Cybersecurity: So Much Time, So Little Progress

Dianna Booher, CEO, Booher Research Institute

As I read of the latest cyberattack, the worst in history, involving hospitals, shipping systems, and corporations in more than 150 countries, I see much hand-wringing. But the first thing that comes to my mind is the old mantra: "Fool me once, shame on you. Fool me twice, shame on me."

That's not to play "blame the victim" as so often happens with crime. It is to say that customers, employees, and investors have been victimized by their government and corporate leaders burying their collective heads in the sand and pretending the cybersecurity problem will somehow correct itself.

After 9/11/2001, America seemed shocked into the reality of believing there was indeed evil in the world—people who actually wanted to do America harm. Seeing our government leaders united—Republicans and Democrats alike standing together on the Capitol steps singing God Bless America —sparked hope that they would begin to take the cyber threat seriously and use all means necessary to identify and stop those using the internet to monitor, communicate, or plan to harm our citizenry.

So what happened?

Very little.

Seventeen years later, experts tell us that our electrical grids are still easily accessible for cyber terrorists, allowing power to be shut off to large regions and paralyze the country.

How about progress in healthcare?

In 2010, the Department of Health and Human Services released the final criteria defining "meaningful use" of electronic health records (EHRs). To get the 700,000 clinicians and 5000 acute care hospitals to comply, they enticed with $30 billion of incentives and the threat of reduced payments for failure to comply. The biggest concern about these records? Privacy and security. Those EHRs include Medicare data (that is, social security numbers), accessible to anyone in the hospital system.

That brings us to the unprecedented rise in identity theft. There are rules and regulations that force companies to disclose data breaches to their customers (stolen customer credit cards or private account information) "in the most expedient time possible and without unreasonable delay." They often do not tell customers—at least until months or years after the fact. Here's their out: They can delay to accommodate "the legitimate needs of law enforcement" during an ongoing investigation.

So what about cybersecurity at the government itself?

In 2013, National Security Agency subcontractor Edward Snowden downloaded the country's top secret domestic surveillance practices and dangled them in front of the government's nose—another huge warning of the country's inadequate protection.

Want to sign up for social security online, as the agency encourages you to do? Until just recently, if you were inclined to create an account on the government site, a message popped up on the screen: "Caution: This site is not secure."

So what action at the very highest levels of government suggest that cybersecurity is taken more seriously there?

The former director of the FBI, James Comey, has described our 2016 Democratic president candidate Hillary Clinton's handling of the nation's top secret classified information on her unsecured server as "extremely careless." And both the left and the right allege that the Russians have interfered with the 2016 presidential elections.

And while the government and social media companies debate the issues, ISIS still uses their platforms to recruit and train followers. To the chagrin of all parties, Wikileaks continues to release information that perplexes and angers politicians on both sides of the aisle.

It's about 17 years past time for Congress to stop their petty bickering and concentrate on protecting this country.

About the Author: *Dianna Booher, MA, CSP, CPAE, works with organizations to improve productivity through clear communication and with individuals to increase impact by a stronger executive presence. CEO of Booher Research Institute and founder of Booher Consultants, Inc., she's a prolific author of 46 books, published in 26 languages.*