My friend and colleague Don Holden, MBA, CISSP, Adjunct Professor of Information Assurance in the MSIA Program at Norwich University, is also an experienced security consultant and an executive with Concordant, Inc. He recently wrote an article for our MSIA students that I hope readers will find thought-provoking. Here it is.

***

In Seminar 2 of the MSIA program, we are looking at the process and people aspects of information assurance rather than the technology. Bob Blakley, the chief scientist for security and privacy at IBM, notes that the current approach to security has failed, and that there is no viable technical model. He calls for a new industry approach based upon a business model in which technical models will evolve. [1]

Although Blakley was speaking as a vendor, we, as security as managers, also need to be able to state the business case and the economic value for the security function. We need to understand and communicate the economic costs of both providing security and failing to provide security. Last year (2004), I knew several chief information security officers (CISOs) at major banks who lost their jobs when the Federal Reserve sent letters reporting security deficiencies to their Boards of Directors. In at least one instance I believe this was a result of a failure of vision: the bank’s business units responsible for implementing corporate security policies did not see the economic value of security and failed to adequately implement security controls.

So we need to have metrics that show how well the security function is performing and what the costs and the business benefits are. We need metrics that show the cost of failed security such as when an e-mail server is taken down due to a virus, or customers’ account information is compromised. If we understand the business value of security, we can also allocate back to the business units their share of the cost of providing security. We can also make better purchasing decisions if we know the cost of installing patches due to poor product quality. And we can make better risk-management trade-offs if we know both the cost of the security measure and the expected loss it will prevent. With recent regulations such as HIPAA[2] and GLBA,[3] affected companies need to have good understanding of the costs involved in these risk management trade-offs.

When we understand that security is a business issue and competes with other business issues for resources, we will have to understand those financial rules such as how capital budgeting decisions are made using return-on-investment (ROI) or Net Present Value (NPV) and when security costs should even be considered a capital item.

By the way, those fired CISOs are now well-paid security consultants.

***
References


* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see < http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2005 Don Holden. 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.