IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA **ITB12706**
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Information Security: Impacts of Leadership and Organizational Culture

Gary Tarbet, University of Fairfax, 2070 Chain Bridge Road #G-100, Vienna, VA 22182, T 703-737-0040, F 703-737-0003, System 1, Inc. 8308 Sung Hill Lane, Potomac, MD 20854, gtarbet@adelphia.net

Theodore Schilie, Departmernt of Management, Lehigh University, Bethlehem, PA 18015

INTRODUCTION

Since the early 1970s computer security has been the focus of many researcher's efforts (Bell and Lapadula, 1976). Following the terrorist attack of 9/11, Congress and the Executive Branch reemphasized the need for security in general and information or cyber security in particular. The E-Government Act of 2002 (Public Law 107-347) kicked off a new national strategy for information security that built upon the previous laws.

On October 30, 2000, the President signed into law the Fiscal 2001 Defense Authorization Act (Public Law 106-398), including Title X, subtitle G, "Government Information Security Reform Act (GISRA)". GISRA brought together existing IT security requirements in previous legislation. This included the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Information Technology Reform Act of 1996 (Clinger-Cohen). Additionally, GISRA enacted in statute existing OMB IT security policies found in OMB Circular A-130 on IT management and OMB budget guidance in Circular A-11. GISRA integrated long-standing IT security requirements. GISRA also introduced new review and reporting requirements and defined a critical role for agency Inspectors Generals in independently evaluating the agency's IT security.

In March 2002 the Director of NIST, in congressional testimony, discussed the ongoing need for attention at all levels within the government to information security (Bement, 2002). The GISRA information security requirements were institutionalized when the President signed E-Government Act of 2002 on December 17, 2002. Title III of that act is called the Federal Information Security Management Act (FISMA). FISMA requires Federal agencies to annually evaluate and assess the status of the security of their information systems according to requirements established by the Office of Management and Budget (OMB), which administers the Act.

Table 1. Consolidated FISMA Scores for 24 Large Agencies

Federal Computer Security Report Card 2002 - 2004							
	2002	2003	2004		2002	2003	2004
Agency of International Development	F	C-	A+	Department of State	F	F	D+
Department of Transportation	F	D+	A-	Department of Treasury	F	D	D+
Nuclear Regulatory Commission	C	A	B+	Department of Defense	F	D	D
Social Security Administration	B-	B+	B	National Aeronautics and Space Administration	D+	D-	D-
Environmental Protection Agency	D-	C	B	Small Business Administration	F	C-	D-
Department of Labor	C+	B	B-	Department of Commerce	D+	C-	F
Department of Justice	F	F	B-	Department of Veteran Affairs	F	C	F
General Services Administration	D	D	C+	Department of Agriculture	F	F	F
National Science Foundation	D-	A-	C+	Department of Health and Human Services	D-	F	F
Department of Interior	F	F	C+	Department of Energy	F	F	F
Department of Education	D	C+	C	Housing and Urban Development	F	F	F
Office of Personnel Management	F	D-	C-	Department of Homeland Security	---	F	F

Despite the law and the pressures to improve security in the aftermath of 9/11 the record of the agencies with regard to meeting FISMA requirements is disappointing (Putnam, 2004). On February 16, 2005 when reporting the annual scorecard results Representative Tom Davis (R-VA) stated "Today, there's good news and bad news. The good news is, the grade for government agencies overall rose 2.5 points last year. The bad news is, the overall grade is a D+. The 2004 FISMA grades indicate that agencies have made significant improvements in certifying and accrediting systems, annual testing, and security training, but significant challenges remain."

Table 1 has been consolidated from the publicly available annual OMB FISMA compliance report cards. The table shows each agency's FISMA score for 2002 to 2004. By examining Table 1, it can be seen that some agencies have had very consistent scores. Others have obviously done something different because their scores show significant fluctuations one year to the next. Another issue seems to be maintaining the improved scores year to year. Most agencies show a significant drop in the year following improvement (see National Science Foundation and Department of Veteran Affairs).

This dissertation examined the role of leadership and organizational culture in the government's overall poor performance thus far demonstrated in meeting Federally mandated information security requirements. The researcher conducted a multiple-case study (Yin, 2004) to examine those factors that promote an organization achieving and maintaining an appropriate organizational security posture. The multiple-case study analysis was conducted at three Department of Energy Office of Science laboratories.

RESEARCH FOCUS

Achieving FISMA requirements is a management responsibility, while carrying out FISMA assessments is the responsibility of the information system professionals in the organization (Harold, 2003). We have found that management continues to claim there is not enough money provided in the budget to hire and/or train people with the skills needed, or to purchase the equipment needed, or to do either of these in the time allowed and that earmarking money to meet these goals would take funds away from the laboratory's primary research mission. Examination of internal DOE budget documents show significant resources are being expended to address information security requirements.

Despite all the resources allocated to, and the guidance provided for, improving information security in Federal Agencies, it hasn't happened. In this study, we assert that providing money and personnel is not enough – **organizational change** is required. For positive organizational change to occur, two factors are of critical importance: **organizational culture and leadership**.

The theoretical framework for this research focused on organizational culture and leadership as the primary drivers causing organizational change. This organizational change is required to achieve FISMA compliance. The degree of FISMA compliance is attributable to the change which has been driven by leadership that is consistent with organizational culture.

Figure 1. Theoretical Framework

Schein (2004) defines culture as "a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems". From an organizational point of view, culture is often established by the founding leaders of the organization.

RESEARCH STRUCTURE

To investigate the impact of organizational culture and leadership on achieving FISMA information security requirements, this study utilizes a multiple-case study approach as described by Yin (2004). Three DOE research laboratories comprise the set of cases. One is a multi-purpose lab and two are large single purpose labs spread across the country.

Although all of the DOE research laboratories have problems achieving FISMA compliance, some of the laboratories have better security controls than others. Therefore, the question to be addressed by this research is: **Why do some of the laboratories achieve better information security than others?** The **dependent variable** inherent in this question is the degree of information security achievement, as measured by a pseudo-FISMA score. The **independent variables** being investigated, as already discussed, include **organizational culture, leadership, and change.**

INITIAL RESULTS

Preliminary results among the three laboratories show one scoring relatively higher and one lower than the other based upon ratings by a panel of experts which included policy and penetration testing personnel. The highest scoring lab has a cultural style and leadership that appreciates information security while protecting their open science status. Work is still underway to try to understand why that has developed. Another site has a charismatic information security leader who has used his personal skills to put in place an effective program. Both of these sites have IT professionals in place. The third site has a physicist managing IT. They have decentralized most security functions and their lack of processes and procedures has resulted in a weak security program. The head of information security recently resigned and the researcher's consulting report on their program highlighted multiple areas of concern. The ramifications of this report are still being measured.

In the initial phases of this research we have identified a number of cultural influences that have affected the DOE Laboratories. Four of them, would appear to have a direct and significant impact on information security. They are: the cultures of the university, basic research, bureaucracy, and Manhattan Project. All of these influences are present to varying degrees in the history and evolution of DOE and its research laboratories.

Like many universities, the laboratories tend to see themselves as a "city on the hill". The "city on the hill" was intended to be a community with culture and values that would be an example for the rest of the world (Abshire, 2004). Universities often see themselves as a "city on the hill" as their culture purports to encourage the free, open exchange of information occurs with scientist and peers from many nations. This informational exchange fosters the growth of knowledge with appropriate checks and balances through peer review. In actual fact, professors and researchers at the university are often highly competitive, but the ideal of free exchange of information remains strong.

While some information is exchanged each individual is in a race with their peers to be published, to obtain recognition in the form of awards or to be recognized by their peers. The culture of basic research is strong at all of the labs.

We have also found researchers fiercely defend their independence. They see rules and regulations as bureaucratic overhead and some actually see regulations as challenges to defeat. The labs defend their open science status in an almost anti-Manhattan Project backlash. The preference is for no information requiring special handling at the labs.

Similarities in the labs we found at the labs include:

- built like campuses
- a "common" area with a food service and large eating area where colleagues can sit and discuss issues
- dress is normally very informal
- researchers have offices with nameplates
- titles are very important and researchers who distinguish themselves receive "tenure" at the laboratory
- extremely low turnover in personnel
- personnel are promoted from within with little outside hiring
- individuals that promote change or new ideas are often seen as not supporting the group and they become ostracized from the group
- new ideas or concepts that would change basic tenants of the organization are strongly opposed
- those presenting new concepts are told they do not understand research or that the suggested or required change would "kill research"
- consensus model of governance is very prevalent at the laboratories, similar to the "faculty governance" model

We have also noticed that budgeting is focused on the accomplishment of research activities. We have heard the same rough quote many times "A dollar spent on overhead is a dollar less for research". Each laboratory receives an information security budget as a separate line item. In our visits we noted little relationship between the security budget and the funding of security related activities. While the money is definitely being used, the exact use is difficult to ascertain.

CONCLUSION

FISMA's goal is to bring order and structure to the information security decisions of an organization. The differences in cyber security achievement among the labs are significant. In one lab we found senior management actively involved in information security. That active involvement flowed through the entire organization with immediacy for action. At other labs the more passive approach was clearly visible in the staff along with the expected results. Organizational change and the understanding that information security is part of the way the laboratories do business will take time to foster and incorporate within the culture of the laboratory. Leadership must understand the role of security and use the labs strengths to promote a security culture.

REFERENCES

Abshire, David (2004). The Grace and Power of Civility. Center for the Study of the Presidency. Fetzer Institute. www.thepresidency.org. *Election Day Edition, 2004*.

Bauer, Martin (ed.). (1995). Resistance to New Technology. Cambridge: Cambridge University Press.

David E. Bell and Leonard La Padula, (1975). *Secure Computer System: Unified Exposition and Multics Interpretation,* ESD-TR-75-306, ESD/AFSC, Hanscom AFB, Bedford, MA 01731 (1975) [DTIC AD-A023588]

Bement Jr., Dr. Arden L. (2002). *Lessons Learned from the Government Information Security Reform Act of 2000.* Before the Committee on Government Reform, Subcommittee on Government Effi-

ciency, Financial Management and Intergovernmental Relations, House of Representatives. March 6, 2002.

Gillham, Bill (2000) *Case Study Research Methods*, Continuum, New York

Harold, Jerry (2003). Washington Gets Tough. *SC Magazine. October 1, 2003*. http://www.scmagazine.com/asia/news/article/419766/washington-gets-tough/

Office of Management and Budget (2004), *FY 2003 Report to Congress on Federal Government Information Security Management*., http://www.whitehouse.gov/omb/egov/fy03_egov_rpt_to_congress.pdf

Putnam, Adam (2004). *View from the Hill*. Military Information Technology, June 17, 2004, volume 8, issue 4

Schein, Edgar H., (2004). *Organizational Culture and Leadership*, John Wiley & Sons, San Francisco, CA.

United States Government (2000). *FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform Act (GISRA)"* October 30, 2000

United States Government (2003). Public Law 107-347. *E-Government Act. HR2458*. http://csrc.nist.gov/policies/HR2458-final.pdf

Yin, Robert K., (2004) *The Case Study Anthology*, Sage Publications, Inc., Thousand Oaks, CA.