Diligent Insights

Resource hub powered by Diligent

5 Principles for Driving a Top-Down Approach to Cybersecurity

November 10th, 2020

Mary Fetherolf

> **“In the 21st century, there is not a single major business decision that does not include cybersecurity considerations. Cybersecurity needs to be woven into the entire process, from R&D through manufacturing through public relations. That’s the message about cybersecurity: We’re all in this together.”**
>
> **– Larry Clinton, President, Internet Security Alliance**

We live in an age when digital transformation has made cybersecurity an enterprise-wide concern. Companies that experience large data breaches feel the consequences in the key measures of success: stock price, profitability, brand and reputation. The coronavirus pandemic has complicated cybersecurity even further. Now that organizations’ administrative teams are largely working from home, videoconferencing and other virtual collaboration tools have become essential. As a consequence of these changes, board members and senior leaders will want to strike a well-considered balance between innovation and risk in their digital strategies.

A New Board Focus: Enterprise Risk

> **“Cybersecurity was traditionally thought of as an appendage issue that you tack on to a board meeting for 15 minutes at the end. [Now,] there is not a single major business decision that does not include cybersecurity considerations. Cybersecurity needs to be woven into the entire process.”**
>
> **– Larry Clinton, President, Internet Security Alliance**

At Diligent’s Modern Governance Summit 2020, technology leaders shared best practices for mitigating cyber risk. Diligent’s Chief Information Security Officer (CISO) Henry Jiang spoke with Internet Security Alliance (ISA) President and CEO Larry Clinton on the “Future of [Secure] Work – How Boards, C-Suites & IT Can Align to Fight the Growing Cyber Threat.” The conversation explored guidance from Cyber-Risk Oversight 2020, which ISA developed with the National Association of Corporate Directors (NACD). This cyber-risk oversight handbook enumerated principles that boards can adopt to strengthen cybersecurity in their organizations from the top down:

1. Cybersecurity as a Strategic Risk
2. Legal and Disclosure Implications
3. Board Oversight Structure and Access to Expertise
4. An Enterprise Framework for Managing Cyber-Risk
5. Cybersecurity Measurement and Reporting

Principal 1: Treating Cybersecurity as a Strategic Risk

> **“Cybersecurity is not an IT problem. It is an enterprise-wide risk management issue. We need oversight from the board of directors to set the environment for a good cybersecurity culture — and then put in [place] parameters for the cultural supports, including**

economic supports, so the entire organization can embrace cybersecurity and follow best practices."

— Larry Clinton, President, Internet Security Alliance

Addressing new cybersecurity challenges can no longer be the work of information technology (IT) or information security professionals alone. Businesses are now embracing best cybersecurity practices at the highest level of leadership, from which new management reporting and collaboration structures, as well as technology frameworks, are emerging.

CISOs are spelling it out: cyber-risk is operational risk. It can't be relegated to an IT or cybersecurity silo. Business owners must own operational risk. The choices to be made about risk (accept, avoid, mitigate and transfer) are business decisions. When the digital age began, cybersecurity was a mere offshoot of IT's core responsibility of automating business processes. Information security managers fought for the budgets, buy-in and policy support that would keep systems secure.

Now that information technology permeates every aspect of business operations, cybersecurity demands a top-down approach that begins with the board and leadership team working together. Cybersecurity warrants the same gravity and diligence as the legal and financial dimensions of business decisions.

Principal 2: Recognizing Legal and Disclosure Implications

Boards can ask their legal teams for a deeper understanding of their organizations' unique legal and compliance obligations. These obligations will vary from one industry to another; they'll also vary by national and local jurisdiction. Requirements shift over time, so organizations will want to monitor legal and regulatory developments for changes that affect their risks and obligations where cybersecurity and data privacy are concerned.

Principal 3: Creating Board Oversight Structure and Building Board Access to Cybersecurity Expertise

Today's directors will want to educate themselves to navigate cybersecurity matters and cyber risk questions with confidence. Boards may engage external experts to accelerate their learning beyond mere awareness to a deeper understanding of cybersecurity matters.

Boards can act now to establish robust collaborations among departments to strengthen the organization's cyber defenses. By building this foundation now, such collaborative teams including leadership, legal, IT, and information security can respond more rapidly and effectively when cyber threats emerge. Ideally, legal, IT and data security teams will act as trusted advisors to one another to collaborate on developing and implementing security policy. Those policies can define the distinct role of each team. Together, the teams can plan and participate in cyber breach exercises, and use lessons learned to strengthen their collective response. They can also collaborate to educate and inform their boards on their progress in managing cyber risk.

Principal 4: Developing an Enterprise Framework for Managing Cyber-Risk

Boards are starting to require both technical and management frameworks to control cyber risk effectively.

- Technical frameworks may be based on broadly-accepted cybersecurity standards like National Institute of Standards and Technology (NIST) or International Standards Organization (ISO).
- Management frameworks determine how cyber risk is controlled within the organization. Ideally, a C-level executive with cross-functional responsibility (a Chief Officer of Risk, Operations, or Finance, for example) would spearhead these efforts.

The management framework would function separately from the IT department and be funded apart from IT budgets.

Principal 5: Measuring and Reporting on Cybersecurity

An economic, empirical calculation of risk establishes a context for determining organizational risk appetite among board members and senior leaders. Clear, explicit agreement regarding risk appetite is foundational, because the organization can then manage cyber risk to a clearly defined, broadly-understood and agreed level of risk the organization is willing to accept.

Organizations can establish key risk indicators (KRIs) as common terminology to measure and communicate with the board about cybersecurity and cyber risk management program effectiveness.

Creating a Successful Culture of Security

> **“Cybersecurity in the 21st Century is the same sort of issue as legal and finance. No board would make a significant decision without consulting with legal and finance. In the 21st Century, there is not a single major business decision that doesn’t include cybersecurity considerations.”**
>
> **— Larry Clinton, President, Internet Security Alliance**

Now that information systems are everywhere, and digital transformation plays a central part in every strategic business decision, understanding cyber risk and ensuring cybersecurity is top of mind throughout the organization are critical new responsibilities for boards. To meet the challenge, directors will want to develop greater cyber-risk management expertise.

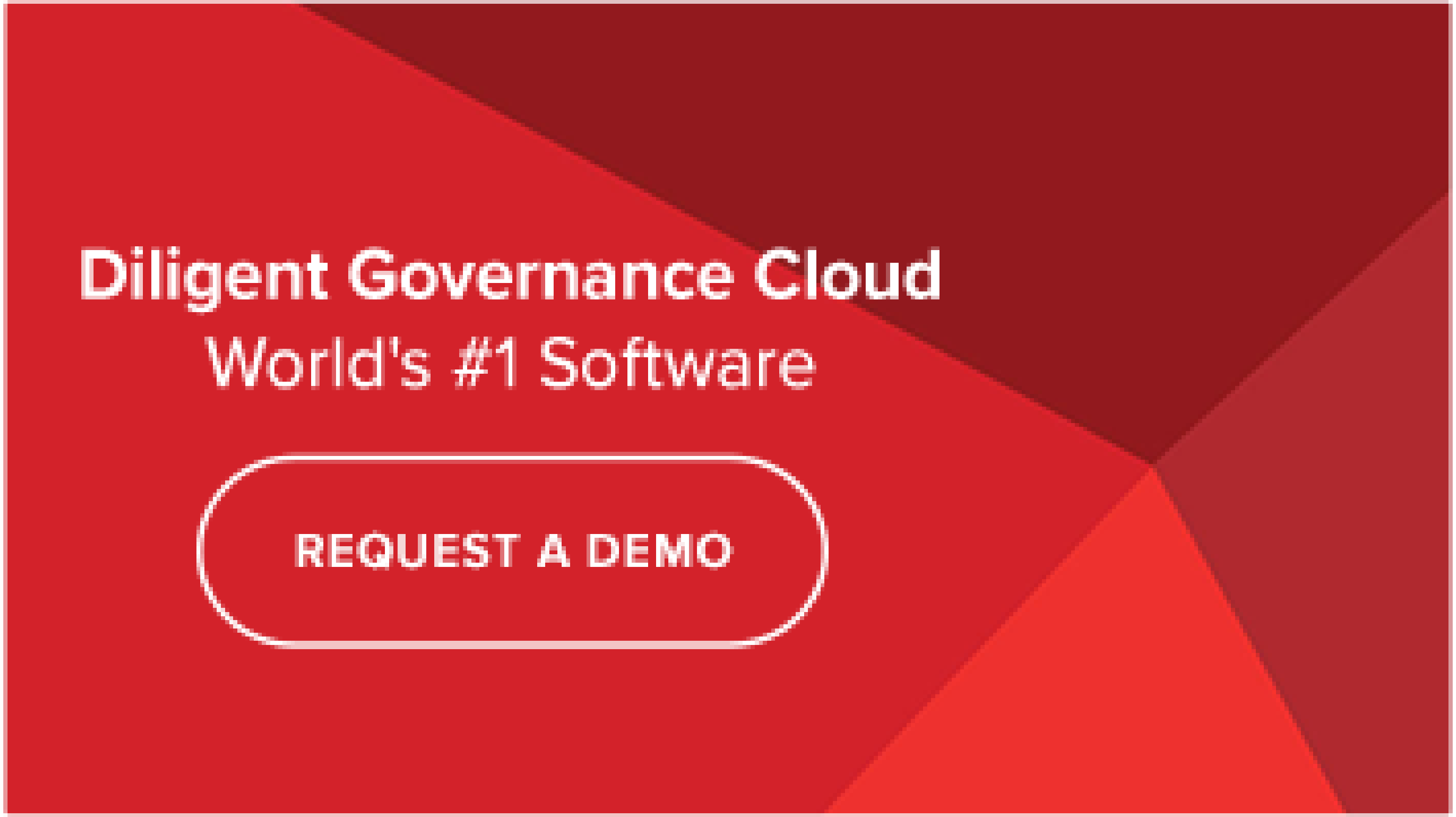
Ms. Fetherolf writes about the impact of new technologies and regulations on business strategy and operations. This second career follows several years consulting with business and technology leaders on program management and governance in regulated industries. Topics of interest include corporate governance, cybersecurity, data privacy, regulation, compliance, and digital transformation.

ARTICLE TOPIC: CYBER RISK, CYBERSECURITY

RECOMMENDED

What is NIST Cybersecurity Framework 1.1 (NIST CSF)

This article explores the NIST Cybersecurity Framework. We show you how to use it and the benefits of compliance with the framework.



Diligent is here to help your organization have the right tools, insights and analytics

Request a demo, pricing or more info to see how.

Or give us a call at:

1.877.434.5443

* First Name

* Last Name

* Company

* Business Email

* Country

United States

* Phone

Download on the App Store

GET IT ON Google Play

REQUEST A DEMO

DILIGENT

PRODUCTS

COMPANY

CASE STUDIES

NAVIGATE

VIDEOS

ARTICLES

WHITEPAPERS

FOLLOW

FACEBOOK

YOUTUBE

LINKEDIN

TWITTER

SUPPORT

1.866.262.7326

SALES

1.866.434.5443

Privacy Policy Terms of Use