## Book Reviews: Enterprise Security For the Executive

Posted by samzenpus on Wednesday January 06, @01:56PM
from the read-all-about-it dept.
brothke writes

> *If Shakespeare were to write an information security tragedy, it would not be titled Hamlet, rather Bayuk. The story of Jennifer Bayuk is tragic in that she spent a decade as CISO at Bear, Stearns, building up its security group to be one of the best in the business; only to find it vaporized when the firm collapsed and was acquired by J.P. Morgan Clearing Corp. After all that toil and sweat, Bayuk was out of a job.*

While the information security engineering group that was at Bear, Stearns is no more, Bayuk has taken her vast expertise and put it in a great new book: Enterprise Security for the Executive: Setting the Tone from the Top. While many other books equate security with technology, and are written for technologists; Bayuk writes that information security is all about management control. And to the extent which a CxO controls assets, is the extent to which others can't use them in unexpected ways.

The book is written to help CxO's and business executives become familiar with information security concepts and techniques to make sure they are able to manage and support the efforts of their security team. This is an issue, as a big problem for the poor state of information security is that CxO's are far too often disconnected from their information security groups. No story is more manifest than that of when Heartland Payment Systems CEO Robert Carr blamed his PCI auditors for his firm's security problems. Carr is a perfect example of the type of person that needs to read this book. As an aside, for an excellent reply to Carr's kvetching, read what Rich Mogull wrote in An Open Letter to Robert Carr, CEO of Heartland Payment Systems.

While many CxO's think that security is about firewalls and other cool security products, it is truly a top-down management approach, and not a technology one. The book notes that the only way for information security to succeed in an organization is when management understands what their role is.

What is unique about the book is that Bayuk uses what she calls SHS (security horror stories). Rather than typical FUD stories, the horror stories detail systematic security problems and how they could have been obviated. By seeing how these companies have done it wrong, it makes it easier for pragmatic organizations to accomplish effective security by setting a strong tone from the top down.

Bayuk details the overall problem in the introduction and notes that many CxO's have wrongly spent significant amounts of money on security to avert security incidents; but have done that without any context of a greater information security methodology. The leads to executives thinking that security as nothing more than one long spending pattern.

Chapter 1 — Tone at The Top, notes that tone exists at the top, whether it is set or not. The tone is reflected in how an organization thinks about the things it really cares about. Employees can tell how a CxO cares about security by their level of personal involvement. Not that a CxO needs to be, or should be involved with minutia of firewall configuration or system administration; the key is rather that they are for example, championing the effective and consistent use of firewalls and how systems are securely administered.

In chapter 5 — Security through Matrix Management — Bayuk does a good job of detailing the various places that the security group can be placed in an organization. The chapter notes that there are as many ways to organize security as there are organization structures. Bayuk writes for example that if CxO's in a given organization are a tight-knit group, accustomed to close coordination, then it should not matter to which CxO the person managing information security reports to. If that is not the case, there may be multiple security programs that end up far too below the required C-levels that are needed for effective security. The chapter provides a number of different organizational scenarios, with requisite roles and responsibilities.

Chapter 5 closes with an important observation that a CxO should task the human resources department to put a line in all performance reviews whereby managers attest (or not) that the person being reviewed follows security policy. A CxO should fire people who willfully avoid compliance with security policy. Whatever tone at the top exists should be employed to make sure that everyone knows that the CxO is serious about the corporate security program. Such a tone clearly demonstrates an organization that is resolute about information security.

One thing that Bayuk does very well repeatedly throughout the book is to succinctly identify an issue and its cause. In chapter 6 — Navigating the Regulatory Landscape — she writes that if a CxO does not have management control over an organization, then the organization will fail the audit. It will fail because even if the organization is secure today, there is no assurance that it will be going forward. In addition, control means that the CxO will ensure that the organization is attempting to do the right thing. And in such cases, passing an audit is much easier.

Overall, Enterprise Security for the Executive is a fantastic book. It provides a no-nonsense approach to attaining effective information security. For those executives that are serious about security, the book will be their guiding light down the dark information security tunnel. In its 8 chapters (and a case study), the book focuses on a straightforward and plain-speaking approach to enable CxO's to get a handle on information security. As such, it is hoped that Enterprise Security for the Executive will soon find its way onto every executives required reading list.

Ben Rothke is the author of *Computer Security: 20 Things Every Employee Should Know* .

You can purchase *Enterprise Security for the Executive: Setting the Tone from the Top* from amazon.com. Slashdot welcomes readers' book reviews -- to see your own review here, read the book review guidelines, then visit the submission page.

Submission: Book review Enterprise Security for the Executive by brothke (1348253)
Enterprise Security For the Executive