In the last of this mini-series, I am responding to students who have asked me for ideas on what they could do in their PhD thesis research in the field of INFOSEC.

(5) Analysis of vulnerabilities: identification, taxonomy and repair.

What are the kinds of vulnerabilities that we need to spot in our systems? Who is using which technique to find and identify such vulnerabilities? What are the taxonomic systems used to describe vulnerabilities? How do products and practitioners fill security holes? This thesis topic would give you an opportunity to work closely with auditors, large IT security consulting firms, penetration specialists (including maybe some of the companies using "ex-"criminal hackers), certifying authorities (e.g., British Standards Institute, National Information Assurance Partnership, ICSA.net), and people and organizations who publicize vulnerabilities (e.g., CERT-CC, BugTraq moderator, contributors to various other lists). Perhaps you would want to study the quality assurance programs of major operating-system manufacturers to illustrate differences in underlying architectures and QA methodologies to explain why some operating systems have more security holes than others. This thesis might also be a good opportunity to study the TCP/IP and IPv6 with an eye to showing how fundamental networking protocols influence security.

(6) Computer anti-virus technology: the never-ending battle.

You would study the history of computer viruses and describe the evolution of virus techniques and the countermeasures used by the anti-virus industry. You could probably get cooperation to interview people at ICSA Labs who run the AVPD (Anti-Virus Product Developers' Consortium), people at _Virus Bulletin_, industry experts from the AV community in industry and academia (you would for example contact Sarah Gordon at IBM, who has been studying the virus-writing subculture for many years), and maybe even some people who write viruses. It would be helpful to describe how the Microsoft operating systems have allowed binary viruses to infect so many systems (in contrast with UNIX-flavored operating systems). Perhaps you could interview the people who were responsible for deciding to allow automatic execution of macros -- thus turning word processors and spreadsheets into suitable platforms for macro viruses and all the trouble they have caused. You could study virus-exchange boards/groups to get a better understanding of the psychology of these people (many of them are kids). It would be great to have a professional study of attitudes towards viruses in different age groups and perhaps even in different countries (a major effort indeed). I guess that the people at ICSA Labs and _Virus Bulletin_ would be happy to help you with access to their anti-virus data (you understand that I can’t assure you of this, since I have not spoken to anyone there about this issue). You might end your thesis with a picture of what the future holds and your opinion on how best to fight this scourge given your findings.

(7) INFOSEC and corporate culture: a psychosocial analysis

You would look at how information security is developed and implemented in a wide range of
corporate, academic, and government organizations. Your work would focus on the state of security policy, the ways policies are developed and implemented, the kinds of reactions and feelings employees express about security policy, and methods currently being used to improve the quality of policies and the rates of compliance with those policies. If you are interested in interventionist work, you could even run some experiments to look at the effectiveness (in terms of compliance) of different approaches to INFOSEC policy implementation. Maybe you could do some cross-industry or even cross-cultural comparisons if that’s interesting to you; for example, what are the factors that might account for observed differences in compliance rates across industries and across cultures?

For more ideas, I suggest that you join the INFOSEC Educators' List run by Dr Fred Cohen; you can join by sending your name and e-mail address to <secedu-subscribe@onelist.com>. You can post your request for ideas there and I'm sure you will receive excellent suggestions from INFOSEC educators around the world.

I wish you the very best in your work, and don't hesitate to correspond further with me if you like.

Best wishes,

Mich

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Copyright © 2000 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.