New Kids Advance New School

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

Do you ever get tired of hearing the same old regurgitated pap about security from the same old bald, graying old-timers (hmmm, I’d better be careful here)?

Two exciting young talents (well, young from my perspective), Adam Shostack <http://www.homeport.org/~adam/> and Andrew Stewart <http://homepage.mac.com/andrew_j_stewart/>, have published an interesting and challenging manifesto urging information assurance (IA) practitioners to break out of conventional thinking. They argue (and I concur) that we have to use the insights of other disciplines in formulating and implementing our security policies to cope with computer-related crime.

_The New School of Information Security_ <http://www.amazon.com/New-School-Information-Security/dp/0321502787/ref=sr_1_2?ie=UTF8&s=books&qid=1220367321&sr=8-2> is an engagingly written, concise book that's suitable not only for security practitioners but also for non-technical executives and for students. It’s already being used in a course at the Carnegie Mellon University and I’m considering it for a course of my own.

Like Bruce Schneier and Ross Anderson, the authors argue strongly for economic analysis of security issues as a fundamentally sound approach to resolving practical questions. The authors discuss the dreadful state of trustworthy, testable information about computer crimes. They support the view of many practitioners that we cannot depend on quantitative risk management in the absence of reliable data. The problem of ascertainment is that we know from historical observations that some computer security breaches are not discovered until long after they occur, leading to the obvious but unanswered question of how many breaches are never discovered at all. The problem of reporting is that we also know that many discovered breaches are not reported – but again, we don't know what proportions are involved.

Surveys, the authors explain, suffer from well-known weaknesses. Not only are the measurement instruments themselves often flawed (with biased questions and zero attempt to achieve internal validation of the results) but the sampling is non-random. We never know to what extent the people responding are a representative sample of the population to which we apply the findings of the survey. Another problem with surveys is that many are sponsored by commercial organizations and they generally do not release the raw data for independent analysis. The authors strongly argue for such release in future surveys.

Without actuarial data, calculations of annualized loss expectancies are of limited use. From my perspective, they can serve well in Monte Carlo simulations <http://www.decisioneering.com/monte-carlo-simulation.html> for sensitivity analysis, allowing us to guess at the relative importance of various aspects of our information assurance infrastructure. However, we cannot rely on calculations based on guesswork for more than a general notion of the relative importance of protective measures.

Another aspect of today's security industry that the authors address is the insularity of our field.
We have little cultural, gender and educational diversity; we could benefit from a wider range of personal and professional backgrounds. In particular, the authors argue, we need more cross-disciplinary thinking, with insights developing from experience in psychology, sociology, organizational dynamics, mathematics, physics, and engineering. Undergraduate curricula in security, they argue, tend to focus too closely on cryptology as if it were the central focus of security today. On the contrary, they argue, although cryptography underlies many of the technological tools we use in securing information, it is far from sufficient for effective implementation of security plans.

On this last point, I’m proud to point out that the Norwich University BSCSIA <http://www.norwich.edu/academics/business/infoAssurance/index.html> and MSIA <http://www.graduate.norwich.edu/infoassurance/> are strongly interdisciplinary. Our IA undergraduates, for example, must complete courses in psychology, management, and economics as part of their security-degree program.

By the way, this is the first book I’ve seen in which the endnotes are almost as interesting as the text itself. The authors have added 50 pages of very interesting discursive commentary and references that are worth reading. That’s followed by a 15 page bibliography that will be particularly useful to professors (for example, I’m grateful for their work because I’m developing a course entitled “The Politics of the Internet”). They also include a good index. In addition, the publisher has added an extract from Phillip Hallam-Baker’s _The Dotcrime Manifesto: How to Stop Internet Crime_<http://www.amazon.com/dotCrime-Manifesto-Stop-Internet-Crime/dp/0321503589/ref=sr_1_1?ie=UTF8&s=books&qid=1220367775&sr=1-1> and from David Rice’s _Geekonomics: The Real Cost of Insecure Software_, both of which readers of this column may find interesting.

Personally, I am delighted to see these young authors expounding on such fundamental issues. I hope that lots of people will read their book and think about changes in our approaches to security.

Good job, fellows!

***

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.