Information Security Governance: Integrating Security Into the Organizational Culture

Position Paper

Laura Corriss
Barry University
11300 NE Second Avenue
Miami Shores, FL 33161
U.S.A.
mcorriss@mail.barry.edu

ABSTRACT

We finally got what we wished for: executive managers are aware of the need to protect their organizational data. However, we still have problems; for example, database breaches, stolen passwords and identity theft continue to be major issues. Aside from usability issues, the major issue is that management usually considers information security governance as under the jurisdiction of their information technology department, separate from corporate governance. They do not realize that security cannot be treated as an "add-on"; security must be made a priority and become integral to the organizational culture. This integration of security must be done from the top down and include everyone in the organization. I propose that the best and easiest way to accomplish this is by focusing on the everyday security issues that employees confront. Management should not initially try to force employee buy-in to the entire security policy. Instead, management should initially limit the policies with which all personnel must comply in order to help shape behavior that will ultimately become second nature. As employees learn and comply with these policies, management can slowly introduce the additional policies so that eventually the entire policy becomes integral to the organizational culture.

Categories and Subject Descriptors

K.6.5 [**MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS**]: Security and Protection; K.6.1 [**MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS**]: Project and People Management —*Strategic information systems planning*; K.4.3 [**COMPUTERS AND SOCIETY**]: Organizational Impacts; K.6.0 [**MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS**]: General—*Economics*; K.5.2 [**LEGAL ASPECTS OF COMPUTING**]: Governmental Issues—*Regulation*

General Terms

HUMAN FACTORS, MANAGEMENT, SECURITY

GTIP 2010 Dec. 7, 2010, Austin, Texas USA

Keywords

Governance, information security, management, organizational culture

1. INTRODUCTION

I propose that the most effective way for an organization to protect its data and ensure compliance with security policies is for executive management to promote security in their daily activities and administration. To achieve this, it becomes necessary to raise the awareness levels of *all* members of the organization so that security becomes an integral part of the organization; in other words, security *must* become part of the organization's culture. This can happen only if everyone in management considers it a priority.

To accomplish this, there are 3 keys points that management and security professionals need to know. These apply to all organizations, including government and military, even though the focus in this paper is on business.

1. Just as we would never want to treat security as an add-on application in the software or hardware world, we need to make security integral to the organizational culture. An organization can best accomplish this by identifying a subset of the security policy that applies to all personnel and that is enforceable and that does not create a hindrance to employee productivity. Awareness and compliance can be achieved through training, incentives, and a demonstration of commitment to the policies by everyone in management, from the top down. Once adherence to these policies starts to become second nature to all employees, management can incrementally add the balance of the policies until all policies that affect daily behavior are accepted as the norm.

2. Integrating security into the organizational culture must come from the top-down, however middle management buy-in is critical, and chief security information officers can help to promote the change.

3. An organizational culture with good security will reap other benefits, such as improved efficiencies, in much the same way that applications with better security tend to have less lifecycle costs due to higher quality. There is also the added benefit of an improved reputation, which may help to increase or maintain the "bottom-line."

Despite executive managers' increased awareness of the need to protect organizational data, security problems such as database

breaches, stolen passwords and identity theft continue to be major issues [26]. Many organizations still do not use technology efficiently and effectively and do not adequately protect their data [6]. Organizations either are not training their employees adequately or are not enforcing compliance; for example, there are still too many organizations where users continue to click on email attachments, thus infecting their computers with viruses. Laptops containing critical and confidential organizational data often continue to be stolen or lost. Part of the problem relates to usability issues [19], but much of the fault is due to the lack of attention to security by executive and middle management. Although many managers truly believe they are strongly committed to security within their organizations, they do not necessarily enforce and demonstrate their support through their actions and decisions.

As an illustration of this problem, in 2002, the U.S. Congress reacted to a series of financial scandals by passing the Sarbanes-Oxley Act (SOX), which focused on transparency and accuracy in financial reporting by public companies [22]. SOX also resulted in increasing attention on Information Technology (IT). Control objectives for information and related technology (COBIT) now provides IT governance for information integrity compliance with SOX [20]. As a result, the number of IT audits conducted by auditing firms dramatically increased [8]. Unfortunately, auditing firms are not necessarily ready for IT auditing [15], and even when they are, the focus is on data integrity as it relates to traditional financial reporting and not on information security. In addition, auditors costs money; as Ross Anderson pointed out in 2001, information security is as much an economic issue as a technical one [5]. Until executive management is convinced that the cost of not auditing their organization's security is greater than the cost of the audit, or until government regulations force the issue, organizations will be reluctant to spend the money. Worse yet, auditing is not the same as compliance; even if management and auditors work together to identify risk and develop a usable security policy, ensuring compliance throughout the organization is not guaranteed.

Although Anderson was referring to organizations when he stated, "Where the party who is a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected" [5], this applies to individuals as well. Requiring knowledge of and adherence to the organization's entire security policy will cause problems when trying to get full employee acceptance because not everything affects all employees. Identifying what issues employees confront on a regular basis and initially limiting awareness and enforcement of the security policy to those items will encourage acceptance and buy-in.

2. ORGANIZATIONAL CULTURE

Homeland Security recognizes the importance of organizational culture for effective security governance. A Google search [1] brings up a document on their website that begins "Governance and management of security are most effective when they are systemic, woven into the culture and fabric of organizational behaviors and actions" [11].

The culture of an organization is basically its personality. It includes the goals, assumptions, beliefs, values, norms, behaviors, customs, rites, history, and even the style of dress of the people who work for the organization. It is what makes employees feel like they belong and what encourages them to work collectively to achieve organizational goals. There is a difference of opinion as to whether culture is something an organization "has" or what the organization "is" [28]. Either way, an organization's culture evolves slowly, generally growing stronger over time. Changing culture is hard. For example, employee turnover generally does not weaken the organization's culture [12]. It is, in fact, difficult to make major changes to an organization's culture. The most common way to do so is to replace the corporate leadership by hiring someone from outside the organization [24].

It might be difficult to move an organization's culture in a different direction or to make major changes, but actually change is occurring all the time due to a variety of influences, internal and external to the organization. The strongest influence comes from the top leadership position, something security professionals can use to their advantage to encourage the change that is needed to achieve a more secure organization.

Many organizations recognize the need to secure their data but do not know how to make it a priority throughout the organization. Jan Thornbury recommends starting with identifying the benefits to the business so that everyone realizes the need for the change, then identifying where you are now, where you want to be, and what specific steps should be taken to implement the change. The organization's leaders must demonstrate their active involvement at all times. This is a strategy she followed when assisting the audit, tax and advisory firm KPMG with integrating its various component partners [27].

3. ORGANIZATIONAL HIERARCHY

Depending on the size of the organization, the top leadership position can be the Chairperson of the Board, the Chief Executive Officer (CEO) or the President. In some instances, the same person can hold all positions, for example, Lou Gerstner was hired as both Chairman and CEO of IBM in early 1993. Other executive positions can include the Chief Operational Officer (COO), the Chief Financial Officer (CFO) and the Chief Information Officer (CIO). Everyone in these top two tiers is considered "executive" or "senior" management. More commonly, the Chief Information Security Officer (CISO) is also on this level, although in some organizations, the CISO reports to the CIO.

The next tier in the organizational chart generally consists of the mid-level managers. Depending on the size of the organization, these can include the general manager (GM), vice presidents, and department heads. Below mid-level management are the front-line managers and supervisors. These are the people responsible for the daily administration of the organization, who interact with their employees on a regular basis and who have a strong influence on employee motivation and behavior.

The reason that executive management influences corporate culture more than the front-line managers is that the culture is affected by the organization's strategy, which is linked to its structure [24]. The organization's structure reflects the chain of command, formal communication channels, and the alignment of people to the work and the work to the organization's goals. Studying IBM under Lou Gerstner demonstrates this. Through the 1980s, IBM was known for its strong corporate culture that rewarded loyalty. Despite extensive technological changes in the computer industry and the marketplace, which resulted in major restructuring changes within IBM, their culture experienced only minor effects. Management continued to recruit and promote talent from within, and loyalty continued to be highly rewarded. IBM reduced personnel through attrition and retirement, not layoffs [29]. However, by 1993 demand for IBM's mainframe computers had slowed dramatically, demand for mini-computers had dramatically increased, and IBM's competitors were getting most of the business. Lou Gerstner was brought in from the outside to help save the company, and over the next decade he lead a turnaround that became one of

[1]Using "+management +governance" as a search term.

the most written-about and cited examples of organizational change in business history. However, to achieve his goals, Gerstner instituted many changes, including massive layoffs, which dramatically changed the organizational culture. The company that was once known for inspiring lifelong loyalty struggled to maintain morale among its employees. Within a decade the organizational culture at IBM was changed due to the influence of one single person, the top leader of the organization. Whether or not that culture change was for the better is not relevant to this paper. What is important is how relatively quickly a major change occurred and how it was achieved

4. CORPORATE CORE VALUES AND CISOs

I submit that a major dichotomy exists between the mindset of top management and the mindset of middle management in many organizations. In these organizations it is as if top management and middle management stand back-to-back, facing opposite directions. An organization cannot align all its employees, including middle management, with organizational principles when the core values express *only* the values of top management but do not include all the values critical to the organizational functions. A commentator on an earlier version of this paper took the view that core values are aimed at articulation of a business philosophy and that therefore they will never mention security and governance because both of these are considered operational issues. This is true; but I submit that this is a fundamental problem, addressed later in this section.

If we want employees to know and to internalize what is critically important to an organization, these values must be explicitly stated; the best place to state them is in the core values because this is what employees read, and which they also understand top-management views as critical. If information security and privacy are not included in these stated core values then employees will not view them as essential to their daily business functions and mindset.

An organization's culture is generally reflected in its mission statement and explicitly stated core values. The core values spell out the organization's basic beliefs and passions, *i.e.*, what the company stands for and what it values. The mission statement is created based on the core values. The core values and the mission statement are used to guide the organization when making strategic, and ethical, decisions [23]. Once core values are internalized, behavior reflecting those values becomes second nature.

A Google search of organizations' core values[2] indicates that very few organizations list privacy or anything relating to information security on their list of core values, even those for whom it is a major issue, e.g. banks, insurance companies, and auditing firms. The most common values include integrity, service, loyalty, honesty, trust, and teamwork.

A search of hospital sites returns a similar list of values. The Health Insurance Portability and Accountability Act (HIPPA) passed in 1996, with an emphasis on patient privacy [1]. Managers in the health care industry are required by law to enforce compliance among their employees and many are turning to technology for help, but compliance has been difficult [18]. Health care managers share some of the problems confronting information security professionals.

Most organizations include a privacy policy on their website, but the purpose is for legal protection. Once written, the privacy policy is generally "out of sight, out of mind" and does not help to promote an awareness of privacy issues among employees.

Inclusion of the words 'privacy' or 'information security' in an organization's list of core values does not guarantee that everyone in the organization will value them unless management demonstrates their commitment. Many organizations periodically review their mission statements and core values, to ensure they reflect the organization's guiding principles. CISOs should use that opportunity to convince top management that information security and privacy should be included among their organization's core values. A Delphi study conducted by Johnson in 2009 examined the drivers behind business executives' and security executives' investment in information security. The two groups agreed that legality and compliance with regulations were the most important drivers [17]. CISOs can use these concerns, cite laws and regulations that punish non-compliance, emphasize the positive impact on employees and productivity, and point out the impression it will make on the organization's customers. This will have the effect of making security a priority for the top leaders in the organization.

5. OTHER RESEARCH

In 2006 Knapp, *et al*. conducted a study consisting of open-ended questions to managers in a variety of industries, including government, in 23 different countries to determine the importance of top management support on the level of security within an organization. The researchers concluded "top management support positively impacts security culture and policy enforcement" [21]. However, there was no mention as to exactly how management could or should influence their organization's cultures other than by showing support.

Coles-Kemp, *et al*. conducted a study that showed that many businesses do not have the tools to relate security risks to business risks and objectives, but the use of a facilitator can help them understand and better communicate security risks and help embed security management into business practices [9].

Another study of security breaches of university databases led Alicia Anderson to conclude that among the steps management needs to take to protect their organizations' data is to promote security awareness by "creating a culture where the community has the knowledge (what to do), skill (how to do it), and attitude (desire to do it) that support information security and privacy objectives" [4]. Once again, there was no "step by step" analysis as to how to make this happen.

John Shook's account of the failure of the joint venture by General Motors (GM) and Toyota to manufacture cars in California provides some answers. His recommendations for managers who want to change the culture of their organization include the following.

1. Start by changing what people do rather than how they think.
2. It's easier to act your way to a new way of thinking than to think your way to a new way of acting.
3. Give employees the means by which they can successfully do their jobs.
4. Recognize that the way that problems are treated reflects your corporate culture [25].

Beauterment, *et al*. suggested creating a "compliance budget" to examine the costs and benefits of security compliance or noncompliance to employees [7]. Included in the suggestions were recommendations for awareness training, monitoring, and sanctions.

[2]Searched using +"core values" and the industry name, e.g. +"core values" +insurance, or +"core values" +bank, or +"core values" +hospital".

These are tools already known to management and which can be used to help generate awareness of the need to make security a priority within the organization.

6. ENTRUST: ISG CASE STUDY

Entrust, Inc. provides identity-based security solutions to over 4,000 government and business organizations. Realizing the need for an information security governance framework, the CEO, Bill Conner, teamed with the Business Software Alliance to create a task force, and their report was released in 2004. Among some of their findings were that executive management, including the board of directors, are often not included in the risk assessment process, even though they are ultimately responsible. Bill Conner lead the task force, using Entrust as a case study, and included all of Entrust's senior management, not just the CIO, in the process. The head of each business unit was responsible for identifying risks and recommending policies. After 5 months the task force met again to review and refine their assessments and policies by considering employee behavior, which lead to a series of narrow assessments, following a model for continuous improvement.

The task force determined that communicating risk needs to be done using simple language that makes it easy to make decisions, rather than one that would require interpretation. Each individual business unit is responsible for assessing and improving their information security program, and an independent audit is conducted each year, with the results reported directly to the board of directors [10].

7. CATERPILLAR: SAFETY CASE STUDY

Caterpillar manufactures diesel and natural gas engines, construction and mining equipment, and gas turbines for the past 80 years. They have locations throughout the United States as well as 23 other countries, manufacture around 500 different products and have around 100,000 employees.[3]

Safety has always been a concern for Caterpillar, and not only because of OSHA (Occupational Safety and Health Administration) regulations in the United States. Aside from the intrinsic value of human life, injuries result in production delays, additional costs and affect employee morale. On rare occasions employees have been killed on the job. So, over time, safety was given more attention, but it had no effect on the number of injuries that occurred.

That started to change in 2005 when CEO Jim Owens declared safety as his foremost concern. Everyone, from the top down and bottom up, was held accountable for their own safety, safety within facilities, and the safety of their products. Safety initiatives were identified and implemented. They sometimes varied by region, country or manufacturing plant, but they all focused on injury prevention. Proactive action was encouraged. Employees in each facility made lists of their own issues and were encouraged to offer suggestions. Training programs were designed around these issues and suggestions, and all employees were required to attend.

Safety was discussed at the start of every meeting, whether it was a brief meeting of supervisors with staff or a meeting of the Board of Directors. Supervisors and managers reviewed each task and any safety issues to determine the level of the risk (high, medium or low), the likelihood of injury and the seriousness of any potential injuries. By breaking processes into their components, everyone was able to see the potential safety issues. The high-risk tasks were addressed first so that procedures could be developed and implemented to proactively prevent injuries. For example, slip and trip hazards were eliminated, as were sharp edges in products and pinch points in equipment. Once safety hazards were identified and removed, employees were responsible for ensuring they stay removed.

Procedures were documented and regularly reviewed. Policies incorporated these procedures and managers were held accountable for their enforcement. Any infraction was recorded.

Safety managers established metrics, such as tracking the frequency of serious injuries, new injury frequencies, and lost time from work. Workers were rewarded for improvements. Results were dramatic. OSHA requires injuries requiring medical treatment or time off from work to be reported. Caterpillar historically had reported injuries that more or less match the standards of the industry. During recent years these injuries started trending down, and by 2008 they had been reduced by more than 50%.

According to one of Caterpillar's regional safety managers a focus on safety and proactively noticing and identifying potential risks became part of the corporate culture [3]. It started very slowly, but because it was emphasized and enforced by the CEO, it gained strength and is now an integral part of the organization. Employees are proud of their safe facilities and products.

In July 2010 Jim Owens retired from Caterpillar. The Tribune Business News reported that Mr. Owens cited as one of his top achievements "his strategy that took Caterpillar from mediocre in terms of plant safety in 2005 to one of the top three of four companies in the country this year." [14].

So what does Caterpillar's safety record have to do with computer security? It demonstrates the importance of upper-level management buy-in. It demonstrates how, in a few short years, employees and managers can become willing partners, changing attitudes and behaviors to create an environment that reduces risk.

Safety and security have a lot in common. Neither can exist in an organization unless and until all members of the organization focus on their behaviors and attitudes. Behaviors and attitudes involving safety, privacy and data security are encouraged or discouraged by the enforcement of policies and practices, which are under the control of management, but who controls management? It all starts at the top. That is the lesson that Jim Owens and Caterpillar can teach us.

8. PRODUCTIVITY AND REDUCED COSTS

Adhering to a strict security policy will probably increase expenses, but that does not have to mean a reduction in profits. Companies lose money and productivity every time a computer virus affects employee's machines. Companies lose money, and sometimes business, every time a laptop containing critical and confidential information is lost or stolen. Companies lose money, and sometimes their reputations, when database breaches are discovered and reported by the press.

Employees want to feel valued, but do not feel valued when they do not have the resources they need to do their jobs or if they believe management does not value their time. When viruses infect employee's computers, not only does productivity suffer, so does employee morale.

Once security becomes integral to the culture, less money will need to be spent on training. Training will still need to be offered, and on a regular basis, but the amount of training will decrease. New hires will learn what behavior is acceptable and expected by watching their fellow employees. Compliance to federal laws and government regulations will be easier, resulting in fewer, if any, fines.

[3]http://www.cat.com

Once compliance becomes part of the organization's culture, risk is reduced, which can result in reduced insurance and auditing costs.

Good security can lead to greater efficiencies, which lead to lower costs.

On the other hand, there is growing evidence that users do not adhere to security policies because the policies are burdensome. Cormac Herley suggests that this is entirely rational because many of the policies concern threats that result in little or no harm to the user. Users eventually realize that adherence to the policies result in a lot of time spent to limit little or no harm, at least to them [16]. Adams and Sasse studied the issue of users and password policies back in 1999 and concluded "security needs user-centered design" [2]. This is why management needs to limit the policies it initially enforces throughout the organization to those that would actually benefit the organization and would not lead to either perceived or real wastes of employee time.

9. THE "BROKEN WINDOW" THEORY

In 1982 criminologists James Q. Wilson and George Kelling presented the "broken window" theory that argued that crime could be reduced by repairing broken windows, removing graffiti, and keeping the streets clean; a window that is not repaired encourages vandals to break other windows. This theory is controversial, but while he served as mayor of New York City, Rudy Giuliani implemented a policy based on this theory. He instructed the police to strictly enforce laws against smaller crimes, such as spitting, panhandling and jaywalking, in order to send a signal that crime would no longer be tolerated; this is credited with dramatically reducing the city's crime rate. Malcolm Gladwell discusses Mayor Giuliani's application of the "broken window" theory in his book, *The Tipping Point*, and makes the case that sometimes it is the little things that make a big difference [13].

What does this have to do with computer security? Managers can influence their employees by paying attention to the little things, to the small details. It is difficult to enforce any kind of policy across an organization unless all of management demonstrates their commitment to the policy. If social security numbers are not to be listed on reports, management should not ask for a report that includes social security numbers. Managers should not leave their computers unlocked when unattended.

Managers should not click on email attachments from unknown sources. Managers should not store critical and confidential data on stored on laptops unless extreme measures are taken to protect it. Managers should not allow exceptions to the security policy. Top-level management should require all managers to know the security policy and to strictly adhere to it. If employees witness their managers paying attention to the minor details of the security policy, employees will pay attention to the little details, too. Eventually, paying attention to the little details will become normal behavior; in other words, security will become integral to the organization.

10. STEPS TO ACHIEVE BUY-IN

1. To convince top management that security needs to be made an organizational priority, CISOs can enlist the support of internal and external auditors, cite laws and regulations that punish non-compliance, emphasize the positive impact on employees and productivity, point out the impression it will make on the organization's customers, and may help improve or maintain the organization's reputation.

2. Obviously the security policy must be clear, must have management buy-in, must be enforceable, must easy to comply with and must be aligned with the organization's goals. Once created, the CISO and top management must work with mid-level managers to identify a subset of the security policies that most affect their employees on a regular basis and which management can monitor and enforce. What policies and how many will differ with each organization, but these are the policies that must be adopted by all employees.

3. Training should be offered, on a regular basis, to ensure that the employees know what behavior is expected. Communication of the policy can be reinforced by posters, screen savers, reminders on mugs or pens or t-shirts, and should be stated often, by all levels of management, to ensure that all employees are aware of the policies. The policies should be posted on the organizations' intranet, so all employees can review them and no one can claim to not be aware of any of the policies.

4. Adherence to the policies should be part of the annual review process for everyone, including management. In addition, all managers must monitor their employees, rewarding adherence to the policy and punishing violations. Initially compliance should be rewarded; eventually it should just be expected behavior. Initially, non-compliance should be noted and the employee reminded or reprimanded; eventually it should always be punished.

5. Enforcement of the policy throughout the organization must be consistent and there must be consequences. Violations must be addressed, resulting in a reprimand, fine, or some other penalty, depending on the nature of the violation and the frequency. Scorecards can be used to assess managers' compliance. This is a tool used by the Bank of America to evaluate their top 300 executives.

6. CISOs should work with managers to establish metrics so that proof of improvements can help to instill a sense of employee pride. Include measurements of how employees' rate the importance of a policy against their understanding of the policy and how easy or difficult it is to adhere to it.

7. To better inform management about information security issues, large organizations can work with local universities to sponsor classes on information security.[4] This can help to make security one of the organization's core values.

8. Both internal and external auditors should be involved in the process and help with annual evaluations.

9. New hires will tend to follow the informal standards of the organization and will learn these from their peers. Once policy compliance is second nature to employees, compliance by new employees will be relatively easy; however, risks change over time, which means policies will change over time. Managers must remain vigilant about enforcing the organization's security policies.

10. As well as having mechanisms to ensure that existing information security policies are adhered to by the organization, management needs to ensure that any changes to the policy due to new laws, regulations, and changing environments are accepted and complied with by the employees.

[4]For example, Baptist Hospital in Miami-Dade county sponsors numerous classes and programs for their nursing staff through Barry University. Classes offered on-site at one of the Baptist locations are offered at a substantially reduced rate.

11. CONCLUSIONS

The problem is that managers are not enforcing security policy because top-level management either is not complying with the organization's security policy or is lax in enforcing it. It is likely that the Chairperson and CEO assume it is the responsibility of the CIO or CISO. This is where CISOs can enlist the assistance of auditors to encourage involvement by the upper levels of management. They need to make the case that by delegating the responsibility for compliance to one department within the organization, upper management is treating security as an "add-on" and not allowing it to become integral to the organization's culture. There is a reason that upper-level managers are called leaders; they need to lead their employees by actively demonstrating their commitment and doing so consistently. They need to lead by example. If the organization's leaders get lax, so will the rest of management, and then so will everyone else.

Obviously a comprehensive and reasonable security policy is required. It must be clear and enforceable. It must be aligned with the organization's goals. All managers must buy in to the policy and be willing to consistently enforce it. All employees should be aware of the policy and have easy access to viewing it. However, the policies that are initially enforced throughout the organization should be limited initially to those that most affect employees in their daily lives and that are easily monitored and enforced.

Government regulations do not necessarily result in compliance. However, CISOs should work with auditors, both internal and external, to help encourage compliance. Auditing firms charge for their services, so upper management is more likely to listen to what they recommend. A commentator on an earlier version of this paper pointed out that we should recognize the role of regulators and that their effectiveness is also integral to the process; I agree, but space limitations do not allow me to do justice to this topic.

Education is an area that has been neglected. Most business schools, and for that matter, many college and university computer science programs, do not include any courses on privacy and information security. CISOs can help by offering on the job training programs and encouraging their *alma maters* to include such classes in the computer science and management programs. If an organization can locate a good on-line class on security for managers and require managers to enroll, eventually word will get out and more colleges and universities will offer such classes and include them in their programs. Another alternative for large organizations is to contact a local university and contract with them to offer such classes.

Compliance to security policy must be part of the evaluation process. Do not promote anyone who does not strictly adhere to the security policy. In the early phases, reward compliance. In the early phases, do not necessarily punish non-compliance, but quickly point out the violation and consequences. Eventually compliance should not be rewarded but non-compliance should be punished. Do not allow anyone to violate the policy without consequences, even if it is just a verbal reprimand. Consistency is key. No one on any level should ever be allowed to violate the security policy.

The small details matter. Top-level managers must enforce the rules within the higher levels of management and demonstrate their commitment by paying attention to the details. They must set the example.

CISOs should work with managers to establish metrics and use analytics for yearly trend analysis. Proof of improvements will help to instill a sense of employee pride, can be used to promote business, and can help lower the cost of risk insurance and possibly even auditing, which will encourage top-level management to continue their adherence to the policy.

If upper management changes their behavior and is consistent about following policy, employees will respect the policy and change their behavior, too. Once behavior changes, mindset changes, and slowly the organization's culture will become one that not only encourages employees to follow the security rules but one where compliance is automatic and behavior is almost unconscious because it is part of the organizational culture.

12. ACKNOWLEDGMENTS

I wish to thank Peter Matthews, the GTIP shepherd for this paper, who gave me insightful comments and valuable criticism which improved this paper. I also wish to thank the GTIP anonymous reviewers. Steven J. Greenwald helped with proofreading and offered some LaTeX tips.

13. REFERENCES

[1] 104th Congress. Health insurance portability and accountability act of 1996, 1996. Available at `http://aspe.hhs.gov/admnsimp/pl104191.htm`.

[2] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):41–46, December 1999.

[3] M. Aeschleman. Safety at caterpillar, February 2009. Presentation to MBA Students at Barry University.

[4] A. Anderson. Effective management of information security and privacy. *EDUCAUSE Quarterly*, 29(1):15–20, November 2006.

[5] R. Anderson. Why information security is hard - an economic perspective. In *Proceedings of the 17thd Annual Computer Security Applications Conference*, page 358, 0-7695-1405-7, 2001. IEEE Computer Society. Available at `http://www.acsac.org/2001/papers/110.pdf`.

[6] W. Baker, M. Goudie, A. Hutton, C. D. Hylender, J. Niemantsverdriet, C. Novak, D. Ostertag, C. Porter, M. Rosen, B. Sartin, P. Tippett, and Men and women of the United States Secret Service. 2010 data breach investigations report. Technical report, Verizon Business, 2009. `http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf`.

[7] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: managing security behaviour in organisations. In *NSPW '08: Proceedings of the 2008 workshop on New security paradigms*, pages 47–58, New York, NY, USA, 2008. ACM.

[8] J. Brazel. How do financial statement auditors and it auditors work together? *The CPA Journal*, 78(11):38–41, November 2008.

[9] L. Coles-Kemp and R. Overill. On the role of the facilitator in information security risk assessment. *Journal in Computer Virology*, 3(2):143–148, 2007.

[10] F. W. Conner. Implementing information security governance (ISG), a case study: Entrust. White paper, Entrust, July 2004.

[11] Department of Homeland Security National Cyber Security Division. Governance and management, Accessed on October 29, 2010. Available at `https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management.html`.

[12] J. R. Detert, R. G. Schroeder, and J. J. Mauriel. A framework for linking culture and improvement initiatives in

organizations. *Academy of Management Review Vol*, 25(4):850–863, 2000.

[13] M. Gladwell. *The Tipping Point*. Little, Brown and Company, 2000.

[14] P. Gordon. After seven years as CEO, Jim Owens retires on July 1. *McClatchy-Tribune Business News*, July 2010.

[15] M. Greenstein-Prosch, T. E. McKee, and R. Quick. A comparison of the information technology knowledge of united states and german auditors. *International Journal of Digital Accounting Research*, 8(14):45–76, 2008.

[16] C. Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 New Security Paradigms Workshop*, pages 133–144, September 2009.

[17] A. M. Johnson. Business and security executives views of information security investment drivers: Results from a delphi study. *Journal of Information Privacy & Security*, 5(1):3–27, 2009.

[18] A. C. Johnston and M. Warkentin. Information privacy compliance in the healthcare industry. *Information Management & Computer Security*, 16(1):5–19, 2008.

[19] A. Josang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara. Security usability principles for vulnerability analysis and risk assessment. In *Proceedings of the 23rd Annual Computer Security Applications Conference*, pages 269–278. IEEE Computer Society, December 2007.

[20] B. Khoo, P. Harris, and S. Hartman. Information security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management and Information Systems*, 14(3):49–55, Third Quarter 2010.

[21] K. J. Knapp, T. E. Marshall, R. K. Ranier, and F. N. Ford. Information security: Management's effect on culture and policy. *Information Management & Computer Security*, 14(1):24–36, 2006.

[22] S. S. Nadler and J. F. Kros. An introduction to Sarbanes-Oxley and its impact on supply chain management. *Journal of Business Logistics*, January 2008. Available at `http://www.allbusiness.com/legal/antitrust-trade-law-sarbanes-oxley-act/11577851-1.html`.

[23] L. Paine. Managing for organizational integrity. *Harvard Business Review*, pages 106–117, March–April 1994.

[24] S. P. Robbins and T. A. Judge. *Essentials of Organizational Behavior*. Prentice Hall, New Jersey, USA, 2009.

[25] J. Shook. How to change a culture: Lessons from NUMMI. *MIT Sloan Management Review*, 51(2), January 2010.

[26] G. Smith. Are you ready for the audit challenges of 2010? *The Journal of Corporate Accounting & Finance*, 21(4):65–68, May/June 2010.

[27] J. Thornbury. Creating a living culture: the challenges for business leaders. *Corporate Governance*, 3(2):68–79, 2003.

[28] E. Van den Steen. On the origin and evolution of corporate culture, April 2003. Preliminary and Incomplete Monograph.

[29] D. B. Yoffie and A. E. . Pearson. *The Transformation of IBM*. Harvard Business School, September 1991.