Tightening financial constraints on any business are requiring information technology (IT) and information assurance (IA) professionals to start showing proof of benefit and cost justifications for their departments, their workforce, their capital expenditures, and their consultants. In an interview, one CISO told me that a consultant or employee has to provide good financial figures, cost justifications, and achievable metrics so she can back up her requests to the Board of Directors for approval and funding; she won’t hire any consultant who fails to provide such details.

Security consultant Gordon Merrill continues his series on fundamental management tools for IA professionals in general and IA security consultants in particular. His insights and recommendations will also help clients choose consultants wisely and judge their performance appropriately.

* * *

It has been said that raising teenagers is like trying to nail Jello to a tree. In the past, asking IT for justification for IA expenditures has received much the same response; for example, we get comments like “You can’t measure what you have prevented because there was nothing to measure.”

Let’s look at the effect of IA on e-mail for example. E-mail is undoubtedly the single most important application to business today.<http://www.wwpi.com/index.php?option=com_content&view=article&id=7474:defying-murphys-law-using-managed-security-services-for-message-continuity&catid=233:storage-security&Itemid=2701197> If a business has 15,000 users and receives over 500,000 e-mails a week, IA might say, “We’ve gone all week without a virus getting through: something is working!” But how does that approach justify the $1.2 million you spent last year for multiple layers of virus and spam and phishing protection? How does the board or the chief financial officer know that your company would not have been as safe without spending the $1.2 million?

One of the best ways for IT security and IA personnel to start showing non IT personnel the value of IT is to start using monitoring and security metrics to prove your point. Looking at that same e-mail example lets provide some metrics to reflect what that 1.2 million did for the company. Scott Berinato’s interview with Andrew Jaquith of the @Stake security consulting firm offers some useful suggestions.<http://www.csoonline.com/article/220462/a_few_good_information_security_metrics/1>

For example, instead of presenting a round number like 500,000 e-mails with no attacks and no down time, one can provide more detail. “Last week the company received 562,478 outside e-mails, including 257,893 attachments. With them came 576 viruses, and 486 spam attacks in 186,765 documents. E-mail security level1 stopped 524 viruses, and 465 spam attacks; level 2 stopped 51 viruses and 19 spam attacks; level 3 stopped 1 virus and 2 spam attacks for 100%...
security and threat elimination.” Now, all these numbers are fictitious in this example but they prove a point. The effectiveness of the e-mail protection can be measured and with numbers that not only prove the worth of IT’s efforts but also the justification for the $1.2 million for upgrading the protection to three levels.

It’s true, as Prof Kabay has long pointed out, that statistics about security breaches are rarely trustworthy and that therefore quantitative risk management calculations, even when they are done right, are of questionable value. What finance officers and accountants do know is the value of inference. Presenting officers with case studies from comparable organizations is an excellent basis for discussion. For example, the TJX security breach was widely reported and several reports even broke down the costs to TJX into costs per record compromised. With that level of published detail, you can discuss the number of records in your organization’s databases and calculate a rough estimate – at least an order-of-magnitude approximation – of the cost of a security breach for your own data.

_In the next part, Gordon discusses the importance of deciding on appropriate metrics._

* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon’s information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.<mailto:merrill.ia@gmail.com>

This series is based on some of the papers Mr Merrill wrote during his MSIA Program<http://infoassurance.norwich.edu/> at Norwich University<http://www.norwich.edu> from 2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP<mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 Gordon Merrill & 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.