Why Aren't We Secure?

By: Mark Cummings, Ph.D., Bill Yeack

Cybersecurity is a hot market. Ten thousand companies worldwide are selling cybersecurity products and services. Governments have agencies, special committees, and organizations dedicated to cybersecurity. And, each year, cybersecurity companies spend millions of dollars each at San Francisco's RSA Conference to capture a small piece of this market.

Despite this, barely a week goes by without another widely publicized cyber breach. Why? One thing seems clear: What we are doing isn't working—and doing more of it will not make things better.

Recently, a new nonprofit has been created to address this situation. Bace Cybersecurity Institute (BCI) seeks to be the catalyst that brings the industry together to create the safe world that we all want to live in. This article explains how we got here and how, with the help of organizations like BCI, we can make things better.

How We Got Here

For the last 75 years, we have been following the same pattern in development and deployment of information systems. When a new innovation emerges, it is quickly rushed to market. The rush is driven by financial pressures and a need to prove that people will buy the new product. New innovations face doubts because many that were technically successful died in the market. The language we use reflect these doubts, as common expressions reflect a perceived inability to predict adoption. One of the most telling is "Will the dogs eat the dog food?" Another is "Fail quickly." And finally, we have, "Move quick and break things."

In short, what happens is that we field a new system. It goes through a period of rapid adoption, reaches critical mass, and then we realize, "Oops, we have to find a way to manage this stuff." Then, we begin to apply management Band-Aids. About the time we can see the light at the end of the management tunnel, we realize, "Oops, we have to find a way to secure this stuff." As we start working on security, the next wave of innovation starts.

This process results in layers of technologies and generations of systems and products that are approximately three-quarters of the way through the management cycle and halfway through the security cycle. This already-difficult landscape is compounded by competitive pressures, including attempts to create vendor proprietary lock-in, attempts to control the market by standards manipulation, geopolitical forces, and so on. As a result, our information ecosystem is built of collections of these technology layers, generations and products. These interact with each other, creating compounding security vulnerabilities.

An example of this kind of interaction was the recent breach of a cellular network OSS (Operations Support System) and BSS (Business Support System) through a previously unexploited vulnerability in SS7 (Signaling System 7), an electronic switching protocol. SS7 was developed in 1975—before the Internet, the PC, the smartphone, the web, the Internet-connected baby monitor, the smart home, and so on. Yet there it is in the bowels of today's cellular infrastructure. Remember the story of the little Dutch boy who stuck his finger in the hole in the dike? The only difference here is that there are too many holes and not enough fingers.

What Needs to Change?

Clearly, the present approach has problems. Will the forces driving this two-thirds manageable, halfway secure ecosystem change?

Unfortunately, no. Deploy/Oops, Management/Oops, Security/Oops is baked in. First and maybe foremost, it is a result of basic human nature. And changing human nature is not an uphill climb, it is akin to climbing a sheer wall. Then, there is our financial system with its fundamental need to limit upfront investment until market adoption is proven. Add to this mix competitive and geopolitical forces. Finally, the frosting on this cake is the accelerating rate of change.

And there is no sign that things will slow down. When the early work on 3G prototypes was underway, it was surprising to run into someone who said that they were working on “beyond 3G.” Now, it is not surprising to hear people working on 6G long before 5G even starts deployment. Technological change is coming at us so fast that we almost don’t see it anymore. It takes something special to catch our attention, like the threat of social media being weaponized, the fear of autonomous vehicles being weaponized, or in-chip security vulnerabilities.

Through all of this pressure and fear, the same process continues. For example, the in-chip vulnerabilities in our current CPU’s (general purpose processors) and GPU’s (graphics and acceleration focused processors) are beginning to be understood, but one of the leading TPU (AI & neural network-focused processors) architects speaking at a private workshop was totally unprepared for a question on in-chip vulnerabilities in his new TPU. As AI technologies, generations and products are layered on top of our current ecosystem, it appears we can expect a repeat of Deploy/Oops, Management/Oops, Security/Oops that stretches into perpetuity.

A New Way Is Needed

No doubt you’ve heard the old adage: The definition of insanity is doing the same thing over and over again and expecting different results.

Back to those thousands of companies competing to capture a small piece of the security market via San Francisco’s RSA Conference: What they are doing is important. Without their efforts, things would be a lot worse, but they alone are not going to change the fundamental problem.

Government agencies are trying but they have fundamental limitations. Key among them is the emergence of government hacking and government-sanctioned pirate organizations engaging in cybercrime. The reality is that governments have divided loyalties. Another problem is the reluctance of corporations to report cybersecurity breaches for fear that releasing the information will hurt their businesses and their stock prices.

Rebecca (Becky) Bace, a leader in the security industry, argued that it will take a change in public perception, and she suggested we need a new book similar to *Unsafe at Any Speed* to energize public sentiment.

One of the key results of the publication of *Unsafe at Any Speed* was the creation of the United States NHTSA (National Highway Traffic Safety Administration). The NHTSA merely published statistics on deaths and injuries in US highway traffic accidents. The publication of this data provided both an incentive and a way to measure results that energized government, industry, and society at large to tackle the problem. Ultimately, the initiative resulted in a 95 percent decrease in the rate of accidental highway deaths.

You Get What You Measure

At the Spring 2019 RSA conference, the USA NIST (United States of America National Institute of Standards) reported on a study of cybersecurity metrics that it had recently

completed. The study had tabulated 1,500 different cybersecurity metrics. But the team felt that this was not enough. They recommended that each corporation create a task force to develop its own cybersecurity metrics.

In business, there is an old saying: “You get what you measure.” The corollary is that if you are not getting what you want, you are not measuring the right things. We are not getting what we want in cybersecurity, so we must not be measuring the right things. If we follow the NHTSA suggestion, one of the key questions is: *what exactly should we measure?*

A Path to a Solution

A group of highly experienced cybersecurity practitioners came together to discuss these problems in an annual, private, by-invitation-only workshop organized by Becky Bace. After Becky’s untimely death, the group started the Bace Cybersecurity Institute in her memory. BCI is a merger of some of the best public and private cybersecurity experts and focuses on realizing Becky’s vision of an information ecosystem that is safe and secure—safe and secure even in this emerging era of cyber blitzkrieg. It seeks to do this through research, technology transfer, education, and public policy. BCI doesn’t claim to have all the answers. But it is committed to asking the key questions.

BCI is seeking to be the catalyst that brings the industry together to create the safe world that we all want to live in. If it is successful, it will generate the kind of cooperation between government, industry, academia, and society in general that is needed to develop and implement the effective cybersecurity solutions we so desperately need.