We All Work In Information Security Now

cio.com/article/2886325/we-all-work-in-information-security-now.html

About | The speed of business today demands that IT become ever more agile, resilient, secure, and innovative. CIOs need to stay abreast of developments in everything from cyber security to compliance require

Admiral Michael Rogers, the director of the National Security Agency, said he expects a major cyberattack. "It's only a matter of the 'when,' not the 'if,' that we are going to see something dramatic." Many other security experts would agree with him:

- John Masserini, the charismatic Chief Information Security Officer at Miami International Holdings, recently told a gathering of 200+ Chief Security Officers that, "Every day Chief Information Security Officers wake up and worry, 'Is today going to be THE Day?'"
- Steven Young, VP Security & Risk Management and CISO at Kellogg Company, is similarly candid when he explains, "Security never ends. It is a boxing match that goes on forever. It is just one big beating."
- Eddie Schwartz, the former Chief Security Officer at RSA, liked to open his talks about information security with a slide featuring one white pawn arrayed against all the black chess pieces.

With quotes and images like this in mind, I queried boards of directors, senior executives, CIOs, and line of business directors as to what they were thinking and doing about information security. I specifically asked if we would ever reach a point where someone knowledgeable about the threat landscape would be able to sleep at night. All agreed that the path to less worry involves not only shrinking the attack surface [infosec speak for giving the bad guys a smaller target] but broadening the defense team [i.e., engaging the entire enterprise in the security endeavor]. Let's take a look at that second point, because broadening the defense team involves you. And me. In fact, to put the matter bluntly, we all work in information security now.

Information Security is Everybody's Business Now

There was a time – not so long ago – when information security issues were perceived as being the sole purview of a small cadre of hyper-specialized über-geeks. This is no longer the case. Information security, if it is to be effective, has to be perceived by all – ALL employees – not as someone else's job or, worse, an activity that is standing in the way of them achieving their personal and institutional objectives.

Mark Connelly, the award-winning CISO at Thomson Reuters Corporation, has spun up at least three global security organizations in his career. One of the keys to success is demonstrating, first to key executives and then to the entire enterprise, that good security

"enables them to be successful." Masserini at Miami International Holdings says you know you have turned the corner on information security when executives start calling and asking, "We want to do this. What are the risks? Can you help us move forward?"

Invest Intelligently by Investing in People

Following the media frenzy associated with the Target and Home Depot breaches last year, projections indicate that annual security spending is growing at close to double digit rates, with expenditures associated with data loss prevention increasing three times as fast as general security spending. Karen Green, the CIO at Brooks Rehabilitation, says the question is not availability of investment, it is "What/where do we spend now versus six months from now, a year from now?"

In answer to that question, Eddie Schwartz believes that much of the money invested to date in the security space is being mis-spent. Schwartz is adamant that firewalls, intrusion detection, anti-virus – most of the things that traditional security people have historically invested in – "are completely worthless against nation-sponsored attacks, determined criminals, anonymous or determined insiders – COMPLETELY WORTHLESS."

Steven Young at Kellogg is an engineer. He loves architecture and has assembled an impressive and technically-sophisticated security team. That said, he is very focused on the human element: the behavioral element of information security. He told me, "I don't think there is a bad dollar you can spend in awareness and training. I really don't." The 30,000 employees at Kellogg are recognized as the first line of cyber-defense.

The official mission of the security organization at Kellogg is "partnering with the business to help them deliver their goals in a secure manner." Similarly, in 2010, Malcolm Harkins, Vice President of the Information Technology Group, Chief Information Security Officer, general manager of Information Risk and Security at Intel and author of *Managing Risk and Information Security*, changed the mission of Intel's security team to "Protect to Enable." Harkins explains that in the new world of information security, "rather than focusing primarily on locking down assets, the mission of the information security group must shift to enabling the business while applying a reasonable level of protection. To put it another way, we provide the protection that enables information to flow through the enterprise." Such protection can never take place apart from people.

When our distant ancestors left the trees for the savannah, they needed to develop a new set of survival skills to cope with their new environment. Modern workers have also entered a new environment: a totally digitized world. To ensure both safety and survival, we all have to recognize our personal responsibility for information security.

This article was originally published on Forbes.