Diligent

Modern Governance: A Guide for Security Professionals

Diligent

Defining Modern Governance

> "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

The technology, processes and skills that today's companies need are evolving as quickly as the business landscape. Organizations must be all at once more informed, more secure, more collaborative and more purpose-driven. Modern governance equips organizations with the tools they need to protect data, streamline collaboration and ultimately drive better decision-making.

At Diligent's Modern Governance Summit 2020, technology leaders assembled virtually to share best practices for driving digital transformation and mitigating operational risk. Their discussions around secure collaboration create the blueprint for CIOs, CISOs and security professionals in a highly dynamic era.

This guide compiles key takeaways from the virtual conference. As we navigate the new normal, Diligent looks forward to continuing as your trusted partner.

Brian Stafford
CEO
Diligent Corporation

1. Align Legal, Technology and Data Security

Recommended Actions

- ☐ Communicate regularly about upcoming security and compliance deadlines and responsibilities.
- ☐ Spearhead written policies and procedures with clearly defined roles for each team and conduct regular run-throughs of cyber risk scenarios.
- ☐ Implement a fully encrypted collaboration platform that helps prevent the loss of sensitive data.

A siloed approach to legal, technology and data security is all too often the norm in corporations. Yet. as Diligent's Chief Information Security Officer, Henry Jiang, and Senior Vice President & General Counsel, Jack Van Arsdale, discussed, this is a less-than-optimal approach to the complex issue of security.

In today's virtual world, legal and technology teams must align more closely to bolster the company's cyber defenses. In the event a cybercrime does occur, robust collaboration among these teams ensures a more effective, quicker response. Yet this requires building the right foundation before a crisis hits.

"Preparation is the most important thing. You want to be organised, you want to have everything in one place…. So when you have an issue, you don't have to run through the basics. You want to be spending your time focusing on the important things."

Jack Van Arsdale
Senior Vice President & General Counsel, Diligent

To prepare themselves, technology and legal teams need to understand how their roles differ yet dovetail with one another. In the most collaborative environments:

- Legal, IT and data security teams are trusted advisors to one another.
- The teams must collaborate on drafting, negotiating and implementing security policies and procedures; each team invites the others to participate in policy design workshops.
- Each team should have clearly defined roles and responsibilities under those policies and procedures.
- The teams build collective "muscle memory" by jointly participating in cyber breach exercises.
- The teams are aligned when presenting to the board.
- Data breaches are handled using predetermined tools and each team operating in concert, according to its defined roles and responsibilities.

2. Focus the Board on Enterprise Risks

Recommended Actions

- ☐ Raise recognition of cybersecurity as an enterprise-wide strategic risk.
- ☐ Help boards understand their organization's unique legal obligations.
- ☐ Provide boards with access to appropriate cybersecurity expertise.

Cybersecurity has traditionally been treated with a bottom-up approach — something that an IT department had to solve on its own. However, as Larry Clinton, President of the Internet Security Alliance, discussed with Diligent's Chief Information Security Officer Henry Jiang, cybersecurity requires a top-down approach that begins with the board and leadership team working together.

> "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

Over the last five years, there's been a significant shift of board attention toward cybersecurity. No longer a single item on the board agenda, cyber risk is now a lens applied to every board decision.

"Cybersecurity was traditionally thought of as an appendage issue that you tack on to a board meeting for 15 minutes at the end," said Clinton, explaining that now cybersecurity must be treated the same as legal and financial decisions. "There is not a single major business decision [today] that does not include cybersecurity considerations. Cybersecurity needs to be woven into the entire process."

According to Clinton, management, led by the CIO or CISO, should present to boards:

1. A cybersecurity framework detailing where data is and how it operates.
2. A cyber-management strategy led by someone with cross-organizational responsibility.

Boards should also expect from management an economic and empirical risk assessment. With this information, boards and senior leadership can work together to set the risk appetite and manage risk to that level.

3. Enable Secure Collaboration in a Virtual World

Email, text messaging and other legacy tools remain the lifeblood of organizational communication and collaboration. In fact, a recent Forrester/Diligent survey found that over 50% of directors and C-suite executives regularly use personal email to communicate about their organization's most sensitive topics. Yet with the pandemic-driven shift to remote work, the threat of an insider-initiated breach – whether through inadvertent human error or malicious privilege misuse – has increased exponentially.

"Overwhelmingly, corporate technology teams have the best interests of their organizations at heart. But by the nature of their roles as data custodians, those employees are considered privileged users if they have the ability to see what the C-suite is working on, talking about, deciding and planning — and they are opening up their organization to additional risks. Malicious actors often target those types of users via social engineering methods or other means of attack in order to gain full access to the system."

Henry Jiang
Chief Information Security Officer, Diligent

Security professionals are quickly realising the need for enhanced solutions that enable boards and management to carry on critical business functions and workflows, while keeping sensitive information protected. Entrusting your organization's most sensitive information to digital tools requires a serious evaluation of your virtual collaboration infrastructure.

Evaluate Your Current Solution for Leadership Collaboration

1. **Is your current platform fully integrated?**
   The system should pull all confidential updates, conversations, workflows and documents out of unsecure channels like email. Board members, executives and legal teams should be able to collaborate without leaving the secure confines of the system.
2. **Have you enabled end-to-end encryption?**
   Protecting sensitive materials does little good if board members and executives are still using unsecure channels (e.g., personal email, texting) to communicate among one another. Ensure you've provided secure alternative for messaging and workflows.
3. **Is you solution easy to adopt and use?**
   To ensure adoption, a platform must mirror the functionality of the everyday tools that boards and management teams are already familiar with. Ensure your solution is as seamless and intuitive as email. It should also enable real-time updates and notifications across groups.
4. **Does it meet security standards for a virtual world?**
   Does the provider invest in security development and conduct penetration testing? Look for customizable user permissions, the ability to remotely wipe compromised devices, and redundant data centers.

4. Data Governance in a Distributed Digital World

Recommended Actions

- ☐ Centralize organization, subsidiary and third-party data in a single source of truth such as **Diligent Entities**. Implement access protocols to ensure the security and accuracy of the data at all times.
- ☐ Automate data processes to efficiently identify red flags and to serve up data to stakeholders.
- ☐ Implement collaboration and communication tools with end-to-end encryption to protect sensitive data while working across a distributed environment.

REQUEST A DEMO >

The digital transformation accelerated by the coronavirus pandemic has highlighted the complications inherent in secure collaboration. In their panel at Modern Governance Summit 2020, Colleen Coda, Managing Director, Technology & Innovations, The Blackstone Group, and Paolo Pelizzoli, Executive Vice President & Chief Operating Officer, International Realtime Payments, Mastercard, discussed some of the key components of an effective data governance program. Chief among them are keeping information secure, managing access and preventing information leakage.

For organizations spread across jurisdictions or managing portfolio companies, centralizing data systems and implementing access protocols are key drivers of effective data governance.

"We've been making a big shift to centralising our data.... How do you ensure that data is correct and people have the right access and visibility to it? We have a strong data governance team who has a set of [automated] processes where they can do quality checks and look at outliers."

Colleen Coda
Managing Director, Technology & Innovations, The Blackstone Group

Further, the need to streamline – and secure – collaboration and communication tools has never been greater. By more broadly implementing techniques and tools that have optimized and secured board operations, technology leaders can drive more effective and more secure workflows within the entire organization.

"What Diligent does for the board [works for the rest of the organization]. It's going to appear different; if you start looking at some of the decisions that have to be made by the board, they're very different from those made with a client, with operations, with security, with product, with finance and so on..... But if you start thinking of [the organization] as mini boards, the similarities are there."

Paolo Pelizzoli
Executive Vice President & Chief Operating Officer, International Realtime Payments, Mastercard

Collaborate Securely While Protecting Your Organization From Risk

Executives and business leaders need a way to collaborate on sensitive topics at the speed of business – without exposure to leaks or attacks. **Diligent's Board & Leadership Collaboration** solution provides CIOs, CISOs and other governance professionals with the software support they need to drive a security-led digitization program that helps boards, executives and their teams to collaborate securely, make agile decisions and mitigate risks.

Board and Executive Meeting Management

Facilitate board and leadership meetings with the industry-leading solution for secure meeting management.

- Secure agenda & material distribution
- Task management

Secure Document Storage and Collaboration

Add an additional layer of security to your processes with key integrations like Office 365. Share documents and collaborate securely with both internal and external stakeholders.

- Secure sharing for native format files
- Data rooms with security parameters
- Vault storage
- Live web-based collaboration

Secure Messaging

Communicate with leadership teams in real-time on an encrypted, uncluttered channel to signify importance and urgency.

- Real-time communications
- Group and individual chats
- Read receipts
- End-to-end encryption

Secure Meeting Workflow

Support workflows and approvals to improve efficiencies when building and distributing meeting materials.

- Secure virtual meeting workflow
- Decisions, actions and outcomes

Cyber Risk Scorecard

Understand cyber risk, how to measure it, benchmark against peers, and prioritize action to improve cybersecurity posture and navigate the digital world with confidence.

Market Intelligence & Reputation Monitoring

Access governance risk scores, organizational health monitoring, market intelligence, and diversity and inclusion data to make agile decisions that affect the entire organization.

Email: info@diligent.com | **Call:** +1-212-741-8181 | **Visit:** diligent.com

REQUEST A DEMO >