Diligent

The New Cybersecurity Imperative: **Cyber Governance**

As cybersecurity vaults to the top of board agendas and risk management frameworks,[1] management teams need to contextualize firm performance and activities for directors as well as protect sensitive board/executive communications from potential leaks.

Emerging Needs for Effective Cyber Governance

From 2019 to 2020 the number of cyber intrusions at corporations increased by 400%, prompting increased scrutiny of how corporate boards oversee cybersecurity issues.

The role of boards continues to come under increased scrutiny as cybercrime grows exponentially.

From 2019 to 2020 the number of cyber intrusions at corporations increased by 400%, prompting increased scrutiny of how corporate boards oversee cybersecurity issues. Consequently, cyber governance — the elevation of cybersecurity risk management to board-level oversight — is critical to effective management of cybersecurity and cyber risks. Investors, industry experts and regulatory bodies all view cyber governance as necessary to fortifying overall cyber resilience. In the new paradigm where any company can expect an attempted hack in the near future, board cyber governance performance is becoming a part of key external assessments across sectors.

Material Risk Drives Growing Investor Interest in Board Oversight of Cybersecurity

Investor focus on companies' cybersecurity and cyber resilience capabilities grows as a result of the increasing materiality of related risks.

Corporations can expect investors' examinations of cyber governance to rise in the future. Two-thirds of institutional investors ranked cybersecurity as the most pressing ESG issue in RBC Global Asset Management's 2019 Responsible Investment Survey, reflecting the increasing materiality of cyber risks.[2]

The high costs of recent breaches, not surprisingly, came with parallel impacts to stock valuations; leaks of highly sensitive information led to more immediate drops in valuation according to a 2021 study.[3] The immediate economic loss is often coupled with longer-term impacts that need mitigation. Costly hacks come with legal and reputational risks damaging both public sentiment and market advantages; in a recent study breached companies were found to underperform in both the short and long term.[4] Strengthened cybersecurity in return can lead to improvements in client trust.[5]

Currently, investment screens and engagements are emerging as key methods by investors to manage the potential investment risk associated with a cyberbreach event at current and potential portfolio companies.

2/3 of institutional investors ranked cybersecurity as the most pressing ESG issue in RBC Global Asset Management's 2019 Responsible Investment Survey.

Regulatory

In 2020, The UK's information commissioner issued 17 fines, with three of those fines averaging close to

$20 million.

As policymakers pay more attention to cyber risk, cybersecurity fines are accelerating.

The European Union's General Data Protection Regulation (GDPR) established in 2018 increased cybersecurity fines to a maximum of €20 million or 4% of a company's global revenue for violations by any firm that collects data in Europe.[6] In 2020, The UK's information commissioner issued 17 fines, with three of those fines averaging close to $20 million.[7] This past year the Securities and Exchange Commission (SEC) fined two public corporations for deficient disclosure on cybersecurity issues indicating, based on the case of First American Financial, that timely disclosure of a material breach occurs in under six months. To take prompt actions to this degree requires active information-sharing on cyber issues with the board.

Meeting Criteria for Strong Board Oversight of Cybersecurity

As investors and other key external stakeholders increasingly ask corporations to confirm the board is literate in cyber risk, directors will need to demonstrate they keep a pulse on cybersecurity management through data-driven insights and company-specific scores.

According to a recent Bloomberg article, demonstration by boards of proactive and prudent efforts to strengthen cybersecurity can provide protection for the boards against future legal actions in the event of a breach.[8] To better understand investor and market expectations for cyber governance, we reviewed a recent two-year engagement by 55 institutional investors representing over US$12 trillion in assets under management,[9] the World Economic Forum's Principles for Board Governance of Cyber Risk, investor statements, as well as industry research. We found an emerging consensus around the need for informed, active and frequent board oversight of cybersecurity (Figure 1).

Diligent's Findings

To this end, directors will need a way to understand cyber risk, measure it, benchmark against peers and prioritize action. Cybersecurity dashboards can provide the foundational insights needed to establish appropriate governance measures. Company-specific metrics that benchmark progress enable companies to demonstrate tangible improvements in their cybersecurity posture, which in turn validates the board's oversight to investors and industry influencers.

Figure 1: Current Criteria — Assessment of Cybersecurity Governance

Investor Assessments

- Evidence of board responsibility (board-level cyber governance)
- Strong board oversight to ensure appropriate cybersecurity procedures
- Active monitoring of cyber issues by the board
- Depth of board's understanding of cyber risk[10]

Industry Assessment[11]

- Cybersecurity risk mitigation
- Response efforts

Identified Corporate Best Practices[12]

- Establish corporate tolerance for cyber risk
- Board briefings from senior management covering risk exposure, threat environment, key industry incidents and how peers are addressing cyber risk

Board-level cyber governance is currently assessed by investors alongside other critical components of a robust cybersecurity strategy. Our review found investors are increasingly seeking more information on (see Figure 2):

Figure 2: Current Criteria — Assessment of Cybersecurity Management

Corporate awareness and preparedness

Including the presence of established training and monitoring of employees and suppliers, work with external cybersecurity specialists, and the current structure for technical expertise

Risk management

Including policies, risk identification, cyber defense enhancements, and the role of enterprise risk management

Data protection and post-breach management

Including data protection policy coverage of the supply chain

Disclosure

Appropriate reporting allowing investors to confirm polices and controls

Cybersecurity **Needs for Board Communications**

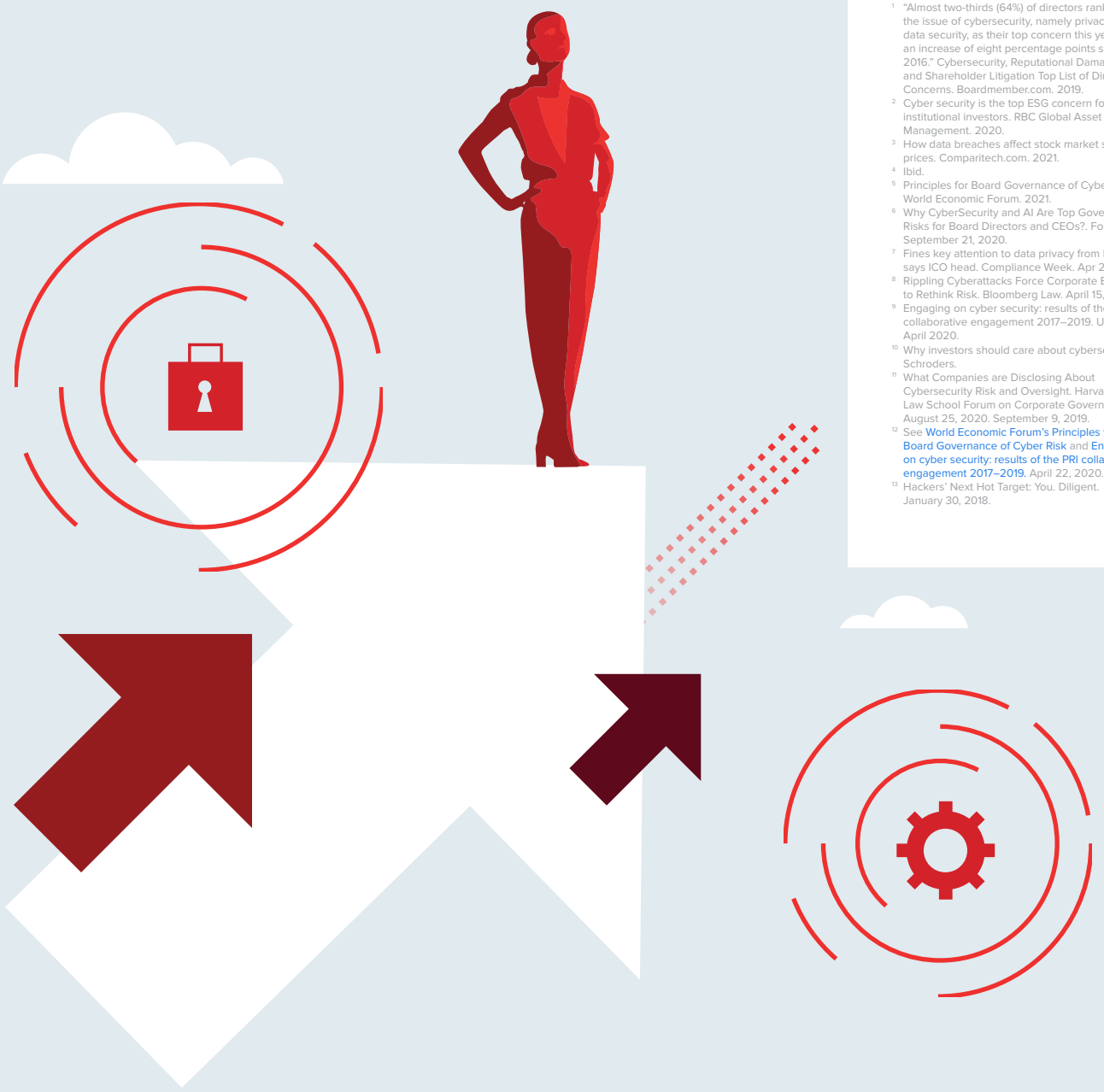
As boards seek to gain greater insight into cybersecurity risks, examining the vulnerabilities of their own communications platforms should be an early step. Infiltration of board communications can reveal sensitive and embarrassing information to the public. A leak at this level can also undermine the credibility of all other corporate cybersecurity efforts.

Boards should expect to be prime targets of increasing cybercrime. With access to valuable data, little oversight from corporate cybersecurity teams, and rampant use of unsecured platforms — 90% of directors use personal email accounts for at least some communications with peers and management — directors are ideal cybercrime targets.[13] A fully secure system for board communications should ensure ease of use — the main driver behind risky board communication practices — as well as:

- Keep sensitive company leadership conversations outside of email via a fully encrypted platform
- Provide remote and mobile access to secure communication tools in the event of a crisis
- Align good governance and operations with improved visibility, robust security tracking features and optimized workflows

If advancing to a new platform is necessary, opt for a secure collaboration partner who thoroughly plans out transitions and addresses clients' concerns. Transferring data to a new system, often from multiple legacy tools, could result in lost data, missed compliance deadlines or other legal headaches if not handled properly.

As a leader in modern governance, Diligent is uniquely positioned to support the establishment of industry-leading cyber governance processes. Our solutions help directors, executives and their teams work securely, increase productivity, and protect their organizations from risk.



Footnotes

1. "Almost two-thirds (64%) of directors ranked the issue of cybersecurity, namely privacy and data security, as their top concern this year — an increase of eight percentage points since 2016." Cybersecurity, Reputational Damage and Shareholder Litigation Top List of Director Concerns. Boardmember.com. 2019.
2. Cyber security is the top ESG concern for institutional investors. RBC Global Asset Management. 2020.
3. How data breaches affect stock market share prices. Comparitech.com. 2021.
4. Ibid.
5. Principles for Board Governance of Cyber Risk. World Economic Forum. 2021.
6. Why CyberSecurity and AI Are Top Governance Risks for Board Directors and CEOs?. Forbes. September 21, 2020.
7. Fines key attention to data privacy from boards, says ICO head. Compliance Week. Apr 21, 2021.
8. Rippling Cyberattacks Force Corporate Boards to Rethink Risk. Bloomberg Law. April 15, 2021.
9. Engaging on cyber security: results of the PRI collaborative engagement 2017–2019. UNPRI. April 2020.
10. Why investors should care about cybersecurity. Schroders.
11. What Companies are Disclosing About Cybersecurity Risk and Oversight. Harvard Law School Forum on Corporate Governance. August 25, 2020. September 9, 2019.
12. See World Economic Forum's Principles for Board Governance of Cyber Risk and Engaging on cyber security: results of the PRI collaborative engagement 2017–2019. April 22, 2020.
13. Hackers' Next Hot Target: You. Diligent. January 30, 2018.

About Diligent

Diligent is leading the way in modern governance and is relied on by more than 25,000 organizations and 1,000,000 leaders in over 90 countries. Diligent empowers leaders to turn governance into a competitive advantage through unparalleled insight and highly secure, integrated SaaS applications. Thrive and endure in today's complex global landscape with Diligent.

Learn more and explore our solutions at **Diligent.com**

Diligent