Seeking Best Practices In The Balancing Act Between Data Security And Operational Effectiveness

Ellen D. Hoadley, Loyola University Maryland, USA
Justin Deibel, Mercy Medical Center, USA
Colleen Kistner, PayPal, USA
Pamela Rice, PayPal, USA
Sandeep Sokhey, Corporate Office Properties Trust, USA

ABSTRACT

This paper develops an interdisciplinary model of data security and privacy effectiveness that blends the information hierarchy model with the principles of the Toyota production system. An application of the blended model is applied in the healthcare setting to evaluate its external validity. The usability and external validity of the model provide a preliminary set of best practices to improve organizational leverage of strategic planning and implementation of security and privacy safeguards. Its contributions include model development with real-world application and interdisciplinary bases.

Keywords: Security and Privacy; Cyber Security; Strategic Planning; Operational Efficiency; Data Security

INTRODUCTION

How can organizations meet the legal requirements and consumer expectations regarding information security and privacy without adversely affecting core business productivity? In many industries, legislative mandates (HIPPA, SOX, FERPA) can create inefficiencies in business processes. Laws and regulations have become more complex and onerous to protect consumers. In this climate, businesses are challenged to interpret legislative content, comply with regulation, sustain absolute data security, integrity, and privacy, while maintaining or improving productivity. The costs associated with data breaches have increased pressure on IT departments to tighten security of information capture, storage, and delivery. As organizations implement security features into core infrastructure, their processes and efficiency can be adversely affected. Those same business processes face increasing pressure to remain cost efficient. How can these competing needs be addressed? What are some best practices as revealed in the literature and in current business practice?

LITERATURE

How expensive is the problem? Since 2005, over 250 million data records of US residents have been exposed to security breaches through credit card fraud (25%), bank fraud (16%), phone or utilities fraud (16%), employment fraud (14%), government documents and benefits fraud (10%), and loan fraud (5%). In the past, most of these breaches were internal to organizations rather than external threats. However, a recent report from Symantec (Ponemon Institute, 2011) states that "for the first time, malicious or criminal attacks are the most expensive cause of data breaches and not the least common one." (Ponemon Institute, 2011; p. 3).

Organizations paid from $174 per record for those organizations that responded cautiously to breaches to $268 per record for those organizations that responded rapidly. However both of these organizational types were able to decrease spending on lost business by the amount spent on detection and escalation. Those paying the highest breach costs (an average of $326 per record) were those organizations that faced their first data breaches involving the loss or theft of more than 1,000 records containing personal information. The report supports

proactive and automated data protection in addition to written policies, procedures, and training. Not surprisingly, this is still a focused IT approach to cyber security rather than an organizational one.

The information systems literature has presented cyber security as an organizational issue rather than just an information technology (IT) issue. A major reality is that individuals within organizations don't always recognize the complexities and interdependencies of their information flow as it corresponds with the flow of goods and services within their own value chain and processes. (Goles et al., 2005) Threats to the technical infrastructure affect critical enterprise information systems that link the value chain and organizational processes globally. Best practices have been presented on how to prevent, detect, and respond to such threats. (Goles et al., 2005)

Business Technology Management (Hoque et al., 2006, p. 7) recommends moving beyond technology alignment to a state of convergence where the business and technology activities and leadership operate seamlessly and interchangeably. This convergence comes about by merging both the "strategic and tactical senses" (Hoque et al., 2006, p. 7) so that organizationally the tactical processes are leveraged for strategic advantage and the strategic planning and engagement considers and exploits the organization's tactical processes. If we look at convergence with a security focus, we seek to learn how organizations specifically can include elimination of data breaches in the strategic, tactical and operational senses.

DEVELOPMENT OF BEST PRACTICES

Conceptually, organizations that view the information of the organization as a strategic resource recognize the specific value of information at all levels differentiated by level (Figure 1). This conceptualization leads to an understanding of different views of security planning: operational planning focuses on compliance and immediate response to security breaches; tactical planning focuses on process improvement through efficiency to reduce disruptions from security breaches; strategic planning seeks security preparedness by leveraging organizational collaboration to avoid (and mitigate) the risks of security breaches.

A pervasive methodology for implementing an organizational process strategy has been to use the example of the Toyota Production System (Collins and Muthusamy, 2007; Liker and Morgan, 2006; Connolly, 2005; NSSC, 2000). Specifically, Spear and Bowen (1999) generalize the concepts and principles into four rules that can be generalized into any industry sector. Those rules are:

1. All work is highly specified in its content, sequence, timing, and outcome.
2. Each worker knows who provides what to him and when.
3. Every product and service flows along a simple specified path.
4. Any improvement to the process must be made through the scientific method, under a teacher's guidance, and at the lowest possible organizational level.

Applying these rules to information security strategy results in best practices to reduce the cost of breaches while not adding costs to business processes. Operationalization of this methodology integrates security processes with organizational information flows where data breaches could occur. However, the alignment takes time and intentionality on the part of the organization. Inefficiencies result when organizations identify a requirement for security and respond with a non-integrated "quick-fix" solution focused on technology infrastructure or compliance only (Sun et al., 2006). The inefficiencies are compounded because the time to prepare and implement an integrated security strategy is limited, and organizations may not see the value in an integrated security strategy.

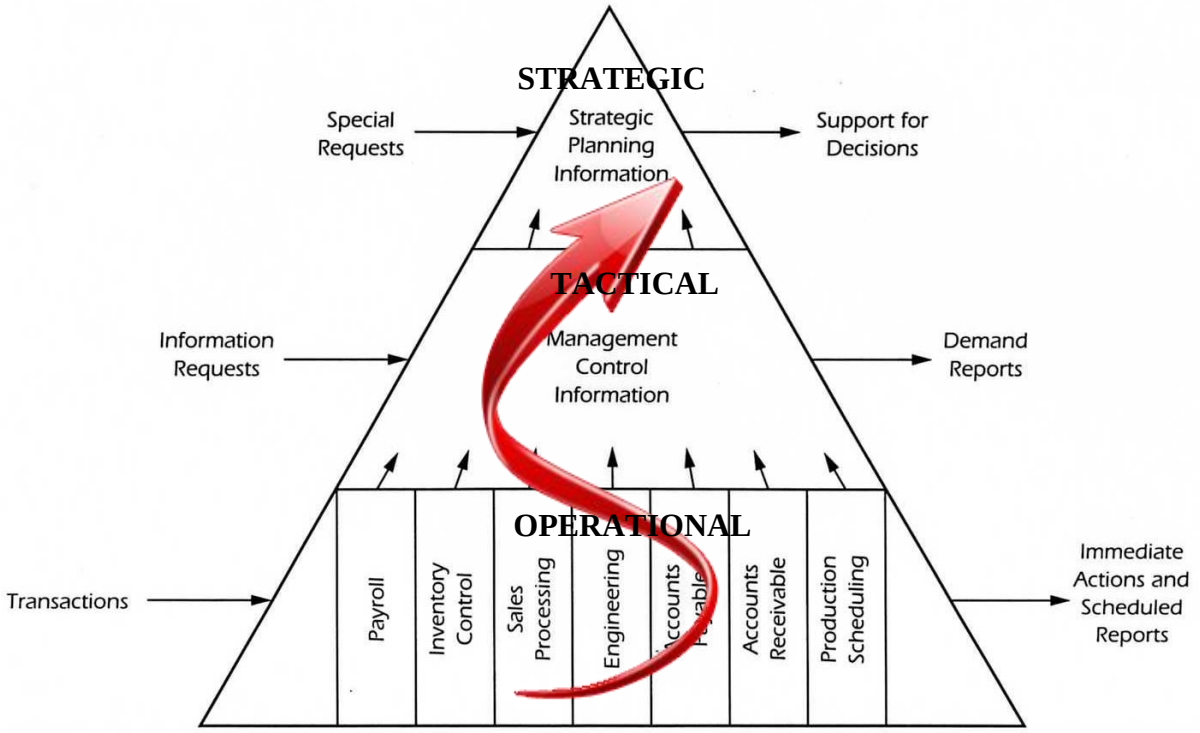

Figure 1: Conceptual integration of security with management/information pyramid

To avoid the inefficiencies, the following best practices (Costantino et al. 2009) resulting from focusing on the Toyota rules on security planning should be applied as follows:

Toyota Rule	Security Integration Best Practice
1. All work is highly specified in its content, sequence, timing, and outcome.	1. Develop and implement a detailed data security plan highly specified in its content, sequence, timing, and outcome.
2. Each worker knows who provides what to him and when.	2. Know where data reside, how, when, and where data flow, and the level of sensitivity and risk of breach.
3. Every product and service flows along a simple specified path.	3. Implement protection capabilities to safeguard the data end-to-end of each process and information flow.
4. Any improvement to the process must be made through the scientific method, under a teacher's guidance, and at the lowest possible organizational level.	**4.** Test, monitor, and continually update your protection capabilities. Plan for a controlled and coordinated response to incidents when they occur.

EXTERNAL VALIDITY

An example of the use of these best practices was identified at Mercy Medical Center in Baltimore, Maryland. The release of information is a typical process within a hospital where a patient or lawyer requests copies of the medical record. Requests are made for several reasons, but are commonly related to litigation (e.g., Workman's Compensation). The Mercy compliance officer identified a problem related to HIPAA compliance and the record release procedures. Mercy was potentially non-compliant with certain releases. The initial "quick-fix" reaction was to require every request be sent to the compliance officer for review and approval. Compliance was assured, but it also created a bottleneck in the process.

In order to fix the bottleneck and streamline the operational process, Mercy compliance professionals taught the staff receiving the requests how to review and maintain HIPAA compliance. Essentially, Mercy gave them a checklist they could use, avoiding the necessity of the compliance officer personally approving every one. This helped the operational process and elevated security planning to the tactical level, but this modification was limited to the receiving department.

Mercy decided to go even further strategically, leveraging the security review process organizationally. They realized that this process was also occurring in other departments and areas within Mercy and that each area was handling the release request differently. So the organization pulled a group together to review the process, including technology, compliance, finance, and medical records to determine the best process for the organization (not just one department). Tools were identified including technology and metrics to facilitate and measure the release process. The overall integrated approach improved both process effectiveness and efficiency.

FUTURE DIRECTIONS

This paper presents the results of a conceptual application of literature in information security and management and operations. The outcome is a set of best practices for improved information security that do not create organizational inefficiencies and that strategically mitigate the risk of security breaches. Future research will investigate specifically which areas of risk are the most and least important for mitigation. The goal is to identify those factors that may provide an opportunity for mitigation at low cost, as well as those risk factors that need mitigation at higher levels of funding or insuring.

CONCLUSION

The problem statement seeks to highlight the organizational tension that exists between operational efficiency and information security. This tension exists in all organizations, but it is most keenly felt in the healthcare industry. To develop best practices, organizations have found guidance in the literature by applying conventional rules from the Toyota system to the information management triangle within the context of information security. The resulting best practices have been applied at the Mercy Medical Center of Baltimore, MD with successful results.

AUTHOR INFORMATION

Professor Ellen Hoadley earned a PhD. from Indiana University, MBA from Indiana University, Post-Baccalaureate work at Georgia Southern University, and a BA at Florida State University. She has recently published in *Journal of Learning in Higher Education*, *The Data Base for Advances in Information Systems*, *Journal of Business & Economics Research*, and *International Journal of Electronic Healthcare*. She is currently Professor of Information Systems and Operations Management at Loyola University Maryland. E-mail: ehoadley@loyola.edu. Corresponding author.

Justin Deibel, Mercy Medical Center, USA

Colleen Kistner, PayPal, USA

Pamela Rice, PayPal, USA

Sandeep Sokhey, Corporate Office Properties Trust, USA

REFERENCES

1. Collins, Kevin F. and Muthusamy, Senthil K. (2007). Applying the Toyota production system to a healthcare organization: a case study on a rural community healthcare provider. *The Quality Management Journal*, 14(4), 41-52.

2. Connolly, Ceci (2005). Toyota assembly line inspires improvements at hospital. *Washington Post*, June 3, 2005, A1 & A6.
3. Costantino, B., Koenig, J, and Smaldon, L. (2009). Medical Identity Theft and Data Mismanagement. PriceWaterhouseCoopers, LLC White Paper #PH-09-0303-B.
4. Goles, T., White, G. B., and Dietrich, G. (2005). Dark screen: an exercise in cyber security. *MIS Quarterly Executive*, 4(2), 303-318.
5. Hoque, F., Sambamurthy, V., Zmud, R., Trainer, T., and Wilson, C. (2006). *Winning the 3-Legged Race.* Upper Saddle River, NJ; Prentice-Hall.
6. Liker, Jeffrey K., and Morgan, James M. (2006). The Toyota way in services: the case of lean product development. *Academy of Management Perspectives,* 20(2), 5-20.
7. NSSC (2000). Develop and implement a 'world class' manufacturing model for US commercial and naval ship construction. *Lean Manufacturing Principles Guide*. June 26, 1-48.
8. Ponemon Institute (2011). 2010 Annual Study: U.S. Cost of a Data Breach. Ponemon Institute, LLC. March, 1-38.
9. Spear, Steven and Bowen, H. Kent (1999). Decoding the DNA of the Toyota production system. *Harvard Business Review*, 77(5), 96-106.
10. Sun, L., Srivastava, R. P., and Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems,* 22 (4), 109-142.
11. Zetoony, David (2009). Ten ways to prevent a data breach from breaching a budget. *Privacy & Data Security Law Journal*, 449-455.

NOTES