Developing a Security Oriented Corporate Culture

JurInnov White Paper

Eric Vanderburg

2012
Table of Contents

Table of Contents ......................................................................................................................... 2
Introduction ................................................................................................................................. 3
Assessment .................................................................................................................................. 3
Traits .............................................................................................................................................. 6
  Valuing Information Security ...................................................................................................... 7
  Open Environment ...................................................................................................................... 8
  Respect for Privacy ..................................................................................................................... 9
  Creativity ...................................................................................................................................... 9
  Long-term Thinking ................................................................................................................... 9
  Embrace of Change .................................................................................................................... 10
Change .......................................................................................................................................... 10
About JurInnov ............................................................................................................................ 14
About the Author ......................................................................................................................... 12
Appendix A ................................................................................................................................. 15
Introduction

Managing the security of an organization can be quite confusing. It can seem like an uphill battle when basic security awareness concepts such as keeping passwords secret or refraining from discussing confidential topics outside the workplace are consistently ignored. Why do some security initiatives fail while others succeed? The answer may lie within the corporate culture. Corporate culture, also known as organizational culture, is the invisible lifeblood made up of the values, priorities, assumptions, and objectives of those within the organization. Just as the body rejects an incompatible organ, the greatest security initiative may fail because of an incompatible corporate culture.

To determine if an incompatible culture exists, a company’s current organizational culture should be assessed to identify its level of security-oriented awareness. Appendix A comprises a series of questions that can be used to identify elements of a corporate culture. Such a cultural assessment can begin by asking these questions to various people within the organization. The answers to these questions will differ between people, thus, illustrating how an individual’s perception of the culture differs from the actual culture.

Frequently, corporate leaders strive to immediately change the corporate culture once it is determined that there is a need for a change. Corporate culture, however, is not a thermostat that can suddenly be changed to incorporate security needs. A corporate culture transforms as employees internalize successful ways of doing business, a process that has occurred gradually over the lifetime of the company. Changing a culture involves consistent, visible, new, and incrementally different
methods to be used, proven successful, and adopted. Successful ideas and supporting behaviors continuously reinforce and strengthen those same behaviors.

**Assessment**

The objective of a cultural assessment is to discover the security characteristics of a corporate culture. Understanding these characteristics will clarify whether or not a culture is concerned with security. Assessing corporate culture requires deep thinking since corporate culture lies underneath the surface. This culture is the model people use for conducting regular activities and the filter used for evaluating options and ideas. However, it cannot be fully comprehended solely by observation of employees’ actions and opinions within the current climate.

Diagram 1: Edgar Schein’s three levels of understanding corporate culture

Three levels for understanding and identifying corporate culture

- **Artifacts**
  - Visible organizational structures and processes

- **Espoused Values**
  - Strategies, goals and philosophies

- **Shared Tacit Assumptions**
  - Beliefs and values

In his book “The Corporate Culture Survival Guide” Edgar H. Schein, a professor of management at the MIT Sloan School of Management, outlines a three-tiered method for understanding and identifying corporate culture. The three levels depicted in Diagram 1 begin with artifacts and gradually move deeper to espoused values, concluding with shared tacit assumptions (1999, p. 15). The artifacts observed at level 1 include such easily-observable things as cooperation,
attitude towards work, office layout, and the number of levels of management. Additional examples can be seen in diagram 2. It is here where observers can begin to make premature assumptions about culture. Level 1 artifacts are interesting but still only pieces of data. Understanding culture requires a deeper analysis.

Diagram 2: Level 1 cultural artifacts

Level 2 involves asking questions to understand why the artifacts exist. A natural prerequisite, therefore, is to have observed artifacts to ask questions about. The answers to these questions will illuminate the espoused values present within the organization. Uncovering these values is important as different cultures could share the same values. For example, one organization may utilize extensive training to prevent social engineering and have an open policy on information where almost all information is available to everyone within the firm while another conducts little training but relies heavily on the “need-to-know” principal. When asked about these artifacts, members of both
companies may state that they do this out of a desire for privacy and confidentiality. Even espousing the same values, the companies express them in different ways.

To aid in discovering these values, Chia, Ruighaver, and Maynard created a model that can be used to evaluate the quality of an organization’s security culture. The model builds on previous work by Detert, Schroeder, and Mauriel (2000) on the values that make up an effective TQM (Total Quality Management) culture. The researchers applied the TQM framework to security culture, organizing it into eight cultural categories or “dimensions” as can be seen in diagram 3 below. Diagram 3: Chia, Ruighaver and Maynard’s eight cultural dimensions

The first dimension, the basis of truth and rationality, is concerned with how employees view current security initiatives and policies. Questions in this dimension identify whether or not employees see their company and its procedures as secure. The second dimension is the nature of time and time horizon. Questions in this dimension determine whether long-term, short-term, or both long and short-term security goals are important. Motivation, the third dimension, addresses how employees are motivated to put security into practice. The fourth dimension is orientation and focus. This dimension is focused on whether the responsibility of creating security initiatives belongs to the business itself or the government. The fifth dimension is stability versus change, innovation, and personal growth. This dimension is centered on how much the culture embraces change. The sixth dimension is orientation to
work, task, and coworkers, and is concerned with how responsible employees feel for security and the impact that security initiatives have on employees. The seventh dimension, isolation versus collaboration, deals with the amount of cooperation that exists between employees. The final dimension, control, coordination, and responsibility, addresses the alignment of security and organizational goals and the direction in which directives flow.

Schein’s third level uncovers an organization’s shared tacit assumptions. It is here where culture is understood as a concrete assumption rather than as an abstract value. Shared tacit assumptions arise out of a history of success. The assumptions and values that bring about success are naturally attributed as successful components. This process forms the experiential knowledge that almost subconsciously governs decision making in the future. Experience shows the members of the organization that these methods produce successful results so the methods are perpetuated. The process of cultural development and cultural acclimation by new members is similar to the way children are socialized by the factors in their environment. In explanation of the concept, Schein argues that as a firm grows, leaders will attract others with similar values and beliefs. After each success, the present values become more internalized and accepted as the proper way to act. To discover these shared tacit assumptions, one must observe the organization’s history. This, Schein states, is the essence of culture.

**Traits**

Research points to certain organizational traits that significantly impact security culture. The traits that define a security-oriented culture consist of valuing information security, an open environment, respect for privacy, creativity, long-term thinking, and embracing change. Recently this field has been a hotbed of research, with a number of researchers making great strides in the field. Michael Caloyannides, an information security researcher and senior fellow at Mitretek Systems,
writes that some traits essential in a security-oriented corporate culture are the freedom to ask questions, respect for privacy, and an environment of creativity. Chia, Ruighaver, and Maynard are credited for their mention of long-term thinking and embracing change and they along with Koh, et al. highlighted valuing information security.

**Valuing Information Security**

Some employees have little regard for information security. They may not conform to security policies or may even bypass security controls entirely. However, a security-oriented culture is composed of members who recognize the value of information security, Chia, Ruighaver, and Maynard argue that the belief that security is of the utmost importance will be reinforced by increasing the participation associates have in making security decisions. Koh, et al. conducted similar research on the effect of security governance on the responsibility and sense of ownership of security initiatives felt by associates. Their study demonstrated that participation is the primary factor contributing to increased responsibility and sense of ownership. Consequently, increased participation levels also motivate employees to be more security conscious and take responsibility for the security of their own projects and clients. This is a natural extension of the level of service each person should provide to his or her client.
Open Environment

An open environment where people are free to ask questions without consequence is required if the organization is to protect against the myriad of attacks faced daily. Resources must be allocated to address the most critical vulnerabilities rather than being blindly dispensed to those recommended by the media or government. Too often, organizations accept at face value information given by sources without questioning the source’s bias or impetus. It is the employee’s responsibility to discern in detail what is heard and read.

Respect for Privacy

The average person may be observed trading their privacy for a chance to win the latest gadget. After clicking on an enticing banner ad with little regard for the real value of the information being traded, people fill out online forms and provide an abundance of private information to a company or person they do not know. A security culture with a proper respect for privacy is essential for information security effectiveness. Caloyannides states in his 2004 IEEE Security & Privacy article “Enhancing Security: Not for the Conformist” that privacy is often sacrificed for what is perceived to be better security but in actuality is just an empty solution with no real value providing substance. A culture that respects the privacy of associates and clients will embrace policies and technologies surrounding confidential information.

Creativity

Creativity is what allows innovative solutions to be created. A security-oriented culture depends on creativity to combat the creative malicious efforts present in the world. Caloyannides cites the need for an environment of creativity which fosters creativity in the individuals in the company. Prior generations were not privy to the entertainment of today that our children are so consumed with
and so they thought more creatively. Creativity and imagination were the requisite in the simplest of games but now it has become scarce. This experience is the preparation crucial for the innovators of our day. Attackers themselves are very creative in the exploits they develop; countering them requires the same ingenuity as the potential attacker.

**Long-term Thinking**

Life is busy but it only gets busier with a lack of preparation. Organizations think long-term by enabling a security culture. Not only do these companies have a long-term goal in place, they also set goals that are possible. Frequently, organizations are so preoccupied dealing with immediate needs that they do not spend enough attention on long-term objectives. Security is not something that can be continually patched; it must be properly designed and thoroughly analyzed. Plans and procedures should contain long-term elements in order to be successful. Chia, Ruighaver, and Maynard in the article “Understanding Organisational Security Culture” state that “organizations with high-quality security culture should ultimately have long-term security plans and strategies”. Such forward-thinking security-minded organizations will foster a culture of security that will reinforce the strategy and goals they advocate.

**Embrace of Change**

Members within a security-oriented culture must be able to adapt in a changing environment. Emerging social and technological threats along with changes to regulatory requirements and legal processes require firms to be able to adapt accordingly in order to remain successful and to serve clients well. A security-oriented culture supports and encourages change.

**Changing your Culture**

Like the wind, it is hard to perceive corporate culture and even harder to manipulate it. As was previously noted, various cultures exist within each organization and they can be revealed by using Schein’s three levels. The present culture, however, may be inhibiting compliance with new
legislation, regulations, and security initiatives which may ultimately cause a company to fail. After
close examination of the current culture, remedies can be established to cure the disparity.

Corporate culture cannot be formed overnight. Rather, Schein affirms that it takes many
successes to build upon the founding values of an organization, which are then internalized by the
members of the organization. Similarly, in order to change a culture, the underlying values and
assumptions of an organization must be challenged and an alternate set of values proven successful
many times before any change can take place. Since values must be internalized by employees,
changing the culture is analogous to convincing a steak lover that meat is unhealthy. Change takes
time, and more importantly acceptance of factual information that verifies a conclusion to make a
conversion.
About the Author

Eric Vanderburg is the Director of Information Systems and Security at JurInnov, Ltd. ("JurInnov"). JurInnov’s consulting practice is a trusted resource for law firms and corporations whose litigation technology needs are as varied and specialized as the organizations themselves. JurInnov’s international consulting practice focuses on the application of technology solutions to today’s challenging business and legal demands, including information security consulting, litigation document management and online review, electronic discovery, legal analytics and review, and computer forensics.

Eric Vanderburg is a graduate from Kent State University with a Bachelor of Science in Technology and a Masters of Business Administration with a concentration in Information Systems. During and after his education he worked as a consultant specializing in the development and maintenance of information management and network security systems for businesses, law firms, and government agencies. Most recently, he was a professor of computer networking at Remington College where he taught courses on information security, database systems, and computer networking. He has been invited to speak at many organizations and campuses on technology and information security. In order to build further competencies in information security, Eric is currently pursuing a doctorate in Information Assurance.

Vanderburg joined JurInnov in 2006 to manage information systems and security for JurInnov and its clients. He holds over 25 vendor certifications including: Certified
Information Systems Security Professional (CISSP), Holistic Information Security Practitioner (HISP), Certified Wireless Security Professional (CWSP), Hitachi Data Systems Certified Professional (HDSCP), and many certifications from Microsoft and Cisco.
About JurInnov

In 2000, Tim Opsitnick was a well-established attorney at Jones Day. His work brought him into contact with electronic data discovery and litigation management. As he worked with technology companies, he began to see a void. It seemed they didn’t speak the same language as the law firms they were helping. They were vendors, not partners. Tim saw an opportunity to start a company that would be a peer of law firms, but with all the technological expertise of a high-tech company. And JurInnov was born.

JurInnov works with IT and legal departments in a wide variety of industries and sectors. We become a link, an extension of both departments. We help them adopt the most current standards and tools. We help companies better manage and track electronic information, uncover evidence, plan for data recovery, and relax a little bit like in the good old days when everything was filed neatly in its place.

JurInnov’s state-of-the-art headquarters is located in downtown Cleveland, Ohio within The Idea Center Building, a historic landmark located in the heart of Cleveland’s Technology Corridor. Featuring leading edge information technology infrastructure, the highly secure office suite includes workgroup-specific gigabyte networking, high performance teaming areas, fire-proof storage rooms and direct fiber optic connectivity to offsite data center and broadband communications providers.
Appendix A

Security-oriented culture sample questions.

1. Would you consider your company an early, medium, or late adopter of technology?

2. In the past three years, have you seen significant value from the adoption of security initiatives?

3. Which people or departments are typically consulted when making security decisions?

4. How much freedom do you have to try new procedures of ways of doing business?

5. In which way do you see your company more at risk; from action or inaction?

6. Is information security one of your company values?

7. Does your company respect a diverse range of opinions and ideas?

8. Do you feel your company has adequate security?

9. Do you feel your company is significantly concerned with security?

10. Do the security practices of the company match the security policies?

11. Do the security controls at your company make it difficult to do your job?

12. Do you feel that your coworkers are generally “on board” with security initiatives?

13. Is security a regular topic in meetings?

14. Are significant security metrics tracked and reported on?

15. Are you held accountable for meeting security goals in performance appraisals?
References:


