Information Security and Business Strategy:  
An Interview with Stephen Northcutt (1)

by M. E. Kabay, PhD, CISSP-ISSMP  
Associate Professor of Information Assurance  
School of Business & Management  
Norwich University, Northfield VT

I’ve known David Greer< http://www.davidgreer.ca/> for over 25 years and have always enjoyed his intelligence, good humor and creativity. And Stephen Northcutt< http://www.sans.org/security-training/instructors.php#Northcutt> is so widely published, cited, and respected in our field that I had trouble deciding which of his many Web sites to cite.< http://www.sans.edu/resources/musings/> It is a great pleasure to publish David’s interview of Stephen in two parts. Everything that follows is by Messrs Greer and Northcutt with minor edits.

* * *

Many information security professionals are overwhelmed with the technical issues they must deal with. But technical solutions must operate in a business environment that deals with customers, partners, and other stakeholders. I interviewed Stephen Northcutt, President of the SANS Technology Institute, < http://www.sans.org > a leader in information security training, and discussed the relationship between information security and business strategy.

DG: How do you see information technology (IT) security and the broader issues how user and customer experience relate to business strategy?

SN: One course that I teach is information security for managers.< http://www.sans.org/security-training/sans-leadership-and-management-competencies-446-tid > On one of the very first slides, the point that I try to make is that you’ve heard frustrated business people say you guys have got to align your security programs with the needs of the business. One of the questions I ask right then is, “Do you guys even know your organization’s mission statement?” I typically see 10% or so of the class that can.

DG: I’ve had trouble finding how information security can enhance business strategy. The focus seems to be on the technology and how it is applied to the broader business issues. What are your thoughts?

SN: The people that I follow on twitter < http://twitter.com/StephenNorthcut > have been posting a whole lot of posts with a little bit of technology but a lot of business comments as well. Our latest newsletter is called SANS ExecuBytes < http://www.sans.org/newsletters/execubytes/> and it covers leadership as well as technology. What really impresses me are people who write and say, “I printed it out and gave it to my boss.”

DG: While searching for thought leaders on IT security and business strategy, I found your Web page on Security Thought Leaders.< http://www.sans.org/thought-leaders/sec_thought_leader > The thought leaders that you mentioned seemed to be biased to the technical side. The interviews that I read were deep into the technical problems as opposed to the broader strategic issues I thought should be there. What is the background for your Security Thought Leaders?

SN: One of my goals for the project is to introduce people that you wouldn’t ever hear of otherwise. There are some people who’ve done some truly amazing things such as Bill Worley.<
Bill was one of the architects of the Itanium and when he retired from HP his wife made him go in the basement so he didn’t bother her all the time. He went in the basement for a year and wrote a new operating system that runs over Itanium. It’s a micro operating system, so it runs a lower risk attack surface. Bill may or may not succeed and his company [which provides DNSSEC solutions to government, enterprise, and service providers] may or may not succeed, but what a great story!

DG: Who else stands out on from your leadership interviews?

SN: I don’t know if you’ve ever heard Gene Kim speak. I want to encourage you to pick up on one of his Webcasts. He is really concerned about good practice in organizations. He is co-founder of the IT Process Institute. Even though he is co-founder of Tripwire, the configuration-management software company, he almost never talks about Tripwire. He talks about organizational process.

All of the thought leaders who have started a company created a kind of aspirin for a particular kind of headache. That’s certainly their common story, but now that that they are running a business, they find that life is far broader. You bring people like that in to close the big sales to customers but then the customers start telling them what the real problems are.

DG: It’s a constant challenge to balance the security risk of IT security solutions versus the usability to employees, customers, and partners. Do you have a set of guiding principles that IT security professionals can follow to provide perspective on the balance?

SN: Start with the SANS Top 20 Critical Security Controls. The idea behind the Top 20 was to actually deal with things that are provable – you can prove that you can break in using these vulnerabilities. We took a bunch of penetration testers and got them to break in; afterwards, we analyzed what went wrong figured out what we needed to do to fix the problems. One of my favorites is number 11 (“Account Monitoring and Control”); another is number 9 (“Controlled Access Based on Need to Know”). As I cover security news, I find that so many of the problems come down to access control. It’s just crazy and I suppose there is some technology but it’s mostly process.

[More of the interview in part 2 next time.]
limit on any Web site, and to republish it in any way they see fit.