Cyber Threats Necessitate A New Governance Model

To protect ourselves and the businesses we oversee, the way we govern absolutely must change. By Gerald M. Czarnecki

Gerald M. Czarnecki is the independent chair of MAM Software Group, chair of the audit committee of Jack Cooper Transport Co.; chair and CEO of the National Leadership Institute; and chair and CEO of the Deltennium Group, consultants on business management issues. He can be reached at gmc@deltennium.com.

Conventional wisdom holds that threats to information technology and data security need to be managed by the corporate risk management process. While cyber security is viewed as a serious threat, it is routinely and appropriately managed by the enterprise risk management (ERM) function as simply another business risk. But, that is also true about financial controls and the integrity of the financial accounting systems. So if that is the case, why do we waste time having a separate audit committee of the board dedicated to oversight of those risks? The answer is quite simple: We have concluded that the risks are simply too important, and too complex to be left to the general risk oversight by the board.

Today, conventional wisdom also holds that your organization has already been attacked and the damage may be incalculable. My view is that technology and cybersecurity risks are the most significant existential threats facing business today. These risks call out for a much higher degree of focus by a careful mix of general management and technical personnel, not unlike what we do for financial controls. They require the same type of commitment as we have made to financial controls.

Boards Unprepared

What are the lessons here? Boards have learned to delegate key issues to committees charged with oversight of the complex or technical areas of audit, compensation, and even governance. These all qualify as critical oversight responsibilities, where highly technical expertise is required.

Other oversight roles in strategy, marketing and sales, customer service operations, even operational monitoring are also generally normal business activities, where most boards have core competences stemming from their professional lives. Most boards feel competent to review and monitor these important activities.

On the other hand, how many boards are actually competent enough to review and approve information technology (IT) issues? How many firms have operations that are not connected to the technology deployed? There are very few firms in the market where IT is a sidebar to the business. Quite often, IT is at the core of the business model. If it is not at the core, it is very high on the risk profile of the enterprise.

Seldom today will you find a board that is not challenged by IT threats. They may be as simple as inadequate resources committed to aging, legacy technology that requires updating to the most serious “threat actor” penetrations that damage core, non-public customer data. Worse still could be the ability of a “threat actor” penetration that legitimately closes down the company operations. These operational threats could destroy databases entirely; disable the networks used to communicate within the company; enable physical access to facilities by disabling all security systems; destroy the operating systems that process routine transactions or even shut down an operational system by infiltrating the power grid. In short, the risk of unauthorized and malicious penetration is huge, and the challenge of managing it is even greater.

Management is not immune and faces huge challenges in protecting against these penetrations, and determining how it responds when a serious breach occurs. The entire company can be at risk by virtue of a simple intervention by malicious hackers, by serious intentional destruction by thieves, or even malware deposited and designed to destroy companies that could be planted by adversarial nation states. In short, even the best management teams are struggling to staff these functions. The board oversight function is seriously weak in its ability to review, monitor, and govern these risks.

So what can a board do to exercise its oversight over technology risk and data security? The current model is that the board as a whole, or the audit committee, or even the risk committee will have general oversight over these challenges.

A New Model

The simple fact is virtually every board today is seeking help in this area. The first perceived “fix” is to attempt to recruit board members with technology backgrounds who can bring their technical experience to the board. The further truth is that as boards seek this talent, they also discover that the average “technically qualified” board prospect may have very little general management or board exposure or experience. It sounds great to search for chief information officers (CIOs) who can become board members, but most are preoccupied with their own corporate risks, and few have had the experience in board governance. The search should go on, but even with that core technology background, most boards still have a gap in their ability to both comprehend the issues and accomplish meaningful oversight.

This lack of technical expertise is precisely what caused the audit functions of many organizations to be too weak to prevent many of the pre-Sarbanes-Oxley crises faced by corporate America. Much to the chagrin of many, it actually took federal legislation to force boards to look at the audit function with a different and more technical perspective. Audit committees of public companies today are expected to have at least one “financial expert” and the relationship between the audit committee and the internal audit function clearly made mandatory the direct reporting of that person to the audit committee. Further, the external auditor in essentially all cases today, public or private, is a direct report to the audit committee. The sense of independence of these two roles has created an unambiguous independence on their part, and they each act in consort with the needs of the audit committee. In a similar way, the compensation committee has found itself reliant on independent expertise to support the very technical aspects of executive compensation.

> There is so much risk in managing data security that that the chief information security officer in many ways holds the keys to the crown jewels of the company.

That leads us to this highly technical area of technology. If the aforementioned independence and technical support are considered appropriate for internal financial controls, then why not for the core technology that drives not just the financial accounting and reporting, but drives, even controls, all of operations? Long gone are the days when we called this function “systems and data processing.” The CIO, the chief technology officer, or however the role is described, is no longer just processing widgets in the organization. That person now has management oversight of the intellectual capital of the enterprise and the technology used today is dramatically different and substantially more complex than anything envisioned two decades ago. As IT has become more complicated and networked so has the board's need to provide oversight. Further, there is so much risk in managing data security that the chief information security officer (CISO) in many ways holds the keys to the crown jewels of the company. With all of this, the board has no real place to turn.

What Now?

What is needed is a fourth standing committee in every public and private company. In addition to audit, compensation, and nominating and governance, my view is that a fourth committee devoted to data and technology is required. This committee should be staffed with operationally based board members, at least one of which can be designated a technology expert. The CIO and the CISO must report to the data and technology committee. It must have an outside technical support advisor who is qualified to provide IT and information security reviews and audits.

In short, this committee needs the same type of independent support from outside advisors as the audit and compensation committees have today.

This new committee must be charged with all the same types of auditing, testing, verification, review, and validation processes that the current audit committees have over the system of internal controls. This committee must be able to look to the external advisor to assure itself that the project management and information systems architecture will support the strategies of the company, and that the information and data security processes are robust enough to maximize the protection against data breaches and threat actor penetrations. It must also be in a position to audit the data security programs, validate the effective use of data security tools, and evaluate data breach response plans as well as the ability of executive management to execute them.