The Impact of Technology on Nonprofit Governance (and its Regulation)

Presented to:

2017 NAAG/NASCO Annual Conference
October 2, 2017
Washington, D.C.

Michael W. Peregrine
McDermott Will & Emery LLP
MPeregrine@mwe.com

© 2017 McDermott Will & Emery. The following legal entities are collectively referred to as “McDermott Will & Emery,” “McDermott” or “the Firm”: McDermott Will & Emery LLP, McDermott Will & Emery AARPI, McDermott Will & Emery Belgium LLP, McDermott Will & Emery Rechtsanwälte Steuerberater LLP, McDermott Will & Emery Studio Legale Associato and McDermott Will & Emery UK LLP. These entities coordinate their activities through service agreements. This communication may be considered attorney advertising. Previous results are not a guarantee of future outcome.
Goals and Objectives

To further the dialogue between the nonprofit sector and its regulators with respect to how technology affects the role and obligations of the governing board.
How We're Going to Get There

- Examples of how charity operations incorporate new technology
- Judicial standards of conduct associated with board oversight
- Relationship to board composition and structure
- What the insurers are saying
- What's on the horizon—digital technology and its application
Examples: Technology and Cyber Risk Impacting Charity Operations

- E-commerce initiatives
- Protected Health Information
- Other patient data
- Medical research
- Donor lists and related information
- Consumer credit information
Examples: Technology and Cyber Risk Impacting Charity Operations (cont'd)

- Use of social media to engage with constituents; survey initiatives
- Consolidated technology based system information platforms
- Direct fundraising and other solicitation activity
- Automation of internal functions (e.g., legal affairs, governance support)
- The need to invest in efficient technology and in "tech training"
Statutory and Regulatory Guidance on How Boards Execute Oversight

- Federal and state regulators (e.g., HHS/OCR; SEC; FTC, NYSDFS, FDA, NIAC, NAIC, NIST, FINRA)

- State laws and guidelines on private entity data security (e.g., health care data, financial or credit information, social security numbers)--see NCSL website for summary

- Industry specific guidance (e.g., HHS cyber security guidance materials for HIPAA covered entities and business associates)

- DOJ/FBI/DHS, and HHS/OCR, guidelines on protection from ransomware
The Most Recognized Cybersecurity Threats to Business Information

- Ransomware attacks (e.g., "WannaCry") or malicious malware disguised as ransomwear (e.g., "Not Petya")
- Insider compromise of business data
- Denial of service attacks
Directors' Duty of Oversight regarding Cybersecurity

Current perspective: the *Caremark* standard is applicable to directors' cybersecurity and related oversight responsibilities.

This, at least as to directors of public companies—as *Caremark* has yet to be meaningfully applied by courts in a nonprofit corporate governance context, under any type of circumstance (cybersecurity or otherwise).
Caremark addresses the "oversight" function of the director's core duty of care; i.e., the application of duty of care principles to the activity of the board in overseeing day-to-day business operations.

It speaks to the exercise of reasonable care to assure that corporate executives carry out their management responsibilities and comply with the law. In this context, it is often associated with compliance programs.
The decision, and its progeny, provides that a director has two principal obligations with respect to the oversight function—the duty in good faith to assure that:

1. a corporate information and reporting system exists, and
2. this reporting system works to provide the board with relevant information in a timely manner as a matter of ordinary operations.
The level of detail that is appropriate for such an information system is a matter of business judgment.

No rationally designed information and reporting system will remove the possibility that the corporation will violate applicable laws or otherwise fail to identify problematic risks.
Under these circumstances, the board's conscious failure to monitor the implementation of a such a reporting system could put the organization at risk and, under extraordinary circumstances, expose individual directors to personal liability for losses.

Yet, the historical standard for establishing Caremark liability is extremely high; e.g., a demonstration of bad faith.
Lessons from Recent Litigation

- *In re Home Depot, Inc. Shareholder Derivative Litigation* (11/30/16)
- *Target Corporation Shareholder Derivative Litigation* (1/24/14)
- *Wyndham Worldwide Corporation Derivative Litigation* (10/20/14)
Lessons from Recent Litigation (cont’d.)

The basic allegations made in these data breach related cases were that the directors breached their fiduciary duties and wasted corporate assets by failing to take reasonable steps to (a) maintain their customers’ personal and financial/credit information in a secure and protected manner; and (b) mitigate losses from a potential data breach.
Lessons from Recent Litigation (cont’d.)

Note the unwillingness of the *Home Depot* court to second guess the board's implementation of a reasonable monitoring system, even "though the Board's decision to upgrade [the] security at a leisurely pace was an unfortunate one...[its decisions on implementation] fell squarely within the discretion of the Board and under the protection of the business judgment rule."
While there has been little indication that the Delaware courts, at least, may back away from the strong deference to the business judgment rule within Caremark, it is reasonable to project a stricter approach to director liability in cases involving particularly egregious facts and circumstances, and substantial losses to corporations and to consumers.

This is especially the case in the nonprofit sector.
Supporting BJR Protection

- Board review of industry-specific guidance
- Advice of outside experts
- Restructuring of board composition
- Restructuring of board committees
- Integration within enterprise risk management processes
1. Balance the benefits of making Cybersecurity the responsibility of the board as a whole, with the utility of delegating Cybersecurity matters to a board committee composed of members with relevant experience.

2. Adding members with technology and Cybersecurity expertise (especially that which is industry-specific) to the board.
3. Assure the effective incorporation of Cybersecurity measures within the organization's enterprise risk function and appropriate coordination of committees and executives with Cybersecurity related roles and responsibilities.

4. As part of the ERM process, assure board clarity on the organization's most critical Cybersecurity threats/risks.
5. Establish a reporting system that provides information to the board or committee level on the frequency and types of Cybersecurity incidents experienced by the corporation, as well as providing education on relevant events.

6. Work with the CEO to confirm that there are CIT/CISO-type officers with appropriate credentials included within the executive suite and the adequacy of their respective budgets.

7. Monitor, through management, the cyber security training provided to organization employees.
8. Be familiar with the organization's Cybersecurity incident and response plan, and the ability of its crisis management plan to respond to the concerns of its various constituencies, as well as the regulators and the media.

9. Periodically inquire as to level of “cyber due diligence” performed by the organization with respect to its third-party service providers and vendors.

10. Confirm the availability and suffice of "cyber insurance" coverage available to address cyber-related risks and costs to both the organization and its officers and directors.
11. Assure that organization has established relationships with necessary third party vendors, e.g.,

- IT Forensics firms
- Law firm with cyber-breath experience
- Credit monitoring vendors

in advance of a catastrophic cybersecurity incident.
The Possible Impact of *Equifax* on Boards

- New calls for greater federal regulation (e.g., note government investigations).
- Increases focus on roles of boards as scale and impact of cyberattacks increase.
- Note recent recommendations from NACD on need for boards to:
  - Ask critical questions of CISO and other key management
  - Identify significant control deficiencies
  - Support a strong “security culture”
The Possible Impact of Equifax on Boards (cont’d)

- Relationship with existing CEO
- Underscores value of emergency succession plan
- Query whether certain events are so catastrophic such that “total accountability” is required.
What the Insurers are Saying

See, e.g., new recommendations from NACD and Marsh & McLennan:

- Directors and officers of major corporations include cybersecurity oversight liability coverage in their overall insurance coverage.

- Coverage should protect directors against oversight liability prosecution in the event of a cyber attack.

- “It is critical the D&O insurance coverage respond in the event of litigation alleging traditional claims for breach of fiduciary duties,” the report said.

- Boards should review the scope and availability of such coverage with their general counsel and insurance advisor.
Looking Beyond Cybersecurity

- An increasingly critical role of the governing board—understanding the role of digital technology in corporate operations, and being prepared for how that technology can disrupt the business model.

- Many nonprofit organizations are following the trend set by public companies, and are now examining the implications of digital technology for their business model, as well as the need to hire and retain executives and managers with the necessary skill sets.

- This places new stress on boards, as they need to familiarize themselves with digital themes.
What Are We Talking About?

PwC’s “Essential Eight” emerging technologies:

- Robotics
- Drones
- Internet of Things
- Artificial intelligence
What Are We Talking About? (cont’d)

▪ Augmented reality
▪ Virtual reality
▪ Blockchain
▪ 3D printing
The increasing existence of incredibly powerful back-office efficiency tools (e.g., artificial intelligence and machine learning applications)

The promise provided by a strong Information technology infrastructure (e.g., EHR systems)

The utilization of consumer IT by providers outside of their "official" IT systems

The expanded access, both in terms of geography and specialty, afforded by technology

The truly disruptive impact AI and other high-tech systems will have on certain service providers
And Then There is the Business Disruption “Angle”

- Amazon in all of its recent permutations (e.g., Whole Foods)
- Netflix
- Uber/Lyft
- The new Google/Walmart Partnership

How can the board add value to management in its consideration of the potential that technological disruption and transformation may affect the organization?
Almost 40% of the respondents to a recent NACD survey reported that technological disruption presents a significant risk oversight challenge for their governance structure.

Directors are finding it difficult to interpret the risks and opportunities offered by new technologies, given technology’s rapid pace of change.
Directors will thus need to focus on improving their technological literacy, with substantial help from management and outside advisors.

The expectation is that greater understanding of these changes will support directors in their efforts to better recognize the potential for emerging technologies to have transformative impact on organizational business models.
Key Factors for Regulatory Consideration

- The extent to which technology is affecting the operation and governance of the nonprofit charitable sector is both significant and unprecedented, and will continue to "play itself out" over the next several years, somewhat behind the pace that it is affecting the proprietary sector.

- Visionary executives and "crossover" board members will help drive this.
Technology related risks arise not only from the significant potential for threats to affect their business model, but also from issues relating to (i) recruitment and compensation of qualified security managers; (ii) the cost of outside advisors to support board efforts to maintain a "culture of security"; and (iii) the availability of corporate and D&O cybersecurity insurance coverage.
The board will need to identify a process by which it engages with expectations regarding digital technology and its potential application to the charity. This may be through a committee with delegated authority for technology matters.
The direct challenges to corporate governance include (i) the ability by which they can become sufficiently educated on cybersecurity, digital technology and related issues; (ii) the recruitment of board and committee members with matter and industry-specific knowledge to support the oversight and decision-making efforts; and (iii) their comfort level with D&O coverage.
From the perspective of board conduct, the key issue will be the level of engagement. Directors should become more focused on technology issues in order to properly exercise their fiduciary obligations. This will be important with respect to both the relationship of technology to the achievement of the charitable mission, and their actions relating to cybersecurity measures.
Perhaps the most important governance consideration is the need to balance vigilance as to both cyberthreats and technology based business disruption, with the potential advantages that technology offers to the effective pursuit of the charitable mission.