LocalTechWire.com
Real Reporting in Real Time.

Cybersecurity and Corporate Governance: A Growing Convergence

By John Yates and Rod Nydam, Special To LTW

Editor's note: John C. Yates chairs the Technology Group and Rod Nydam is in the Corporate Technology Group of the law firm Morris, Manning & Martin, LLP.

ATLANTA - Cybersecurity is a concern for every business with a computer and Internet access. Cybersecurity threats pose increasingly complex and expensive problems for private industry.

How should technology businesses address the cybersecurity challenges, especially from the standpoint of corporate governance?

From a legal perspective, there are guidelines for certain industries through laws such as HIPPA, Sarbanes-Oxley and Graham-Leach-Bliley. But best practices and security standards for much of private industry are still being developed. Private industry through partnership with the government is in the process of developing recommendations for addressing cybersecurity and corporate governance oversight.

Given liabilities and costs that can arise from a cyber attack, companies of all sizes are well advised to consider ways to protect their assets, customer and employee information from these attacks.
Corporate governance can play an important role in this protection. Companies should reconsider the structure of their Board of Directors, management team reporting mechanisms, budgets and daily operations in light of cybersecurity concerns.

There are several unanswered questions regarding corporate governance in cybersecurity. Unfortunately, there are no clear answers to these questions, but several private organizations are attempting to address them through initiatives with government agencies such as the Department of Homeland Security.

Some of the key questions to be addressed in this area include:

Should reporting requirements within a company be changed to address cybersecurity risks? In other words, should cybersecurity issues and responsibilities be elevated within the corporate organization? To address these issues, many companies are adding a Chief Security Officer (CSO) or other similar corporate executive. This executive officer may be responsible for:

- Developing and implementing a plan to protect the company from cyber attack.
- Educating the work force on cybersecurity threats.
- Developing systems for preventing cybersecurity breaches.

- Establishing backup plans for the contingency of a breach of security and adverse impact on the business.

Quite often, the CSO faces challenges within the company in measuring success or failure. The security executive's job may be perceived as a cost rather than a revenue producing division. Part of cybersecurity awareness and success is to assist the CSO in carrying out his mission. Also, the success of the position may depend on the security executive finding allies within the company - the CEO, CFO and General Counsel.

What about private companies that have small executive teams and are unlikely to appoint a CSO? These companies should allocate the responsibilities otherwise handled by a CSO to other officers in the company. The CFO or IT Director will be the most likely candidate to assume these duties.

What's the role of the Board of Directors? The Board should clarify the scope of authority and responsibility of the CSO or other designated security officer. The Board should also establish the chain of command in addressing cybersecurity threats. This may require the allocation of responsibilities to various Board committees with regard to these issues.

What's the role of the Compensation Committee? The Compensation Committee needs to determine the performance guidelines for measuring the success or failure of the CSO. This is a tricky task because success for the CSO is often defined as "nothing bad happening." The Committee should consider other measures of success:

- The number of times the system has been attacked and thwarted

- How well the system recovers from an attack or how the cost of an attack is minimized

- A measurement comparing your company with a peer group relative to cyber attacks.

- The controlling of costs with regard to building the infrastructure for preventing cyber attacks.

In any case, the performance criteria should be established by the Compensation Committee and measured for compliance on an ongoing basis (rather than once a year).

What's the role of the Audit Committee? The Audit Committee should play a more strategic role in approving the company's cybersecurity program. The Audit Committee should confer with senior management and the CSO to confirm that the industry standards for security are being met.

In high risk businesses such as financial services or transaction processing, the Audit Committee will need to exercise even greater vigilance. The Audit Committee should consult with the auditors to determine the scope of audit review and the need to conduct a special examination of controls and procedures used by the company.

When will guidance be provided on corporate governance protections in the cybersecurity area? If your industry is outside of the scope of current legislation, there are no clear guidelines

for implementing a cybersecurity program or corporate governance steps to monitor compliance. However, there are several places to look for guidance. In some respects, these are evolving standards and parallel the standards of legal care generally required in other industries.

For example, in 1890 a bank would probably be considered to have adequate physical security if it merely had a large safe in a back room of a wooden frame building. Of course, today, such "security" would be considered woefully inadequate if not negligent. The same is true with cybersecurity. It's just that the standards will be much more complex and evolve much quicker.

There are already several possible sources of guidance for determining standards of care in cybersecurity:

- Private industry groups and government agencies – Many private industry and government agencies are working together to address this important issue since it affects both our economic and physical security. Over the next several months, many public-private partnership groups will be proposing best security practices and corporate governance recommendations to implement those practices.

- Case Law – We expect major court cases to be decided in the next few years that will define the standard of care for a company to exercise in cybersecurity. It may be years and dozens of court cases before a practical set of rules are promulgated to serve as the standard of care in this area. However, it is likely that such cases will look toward existing government regulations and private industry standards in determining the standard of care.

- Security Consultants – Until these standards have evolved, you may want to consider retaining the services of a qualified computer consultant to serve as your cyber expert to address security concerns.

Cybersecurity will become an increasingly important issue for businesses of all sizes. The legal standards will be evolving over time and may take years to be widely adopted as best practices. Those companies paying the most attention to the threat of cybersecurity will be less likely to be taken by surprise and may be able to avoid unexpected liabilities.

John C. Yates chairs the Technology Group of the law firm Morris, Manning & Martin, LLP, which has offices in Atlanta, Charlotte and Washington, D.C. He can be reached at jcy@mmmlaw.com and (404) 504-5444.

Rod Nydam is in the Corporate Technology Group of the law firm Morris, Manning & Martin, LLP, in its Washington, D.C. office. He can be reached at rjn@mmmlaw.com and (202) 842-0217.