Using Words To Battle Cyber Losses

This article was originally published in the *Wall Street Journal*: *CIO Journal* on June 23, 2014.

by Brian E. Finch

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

Brian E. Finch (@BrianEFinch) is a partner at Pillsbury Winthrop Shaw Pittman LLP. He also is an adjunct professor at The George Washington University Law School, and can be reached at brian.finch@pillsburylaw.com.

Words matter when it comes to cybersecurity.

With security concerns dominating today's corporate planning from the Board on down, the CIO often comes in as a technical expert, providing an analysis of the threat environment and what measures should be taken to prevent successful cyberattacks. And of course, the CIO is there to explain what happened when the inevitable successful attack happens. However, CIOs can do much more—and better protect the corporate bottom line–with just a little thought and some assistance from their lawyers. By using some careful contract language developed in collaboration with counsel and contract administrators, CIOs can be in a prime position to shift liability away from their company in the event of a successful cyberattack.

Let's start with a fundamental premise: when entering into a contract, the terms and conditions of the contract should be clearly spelled out, which each party's responsibilities clearly defined. That's something every first year law student is taught, and every good business executive knows by instinct.

Take for instance a landlord negotiating a lease for a commercial tenant. The lease is not just "I will pay landlord X in rent per month for Y time period." Innumerable obligations are subject to negotiation and documentation in that lease: who provides common area maintenance and building security; who is responsible for utilities; what the expectations are for the condition of the building, and so on. That is Business 101.

Contracts for information technology and cyber security at their core are not fundamentally different. When a CIO is considering new information technologies purchases – specifically for cyber security or just "general" information technology – security has to be a core component of the decision making process. That includes reviewing the security characteristics of the products and services, as well as specifying in writing security expectations regarding obligations.

Such language can take any number of forms. For instance, when entering into a services agreement with a cloud security provider, a CIO should make sure the contract sets forth who is responsible for securing data in motion, data at rest, and what controls will be used to prevent the lateral spread of malware. Further, the obligations should be couched in specific language, not broad statements. References to "industry

best practices" or "reasonable efforts" are insufficient as they are too vague to do any good. If nothing else, they will lead to expensive litigation to determine what exactly they mean.

Avoiding that battle can be accomplished more easily by setting forth specific benchmarks and obligations in contract language. For instance, references to objective standards such as the SANS Top 20 controls should be specifically included in the contract.

Specific language should also be used when contracting with third parties who will have access to a company's network. The obvious example here is the recent Target Corp. data breach, which apparently was conducted via a HVAC contractor with unsecured access to Target's systems.

CIOs need to spell out specific security requirements in such contracts. Even though they may seem generally unrelated to cyber security, experience demonstrates otherwise. A good example here then would be a requirement that the contractor with access to a company's IT system must use behavior-based malware detection systems such as those spelled out in NIST Special Publication 800.53 Revision 4 (SC-44, calling for the use of "detonation chambers.") Using such language, companies will have a much firmer grasp of what their contractors are or should be doing to help mitigate cyberattacks.

Critically, the failure of a company to adhere to the language of the contract will create a much simpler argument for liability post-event. Obviously the goal of such language is to prevent cyberattacks, but we are all aware that successful attacks are inevitable. With specific requirements set in place, it will be much easier to determine whether a contractor failed to honor their security obligations.

In a similar vein, CIOs should incorporate into any security-related contract that the vendor must either hold or pursue liability protections under the SAFETY Act. The SAFETY Act is a safe harbor law administered by the Department of Homeland Security, with the aim of providing liability protections to companies that offer cyber security and anti-terrorism products and services. In addition to the liability protections granted to a company's specific product or service, the SAFETY Act also precludes certain claims from being asserted against the buyers of those items.

Stated another way, if a CIO purchases a cybersecurity technology or service that has SAFETY Act protections, the company will then be able to be immediately dismissed from lawsuits alleging that they negligently selected those items or that they did not work as intended. That's a very powerful offering indeed.

The benefits from buying SAFETY Act protected items are many, including the comfort of buying items that have been vetted by the Department of Homeland Security and possible decreases in risk management cost. This is also a situation where the CIO can work closely with the general counsel's office and risk manager to truly integrate technology purchases into the overall risk management program for the company.

Lest you think using careful language in contract vehicles will have only a minimal impact on security, recent experience demonstrates otherwise. The U.S. Navy suffered in 2013 one of its most devastating cyberattacks at the hands of Iranian-aligned hackers. The cyberattack worked its way into the Navy Marine Corps Intranet system, burying itself deeply into the infrastructure. It took several months of concerned, expensive efforts to fully root out the malware. How did this attack succeed? Well, according to the *Wall Street Journal's* Siobhan Gorman, it was because of a poorly written Navy contract for the Intranet. As Ms. Gorman noted, the Navy's contract did not require the vendor "to provide specific security for a set of Navy Department databases, and as a result, no one regularly maintained security for them." That is about as clear an example as one can provide with respect to poor contracting leading to serious cyberattacks.

CIOs have a real opportunity to be a value-additive part of corporate management. Instead of simply designing or implementing security plans, CIOs can use contract language to better protect the financial health of their enterprise. Being stewards of the company's value is an excellent way to show that security is not merely a cost center, but rather a key part of the company's overall financial health.