Information Technology Governance

by Bob Zukis

Corporate boards have been receiving regular warnings on cybersecurity and digital disruption for years now. Yet a follow-up question remains unanswered: What should they do about it? How should boards reshape their membership, structure and processes to properly oversee their new digital reality?

From Yahoo to Target to Equifax, and now Facebook, the data breaches that have occurred over the last several years have significantly raised cybersecurity risk awareness at the corporate board level. The Global Data Protection Regulation (GDPR) in Europe has also highlighted a growing regulatory landscape that is waking up public interest on data issues.

SEC Commissioner Robert E. Jackson Jr. has called the rising cyber threat "...the most pressing issue in corporate governance today."

Boards are also wrestling with the dynamic nature of technology driven disruptors that are altering the competitive landscape and changing industry dynamics. A Protiviti 2018 survey of global directors concerns summarizes their top risk issues as: "The rapid speed of disruptive innovations and new technologies within the industry may outpace the organization's ability to compete or manage risk appropriately."

Often referred to as "The Amazon Effect," the seismic ability for digital transformation to disrupt and alter foundational competitive and economic drivers is becoming a high priority boardroom issue.

Frank Modruson, former Accenture CIO who currently serves on two public company boards explains it this way:

"This rapid evolution of digital capabilities puts enormous pressure on businesses to keep up with new capabilities and to replace outdated ones. IT is also one of the largest G&A [general and administrative] budget line items for any business, and one that is often poorly understood by business leadership outside of IT.

"Add to this the fact that there is a skills and competency shortage of talent who knows how to transform both IT and the business through these new digital capabilities. Plus, the very real and expanding risk of cyber disruption creates an environment where companies have to continually transform alongside protecting what they have, while always being focused on being more efficient and effective.

"From a governance perspective, it creates a volatile risk situation that extends throughout the business with huge implications."

So now what? Directors are also starting to become aware of the disruptive impact that Amazon, and other digital natives have when they set their sights on a new industry. What do boards, and individual directors need to do next to make sure that digital transformation and cybersecurity risk oversight is a meaningful part of their contributions?

Digital governance is not a mature competency or practice in the U.S. corporate boardroom. Not one of the companies in the DJIA has a dedicated board level cybersecurity committee.

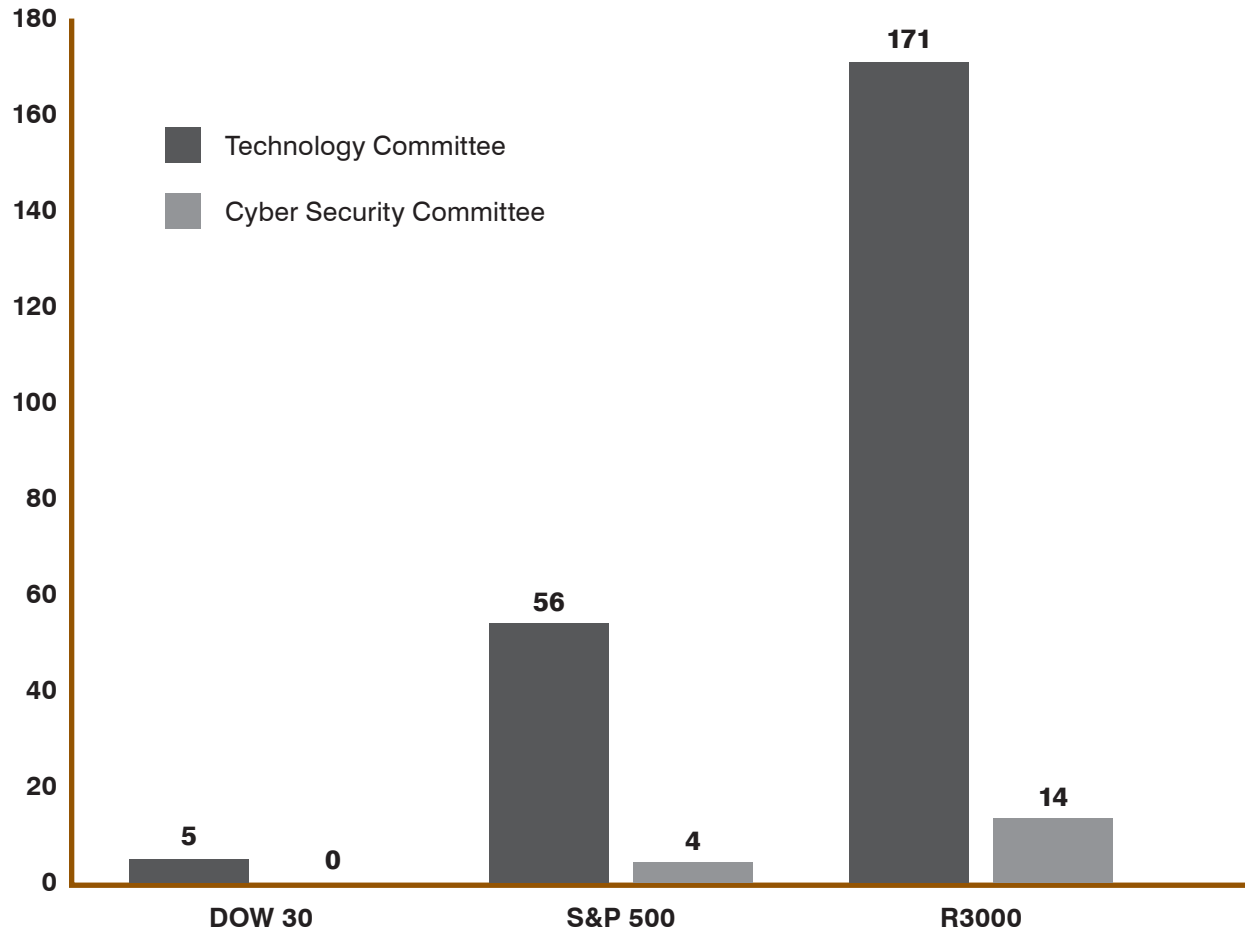
Awareness is a necessary first step, but has largely happened passively (except for the companies and boards that have unfortunately found themselves in crisis management mode as the result of a breach). Governing these issues is a new undertaking for most boards. The challenges include having the skills within the boardroom to understand these issues, organizing the board to manage its resources and time together, and executing a digital governance agenda for an unstable digital/cyber landscape.

Digital governance is not a mature competency or practice in the U.S. corporate boardroom. This is reflected in research conducted by public company

Bob Zukis *is chief executive officer of Digital Directors Network and a professor at the USC Marshall School of Business. [www.digitaldirectors.network]*

Few And Far Between

How Common Are Tech And Cyber Committees?



Source: MyLogIQ

intelligence firm MyLogIQ. They analyzed whether a boardroom technology or a cybersecurity committee exists for U.S. public companies as a starting point.

Based upon their data, this is currently an uncommon practice. Of the thirty companies in the DJIA, only five have dedicated technology committees, and not one has a focused cybersecurity committee.

The practice does not materially improve across the S&P 500 or Russell 3000, indicating that there is little distinction in digital governance maturity level regardless of company size. However, some companies have adopted the practice. The five companies in the DJIA with technology committees are American Express, J&J, Pfizer, P&G and Wal-Mart.

A remarkable 35 percent of the S&P500 make no mention of cybersecurity oversight in their disclosure documents.

These findings do not mean cybersecurity or technology oversight is an issue that corporate boards are ignoring. Rather, it identifies how they have organized themselves to govern these issues. According the MyLogIQ research, 42 percent of the S&P500 task their audit committees with cybersecurity oversight. Notably, Facebook tasks its audit committee with cybersecurity oversight. Still, a remarkable 35 percent of the S&P500 make no mention of cybersecurity oversight in their disclosure documents.

Tasking an audit committee with cybersecurity oversight, which may not have the necessary skills or time to focus on this complex issue, may limit the effectiveness of the cybersecurity oversight approach, as well as take time, focus and resources away from the significant responsibilities of an audit committee.

Robert Dixon is an Anthem and Build-A-Bear director, and former PepsiCo CIO and P&G executive. He was an early champion of boardroom digital diversity, and recalls:

"When I joined Anthem's board, they were looking for a qualified business-savvy, technology executive who could provide thought leadership on the board's governance agenda and management's technology agenda. Those skills normally come with significant experience leading large-scale enterprise-wide transformations, innovation programs and an appreciation for all of the related cultural and change management sensitivities.

"While growing in importance, critical factors for increasing digital diversity, either through more representation or a Tech Committee, include the role of technology for your business. Does technology define your brand's value proposition? Is technology at the core of your customer's experience? Is it a strategic, 'where to play' plank in the broader enterprise strategy?"

Board committees play a vital role in how boards perform their duties. Research conducted in 2016 by University of Pennsylvania and Harvard Professors Kevin Chu and Andy Wu shows that committees convey several specific benefits. These include knowledge specialization, greater task efficiency and greater accountability of the board to the firm. They note that most of the work that a board accomplishes is done at the committee level, and a secondary benefit is that they signal commitment and focus around an issue to all stakeholders, internal and external.

However, committees do come with a cost, primarily the cost of information segregation. This can be mitigated, though. A director who sits on multiple committees, such as an audit committee and a technology committee, allows knowledge and information to more easily be shared and distributed across the entire oversight agenda.

While committees play a significant role in the effectiveness of overall board oversight, they also play an important role to the companies and management teams they oversee. Chen and Wu note that committees are generally empowered to "...directly set firm policy, inform the board via informal knowledge sharing or formal reports, and propose actions to be executed by the full board." Moreover, committees work closely with firm management, thereby directly influencing the firm.

American boardroom committee structures gained a significant amount of standardization with the passing of Sarbanes-Oxley (SOX) in July 2002. After SOX, the audit committee, compensation committee and nominating and governance committee became the *de facto* baseline committee structure for U.S. listed companies. Beyond these three, however, structure varies greatly.

SOX also required boards to have an independent and qualified financial expert on their audit committee. This requirement was a first, and offers a lesson on qualified technology experts in the boardroom. A decade from now, most boards will have such deep digital and cybersecurity governance skills, and fully disclose this qualified expertise.

It took regulation to force qualified financial expertise into the U.S. boardrooms 16 years ago. Are we now at a similar point with the issue of digital oversight, and the need for qualified technology experts in the boardroom? Will regulators force this issue?

The proposed Cybersecurity Disclosure Act of 2017 (S. 536) would require U.S. public companies to disclose cybersecurity skills on their board. Despite languishing in Congress, it does signal regulatory attention on this issue. Former SEC Commissioner Luis Aguilar has cautioned, "[B]oards that choose to ignore or minimize the importance of cybersecurity oversight responsibility, do so at their own peril."

An SEC interpretive release on cybersecurity disclosure in February 2018 leads off with: "Cybersecurity risks pose grave threats to investors, our capital markets and country." The unmistakable regulatory trend is to assure transparency and corporate accountability on cybersecurity risk. This issue is squarely seen as in the public interest, which almost ensures

the inevitability of boardroom digital oversight. Policy will come, with or without corporate involvement.

"Whether or not you have a tech expert or a technology committee on the board, understanding the ramifications of technology is a full board responsibility."

Sheila Stamps, board member at Atlas Air Worldwide Holdings, Inc. and CIT Group Inc., observes: "Of late, there has been a significant emphasis placed on cyber security risk; and this is important. However, we must be both defensive and progressive. We must build defenses against cyber incursion while putting in place innovations to better serve end users.

"There is also an opportunity cost (or risk) that should not be overlooked. How information technology creates and shapes sustainable competitive advantage, its impact on industry dynamics and its role in profitability and growth are all emerging boardroom issues."

"Whether or not you have a tech expert or a technology committee on the board, understanding the ramifications of technology on your business is a full board responsibility," Stamps adds.

Effective digital governance starts with getting the right skills and competencies into the boardroom. From here, how boards organize themselves around technology and cybersecurity oversight and what they spend their time on drives the effectiveness of their oversight. Boards will naturally evolve their approach as they gain a greater understanding of these issues—or it will be forced upon them through regulation.

One suggested model is the creation of a dedicated board committee that addresses *both* technology and cybersecurity risk oversight. This would place a technology and cybersecurity committee alongside audit, compensation and nominating/governance committees in the standing U.S. public company committee structure. One committee focused on both technology transformation and cybersecurity risk can minimize information segregation costs as well as effectively govern the management and organizational issues and conflicts that can exist between CIO and CISO reporting lines.

Digital transformation and cybersecurity risk are two sides of the same coin. Both need to be represented in the corporate boardroom for a board to be sufficiently digitally diverse. Boardroom research indicates that the most important boardroom topics of the future are technology, cybersecurity and digital disruption—all ahead of strategy as a boardroom priority.

Survey data also indicates that information technology expertise is the most underrepresented boardroom skill. This gap almost ensures that cyber breaches will continue, and the benefits of technology innovation will go underrealized.

The scope of corporate digital governance oversight covers a very broad range of issues for any company. These include:

- Alignment of business strategy and IT with enterprise architecture.
- Business continuity and disaster recovery.
- Cybersecurity risk, insurance and D&O obligations.
- Cyberthreat intelligence.
- Data privacy and information lifecycle management.
- Device management.
- IT investment and strategy.
- IT service delivery.
- IT project prioritization, implementation and portfolio management.
- IT skills and capability management and organizational structure.
- IT hardware/software lifecycle management.
- New and emerging technologies.
- Regulatory policy advocacy and management.
- Social media monitoring and engagement.
- Third-party IT vendor and service risk management including business continuity.

The strategic and operational risks presented by the rapidly evolving IT environment create a daunting oversight environment. Corporate boards can and should address these issues themselves or regulators will force this issue if boards fail to do so. ■