Science and Security

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

I buy TIME magazine now and then when I’m waiting in a long line at the local supermarket – it’s the only magazine on the racks that doesn’t have covers with starlets falling out of their dresses or space aliens impersonating politicians – or impregnating the starlets (no, really).

The February 13, 2006 issue (available online at <http://tinyurl.com/8mqal>) has some interesting articles in the cover series (“Is America Flunking Science?”). I was struck by the following comment on p. 24 of the paper version in the article by Michael D. Lemonick, “Are we losing our edge?” (<http://tinyurl.com/7b3u4> online for subscribers only or temporary access for $1.99):

>… [E]xperts in business and academia have been warning for decades that U.S. science was heading for trouble for three simple reasons. The Federal Government, beset by deficits for most of the past three decades, has steadily been cutting back on investment in research and development. Corporations, under increasing pressure from their stockholders for quick profits, have been doing the same and focusing on short-term products. And the quality of education in math and science in elementary and high schools has plummeted, leading to a drop in the number of students majoring in technical fields in college and graduate school.<

I won’t address the government-funding issue here, but the second comment reminded me of a long-standing theme that bears repeating: short-term horizons are inimical to information security. During the dot-com boom of the 1990s, it seemed that many executives were hopping from job to job, often more than once in a year. With short residency in an organization, irresponsible managers could look good in the short term by skimping on longer-term cost avoidance measures of all sorts, inflating short-term profitability, and then getting out as they hopped to the next company. The consequences of their short-term strategy would then fall on the next managers to take over.

Information security suffers from a serious structural problem: the better we are at preventing harm to our information, the less hard evidence we can present to naïve colleagues that our measures are effective. We are accused of being like the madman on the street corner who is waving a dead chicken around his head. “Why are you doing that?” people ask. “To keep the flying elephants away.” “But,” people protest, “there are no flying elephants.” “See?” he responds in triumph. “It works!”

Unless we have carefully implemented intrusion detection systems (IDSs), we can’t show our bosses that our security measures are resisting real attacks. But even getting the money to implement IDSs – let alone all the other expensive toys and the potentially burdensome policy changes we want – requires cost justifications. Cost justifications usually require return-on-investment (ROI) calculations. ROI usually involves annualized loss expectancies (ALEs). ALEs are calculated by summing the products of event-probabilities by their expected costs (e.g., the probability that a disaster will happen times the cost of the disaster + the probability that the disaster won’t happen times the cost of the disaster-prevention-mitigation-recovery
efforts). Unfortunately, we don’t know the probabilities because (1) people don’t notice all the
security incidents that happen; (2) people don’t report all the incidents that they notice; (3) there
is no central database of reported incidents; (4) there is no classification scheme allowing
actuarial accuracy in predicting the rates of occurrence of security incidents as a function of the
nearly infinite range of user classes, network and system configurations, software products and
software versions implemented in organizations.

So what’s left? We have to convince our non-technical colleagues to pay attention to legal
requirements for data protection such as (in the US) the Sarbanes-Oxley Act, the Gramm-Leach-
Bliley Act, and the Health Insurance Portability and Accountability Act. The European Privacy
Directive is critically important in Europe and also helps us build a case even in the US for
transnational corporations or those doing business in the European Community.

Oh well, at least I got something from my time in the checkout line in addition to this week’s
groceries.

* * *

New information assurance journal – Norwich University Journal of Information Assurance

M. E. Kabay, PhD, CISSP-ISSMP 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 © 2006 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.