Will business and government respond rationally to cybercrime news? Or will we continue to see reports of inadequate funding for information assurance (IA) and national security across government agencies and corporations?[1]

Sometimes it seems as if the information age has made the number of bad people increase exponentially – we hear more and more about the involvement of organized crime rings in computer crime today.[2] However, I doubt that there are any more malicious individuals than there were before the Internet existed; we just hear more about what the bad guys are doing and how they are accomplishing their misdeeds because of increases in the speed and distribution of information.

Developing and implementing technical, administrative, and physical security countermeasures is a cost of doing business that subtracts directly from a company’s short-term bottom line. If a company’s senior management do not understand the justification for incurring security expenditures, they won’t fund security. Generally speaking, the management of traditional brick-and-mortar companies understand the need to invest in _physical_ security controls better than they grasp the value of IA. Similarly, most individuals are well aware of how to protect themselves against theft and assault, but they are less likely to resist phishing, Trojans and other computer-mediated attacks. Many business people have no awareness at all of simple IA measures such as avoiding discussions of confidential matters on cell phones while in public places; many well-meaning people commit elementary blunders such as picking bad passwords or writing them down on sticky notes.

Unfortunately some managers still don’t understand that information security needs to be integrated into their products and services in the design phase, not added later as an afterthought or as a belated response to a cyber attack. Businesses that store their clients’ personally identifiable information (PII) must accept that there is no precisely quantifiable return on investment for properly incorporating IA personnel and practices into how they do business.[3] Instead, they need to realize that having a good IA program is another form of insurance – a method of spreading risk through loss avoidance and loss mitigation – that has to have a high funding priority. The recent series on Veterans Affairs’ data losses should be warning enough of the potential liability of losing control over PII! Consumers should demand that companies
properly safeguard their information by looking into privacy policies and expressing their displeasure at sloppy handling of PII. The media should continue to broadcast IA stories to raise security awareness levels and to provide practitioners with concrete examples of security issues with which to reach non-technical executives.

IA professionals must continue to improve the availability, integrity, confidentiality, control, authenticity and utility of information. A growing number of highly skilled IT professionals are becoming IA specialists.[4] Some are educating the public by providing good information about effective IA practices; some are being hired by and educating businesses to improve information security within their products; some are in colleges and universities educating the next generation of IT professionals to think about security first. I think that there is hope for the future of IA as long as awareness, training and education continue to match the growth in offensive capabilities of our enemies.

M. E. Kabay adds:

In practical terms, I recommend that readers engage in discussion of IA with upper managers in their place of employment. In the MSIA program at Norwich University, students have to interview their colleagues throughout the 18 months of study and it is an eye-opening experience that helps everyone, students and managers alike. Find out how your colleagues think (and feel) about IA throughout the organization. You may be surprised at how far you have to go in changing ingrained attitudes about security in some circles; you may be surprised at the allies you can identity through personal contact. Such personal contacts be useful not only in instituting corporate culture change about security but also in long-term development of your own career.[5]

***

Steven Zeligman, MSIA, MCP, CISSP is a Senior System Analyst at Dataline. Inc. and has over 15 of experience in information technology and security. You are welcome to write to him <mailto:steve@z-nets.com> with comments on this essay.

***

For Further Reading

Lowey, N. M. (2006). Lowey calls for immediate overhaul of department of homeland security national asset database: While New York’s homeland security funds are significantly reduced, a popcorn factory and mule festival are categorized as top terrorist targets <http://www.house.gov/list/press/ny18_lowey/hs071406.html>;


* * *

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 © 2007 S. Zeligman & 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.