This is the second of two parts of an interview with Daniel Kennedy, MSIA, who graduated from the Master of Science in Information Assurance<http://infoassurance.norwich.edu/> program in the School of Graduate Studies<http://graduate.norwich.edu/> of Norwich University<http://www.norwich.edu/> in 2008. He has recently become a contributor to an interesting, thoughtful and valuable blog at Forbes Online<http://blogs.forbes.com/firewall/> and I interviewed him recently about his new project.

* * *

**What do you think your focus will be in the coming months?**

I’m still finding my voice on this Web site, but my primary focus will be on what I think is most missing: fundamental security strategy within companies and its effective execution. I am very much in favor of the capabilities new and innovative products can provide, but I find their implementation in many organizations is haphazard; the products lead the implementation calendar rather than allowing internal teams to find the right products that fit into an overall, strategy that prioritize the rollout of its component parts.

For example, there are organizations which provide privileged access to all users and have no Web filtering, yet they are asking about high end data leakage protection (DLP) products<http://www.networkworld.com/community/node/23754>. Companies may have no patch management<http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch40_patches.pdf> and no validation of their anti-virus, yet they want to discuss high end log review security information and event management (SIEM)<http://www.networkworld.com/news/tech/2009/031909-tech-update.html> products. Many companies are not doing intrusion detection<http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/csh5_ch27_ids_ips.pdf> at all, doing it in baffling ways, or outsourcing it to providers who aren’t actually monitoring anything. In most cases all of these things should be part of a strategy, but more complex projects will only be successful if built on a foundation of getting the basics right.

Those basics involve the somewhat less sexy implementation of security policies<http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch44_security_policy_guidelines.pdf>, awareness programs<http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch49_security_awareness.pdf>, communication plans<http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch56_csirts.pdf>, and other aspects of information security programs that people try to run from because they are uncomfortable, they involve the entire organization, and they require putting oneself ‘out there’.
So there are security teams looking busy but crippled by the lack of organizational power afforded them in the environment they’re in and by the inability to set their own reasonable agenda, and thus not advancing the state of security within their organizations. There are people responsible for information security in different areas of the enterprise, but organizationally its implemented such that there is no central strategic leadership in the form of a CISO. I hope I will support these teams by showing that many security events that get highlighted in the media are not caused by some especially advanced attacker but rather by exploiting simple, fixable and preventable vulnerabilities. And even when the attack is advanced, that in many cases the incident response, forensics response, and corporate handling of the event left room for improvement.

*How are you finding the experience of writing regularly for public consumption?*

It is difficult, both from the perspective of clearing time to write and in trying to create content that is meaningful without appearing to sell something, parrot back old content, or publish unsubstantiated personal opinions without a relevant story from experience or an observed condition.

I got back into writing seriously while in the Masters of Science in Information Assurance program<http://infoassurance.norwich.edu/> up at Norwich University<http://www.norwich.edu> in Vermont, which had as part of its curriculum a demanding schedule of writing security papers as well as a strict evaluation of that writing. That training made creating 1,000 word essays easier.

That said, putting ideas before the public, especially controversial ideas, and seeing how people react is interesting. When publishing on a Web site, one does receive comments that are not well thought out or are just silly, but sifting through user responses is always made worthwhile when you hit upon someone who posts a reaction that requires you either to defend your position more effectively or to radically reassess the way you’ve been approaching a topic.

* * *

Daniel Kennedy, MSIA, CISSP, CEH leads initiatives in policy and operational security management, directs strategy on risk assessment and certification, and is head of business continuity planning and disaster recover objectives at Praetorian Security Group, LLC.<http://www.praetoriansecuritygroup.com/company/management-team/>


Copyright © 2010 Daniel Kennedy & 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.