

SELF EXPOSURE



Richard Bejtlich
A founder of TaoSecurity. He has authored or coauthored several security books, including *The Tao of Network Security Monitoring*

Where did you get your first PC from?

My first PC was a 1980-era Timex-Sinclair ZX-80. My dad paid \$100 for the build-it-yourself kit, but Sinclair sent us a fully-assembled model. My first IBM-compatible was a 386SX I bought at Radio Shack in 1993.

What was your first IT-related job?

I started my hands-on, technical security career as a Captain in the Air Force Computer Emergency Response Team, part of the Air Force Information Warfare Center and Air Intelligence Agency, in 1998.

Who is your IT guru and why?

I have three "Wise Men" whose opinions I respect greatly: Ross Anderson, Marcus Ranum, and Dan Geer. Gene Spafford would be the fourth. Robert "Bamm" Visscher helped mentor me and continues to do so.

What do you consider your greatest IT related success?

Any time I detect and eject a bad guy from a customer network, I consider it a win.

What are your plans for future?

I am Director of Incident Response (and detection) for General Electric, and I look forward to building the GE Computer Incident Response Team and corresponding capabilities.

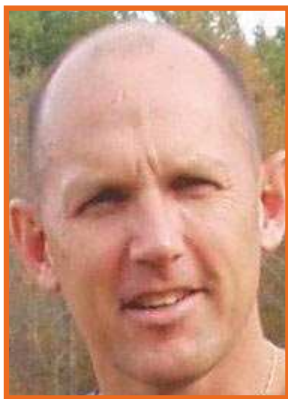
What advice do you have for the readers planning to look for a job on the IT Security field?

Here are seven ways you can make yourself more attractive to security-minded employers: represent yourself authentically, stop using Microsoft Windows as your primary desktop, attend meetings of local security group, read books and subscribe to free magazines, create a home lab, familiarize yourself with open source security tools, practice security wherever you are, and leverage that experience. For more detailed answer, please, visit this blog post:

<http://taosecurity.blogspot.com/2006/12/starting-out-in-digital-security.html>

What OS do you use and why?

I am a big FreeBSD fan!



Harlan Carvey
A computer forensics author, researcher and practitioner. He has written several books and tools focusing on Windows systems and incident response.

Where did you get your first PC from?

My first PC was a Timex-Sinclair 1000, and I wrote programs in BASIC and saved them to a tape recorder. I later programmed in BASIC on an Apple IIe, and then Pascal on TRS-80s and an Epson QX-10.

What was your first IT-related job?

I've been interested in computers for a while, but the first job that I had that was directly related to IT was setting up and managing my own lab in graduate school. I had set it up for my thesis work, as well as for use as a demonstration piece for basic networking courses.

Who is your IT guru and why?

I have several folks I look up to... for example, the ultimate hacker, Steve Wozniak. Also, Jesse Kornblum and Rob Lee.

What do you consider your greatest IT related success?

My book, *Windows Forensic Analysis*. This book is the kind of book that I've been looking for, and I can only hope that others find it useful.

What are your plans for future?

To contribute to the computer forensics community, specifically with regards to incident

response and forensic analysis of Windows systems. I would like to do this through a variety of media and forums, such as books, articles, seminars, training, conferences, etc.

What advice do you have for the readers planning to look for a job on the IT Security field?

Do not wait for someone to hand you something. Dig, think critically, and ask questions...but do so intelligently.

What OS do you use and why?

I use it for several reasons. The first of which is that's what most of the customers that I deal with use. I am not averse to Linux, and will use a variant or distribution as necessary, but for research purposes, there are far too few people doing any real work in the area of Windows (as compared to *nix), and yet in every position I've been in, the predominant OS in use is Windows. Another perspective is that a great many folks in the forensic analysis community use nothing more than EnCase, running on Windows. In attempting to educate them in "going deeper" into forensic analysis, it would be impossible to have them install Linux. Instead, I write tools and scripts that run on the platform they are using.