Expanding Roles for the CISO
Jackie Bassett & Daniel Rothman’s Book Worth Reading

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In this series of three columns, I’m reviewing and commenting on ideas in _A Seat at the Table for CEOs and CSOs: Driving Profits, Corporate Performance & Business Agility_ by Jackie Bassett and Daniel Rothman and edited by Raquel Filipek.<http://tinyurl.com/4kqfxv> Today I’ll finish with a brief summary of the rest of the book, although I think I could write another six or seven columns on it if that wouldn’t give my editor apoplexy!

Chapter 2, “Show Me the Money,” makes the point that security problems should be treated with urgency at the _strategic_ level, not just as tactical glitches that can be relegated to low-level staff as minor details. “Because a security breach represents an underlying revenue and profitability problem that has gone undetected, preventing a security breach should be managed with the same level of urgency.”

The authors argue that identity management should not be seen as a nuisance: identity management can be a key to effective knowledge management about customers and competitors. For example, “When new customers are integrated into a company’s business processes seamlessly, the results translate into improved cash flows from revenues that are identified sooner and higher levels of customers satisfaction.” Inefficient, drawn-out assignment of unique, trackable identifiers “also gives the social engineer ample time to troll the system looking for an opportunity to exploit a weakness or even get signed up as a new customer” and then penetrate defenses through further social engineering. Good identity management can also be linked to customer relationship management (CRM) because a customer whose access is terminated can be identified immediately to the VP of sales for analysis and possible recovery.

Chapter 3, “Customer-centric Innovation,” includes several interesting examples of how improved security and greater integration of the CISO can support strategic planning of the sales function.

Chapter 4, “Security as a Catalyst for Innovation,” continues the theme with a discussion of the many ways that thinking about information security supports good application development, improved information management, and more productive knowledge capture.

Chapter 5, “Maximizing Shareholder Value in an M&A [Merger & Acquisition],” specifically addresses how good security practices are important for both the purchasing and the acquired organizations. They offer practical questions for boards of directors and guidance on reading audit reports, including in particular security aspects. They suggest a systematic series of steps for CISOs when becoming involved with M&As.

Chapter 6, “Turning Problems into Profits,” looks at the financial side of corporate governance from the CISO’s perspective and includes several specific examples from published reports and from the authors’ consulting experience. Some of the section headings are
- Boosting Sales Productivity
Chapter 7, “Leadership – Managing Human Assets,” starts with a stirring call to action on integrating security into every employee’s explicit job definition. Such a strategy

- Improves individual leadership skill through collaboration and team building.
- Strengthens corporate allegiance.
- Helps to provide a sense of community.
- Builds an intelligent workforce where every employee is recognized and watched by their peers for their individual contribution to the team’s strength.

The authors provide a seven-point summary of why security awareness programs can be good for the organization as whole. They emphasize that protection of intellectual property “can directly impact a company’s balance sheet” and that thinking about security can expose flaws in business process – with direct improvements to the bottom line _and_ to security at the same time. They emphasize something that I’ve been teaching for many years: that we can increase acceptance of secure procedures by showing employees how improved security can help them in their personal and family lives. Their section “What’s In It For Me?” looks at security from the perspective of employees in sales, marketing, operations, finance, and human resources.

Buy this book!

[On the off chance that there’s any question about it, I have never met Ms Bassett or Mr Rothman and have no financial interest in their publication or their work. However, I hope to meet them some day!]

***

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.