Communications of the IIMA

Volume 11 | Issue 3 Article 4

2011

Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security

Celia Paulsen
California State University, San Bernardino

Tony Coulson
California State University, San Bernardino

Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security

Celia Paulsen, Graduate Student
California State University, San Bernardino, USA
celia.paulsen@gmail.com

Tony Coulson
California State University, San Bernardino, USA
tcoulson@csusb.edu

ABSTRACT

Employees, intentionally or not, cause a large percentage of security incidents. For an organization to be secure there must be a culture of information security, meaning that employees make good security-related decisions. Business intelligence (BI) systems, with their ability to promote change through goal-setting and accountability, could help create a culture of information security, if implemented appropriately. This paper provides an overview of information security culture and business intelligence, and explains what will be needed if BI is to be used to help organizations develop a security-aware culture.

INTRODUCTION

Organizational information systems are increasingly coming under attack from viruses, hackers, denial of service attacks, and other threats (Bodin, Gordon, & Loeb, 2005; Jourdan, 2010; Mitnick & Simon, 2002). According to the Ponemon Institute, in 2010, the average cost for a data breach in the US was $6.75 million. The security breach in Sony's online PlayStation Network and Qriocity music service is expected to cost Sony $10 million in lost revenue per week, and at least $70 million in lawsuits (Pham, 2011). The leading cause for data breaches is negligence (41%) with malicious or criminal attacks second (31%) (Ponemon Institute, 2010).

While traditionally, information security has been the domain of the IT department, more and more researchers are discovering that, for an organization to be secure, all employees must be fully engaged. Business intelligence (BI) systems have been used to promote other changes in organizations, capitalizing on BI systems' ability to monitor activity, set goals for users, and provide accountability. Because of this, BI systems should also be able to help organizations create a culture of information security. However, for such an approach could be effective, an understanding of both the organizational psychology surrounding information security and how business intelligence tools are used is needed.

INFORMATION SECURITY

Information security traditionally means protecting the integrity, availability, and confidentiality of data and systems, which may be vital to maintaining an organization's operations (da Veiga, Martins, & Eloff, 2007; Tipton & Krause, 2009). Because of the focus on information systems, information security has traditionally been treated as a technology issue and the domain of the IT department (Anderson & Moore, 2009; Salazar, 2006). According to Professor Basie von Solms, before the 1980s, information security was viewed as something that could be addressed through technology alone (von Solms, 2000).

Then, increased media attention and regulations made the information security field more visible. In the last several years, several regulations, standards and frameworks have developed. Multiple documents, *ISO/IEC 27002:2005, NIST Special Publication 800-53*, and the *Health Insurance Portability and Accountability Act (HIPAA)* Security Rule, for example, define controls that are needed to protect certain information systems (United States Department of Commerce, 2010). Respondents to a 2010 survey indicated that regulatory compliance has had a "positive effect on their organization's security programs" (Computer Security Institute, 2011, p. 7), and as of 2010, executives reportedly are increasingly more interested in the state of their organizations' information security (Hoehl, 2010).

However, even in 2006, many organizations in developed countries still had not taken this first step towards a more secure organization and lacked basic, foundational information security policies or programs (Dimopoulos, Furnell, Jennex, & Kritharas, 2004; Gupta & Hammond, 2005; ISBS, 2006). In 2008, Martin wrote that many organizations are "willing to commit resources to technology purchases, but . . . much less willing to dedicate any resources at all to the less technical aspects of information security" (p. 6). In fact, many organizations would likely prefer to have no dealings with information security. West argued that "the vast majority [of users] would be content to use computers to enrich their lives while taking for granted a perfectly secure and reliable infrastructure that makes it all possible" (West, 2008, p. 40).

This concept can be seen in software and hardware systems designed to improve information security. In 2008, some of the most common technologies used were anti-virus software, anti-spyware, and firewalls (Richardson, 2008). These tools often rely heavily on alerts, meaning that, when a measurement goes out of a designated range, or when a specific event happens, an alarm is triggered and the user notified. Because these technologies are typically an add-on to existing software/hardware, tend to interrupt users in their activities, and frequently expect users to make an educated decision, information security becomes a nuisance and users may become frustrated, begin to ignore the alerts, or even turn off the protection (West, 2008; Zurko & Simon, 1996). These traditional methods are thus ineffective at ensuring the security of an organization's information and systems.

CURRENT TRENDS

One significant development in information security management is the understanding that it requires a more holistic approach rather than being confined to the IT department. Mitnick & Simon (2002) proposed that anyone who thinks that technical and physical security products

alone offer real protection is settling for an illusion. Many researchers now agree that an information security program should include people, processes, and technology (Connolly, 2000; da Veiga et al., 2007; Ghonaimy, El-Hadidi, & Asian, 2002; von Solms, 2000). Tudor (2000) proposed a framework of five key principles for implementing an organization-wide information security program and the PROTECT framework recommends an approach to information security that includes Policies, Risks, Objectives, Technology, Execute, Compliance and Team (Eloff & Eloff, 2005). With this shift in thinking, two major approaches to a holistic information security program have emerged: a business- and a people-centered approach.

A Business Approach

As executives become more interested in information security, they want to know how it affects the bottom line and design an information security program accordingly. It has been said that the goal of information security is to protect the business (Cattaneo, 2009; Colwill, Todd, Fielder, & Natanson, 2007; Jones, 2007; Moore, Ellison, & Linger, 2001) and an organization's budget has an influence on the level of security an organization can maintain ((Dojkovski, Lichtenstein, & Warren, 2007; Martins & Eloff, 2002a). As a result, some have proposed using a risk-analysis process that uses estimated cost of a breach and associated mitigating controls to help develop a cost-effective security program (Dojkovski et al., 2007). Unfortunately, in these and other business approaches, information security is still a supplemental and unwelcomed expense that many would likely choose to ignore, if possible.

A People-Centered Approach

People are often seen as the enemies of information security, with good reason. In 2004, 59% of incidents were caused by insiders (Gordon, Loeb, Lucyshyn, & Richardson, 2004). In 2009, Verizon found that insiders were still behind most data breaches, whether intentionally, or through ignorance, thoughtlessness, or impatience (da Veiga & Eloff, 2010; Verizon Business RISK Team, 2009). Martins and Eloff argued, "Human interaction with information resources is often the weakest link in protecting information assets" (2002a, p. 1). West (2008) suggested that users are simply unable to pay full attention to security procedures and as a result, don't always consider the consequences of their actions. A recent survey of database administrators and managers revealed that, due to lax practices and oversight, sensitive data is still being left vulnerable to tampering and theft (McKendrick, 2011).

However, while many information security professionals view the user as the threat, other research suggests that insiders can become a strength (Mitnick & Simon, 2002; Rotvold, 2008a). Schlienger and Teufel proposed a "paradigm shift" from the common thought of "my user is my enemy" to "my user is my security asset" (2002, p. 191). Researchers have agreed that well-educated employees not only minimize the insider threat, but can act as sentinels, providing an additional layer of security (Albrechtsen, 2007; de Veiga & Eloff, 2010; Kraemer & Carayon, 2007; Stanton, Stam, Mastrangelo, & Jolton, 2005).

Unfortunately, while several researchers have promoted awareness (Kruger & Kearney, 2006; Puhakainen, 2006), managerial policies (Siponen, Pahnila, & Mahmood, 2005; Vroom & Solms, 2004), training and other methods to help users become better educated (da Veiga & Eloff, 2010; Thomson, 1998; Mitnick & Simon, 2002), many organizations view these programs as

inefficient and not worth the cost. In 2008, less than half of organizations provided employees with ongoing security awareness training (Martin, 2008). John Walker, a member of the Information Systems Audit and Control Association (ISACA) Security Advisory Group, simply stated, "No matter what anyone says, it's a really hard job and a lot of people are just not interested," (Everett, 2010, p. 6).

CULTURE

It is clear that a solution is needed whereby information security is no longer seen as a nuisance to be ignored or an add-on to be marginalized, but instead as a core component of the people, processes, and technologies of an organization. A culture of information security is needed (Andress, 2000; Connolly, 2000; da Veiga et al., 2007; Everett, 2010; Furnell, 2007; Ghonaimy et al., 2002; Stewart, n.d.). Culture is defined most simply as "the way things are done here" (da Veiga & Eloff, 2010; Lundy & Cowling, 1996). It is the personality of an organization (Robbins & Judge, 2008). In information security, culture is defined as the behavior in an organization that contributes to the protection of data, information and knowledge (Dhillon, 1997) and includes the perceptions, attitudes, assumptions, and beliefs of the employees regarding information security (da Veiga & Eloff, 2010; da Veiga et al., 2007; Martins & Eloff, 2002b).

Researchers have tried to identify what elements compose an information security culture–where information security is a core part of an organization's "personality." The information security Forum and the OECD identified several factors, including awareness and responsiveness (da Veiga & Eloff, 2010; Information Security Forum, 2000; Organisation for Economic Co-operation and Development, 2002). Others have stressed the importance of values-based behavior (Dhillon & Backhouse, 2001; Dojkovski et al., 2007; Martins & Eloff, 2002b; Schlienger & Teufel, 2003; van Niekerk, 2005). Von Solms discussed several stages of information security awareness maturity (2000), and Ruighaver, Maynard and Chang (2006) related the eight dimensions of culture defined by Detert, Schroeder and Mauriel (2000) to information security.

Van Niekerk proposed that the fundamentals of an information security culture could be condensed into two dimensions: knowledge and behavior (2005). Van Niekerk and von Solms (2003) further stated that it is impossible to secure an organization's information resources without first instilling in employees both the understanding of its importance and the desired attitude, and Nosworthy (2000) stated that people must be educated to *want* to be more secure so that they seek the knowledge and apply correct practices.

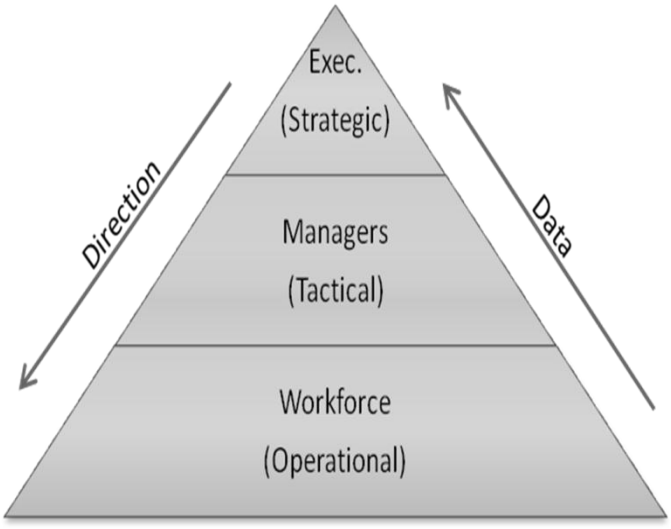
Thus, in order to create a truly holistic information security program wherein users actively support security instead of hindering it, organizations must create a culture wherein users, at all levels of the organization, understand security threats and guidelines, actively practice good security habits, make security-minded decisions, and view information security as an integral part of their job instead of as just an annoyance.

USING BUSINESS INTELLIGENCE (BI) FOR INFORMATION SECURITY

Business intelligence systems are, at their core, decision-making tools. Using Negash's definition, "BI systems combine data gathering, data storage, and knowledge management with analytical tools to present complex internal and competitive information to planners and decision makers" (2004, p. 177). Using dashboards, scorecards, charts, and other displays, BI tools improve the transparency and visibility of data.

Because of these abilities, BI is frequently used for two purposes: (1) to monitor and improve processes and (2) to drive change (Elbashir & Williams, 2007; Golfarelli, Rizzi, & Cella, 2004; Liebowitz, 2006; Willcocks & Smith, 1995; Williams & Williams, 2004). In addition, BI can also be used to monitor information security and to create an information security culture in an organization.

Figure 1: Organizational information flow diagram.



Metrics are the building blocks for business intelligence and the key to building an information security culture using BI. Gonzalez explains that metrics are "a direct numerical measure that represents a piece of business data in the relationship of one or more dimensions. An example would be: 'gross sales by week.' In this case, the measure would be dollars (gross sales) and the dimension would be time (week)" (2005, p. 4). When tied to a target or a goal, a metric is called a Key Performance Indicator (Gonzales, 2005; KPI, n.d.). Metrics feed dashboards, scorecards, charts, alerts, and other data visualizations readily accessible and understandable to the various users. When asked what security solutions they want, security managers and executives responded that they want tools that would improve their visibility, such as log and event management, data visualization, and dashboards (Richardson, 2008). BI tools provide exactly these things.

Information Levels

Different users of business intelligence tools use different information security metrics. Figure 1 shows three levels of BI Users: Strategic, Tactical, and Operational. BI at the strategic level is used to support long-term corporate goals and objectives (White, 2007). At the tactical level, BI translates long-term strategic decisions into operational metrics. Targets for each metric are set, performance monitored to provide timely feedback, and corrective actions initiated (Rose, n.d.). Experts have proposed that information security cultural development is based on management initiatives like policies, awareness, and training (Dojkovski et al., 2007; Knapp, Marshall, Rainer, & Ford, 2006; van Niekerk & von Solms, 2003). At these levels, BI can be used to measure compliance with information security policies and promote awareness and training in a visually appealing and easily understandable fashion.

The operational level uses BI to measure and monitor performance. This level utilizes near real time, data-centric information to support daily business needs (White, 2007). Business intelligence software has historically been used to support information security at this level, providing "managers with all the information [they need] to properly manage information security moment by moment" (von Solms, 2000, p. 15). Some research has indicated that a security-aware culture develops through employee interaction with security controls such as access cards or passwords (Martins, 2002). At this level, BI can provide another such control by engaging user interaction with information security metrics or even by limiting a general user's ability to continue working without first addressing a security concern, such as changing a password or downloading an update.

Goals

One of the most useful aspects of business intelligence software for supporting an information security program is that it can help align operational, tactical, and strategic level decision-making through goal-setting (Dave, 2009; Locke & Latham, 1990; Smith, 2002). Goals serve as a benchmark for determining success and providing feedback (Koskosas & Paul, 2004; Latham & Locke, 1991) and as such, can be used to promote change in an organization's culture. Group-oriented goals help to unify an organization through mobilizing and directing employee efforts toward a common task. They direct attention and effort, prolong effort over time, and motivate people to develop appropriate solutions (Bradford & Cohen, 1984; Koskosas & Paul, 2004; Latham & Locke, 1991; Locke & Latham, 1990).

BI tools have been shown to be extremely effective in helping organizations track and meet their goals (Betts, 2011; Felix, 2009; Frye, 2010; Harkleroad, 1992; McClure, 2008; Smith & Marinakis, 1997). BI metrics "[increase] accountability and transparency, and [put] everyone on the same page when it comes to goal-related performance" (Klipfolio, 2010, p. 4). Depending on how they are chosen, either through a process-based or top-down approach, metrics can support different information security needs (Heesen, 2011; Kaplan & Norton, 1996). Most organizations would likely use a combination of the two approaches.

The Six Sigma strategy is an example of a process-based approach. In this technique, metrics come from an analysis of the processes of an organization. Processes are analyzed and potential

vulnerabilities or weaknesses identified. Metrics are designed to monitor and improve those weaknesses (Betz, 2007; Breyfogle, Cupello, & Meadows, 2001). The metrics developed from this method would most likely be seen in the operational level of an organization, supporting real-time decision making of time-sensitive problems.

With a top-down approach, metrics come from the objectives and strategy of the organization, such as in the balanced scorecard method. The overall vision of the organization is translated into long-term objectives, which then feed strategies, which turn in to short-term goals (Heesen, 2011; Kaplan & Norton, 1996). This method helps BI tools "[transform] strategic planning from an academic exercise into the nerve center of an enterprise" (Balanced Scorecard Institute, 2010, p. 3). Likewise, it can turn information security from an afterthought into a core component of the organization by ingraining it into the objectives of executives and managers and highlighting its importance through continuous monitoring and evaluation.

Motivation

It has been said that having a security policy without enforcing that policy is like having laws but no police (West, 2008). To be most useful in shaping the culture of an organization, information security metrics must have some kind of motivation attached to them, such as performance reviews, bonuses, and rewards. In information security, the top motivators seem to be self-efficacy, the responsibility or the expectations of superiors, perceived susceptibility, perceived benefits, and the importance placed on information security (Herath & Rao, 2009; Ng, Kankanhalli, & Xu, 2009; Rotvold, 2008a).

Extrinsic motivators such as rewards and punishments, while less effective than intrinsic motivators, are easier to control and have been found to have a positive impact on information security behavior (Dojkovski et al., 2007; Herath & Rao, 2009; Ng et al., 2009; Rotvold, 2008a). Cause and effect are best learned when the effect immediately follows the act, but in information security, there is usually no immediate reward or punishment for good or poor security behaviors (West, 2008). Thus, rewards and punishments must be created by an organization. While punishment systems are much more widely used than rewards in the information security world, neither is commonplace. Only 48.8 percent of organizations in a 2008 survey stated that there were penalties for security breaches in their organization; 13.8 percent used compliance as a factor in employee evaluation, and 2.3 percent provided incentives and rewards for complying with information security policies (Rotvold, 2008b).

Password strength, time spent on suspicious websites, reporting of suspicious activity, or the number of viruses detected on a machine are all possible measures that employees could be quickly rewarded or punished for. Some websites have an indicator next to where one creates a password indicating the strength of that password. If the password is not strong enough, the website may reject that choice and indicate how to create a stronger password. In this way, the system both provides punishment (rejection of choice), and increases a user's knowledge of information security (providing a visual indicator of how strong their password is and showing the user how to create a stronger password).

In a long-term scenario, if a user makes several poor choices, they can be labeled a threat and have increased controls placed on them. This kind of system both provides rewards and punishments: those with good security behavior receive more freedoms, while those with poor security receive less. Freedoms may include being able to download things from the Internet, use a BlackBerry to access work email, or bring their own device to work. With a BI system for information security, users could be monitored, their behavior measured, and either rewarded for good practices like reaching organizational information security goals, or be restricted for poor security practices. Thus, using motivators tied to KPIs and other goals, BI tools can help an organization shape employees' information security-related perceptions and behaviors, improving the overall security posture of the organization.

SURVEY

Purpose and Methods

If business intelligence is to be used to shape culture, it is necessary to determine how BI is currently used in order to determine what is needed. While several case studies have been done, there is little research on how business intelligence is used generally, across all management and discipline levels. Thomson (1998) listed three categories of users that need to be educated in information security awareness: End user, IT personnel, and top management. Additionally, experts have repeatedly stressed the necessity of top management buy-in for security and BI projects to succeed (Knapp et al., 2006; Schlienger & Teufel, 2003). Thus, a pilot survey was sent to business owners, executives, managers and IT personnel from all industries and organization sizes. Because BI is primarily a decision-support tool, the survey asked participants how often they receive certain metrics, and how often they would use those metrics to make decisions. The survey also inquired about how much choice users had in choosing and developing the metrics they receive, how they receive the metrics, and where the metrics come from. A sample of the questions follows:

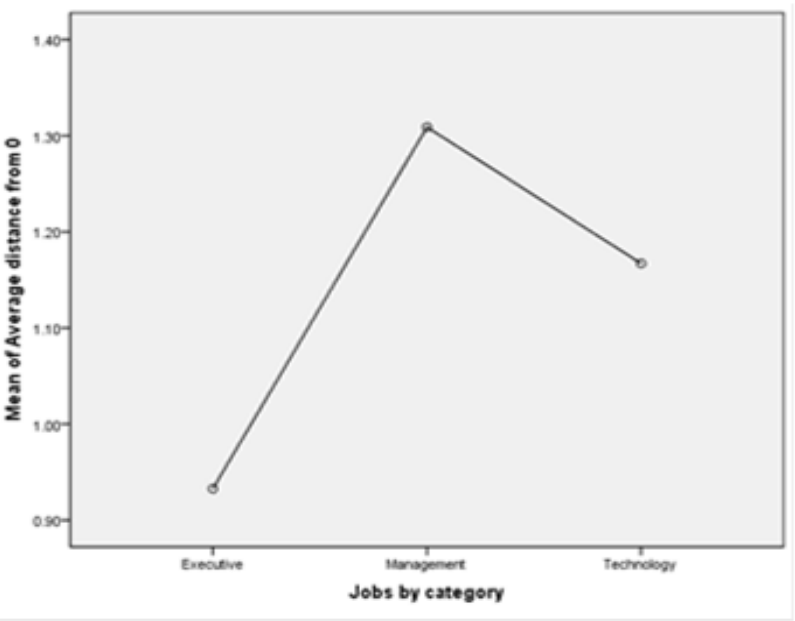
- On average, how often do you receive/see metrics related to (multiple times daily, daily, weekly, monthly, quarterly, yearly, rarely, never): Projects, employees, down-time, financials, budgets, policies, logistics, customer satisfaction, incidents, etc.
- How often do you (or would you if given the option) use metrics related to the following to make decisions (multiple times daily, daily, weekly, monthly, quarterly, yearly, rarely, never): Projects, employees, down-time, financials, budgets, policies, logistics, customer satisfaction, incidents, etc.
- You were given a choice as to which metrics you see (strongly agree, agree, neither agree nor disagree, disagree, strongly disagree, N/A)

Two hypotheses directed the study:

1. Managers will display the most disparity between metrics they need to make decisions and the metrics they receive because most metrics are formed either for strategic direction or operations management and mid-level managers may require a unique mix of the two (Pinsonneault & Kraemer, 1993; Williams & Sawyer, 2002).

2. Those who have more input into the development of the metrics they receive will have less disparity between metrics they need to make decisions and the metrics they receive. Experts have suggested that to be successful, BI development requires user input (Laudon & Laudon, 2002; West, 2008).

Figure 1: Average Disparity by Job Category



The survey was made available online and received 68 responses, representing about a 5 percent response rate of those solicited. After outliers and incomplete responses, 46 useable responses remained for analysis. Most respondents (53 percent) worked in an IT-related position, 28 percent in general management, and 19 percent were at the executive or owner levels. Respondents represented thirteen different industries, including construction, healthcare, technology, financial, education, and government. Forty-seven percent were from organizations with less than 100 people, 31.3 percent from organizations between 100 and 2,500 people, and 21.5 percent with 2,500 or more people. As this was a pilot survey, the number and spread of respondents were deemed satisfactory.

RESULTS

The survey results suggest that BI users generally receive too little information. **Error! Reference source not found.** shows that managers indeed had the most disparity between metrics they received and metrics they needed to make decisions, supporting the hypothesis. They received both too much information they didn't need, and not enough of the information they did need. This information was found by subtracting how often users see metrics by how often they would use those metrics if they were available. Positive numbers indicated respondent received too much information they didn't need, and negative numbers indicated they weren't given the information they needed when they needed it.

Most users had some combination of too much and too little information, but on average, users had 37 percent more negative results (too little information) than positive (too much information), for an average total disparity of 1.1821 points. Managers had the most total

disparity at 1.3088 points with about 100 percent more of too little information. Executives had a total disparity of .9328 with about 52 percent more of too little information. Technicians had a total disparity of 1.1672 with 150 percent more of too little information. The metrics that had the most disparity overall were those related to budgets, customer satisfaction, utilization, forecasts, down-time, and time spent on activities. Table 1 shows a break down of disparity in metrics by job category.

While the survey did not measure the impact of the disparity on users, the results would suggest that middle managers' information needs are not currently being met. This is critical if BI is to be used to create an information security culture, as it has been established that involvement of first-line supervisors is a critical factor (Herath & Rao, 2009; Ng et al., 2009; Rotvold, 2008a).

Table 1: Disparity of metrics.

Metric **Jobs by Category**	**Forecasts**	**Customer Satisfaction**	**Down-time**	**Time Spent on Activities**	**Budgets**	**Utilization**
Executive	-.2857	-.4286	**-1.1429**	**-.8571**	**-.8571**	.1429
Management	**-1.0625**	**-1.3750**	**-.8125**	**-1.0000**	**-.9375**	-.1875
Technology	**-1.5789**	**-1.2632**	-.5789	-.3684	-.3158	**-1.1053**
Total	**-1.1667**	**-1.1667**	-.7619	-.6905	-.6429	-.5476

Metric **Jobs by category**	**Usage**	**Incidents**	**Projects**	**Policies**	**Results of Internal Audits**	**Help Desk/ Support**
Executive	-.1429	**-1.1429**	**-1.0000**	-.2857	.2857	.1429
Management	.2500	.2500	-.1250	-.1250	-.6250	-.3125
Technology	**-.9474**	-.5263	-.2632	-.5263	-.3158	-.3158
Total	-.3571	-.3333	-.3333	-.3333	-.3333	-.2381

Metric **Jobs by Category**	**Software**	**Logistics**	**Employees**	**Financials**	**Historical Data**
Executive	**1.2857**	.5714	.5714	.0000	-.1429
Management	.0625	**-.8125**	**-.8750**	.1250	.0625
Technology	-.0526	.0526	.1053	-.4737	-.2105
Total	.2143	-.1905	-.1905	-.1667	-.0952

In addition, there was no statistical evidence suggesting that users with more input in the development of metrics have less disparity between metrics they need and metrics they see, as shown in Table 1 and Figure 2. This suggests that user involvement has little value when designing BI applications. This is contrary to the hypothesis, which took into account popular belief that users with more development choice in the metrics they see would choose those metrics that they would need.

However, as can be seen in Table 2, there is also some evidence to suggest that the same people who receive a significant amount of information they don't need also do not receive enough of the information they do need, regardless of the amount of input they have in designing the metrics. These results suggest there may be a lack of understanding at the user level about metrics or the BI Tools being used. Unfortunately, information security alone is notoriously difficult to understand (Dojkovski et al., 2007; West, 2008), and many studies have shown that people don't have a strong understanding of the importance of information security controls (Dimopoulos et al., 2004; Gupta & Hammond 2005; U. K. Department of Trade and Industry, 2006). If people do not have a strong understanding of the BI metrics they use, using BI to create a culture of information security would be futile.

Table 2: Pearson correlation for development choice and disparity of metrics.

		Too Much Info	**Too Little Info**	**Distance from 0**	**Development Choice**
Too Much Info	Pearson Correlation	1	.440	.091	-.010
	Sig. (2-tailed)		.002	.546	.946
Too Little Info	Pearson Correlation	.440	1	-.854	-.164
	Sig. (2-tailed)	.002		.000	.280
Distance from 0	Pearson Correlation	.091	-.854	1	.175
	Sig. (2-tailed)	.546	.000		.249
Dev. Choice	Pearson Correlation	-.010	-.164	.175	1
	Sig. (2-tailed)	.946	.280	.249	

Correlation is significant at the 0.01 level (2-tailed).

Figure 2: Amount of development choice vs. disparity of metrics.

CONCLUSION

Creating a culture requires setting goals and motivating employees towards those goals. BI has already proven its ability to promote change in an organization by focusing employees attention on metrics designed to measure some strategic goal. By ensuring those goals are tied to

motivational factors, either positive or negative, business intelligence tools could help organizations develop a security-aware culture.

However, in order for BI to successfully promote a culture of information security, developers must make sure to include general managers. Research has shown that a successful security-aware culture depends on managers who can balance risk and rewards based on adequate information (Tipton & Krause, 2009). As supervisor actions are a strong motivator for information security, it is important that developers give middle managers the same consideration that executives and IT personnel receive.

Developers must also address the lack of understanding that surrounds BI. A security-aware culture requires both awareness or knowledge and behavior (van Niekerk, 2005). For a culture to develop, users must understand information security concepts such as strong passwords and why they're important, and they must understand the BI tools they use. Research has shown that people often fail to recognize security risks or the information provided to cue them (Dhamija, Tygar, & Hearst, 2006; Downs, Holbrook, & Cranor, 2007; West, 2008). While it has been suggested that user involvement in the development of metrics should reduce this problem, the pilot survey suggests otherwise. It is likely that users lack understanding of both the metrics they use and the BI tools they use. Developers must understand how and why users make decisions regarding security and how they use BI tools in order to develop appropriate and understandable BI metrics and systems that can be used to create a culture of information security.

REFERENCES

Albrechtsen, E. (2007). A qualitative study of users' views on information security. *Computers & Security, 26*(4), 276-289. doe: HYPERLINK "http://dx.doi.org/10.1016/j.cose.2006.11.004" 10.1016/j.cose.2006.11.004

Anderson, R., & Moore, T. (2009, July 13). Information security: Where computer science, economics, and psychology meet. *Philosophical Transactions of The Royal Society: A, 367*(1898), 2717-2727. doi: 10.1098/rsta.2009.0027

Andress, M. (2000, November 13). Manage people to protect data. *InfoWorld, 22*(46).

Balanced Scorecard Institute. (2010). *Balanced scorecard basics.* Retrieved from http://www.balancedscorecard.org/BSCResources/AbouttheBalancedScorecard/tabid/55/Default.aspx

Betts, M. (2011, January 24). BI tools can help evaluate green programs. *Computerworld*, 6. Retrieved from http://computerworld.com.my/resource/data-center/bi-tools-can-help-evaluate-green-programs/

Betz, C. T. (2007). *Architecture and patterns for IT service management, resource planning, and governance: Making shoes for the cobbler's children.* San Francisco, CA: Elsevier.

Bodin, L., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy. *Communications of the ACM, 48*(2), 78-83.

Bradford, D. L., & Cohen, A. R. (1984). *Managing for excellence: The guide to developing high performance in contemporary organizations.* New York, NY: Wiley.

Breyfogle, F. W., III, Cupello, J. M., & Meadows, B. (2001). *Managing six sigma: A practical guide to understanding, assessing, and implementing the strategy that yields bottom-line success.* New York, NY: John Wiley & Sons, Inc.

Cattaneo, M. (2009, November 1). *Information Security Management Objectives.* Retrieved March 5, 2011, from http://www.youtube.com/watch?v=yFDzmtqtvXU

Colwill, C. J., Todd, M. C., Fielder, G. P., & Natanson, C. (2007). Information assurance. *BT Technology Journal, 19*(3), 107-114. doi: 10.1023/A:1011998517801

Computer Security Institute. (2011). CSI computer crime and security survey. Retrieved July 2010 from http://gocsi.com/survey

Connolly, P. (2000, July 10). Security starts from within. *InfoWorld, 22*(28), 39-40.

da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computer & Security, 29*(2), 196-207. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404809000923

da Veiga, A., Martins, N., & Eloff, J. H. (2007). Information security culture: Validation of an assessment instrument. *Southern African Business Review, 11*(1), 147-166.

Dave, P. (2009, July 27). *Business intelligence: Aligning business metrics.* Retrieved from http://dotnetslackers.com/articles/sql/Business-Intelligence-Aligning-Business-Metrics.aspx

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A framework for linking culture and improvement initiatives in organizations. *The Academy of Management Review, 25*(4), 850-863.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, & G. Olson (Eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581-590). New york: ACM. doi: 10.1145/1124772.1124861

Dhillon, G. (1997). *Managing information system security.* London: UK: MacMillan.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153. doi:

HYPERLINK "http://dx.doi.org/10.1046/j.1365-2575.2001.00099.x" 10.1046/j.1365-2575.2001.00099.x

Dimopoulos, V., Furnell, S., Jennex, M., & Kritharas, I. (2004). *Approaches to IT security in small and medium enterprises* (pp. 73-82). In *Proceedings of the 2nd Australian Information Security Management Conference 2004.* Perth, Australia.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. In *Proceedings of the 15th European Conference on Information Systems* (pp. 1560-1571). St. Gallen, Switzerland. Retrieved from http://is2.lse.ac.uk/asp/aspecis/20070041.pdf

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit* (pp. 37-44). New York, NY: ACM. doi: 10.1145/1299015.1299019

Elbashir, M., & Williams, S. (2007). BI impact: The assimilation of business intelligence into core business processes. *Business Intelligence Journal, 12*(4), 45-54.

Eloff, J., & Eloff, M. (2005). Integrated information security architecture. *Computer Fraud and Security, 11*, 10-16.

Everett, C. (2010, November). Embedding security: When technology is no longer enough. *Computer Fraud & Security, 2010*(11), 5-7. doi: HYPERLINK "http://dx.doi.org/10.1016/S1361-3723(10)70143-3" \t "doilink" 10.1016/S1361-3723(10)70143-3

Felix, K. (2009, July/August). Take action with business intelligence. *EContent, 32*(6), 22-26.

Frye, G. W. (2010, February). Using business intelligence to build optimal decision support. *Benefits Compensation Digest, 47*(2), 1-21.

Furnell, S. (2007). IFIP workshop: Information security culture. *Computers &Security, 26*(1), 35.

Ghonaimy, M., El-Hadidi, M. T., & Asian, H. K. (Eds.). (2002). *Security in the information society:Visions and perspectives: IFIP TC11 17th international conference on information security (SEC2002)*, Cario, Egypt.

Golfarelli, M., Rizzi, S., & Cella, I. (2004). Beyond data warehousing: What's next in business intelligence? In *Proceedings 7th ACM International Workshop on Data Warehousing and OLAP*. New York, NY: ACM. doi: 10.1145/1031763.1031765

Gonzalez, T. (2005). *Dashboard design: Key performance indicators & metrics.* Retrieved from http://www.brightpointinc.com/Articles.asp?File=Dashboard%20Design%20Metrics%20and%20KPIs.htm

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). *2004 CSI/FBI computer crime and security survey.* Retrieved March 2, 2011, from https://gocsi.com/sites/default/files/uploads/FBI2004.pdf

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security, 13*(4), 297-310. doi: 10.1108/09685220510614425

Harkleroad, D. H. (1992, October). Competitive intelligence: A new benchmarking tool. *Management Review, 81*, 26-29.

Heesen, B. (2011). *Effective strategy execution: Improving performance with business intelligence* (Vol. 1). New York, NY: Springer.

Herath, T., & Rao, H. R. (2009, May). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi: 10.1016/j.dss.2009.02.005

Hoehl, M. (2010, December 24). *Creating a monthly information security scorecard for CIO and CFO* [White paper]. Retrieved March 23, 2011, from http://www.sans.org/reading_room/whitepapers/leadership/creating-monthly-information-security-scorecard-cio-cfo_33588

Information Security Forum. (2000). *Information security culture: A preliminary investigation.*

Jones, R. (2007). *Survival of the fittest: Disaster recovery design for the data center.* Midvale, UT: Burton Group.

Jourdan, S. Z. (2010). *An investigation of organizational information security risk analysis.* Auburn University (Doctoral dissertation). Auburn University, Auburn, Alabama.

Kaplan, R. S., & Norton, D. P. (1996). *The balanced scorecard: Translating strategy into action.* Boston, MA: Harvard Business School Press.

Klipfolio. (2010). *Operational BI dashboards: Metrics beyond the boardroom* [White paper]. Retrieved from http://www.klipfolio.com/docs/Operational_BI-A_Klipfolio_White_Paper.pdf

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36. doi: 10.1108/09685220610648355

Koskosas, I. V., & Paul, R. J. (2004). Information security management in the context of goal-setting. *Risk Management: An International Journal, 6*(4), 19-29.

KPI Library. (n.d.). Retrieved May 12, 2011, from http://kpilibrary.com/

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38*(2), 143-154.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296. doi: HYPERLINK "http://dx.doi.org/10.1016/j.cose.2006.02.008" 10.1016/j.cose.2006.02.008

Latham, G. P., & Locke, E. A. (1991). Self-regulation through goal setting. *Organizational Behavior and Human Decision Processes, 50*(2), 212-247.

Laudon, K., & Laudon, J. P. (2002). *Management information systems: Managing the digital firm* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Liebowitz, J. (Ed.). (2006). *Strategic intelligence:Bbusiness intelligence, competitive intelligence, and knowledge management* . Boca Raton, FL: Auerbach Publications.

Locke, E. A., & Latham, G. P. (1990). *A theory of goal-setting and task performance.* Englewood Cliffs, NJ: Prentice-Hall.

Lundy, O., & Cowling, A. (1996). *Strategic human resource management.* London, UK: Routledge.

Martin, L. (2008, August 3). *Is security too hard?* Retrieved March 5, 2011, from http://superconductor.voltage.com/2008/08/hard-and-soft-s.html

Martins, A. (2002). *Information security culture* (Master's thesis). Rand Afrikaans University, Johannesburg, South Africa.

Martins, A., & Eloff, J. (2002a). Assessing information security culture. In *Proceedings of the 2nd Information Security for South Africa Conference (ISSA 2002).* Gauteng, South Africa/

Martins, A., & Eloff, J. H. P. (2002b). Information security culture. In A. Ghonaimy, M. T. El-Hadidi, H. K. Aslan (Eds.), *Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives.* Cairo, Egypt.

McClure, A. (2008, May). Driving the data: Applying business intelligence is helping communty college leaders reach their goals. *University Business, 11*(5), 42-43. Retrieved from http://findarticles.com/p/articles/mi_m0LSH/is_5_11/ai_n25450975/

McKendrick, J. (2011, March). Culture of complacency--and misunderstanding hampers--information security. *Database Trends & Applications, 25*(1).

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security* (1st ed.). Indianapolis, IN: Wiley Publishing.

Moore, A. P., Ellison, R. J., & Linger, R. C. (2001). *Attack modeling for information security and survivability.* Carnegie Mellon University, Software Engineering Institute.

Negash, S. (2004). Business intelligence. *Communications of the Association for Information Systems, 13,* 177-195. Retrieved from http://site.xavier.edu/sena/info600/business intelligence.pdf

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825. doi: 10.1016/j.dss.2008.11.010

Nosworthy, J. D. (2000). Implementing information security in the 21st century: Do you have the balancing factors? *Computer & Security, 19*(4), 337-347. doi: HYPERLINK "http://dx.doi.org/10.1016/S0167-4048(00)04021-9" 10.1016/S0167-4048(00)04021-9

Organisation for Economic Co-operation and Development. (2002). *OECD guidelines for the security of information systems and networks.* Retrieved April 12, 2011, from http://www.ddsi.org/htdocs/DDSI/Final/Pres-docs/OECD%20Guidelines% 20INTERNET%20version%20-%20English.pdf

Pham, A. (2011, April 28). PlayStation network security breach will cost Sony much more than money. *Los Anglese Times*. Retrieved from http://articles.latimes.com/2011/apr/28/business/la-fi-0428-ct-sony-hack-20110428

Pinsonneault, A., & Kraemer, K. L. (1993). *The impact of information technology on middle managers.* Irvine, CA: University of California, Irvine, Graduate School of Management. Retrieved from http://www.jstor.org/pss/249772

Ponemon Institute. (2010, April 19). *Five countries: Cost of data breach.* Retrieved March 12, 2011, from http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010% 20Global%20CODB.pdf

PR Newswire. (2009, April 17). ClearPoint Metrics introduces the industry's first catalog of fact-based security metrics. *PR Newswire*.

Puhakainen, P. (2006). *A design theory for information security awareness* (Doctoral dissertation). University of Oulu, Oulu, Finland. Retrieved from http://herkules.oulu.fi/ isbn9514281144/isbn9514281144.pdf

Richardson, R. (2008). *2008 CSI Computer Crime & Security Survey: The latest results from the longest-running project of its kind.* Retrieved March 4, 2011, from http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf

Robbins, S. P., & Judge, T. A. (2008). *Organizational behaviour* (13th ed.). Upper Saddle River, NJ: Prentice Hall.

Rose, M. (n.d.). *Designing a metrics dashboard for the sales organization.* Retrieved 2010 йил July from http://hosteddocs.ittoolbox.com/MRose62706.pdf

Rotvold, G. (2008a, December). *How to create a security culture in your organization*. Retrieved March 23, 2011, from http://content.arma.org/imm/NovDec2008/How_to_Create_a_Security_Culture.aspx

Rotvold, G. (2008b, November). How to create a security culture in your organization: A recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs. *Information Management Journal, 42*(6), 32-38.

Ruighaver, A. B., Maynard, S., & Chang, S. (2006). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 55-62.

Salazar, V. (2006, October 11). *Management of information security.* Retrieved April 20, 2011, from http://www.cgiar.org/pdf/iau/Management%20of%20Information%20Security%20GPN.pdf

Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. *South African Computer Journal*, (31), 46-52.

Schlienger, T., & Teufel, S. (2002). Information security culture: The socio-cultural dimension in information security management. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Eds.), *Security in the Information Society: Visions and Perspectives* (pp. 191-202). Norwell, MA: Kluwer Academic Publishers.

Siponen, M., Pahnila, S., & Mahmood, A. (2005). Employees' adherence to information security policies: An empirical study. In *New Approaches to Security, Privacy and Trust in Complex Environments, Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), 232, (*pp. 133-144). Sandton, South Africa. doi: 10.1007/978-0-387-72367-9_12

Smith, M. (2002). *Business process intelligence.* CMP Media LLC. Retrieved from http://www.providersedge.com/docs/km_articles/business_process_intelligence.pdf

Smith, M. S., & Marinakis, S. A. (1997, Autumn). Measuring HR value-added from the outside in. *Employment Relations Today, 24*(3), 59-73.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers & Security, 24*(2), 124-133.

Stewart, J. N. (n.d.). *Establishing an organization's security culture: CSO to CSO: Establishing the security culture begins from the top.* Retrieved April 20, 2011, from http://www.cisco.com/web/about/security/intelligence/05_07_security-culture.html

Thomson, M. (1998). *The development of an effective information security awareness program for use in an organization* (Unpublished master's thesis). Port Elizabeth Technikon, Port Elizabeth, South Africa.

Tipton, H. F., & Krause, M., (Eds.). (2009). *Information security management handbook,* (6th ed., Vol. 3). Boca Raton, FL: Auerbach Publications.

Tudor, J. K. (2000). *Information security architecture: An integrated approach to security in the organization.* Boca Raton, FL: CRC Press.

U. K. Department of Trade and Industry. (2006). *DTI information security breaches survey 2006: Technical report.* Retrieved from http://www.infosec.co.uk/files/Survey_DTI_ISBS_2006.pdf

U. S. Department of Commerce, National Institute of Standards and Technology (NIST). (2010). By legal requirement. Retrieved from http://csrc.nist.gov/publications/PubsByLR.html

van Niekerk, J. F. (2005). *Establishing an information security culture in organizations: An outcomes based education approach* (Doctoral dissertation, Nelson Mandela Metropolitan University). Retrieved from http://www.nmmu.ac.za/documents/theses/VanNiekerkJF.pdf

van Niekerk, J., & von Solms, R. (2003). Establishing an information security culture in organisations: An outcomes-based education approach. In *Proceedings of the ISSA 2003: 3rd Annual IS South Africa Conference,* (pp. 9-11). South Africa.

Verizon Business RISK Team. (2009). *2009 data breach investigations report*. Retrieved from http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

von Solms, B. (2000). *Information security: The third wave?* Computers & Security, 19(7), 615-620. doi: HYPERLINK "http://dx.doi.org/10.1016/S0167-4048(00)07021-8" 10.1016/S0167-4048(00)07021-8

Vroom, C., & Solms, R. V. (2004). Towards information security behavioral complaince. *Computers and Security, 23*(3), 191-198.

West, R. (2008). The psychology of security: Why do good users make bad decisions? *Communications of the ACM, 51*(4), 34-40. doi: 10.1145/1330311.1330320

White, C. (2007, July). *A process-centric approach to business intelligence.* Retrieved from http://www.technologytransfer.eu/article/55/2007/7/A_Process-Centric_Approach_to_Business_Intelligence.html

Willcocks, L., & Smith, G. (1995). IT-enabled business process reengineering: Organizational and human resource dimensions. *The Journal of Strategic Information Systems*, *4*(3), 279-301.

Williams, B. K., & Sawyer, S. (2002). *Using informaiton technology: A practical introduction to computers and communications* (5th ed.). New York, NY: McGraw-Hill.

Williams, S., & Williams, N. (2004). The business value of business intelligence. *Business Intelligence Journal*, *8*(4).

Zurko, M. E., & Simon, R. T. (1996). User-centered security. In *Proceedings of the 1996 Workshop on New Security Paradigms,* (pp. 27-33). New York: ACM. doi: 10.1145/304851.304859