Information Security and Business Strategy:  
An Interview with Stephen Northcutt (2)

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

This is the second of two parts of an interview of Stephen Northcutt<http://www.sans.org/security-training/instructors.php#Northcutt> by technologist David Greer.<http://www.davidgreer.ca/> Everything that follows is by Messrs Greer and Northcutt with minor edits.

* * *

DG: It seems like many of the current security issues are problems that we have been dealing with for decades. How do you see the evolution of the problem space of information security?

SN: Twelve years ago, we were standing up for a cyber capability for the United States. All the things we are saying today and the stuff we are doing to our cyber capability I heard twelve years ago. We do make progress; for instance we now have the Cyber Guardian program<http://www.sans.org/cyber-guardian/> and have already graduated the first class. The attack surface just continues to get larger and larger and larger. So we’re dealing with more lines and more kinds of codes. We are more connected, so there’s a lot more vulnerability points because we are increasingly connected and more code is exposed to potential attacks.

We are not dealing with that many fundamental problems. The specifics are changing, but the classes of the problems haven’t changed very much. There is an ever-greater need for security people who can integrate with the business. I was just trying to explain to someone that the number one thing a manager wants out of a security person is communication skills. We’ve done survey after survey after survey. Our challenge is to develop people’s communications skills. You can’t do business without communication.

I would also say that my personal observation is that people often think complexity is its own reward. If we don’t put a tremendous amount of attention and simplify, simplify, simplify, we end up with things we cannot manage. This is true on the security level, technology level, and organization-process level.

DG: How do you see evaluating and managing risk in the security environment today?

SN: A couple of years back I spent some time with the trade organization that represents the 100 largest banks in the US. We were trying to do some work around information security risk. More than once I heard the finance guys say “You information security folks have no idea what you’re doing in terms of risk management. You are using qualitative methods when you need quantitative. In finance we know for any set of financial transactions within a few dollars of what our risk is.” One of those quants was in the risk management department at Bear Stearns<http://www.bearstearns.com/> which is gone now.<http://www.peimedia.com/Article.aspx?article=31636&hashID=3052F49C040841D0210CA22F  
BFF7C1449702B776> The finance folks have an advanced terminology and methodology. I am sure senior management were briefed on the risks, but because house prices and stock prices kept going up they thought this incredible risk of bubble deflation was an acceptable risk and they
found out they were wrong.<http://money.cnn.com/2008/03/28/magazines/fortune/boyd_bear_fortune/> We need to make sure in information security we are never arrogant and that we make every effort to present risk to senior management in such a way that they can govern wisely. I think there are three parts to that.


2. We need to describe risk in terms of the business objectives. Instead of just saying “We might get hacked,” we should explain the financial cost of a data breach or the destruction or manipulation of our data.

3. Finally, we need to present the information well and at the management level. I know that is a strength of the MSIA program at Norwich. I think every security person needs to read The Exceptional Presenter: A Proven Formula to Open Up and Own the Room <http://www.amazon.com/Exceptional-Presenter-Proven-Formula-Open/dp/1929774443/> by Timothy J. Koegel and The Cognitive Style of PowerPoint: Pitching Out Corrupts Within by Edward R. Tufte <http://www.amazon.com/Cognitive-Style-PowerPoint-Pitching-Corrupts/dp/0961392169/> once every 18 months or so and struggle to apply that information to our lives.

DG: As we move toward cloud computing<http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031> do you see these risks increasing?

SN: Somebody could write a very effective worm for instance and it could go through and wipe out all the data on a hosted drive. We have rarely ever faced anything that destructive so far. But earlier this year there was an attack that broke into Vaserve <http://www.vaserv.com/> and deleted 100,000 Websites of which half didn’t have backups so they are gone forever. I think this is a big illustration of the level of risk we are facing. What I find amazing is people rushing into cloud computing without evaluating the risks. The level of risk taking could actually exceed what the banks did with sub-prime mortgages.

DG: Any final thoughts on helping information security professionals think about the broader business and organizational issues?

SN: Let me leave you with one more thought. The department of defense several years ago issued a directive called DOD8570.<http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf> The directive said that if you’re working in IT and IT security, your people have to get a certification that includes leadership. Students certifying for DOD8570 take my course in IT leadership and security. I think it’s a huge indicator of how importance this is that the DOD says “We want the managers to have a leadership course that is devoted to security issues.” There are some signs that people are realizing that security can’t be all technical.

DG: Thanks for your insight into information security, strategy, and leadership.

***
David Greer <mailto:david@davidgreer.ca> has a background in software engineering and specializes in launching and growing emerging companies. Stephen Northcutt <mailto:stephen@sans.edu> is President of the SANS Technology Institute and the author of many books and articles on security.

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 Stephen Northcutt, David Greer & 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.