risk
solutions
international

Corby: After All These Years, It’s Still About the People

Posted on SecureWorld Post - January 31, 2012

You know you’re getting old when you start thinking about how things used to be, and for starters, I’ll give you that one. My days beating the 20-somethings in beach volleyball, running a marathon with little or no serious training and eating 2,500 calories per day without moving to the next hole in my belt are past, but for my initial reflection, I thought it would be a good topic to get you warmed up. Several reasons: First, the future is much harder to predict than the past. Second, there’s a wealth of anecdotal stories that form the core of our collective experiences. Third, occasionally, we can often apply lessons of the past to create a fairly successful program for the future.

Security technology has steadily improved, and the new generations of software and hardware have adapted to the hostile environment pretty well. Like their biological counterparts, the fittest have survived and the weakest have been incorporated into the bellies of their neighbors. Looking at the products that are available for intrusion management secure e-mail, file transfer, application integration, compliance response and disaster recovery, we’ve made remarkable progress. Some advances are made at the cost of machine cycles, increased memory, expanded disk space and super-speed of network bandwidth. Some are made by watching carefully how people work and providing tools to make them more productive.

The use of the available technology advances continue to fertilize the growth of products that do more, and do it faster and frequently. Looking at historic trends of these offerings, I see a zero-sum game. You get nothing for free, and the benefit of the advanced functionality in the world of security components is offset by the cost of acquiring new, improved, expanded infrastructure architectures. Like death and taxes (and a few other inarguables), we continue to see products get bigger, faster and more integrated.

Organizational belt-tightening of the past decade or so has fostered the need to provide fewer and fewer people with the tools to get more and more accomplished. To achieve this objective, what I see is a renewed attention to who is doing what, and when they are doing it. Years ago, there was an organization called the “Human Firewall Council”. The organization theory is that by teaching all employees, not just security professionals, to be vigilant, many nasty events could be prevented or responded to more quickly. For many, this goal of awareness has been attained. Data privacy, file protection, malware rejection, e-mail authentication are now expected in all business operations. These protections are not just the job of the folks in IT Security. Applications are being designed and developed to pay attention to protecting personal identifiable information, to create redundant file stores, and to do much of the authentication work that was once captured by error reports or worse, program failures.

For those with real security departments, the trend is to use more tools and fewer people. To be successful with this approach, each person must have a tight focus and “handoffs” need to be crisp and clean. For those with sole practitioners of security services, it’s about watching more data points, and doing it constantly. For those who have dissolved the security component completely, the trend is to put software and/or hardware expertise into the hands of a non-expert.

None of these solutions are easy. None are intuitively obvious. All require the proper knowledge of a cadre of focused, capable people. After all these years, it’s still all about the people.

Michael Corby, CISSP, CCP, CBCP PMP
Vice President
Risk Solutions International LLC
877-774-1900
www.rsi-llc.com