Herding Cats:
Spy vs. Spy

September 2012

BrandenWilliams
SECURE BUSINESS GROWTH

The theme for this issue is the History of Infosec, and while it is a broad topic that invited tons of great articles this month, I find that it is incredibly timely as I sense a shift in the functions and behaviors of security professionals. If you all would, for a moment, indulge me a bit and hop into the Way Back Machine with me. Don't worry about the missing seat belts and cracked CRT monitors, it's totally safe.

When I got my start into information security (mid 1990s), I had already been a Unix system administrator, network administrator, and software developer. Security became something I did out of necessity. I had to protect the root account, lock down access to the console (vty or not), and ensure I didn't build buggy software. I realized very early on that carbon-based life forms are both insanely beautiful creations and catastrophically destructive meanies. Anyone who has parented a three-year old will confirm this. As grown-up three-year olds, adults enter information wrong, they flip switches and buttons that say "Do not touch," and they always blame the system for the failure (because it's never their fault). We had to use security controls to protect users from themselves and keep the systems running. Good admins knew that they had to understand and manage security in order to keep their jobs. It was just part of the routine.

Then things started to change. Information security started to become legitimate as more of our business depended on technology to function. Some companies were lucky enough to have a person whose sole job was information security! We started to see tools beyond the basic anti-virus pop up, and even leverage some of these new technologies to deliver services. The web wasn't only for ordering books and pizzas anymore!

Then compliance came along, more accurately described as a mechanism to track and enforce adherence to defined standards[1]. Some of this came from the collapse of Enron, Worldcom, and Tyco. While not directly related to IT, many of the processes that were now governed by Sarbanes-Oxley relied on IT systems to function. Security people started to split into two camps here: policy and compliance gals and hardcore hacker dudes. I was the latter and spent my time being a destructive, adult-sized three-year old electronically breaking things and helping companies put them back together better and stronger.

Then comes PCI DSS—something I became all too familiar with as I helped companies cope with this gnarly and over-reaching set of requirements. To date, there has been nothing quite like PCI DSS[2]; nothing that was so detailed, centrally maintained, and economically impacting. Successful information security folks changed their attitudes and behaviors a bit. Security people that learned how to work with the business to solve these issues became very valuable. Once the big problems were solved, these guys ended up getting folded into compliance or incident response.

Today we see security inside companies taking the form of policy makers, compliance managers, and incident responders. But this doesn't totally work either. This crew of folks, while serving a purpose, spends all of their time looking behind them. Sure, new compliance initiatives will come along, but by the time most of these folks are taking any real action to addressing them, they have been public for a while. They are looking behind, and not ahead to what is happening.

Where I believe information security is going next is a focus on defense and intelligence.

FOOTNOTES

[1] Yes, I'm laughing as I am typing this. Many compliance initiatives are based on extremely broad requirements that encourage debate among auditors.

[2] HiTRUST gets an honorable mention here.

Compliance and policy will be spun off into the larger governance function of the company, incident response will still remain critical but operationalized, and the really fun work will be in intelligence and defense. Security professionals will start to take an active role in looking ahead of themselves. Correlating things that happen within their control with intelligence fed into the company. They will make risk-based decisions, with the business, to adjust controls on the fly. They will actively hunt for bad guys hiding in their systems. They will look more like clandestine agents than computer geeks.

How can you not be excited about this coming shift? After all, isn't everyone's dream to be a spy?

About the Author:

Branden R. Williams, CISSP, CISM, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school junior. Now, a graduate of the University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004. Williams is sought after as both an speaker and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174

BLOG brandenwilliams.com

EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH