CIOs Spur Revenue Generation Through Smart Cybersecurity

This article was originally published in *The Wall Street Journal's* CIO Journal on September 11, 2014.

by Brian E. Finch

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

Brian E. Finch is a partner in Pillsbury's Washington, DC office. His practice focuses on counseling on regulatory and government affairs issues involving the Department of Homeland Security, Congress, the Department of Defense, and other federal agencies.

Today as companies increasingly realize the value of strong cybersecurity, those CIOs who successfully implement an effective cybersecurity system should be viewed as a critical part of the revenue generation effort. An effective CIO who maintains a robust cyber risk management program will not only help ensure efficient operations, but will also play a role in crossing cybersecurity thresholds established by customers that would otherwise serve as a barrier to entry.

The shift from regarding cybersecurity–and the people responsible for implementing it–as a "tax," to something that can further the business comes after some hard lessons. The value of intellectual property stolen by cyber espionage is measured today in billions of dollars. Meanwhile, operational disruptions caused by other malicious cyber events have managed to cripple productivity and harm relationships with customers.

The real game change for many CIOs is the emerging movement to consider a company's cybersecurity posture when making procurement decisions. To put it bluntly, companies with weaker cybersecurity are increasingly being viewed as less attractive vendors.

This is not a trend that is going away – in fact it is only going to accelerate. The federal government, somewhat surprisingly, has taken a strong lead in this area. It issued a **report** earlier this year calling for a fundamental reform to procurement, under which cybersecurity would be a baseline consideration in awarding and managing contracts. Emile Monette, a General Services Administration official who played a key role in crafting the recommendations, has **commented** that federal employees in the acquisition lifecycle must consider cybersecurity capabilities and needs when reviewing procurement requirements.

Already companies that have suffered successful cyberattacks are finding themselves cut off from revenue streams. Just ask USIS, which performs background investigations for the U.S. government. USIS recently suffered a serious data breach, resulting in the personal information of tens of thousands of government employees being compromised. The response from its federal customers, the Department of Homeland Security and the Office of Personnel and Management , was swift: it was issued "stop-work" orders. And "stop-work" means no money coming in from either DHS or OPM. Worse yet, OPM announced earlier this week that it

was not renewing its background check contract with USIS.

Not good for the bottom line.

In this climate, a CIO who properly manages security as well as expectations, can and will be viewed as an essential contributor to business generation – indeed one on par with other C-suite officers such as the COO and the General Counsel.

Below are some thoughts on how a CIO can perform his/her task in a way that fosters this notion of their position being a "value add:"

Manage expectations, especially upwards: Companies are comfortable with the notion of an Enterprise Risk *Manager*, someone whose job it is to minimize losses. But when it comes to cybersecurity, leadership often expects the CIO to be a risk*eliminator*. Whether through accidents, benign neglect, or a simple mismatch of resources, companies will at some point suffer a successful cyber breach.

Still, many C-suite officers, as well as directors, are misinformed and believe that the cyber threat problem can be "solved" through a magical combination of money and technology.

The first requirement for an effective CIO is brutal honesty, meaning that they must properly manage expectations up the chain of command. This means bluntly telling senior leaders that successful attacks will occur, and that the company needs to focus significantly more resources on recovery and mitigation than one might expect.

Emphasize process over technology: People can too easily think that the latest and "greatest" widget will fix their security gaps. When it comes to cybersecurity, that simply is not true. So much malware is being created daily that now cyber criminals can use it just once or twice before moving on to the next piece. That kind of unlimited ammunition does not bode well for any company's security posture, especially in light of all the other cyberattack entry points (USB drives, insider threats, counterfeit parts with preloaded malware, etc.).

In practical terms, an effective CIO needs to focus more on the process of security than the actual systems deployed. CIOs need to develop continuous improvement cycles that allow for rapid integration of threat information, near real-time response to threats, and the ability to adjust defenses and response protocols quickly to adapt to the quick advances being made in cyber-attacks. Focusing on the process of security will demonstrate to customers and shareholders that the company can adapt to meet emerging threats.

Enable a positive record: Inevitably following successful cyberattacks will be an avalanche of lawsuits. The plaintiffs could be anyone from injured customers, third parties, business partners, and even shareholders. Every one of them will argue that the company's cybersecurity plans and procedures were at best inadequate, at worst grossly negligent.

This is where the CIO can make an extraordinary contribution to the health of the company. Part of a good cybersecurity program is demonstrating that the defenses erected logically relate the threats faced. A company could go bankrupt when spending on cybersecurity yet still suffer a serious breach. So it is the job of the CIO to work closely with management, especially the general counsel, to break down what the threats look like and where the company would be better off focusing on detecting a successful penetration and stopping it before it causes serious harm, versus just blocking all attacks.

As part of that duty, a record demonstrating the thought process leading to specific security decisions will be absolutely critical. A company is going to be in a much better position if it can show a rational basis for security decisions versus one that appears ad hoc and disjointed. This means working with the general counsel and risk manager to structure security contracts to take advantage of insurance policies, the SAFETY Act, and other key risk management tools.

Going forward, the CIO can and should play an integral part of any company's management program as they will play a key part in burnishing the profile and attractiveness of a company. Their decisions will also be vital in determining whether litigation following the inevitable cyber-attack will be relatively quickly and painless or expensive and protracted.

So make room at the big kids table for the CIO – they have earned their place there.