In 1994, I was asked by the Institute for Government Informatics Professionals of the Government of Canada to create a follow-up for the information security (INFOSEC) course I taught under the aegis of the University of Ottawa at the Institute. Students were interested in learning about developments across the field of INFOSEC since they had graduated.

So began the series of two-day workshops that I have been giving for a decade called INFOSEC UPDATE. These short courses are intended for security specialists such as CISSPs wishing to remain current on developments in information technology security and in general for any information technology personnel interested in security. We review major developments across the entire field of information security, including

* computer crime cases and trends, including information warfare issues;

* developments in law enforcement technology;

* emerging vulnerabilities (e.g., the course warned of the dangers of MS macro viruses and the threat from denial of service attacks long before they hit the headlines);

* management and corporate policy issues (e.g., we discussed spam and cybersquatting in the mid-1990s as the problems were blips on the horizon and emphasized privacy issues before the topic became popular);

* cyberlaw, e-commerce and cryptography (e.g., the course provided early warnings about developments in intellectual property law, public-key infrastructure and changes in cryptography exports).

The course is based on my long-running INFOSEC Year in Review project, in which I organize information about information security into a coherent structure so that I can find examples easily for my courses and writing. On the other hand, organizing stuff may also be a sign of a personality flaw; one of my colleagues laughingly pointed out that I sort my CDs by year within artists, DVDs alphabetically by title (except series) and the bills in my wallet by face value. What, other people don’t do that? Anyway, the workbooks produced from my database of security news for each year since 1994 are available as PDF files at <http://www.mekabay.com/iyir/index.htm>; take a look at the latest ones to get a sense of the kind of material we discuss. The complete taxonomy of topics is available separately at <http://www.mekabay.com/iyir/Codes.pdf>.

These workshops are enormous fun for me and, I’m told, for the participants. It’s a free-wheeling discussion of hundreds of cases (the workbooks are typically from 250-400 pages long depending on how tiny the print is) and I emphasize lessons for the participants’ real-world
working environments. Much of the value of these sessions comes from lively discussion among
the participants. It’s an intense experience – a bit like total immersion in INFOSEC for eight
hours a day over two days.

The next INFOSEC UPDATE workshops will be in Montréal, Québec, Canada in November.
There’s an English session on Monday and Tuesday the 24th and 25th of November and a French
session on the 27th and 28th. Both will be held at the Dorval Airport Hilton, which is about two
minutes from the Montréal International Airport terminal and has always been a lovely hotel for
these sessions (members of the Montréal Regional HP Users’ Group will remember that we had
our quarterly meetings there). The airport is only 20 minutes away from downtown Montréal for
those who’d like to visit that beautiful city after the course sessions.

For complete information, including course fliers and registration, please visit the Web site at <

I hope to see you in Montréal!

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information
Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <
mikkaay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2003 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.