SEPTEMBER, ISSUE 9

Thai Institute of Directors

CG NEWS UPDATE

FIVE PRINCIPLES FOR OVERSIGHT OF DIGITAL TRANSFORMATION

September 4, 2019 By Leslie Chacko, Stessy Mezeu, and Friso van der Oord

Automated retail kiosks, robotic processes, autonomous vehicles, and digital payments are all innovations shaping how the lives of consumers and workers are being streamlined. The economic value generated from these new digital solutions and business models, combined with the speed of their adoption, is staggering. In fact, the World Economic Forum estimates that the “combined value” of digitalization in every industry could generate upwards of $100 trillion over the next six years.

Given the near-term disruptive potential of new business models that are enabled by emerging technologies, many boards are actively reassessing their oversight role in governing digital transformation initiatives. As stewards of long-term value creation, boards will need to strengthen their oversight of digital transformation and emerging technologies.

Though directors are realizing that the current state of technology oversight at their companies may be insufficient to fulfil their fiduciary duties, they may also not know what a road forward should look like. Several challenges stand in the way of board readiness in this area, including:

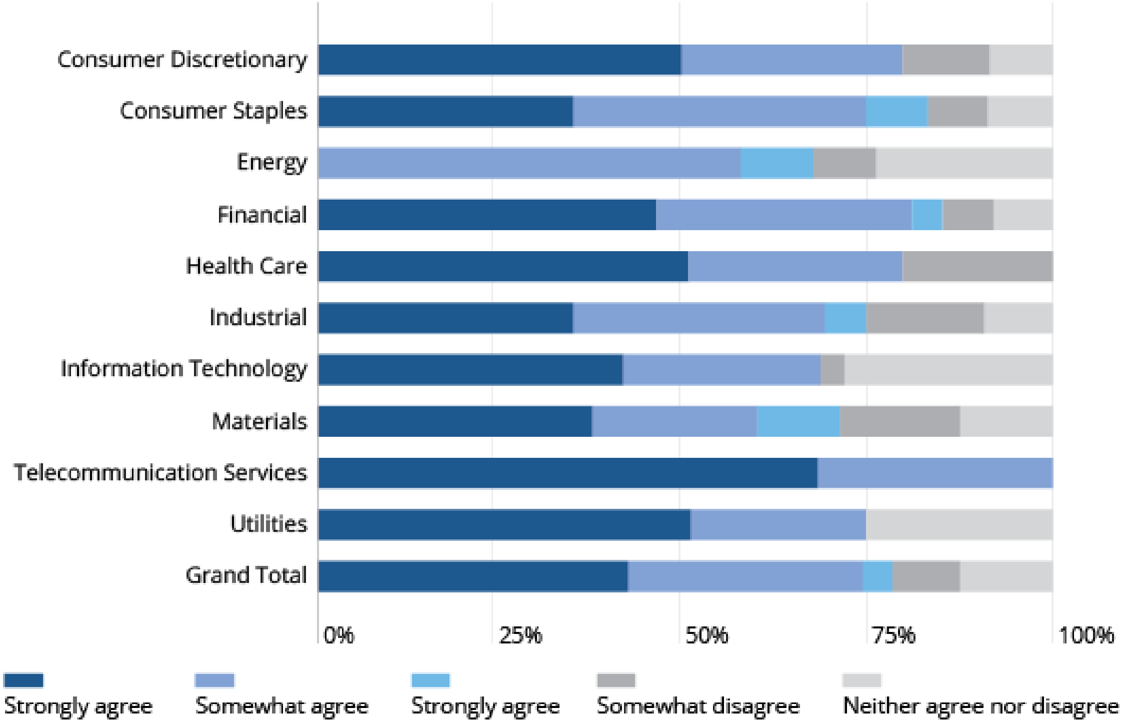
- a lack of clarity on what digital transformation entails;
- metrics that are inadequate for acceptable oversight;
- ingrained habits about board composition that block the necessary talent from stepping onto the board; and
- a prevailing, largely protective oversight bias driven by recent attention to cyber- and data privacy risk.

How can directors enhance their oversight approach and confront these challenges?
A new report, Governing Digital Transformation and Emerging Technologies, developed jointly between NACD and Marsh & McLennan Companies, offers five flexible and practical governance principles for oversight of digital transformation and emerging technologies.

CG NEWS UPDATE

Exhibit 1: **Boards across industries expect near-term disruption from emerging technologies**

My company is vulnerable to the impact of disruption from emerging technologies within the next 12 months.



Source: NACD 2019 Digital Governance Pulse Survey

1.) Approach emerging technology discussions as a strategic imperative—not just an operational issue.

All members of the board should prioritize understanding how new technologies could solve specific business operations or customer experience problems. Additionally, board members and their management teams should have a shared, well-defined vision of the business goals required for "going digital." Is the objective to increase efficiency, accelerate growth, or develop new partnerships? Defining objectives will focus allocation of resources and identify time horizons to success.

Finally, board members can evaluate whether management is thoughtfully building the necessary conditions to drive change in the long term, and help management assess how core businesses and capabilities will be impacted.

2.) Develop specific goals that lead to continuous learning about technology.

Directors cannot appropriately oversee what they don't understand. When they don't feel prepared to engage management on emerging technologies, they are not fulfilling their fiduciary duties. Continuing education will be critical to bridging this gap.

CG NEWS UPDATE

Boards should adopt a mindset of ongoing learning and development that supports effective oversight of emerging technologies. These learning objectives should support the board's oversight of the exploitation and risk mitigation of adopting new technologies. Goals should be developed by assessing collective and individual director knowledge gaps and skills, and should inform future recruitment needs.

3.) (Re)align board structure and composition to reflect the growing significance of technology risks.

Given the pace of change, the stakes for having individuals with technology experience in the boardroom are high. Boards would be well served by assessing whether their current composition and structure will continue to be fit-for-purpose in delivering effective oversight. Some boards are addressing this by recruiting directors with digital expertise, though this practice remains uncommon. The need for the recruitment of a digital director may not apply equally to all boards, but for those boards that deem the expertise a necessity to fulfill the board's fiduciary duties, the recruits should have business acumen, a commercial track record, and governance experience. Notably, the addition of a digital director doesn't absolve the rest of the board of their responsibility to oversee technology-related initiatives.

Boards are also exploring changes to committee structure. These committees can focus on risks, investments, the renewal of technology, business continuity, technology talent, and controls. When determining whether to establish a technology or innovation committee, directors should avoid making hasty or uninformed decisions, as doing so can result in vague and ineffective mandates. Instead, boards should carefully weigh the merits and risks of establishing a dedicated, board-level committee for oversight of this issue.

4.) Demand frequent and forward-looking reporting on technology-related initiatives.

Many directors struggle to assess how technology makes a meaningful impact on business performance. According to the report, sixty-five percent of directors found metrics on the effect of emerging technologies to be inadequate, and were a critical barrier to delivering effective oversight of technology. As boards request related metrics from their management teams, they should require forward-looking visibility into technological disruptors and how they will affect the company's strategy.

CG NEWS UPDATE

Directors should establish clear reporting guidelines to ensure that they receive transparent, actionable, and succinct information for their oversight. Finally, boards and management teams should focus on metrics that are clearly tied back to the business objectives. The metrics should include targets or indicators that signal if a long-term effort is on track or stalling.

5.) Periodically assess the organization’s leadership, talent, and culture readiness for technological change.

A company’s people—employees, vendors, and contractors—are at the core of its business. As such, there can be no digital transformation without workforce transformation. As companies set about transforming their business models and strategies, corporate leaders need to prioritize the recruitment and retention of a workforce that is properly positioned to support business goals. Leading companies need management teams that have the expertise to carry forward a technology-enabled vision. As they recruit and evaluate the CEO and executive team for technology leadership, directors can focus on experience in digital strategy, a reliable record of delivery, their demonstrated ability to drive organizational change, and the confidence to face challenges head-on.

Innovation cannot be achieved by members of management alone. Directors should also assess the strength of corporate culture in every corner of the business, ensuring that change, innovation, and experimentation are characteristics embraced across ranks. Organizations can’t encourage risk-taking and simultaneously punish commercial failures. Directors should ask management to develop an integrated human capital strategy that incorporates a skills inventory of the current workforce, what will be needed to deliver on the company’s future strategy, any retraining that will be necessary, and a plan for retaining talent. Boards recognize the need to actively reassess their oversight responsibilities in governing digital transformation initiatives. To succeed, directors don’t need to be experts on every technology trend, but they will need to understand how new technologies can threaten existing business models or drive business model innovation. These guidelines offer an actionable framework for directors seeking to ensure their companies reap the commercial benefits of digital transformation and emerging technologies.

Ref. https://blog.nacdonline.org/posts/principles-oversight-digital-transformation

SEPTEMBER, ISSUE 9

CG NEWS UPDATE

THE ECONOMICS OF CYBERSECURITY

September 18, 2019
By Paul Lehman

For many directors and business executives, cybersecurity spending has long been a mystery. Understanding where to invest, how much to invest and, most importantly, the return on that investment has been largely a guessing game. It is also how cybersecurity has earned the reputation of being a “black hole of spending”—chief information security officers (CISOs) continuously request more budget to stay apace of the constantly changing threat landscape, but there is little clarity around how that budget actually delivers value to a company.

If cybersecurity is a black hole, then it is also expanding rapidly while devouring ever-more money. Gartner projects that spending on cybersecurity products and services will hit $124 billion in 2019, an 8.7 percent year-over-year increase. This dwarfs Gartner’s projected 1.1 percent increase in overall IT spending for 2019.

The Business Consequences Aren’t Always Clear

Much of cybersecurity spending has been on technologies built to identify and mitigate risks—and the tech industry has eagerly fueled this phenomenon: for every new threat, there’s a new technology to deploy and manage. This has created a cost and complexity problem in many enterprises. Organizations have deployed so many technologies to keep up with cyber risks that they struggle to manage it all, which, ironically, can leave companies open to attack when systems are not configured and supervised properly.

So today, we see a situation in which all of this spending on cybersecurity technology has not curbed the data breach epidemic, is not reducing enterprise cyber risk, and executive leadership and boards are struggling to understand how cybersecurity investments translate into tangible business benefits.

Bringing Clarity to Cybersecurity

This situation must change. Organizational competency in cybersecurity impacts everything from customer trust, to competitive position, to implementing innovation and increasing earnings per share. The good news is, it is possible to manage cybersecurity like other business functions. It’s possible to quantify cybersecurity risk, and to understand the investment required to mitigate that risk.

And, it’s possible to deliver the financial data required for company leadership to treat cybersecurity for what it is: a potential business driver.

The key to all of this is for companies to move away from their technology-centric approach to cybersecurity, and instead adopt a risk-centric approach. Instead of trying to combat every conceivable attack with technology, C-suite executives and boards should develop an enterprise cyber-risk model that identifies and prioritizes what most needs to be protected, from whom it needs to be protected, and what controls are necessary to deliver that protection.

Quantifying Cyber Risk

Once that risk model has been established, organizations can make logical financial decisions around specific assets, focused on four dimensions:

- Expected Loss—The potential cost of remediation for an IT asset’s compromised security. For example, one could calculate the cost of a customer database breach based on industry data around other organizations’ breach recovery efforts.
- Cost of Control—The technology, services, and personnel costs needed to implement and maintain the security control required to protect against an IT asset being compromised.
- Effectiveness of Control—The benchmark for a control’s ability to keep the asset secure. For example, if industry data shows a control is 95% effective, then that can be factored into calculating the probability for a loss once the control has been implemented.
- Return on Control—The previous three data points can be used to calculate the overall return on the control. Obviously, the controls with the highest returns are the ones to invest in first.

With this type of return-on-control information, CISOs should be able to secure budgets and staffing when meeting with executives and board members. More importantly, with an economic framework around cybersecurity, executives can begin managing it like they do other business disciplines such as sales, marketing, and product development. Investment decisions can be made based on risk-analysis rather than best guesses, and cyber risk will become a measurable that can be reported to investors and the marketplace. When that happens,

markets will reward the organizations that manage cyber risk most effectively and transparently.And, it’s possible to deliver the financial data required for company leadership to treat cybersecurity for what it is: a potential business driver.

The key to all of this is for companies to move away from their technology-centric approach to cybersecurity, and instead adopt a risk-centric approach. Instead of trying to combat every conceivable attack with technology, C-suite executives and boards should develop an enterprise cyber-risk model that identifies and prioritizes what most needs to be protected, from whom it needs to be protected, and what controls are necessary to deliver that protection.

Once that risk model has been established, organizations can make logical financial decisions around specific assets, focused on four dimensions:

Ref. https://blog.nacdonline.org/posts/the-economics-of-cybersecurity