectations are highly influenced by negative exemplars.

ETHNOCENTRISM AND INFORMATION SECURITY

Past research on intergroup bias has primarily focused on societal level biases; however, these same principles can be applied to business organizations and the methods they use to establish their information security strategies. Perceived threats from outsiders seem to be the driving factor for an organization's information security strategy.

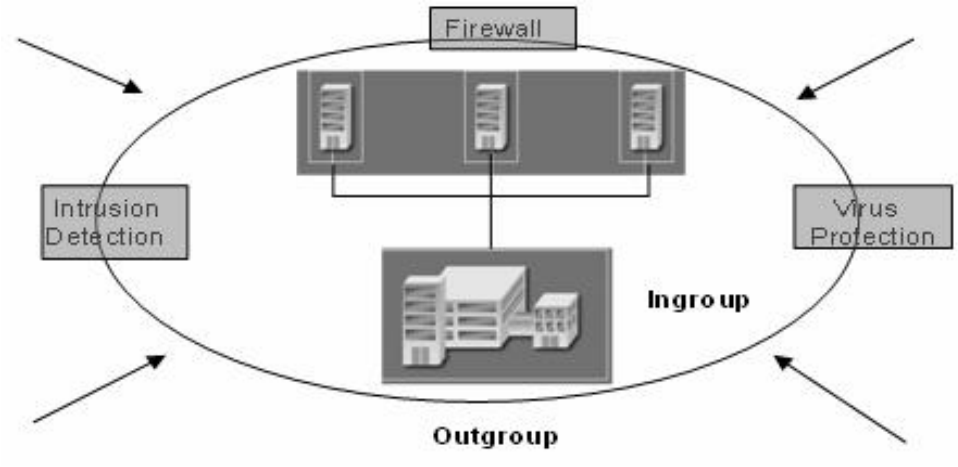

Figure 1: The current focus of information security strategies

Outgroup-distrust is evident in all aspects of an organization's security strategy. Physical security management strives to keep the organization protected from outsiders through the use of door locks, electronic entry systems, video cameras, and security guards. Organizations approach information security management in the same manner. Technology-based solutions such as firewalls and intrusion detection systems are put in place for the primary purpose of keeping an organization's information protected from outsiders—the outgroup. Outgroup members are associated with negative exemplars (Judd & Park, 1988), such as infamous hacker Kevin Mitnik, resulting in an amplification of fear. Outgroup-distrust thus seems to be the focus of information security management practices.

Focusing only on the outgroup as threats to organizational information has led to 'security blindness' by management (Dhillon and Backhouse, 2000). Research conducted on over 3,600 large organizations revealed that only 25% of the organizations reported attacks by (outgroup) external hackers, however approximately 70% reported attacks by (ingroup) internal hackers (Security Management Index, 2003). These statistics and other research (Dhillon, 2001) confirm that ingroup-trust as a factor in information security management is grossly overlooked, and potentially the greatest threat to organizational information. Information security management is also influenced by positive exemplars (Judd & Park, 1988), often the manager(s), who are ultimately responsible for security management. Managers trust that employees are reading information security policies and adhering to established norms to protect the organization's information. These expectations exist because the manager himself/herself follows policies and norms and therefore blindly trust that other employees (ingroup members) will do the same.

Therefore, the argument can be made that ingroup-trust is the greatest contributor to information security risks. As long as organizations continue to focus on the outside threats, organizations will remain vulnerable to threats from insiders. Ingroup-trust can result in inadequate internal information security countermeasures and low levels of employee monitoring (Dhillon, 2001), both of which have been identified as factors in increased information security risks (Straub & Welke, 1998).

METHODOLOGY

A case study was conducted at a financial institution in the Southwest U.S. A financial institution was chosen because of the extreme sensitivity of information within the financial industry. Case research is effective when researching a complex subject such as information security, where it is difficult to study outside the context in which it occurs (Benbasat, Goldstein, and Mead, 1987). It may be difficult to get honest answers to questions regarding information security, therefore the case study method will allow the researcher to conduct probing interviews as well as observe behavior within the organizational context. Yin (2003) also suggests that the case study method is effective to test existing theory as it applies to a phenomenon. The goal of this research is to test ingroup bias theories as applied to information security, therefore making the case study method appropriate. Finally, Yin (2003) suggests that the case study method is effective when attempting to answer "how" questions about a set of events.

To investigate the relationship between ethnocentrism and information security management, the case study involves in-depth interviews of all levels of employees within the organization, from the CEO to tellers. Interviews of the executive staff attempted to determine the information security threats that were perceived to pose the greatest risks to the organization. Additional queries involved probing to uncover the reasons for these risk perceptions. Questions were then posed to the executive staff regarding their level of employee trust within the organization, specifically focusing on their beliefs that employees follow established information security policies. Again, the executives were asked to explain their reasoning for their employee trust. To gauge the accuracy of the executives' beliefs, employees were interviewed to determine their compliance with information security policies and their trust in other employees within the organization. To triangulate the data, documents were reviewed and employee behavior was observed (Yin, 2003).

Ethnocentrism was used as a theoretical base to test the following hypotheses regarding information security management:

Hypothesis 1:	The focus of current information security strategies involves protection organizational information from outgroup members.
Hypothesis 2:	Negative exemplars affect management's perceptions of threats posed by outgroup members.
Hypothesis 3:	Ingroup-trust results in increased information security risks within organizations.
Hypothesis 4:	Positive exemplars affect management's perception of ingroup members' information security behavior.

PROGRESS TO DATE

The data collection phase has been completed and analysis in underway. Data collected from interviews, documentation, and observations seem to provide support for the ethnocentrism theory, including the following comment from the CEO regarding outsiders:

> *"There are always people who might try to get into your system. That's why I stress that we do everything to make sure these people can't get into our systems. We install firewalls and different software, we have all of our email attachments scanned, plus we are installing some new high-tech security firewall system that is supposed to do even a better job at keeping people out. But I'm never totally satisfied. There are some smart people out there that spend all of their time trying to figure out ways to get into other people's systems. Hell, if people can break into the FBI and the Pentagon, I guess they wouldn't have too much trouble getting in here."*

Further analysis will be conducted to provide a more complete test of the theory, building upon these initial findings.

CONCLUSION

This study takes a new look at information security management, by including theories that have, in the past, been reserved for studies of bias and discrimination. However, these theories can provide a new lens with which to view the organizational trust that develops among members of an organizational ingroup and how that relationship affects information security. This research is not suggesting that trust within organizations be decreased, because research has shown that organizations that create trusting environments are more productive (Coleman, 2002). However, organizations can benefit from understanding how these high levels of trust can also have negative ramifications. Organizations should realize that monitoring of employee behavior and the implementation of security countermeasures are not necessarily signs of distrust. It is the fiduciary responsibility of management to insure that organizational information is adequately protected. They surely have to take adequate measure to protect their information from outgroup members who may attempt to gain unauthorized access, but they cannot stop there. They must also insure that members of their ingroup are not abusing the trust relation within the organization. This research can help organizations better understand behavioral issues that contribute to information security risks. By understanding these behavioral issues, organizations can learn to counteract behavior that causes these risks.

REFERENCES

1. Allport, G.W. (1954) The *nature of prejudice*. Cambridge, MA: Addison-Wesley.
2. Benbasat, I., Goldstein, D, and M. Mead. (1987) The Case Research Strategy in Studies of Information Systems, *MIS Quarterly*, (11:3), 369-386.
3. Brewer, M.B. (1979) In-group bias in the minimal intergroup situation: A cognitive motivational analysis. *Psychological Bulletin*, 86, 307-324.
4. Brewer, M.B. (1999) The Psychology of Prejudice: Ingroup Love or Outgroup Hate?, *Journal of Social Issues*, 55(3), 429-444.
5. Brewer, M.B. and R.J. Brown. (1998) Intergroup relations. In Gilbert, D.T., Fiske, S.T., and Lindzey, G. (eds), *The Handbook of Social Psychology*, Vol. 2. Boston: McGraw-Hill. 4th ed.
6. Coleman, James S. (2002) Social Capital in the Creation of Human Capital, In Calhoun, Gerteis, Moody, Pfaff, and Virk (Eds.) *Contemporary Sociological Theory*, p.110.
7. Deutsch, M. (1962) Cooperation and trust: Some theoretical notes. *Nebraska Symposium on Motivation*: Lincoln: Nebraska University Press, 275-320.
8. Dhillon, G. (2001) Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns, *Computer & Security*, 20(2), 165-172.
9. Dhillon G. and J. Backhouse. (2000) Information System Security Management in the New Millennium, *Communications of the ACM*, 43(7).
10. Esses, V.M., Jackson, L.M., and Armstrong, T.L. (1998) Intergroup competition and attitudes toward immigrants and immigration: an instrumental model of group conflict. *Journal of Social Issues* 54, 699-724.
11. Frolick, M. (2003) A New Webmaster's Guide to Firewalls and Security, *Information Systems Management*, Winter, 29-34.
12. Gambetta, D. (1988) *Trust: Making and breaking cooperative relations.* New York: Basil Blackwell.
13. Hewstone, M., Rubin, M. and H. Willis. (2002) *Annual Review Psychology*, 53, 575-604.
14. Hoffer, J.A. and Straub, D.W. (1989) The 9 to 5 Underground: Are You Policing Computer Crimes?, *Sloan Managemen Review*, Summer, 35-43.
15. Hogan, R., & Hogan, J. (1994) The mask of integrity. In T. Sarbin, R. Carney, & C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal*: 107-125. Westport, CT: Praeger.
16. Insko, C.A, Schopler, J., Hoyle, R. Dardis, G. and K Graetz. (1990) Individual-group discontinuity as a function of fear and greed. *Journal of Personal Social Psychology*. 58, 68-79.
17. Judd, C.M. and B. Park. (1988) Out-Group Homogeneity: Judgments of Variability at the Individual and Group Levels, *Journal of Personality and Social Psychology*, 54(5), 778-788.
18. Mayer, R., Davis, J. & Schoormann, F.D. (1995) An integrative model of organizational trust, *Academy of Management Review*, 20: 709-734.
19. Richardson, R. (2003) *Eighth Annual CSI/FBI Computer Crime and Security Survey*, Computer Crime Institute.
20. Security Management Index (2003) *The Alarming State of Security Management Practices Among Organizations Worldwide*, The Human Firewall Council.
21. Sitkin, S., & Roth, N. (1993) Explaining the limited effectiveness of legalistic "remedies" for trust/distrust. *Organization Science*, 4: 367-392.
22. Stephan, W. G., & Stephan, C. W. (2000) An integrated threat theory of prejudice, In S. Oskamp (Ed.), *Reducing Prejudice and discrimination*, 23-45. Mahwah, NJ:Lawrence Erlabaum.
23. Straub, D. and R. Welke. (1998) Coping With Systems Risk: Security Planning Models for Management Decision Making, *MIS Quarterly*, 22(4), 441-469.
24. Sumner, W.G. (1906) *Folkways*. New York: Ginn.
25. Yin, R.K. (2003) Case *Study Research, Design and Methods* (3rd ed.), Sage Publications, Beverly Hills, CA.