IT Workers of the World Unite!

This article was originally published on Fox Business on January 7, 2015.

by Brian E. Finch

Brian E. Finch
Public Policy
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian E. Finch is a partner in Pillsbury's Public Policy practice in Washington, DC. He is a recognized authority on global security matters and is co-leader of the firm's Global Security practice.

CISOs and CIOs, this is your big your chance. Seize it.

The Sony Pictures data breach could well be a curse for many of you, but it is also a golden opportunity. You'll never again have such a great chance to call attention to your needs, much less your challenges.

Executives across the globe are paralyzed with fear that their companies will be next, so they will be turning to you, CISOs and CIOs, to figure out how to make them a less inviting target.

That means it is your opportunity to have your security wish list filled.

If I were you, I would be taking the following actions:

1. Organize!
Now more than ever, CISOs and CIOs need to be acting with a unified voice that can be heard, especially inside Washington, D.C. A mad scrum will soon break out between Congress and the White House over how to increase private sector information security. Proposals and counter-proposals will be thrown against the wall, and what sticks will likely be only half measures that have more potential to do harm than good.

CISOs and CIOs, you need a united voice in Washington. While there is already an organization for state government CIOs, nothing really exists for private sector CIOs or CISOs.

It's time to change that. Form a trade association, think tank, or whatever. Develop policy papers and talking points. Most importantly, get out and tell your story.

Why is organizing so critical? To be blunt, if you are not telling your side of the story, it likely isn't being told by anyone. CIOs and CISOs need their own voice in policy debates, and a trade association is one very easy way to do so. It will do an awful lot of good in educating the Washington community at large about what CIOs and CISOs go through on a daily basis and what they need to do their job successfully.

So get organized, fast.

2. Demand more aggressive action by the government to take the pressure off of you.
This is a big one. Every CISO and CIO knows that they are outgunned, bullied, pushed around, and shaken down by cyber criminals. The worst part is that no matter what you do to protect yourself, the hackers find a way to defeat your defenses. If this were the 1980s, you might have to call in Hannibal Smith and "The A-Team" to help you out.

There is an alternative, however. Remember, in all of this you are victims of crimes. And what should crime victims do? Go to the authorities and demand action. That's what CIOs and CISOs should be doing right now.

What you need is aggressive action by law enforcement, and even the military. The FBI, Secret Service and other agencies need to be out arresting hackers wherever they are. The military needs to be disrupting cyber-criminal operations across the globe, so they don't have the chance to reconnoiter endlessly until they find a weak spot.

This is where the CIO/CISO trade organization can play such a huge role. If enough of you gather together and say in a unified voice, "Enough!", Washington will listen. The hopeful result will be hackers who think twice before launching an attack.

3. Support and use the SAFETY Act so you cannot be second-guessed so easily.

The scourge of a CIO or CISO's existence is being second-guessed after a successful cyberattack. Already with the Sony attack there have been a number of articles accusing Sony of "sloppy" security practices or simply having inadequate defensive measures in place. Someone will say that "but for" that inadequacy/negligent behavior/mistake, the attack would not have succeeded.

Enough with that. Your job is hard enough without having to constantly look over your shoulder and endure public pronouncements from people who have no idea what really happened.

There's a relatively simple solution to this: get your work approved under the SAFETY Act. The SAFETY Act is a federal program that allows companies to ask the Department of Homeland Security (DHS) to review their cyber security programs. If DHS is presented with sufficient information, it will issue an award stating that the system is useful and effective against cyber or terrorist attacks.

What makes this better than seeking, say, an ISO type of certification is that the SAFETY Act award is 1) issued by the U.S. government and 2) comes with *liability protections*. That last point (obviously) is critical—instead of hoping that complying with a standard will insulate you from liability (and criticism), obtaining a SAFETY Act award can grant you a limit on damages or even immunity from lawsuits following a cyberattack.

You can even use your trade association to push for easier use of the SAFETY Act by having Congress clarify the law with the simple addition of a few words related to cyberattacks.

Think about it: legal defenses guaranteed under U.S. laws. Sounds pretty good, right? It does, so hop to it.

4. Don't let people scare you with talk about a "standard of care."

This is a pet peeve of mine. Lots of people, including some fellow bar members, are running around saying, "If you don't follow program X, you will not be meeting the existing standard of care and will expose your company to all sorts of lawsuits."

Blech. I hate those comments. They are tenuously supported at best, and distract CIOs and CISOs from things they really could be doing to protect themselves (like the aforementioned SAFETY Act).

These comments mostly come up in the context of encouraging companies to adopt the National Institute of Standards and Technologies Cybersecurity Framework. Many people, including a lot of lawyers, say if a company fails to "adopt" or "adhere" to the Framework, they've put themselves at significant risk of liability because the Framework is fast becoming the benchmark against which a company's cybersecurity posture will be measured.

Baloney.

The NIST Framework is nothing more than that, a framework. Don't get me wrong—it is an excellent document that companies should look to. But so much of it is so basic that it cannot possibly be considered a "standard of care." Moreover, NIST itself avoids using terms like "adoption" or "adherence" when it comes to the Framework. It does *not* view it as a compliance program, and thus neither should CISOs, CIOs, or even lawyers. So stop worrying about it already.

Life for CISOs and CIOs is hard enough. When things go right, no one really notices. When things go wrong, well let's just say bad things tend to happen to all involved.

The status quo is unacceptable. CISOs and CIOs need to find their voices, take proactive steps, and push back on those who would lay blame squarely at their feet.

The steps I laid out above are a good start. And they can be easily accomplished.

Go for it. You're good people.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | +1.877.323.4171