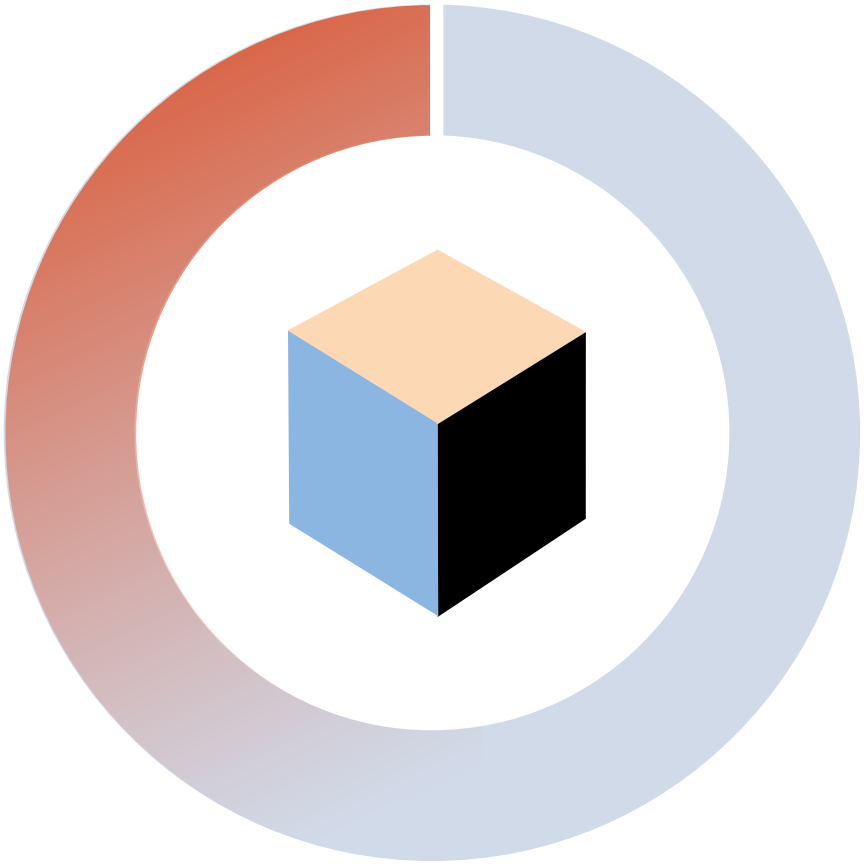
CYBER RISK VIGILANCE



Marie-Noëlle Brisson, FRICS, MAI
Co-Founder
CyberReady, LLC

Michael Savoie, PhD
Co-Founder
CyberReady, LLC

Real estate leaders have a fiduciary duty to act in the best interests of their companies and shareholders, and increasingly, this means incorporating cybersecurity awareness to board governance. But what does good governance actually look like in the real estate space?

Real estate leaders have a fiduciary duty to act in the best interests of their companies and shareholders, and increasingly, this means incorporating cybersecurity awareness to board governance. Broad cybersecurity measures will enable a safe digital strategy, protect sensitive information and prevent cyber risks as much as possible.

This article explores how legislation and regulation has responded to rising cyber risks, what corporate compliance looks like, and how boards can be prepared to perform cyber oversight (as illustrated in *Exhibit 1)*.

EXHIBIT 1: SOUND CYBER GOVERNANCE

Source: Principles for Board Governance of Cyber Risk Insight Report March 2021, page 6

ATTACKS ARE INCREASING AND COMING FROM MULTIPLE DIRECTIONS

As digital business grows, so do third-party ecosystems (e.g., vendors, suppliers, partners, etc.). Most organizations have invested in digital technologies without prioritizing the supply chain. As digital risk expands, there is often a fragmented response. Due to a lack of proper integration into governance strategies, digital risk is often treated as an IT-only issue, despite the fact that such risk is manifested across entire organizations and supply chains.

And on an operational level for business use, AI, in the form of large language models (LLMs) and generative AI is a set of technologies that are based primarily on machine learning and deep learning, used for data analytics, predictions and forecasting, object categorization, natural language processing, recommendations, intelligent data retrieval, and more.[1] As the use of AI grows within the organization, and between its suppliers and customers, the cyber risk to the organization increases dramatically.

RISING RISKS RAMPS UP CYBER REGULATION AND BOARDS NEED TO BE AWARE OF NEW REGULATIONS

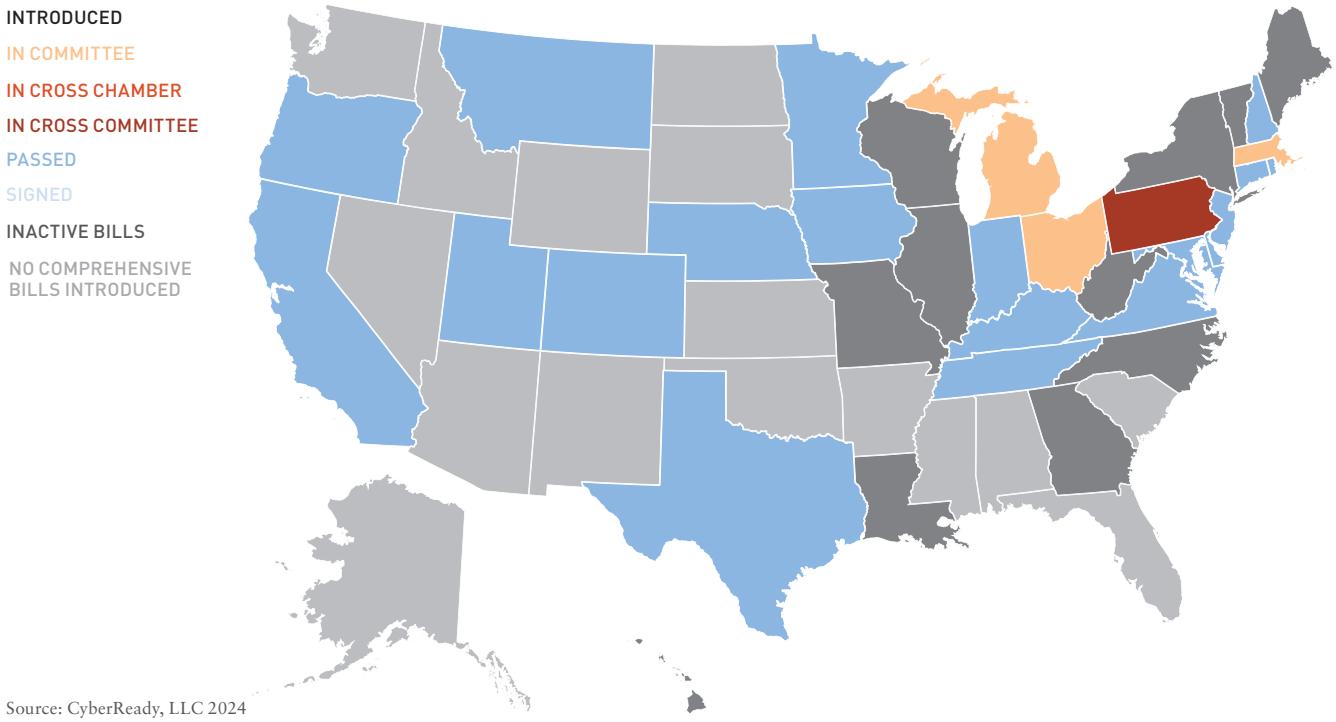
New Federal Laws

Although there is not a specific federal law governing cybersecurity or artificial intelligence oversight by directors, there are legal obligations to keep in mind. For example, the Gramm-Leach-Bliley Act (GLBA) includes the requirement to implement safeguards against cyber threats.[2] The Sarbanes-Oxley Act (SOX) requirement to maintain adequate internal controls over financial reporting, could include cybersecurity controls if they are deemed material.[3]

Besides sector-specific cybersecurity laws, below are the main recent laws and trends directors need to be aware of at the federal level:

- The Internet of Things (IoT) Cybersecurity Improvement Act of 2020
- The proposed American Data Privacy and Protection Act (ADPPA), not yet signed into law, but which would establish nation-wide consumer data protections.
- The 2023 Executive Order calling for the evaluation and mitigation of privacy risks of AI, and the formation of a new AI Safety Institute to create guidance and benchmarks for evaluating AI capabilities.

EXHIBIT 2: US STATE PRIVACY LEGISLATION TRACKER, 2024



Source: CyberReady, LLC 2024

State Privacy and AI Laws

At the state level, data privacy laws are rapidly gaining traction. While a growing number of states have passed such legislations, their respective contours are not the same and directors need to exercise caution.

Similarly, AI legislation is a developing patchwork. As of the writing of this article, only three states (California, Colorado, and Utah) had signed laws (effective Jan, Feb 2026) while Illinois, Massachusetts, and Ohio had active bills under committee review.[4]

New SEC Rules

The Securities and Exchange Commission (SEC) in July 2023 adopted rules requiring public companies to disclose (i) material cyber incidents within four business days; and (ii) material information regarding their cyber risk management, strategy, and governance on an annual basis. This rule introduces two new notions for directors: accountability to investors, and materiality whereby companies will need to develop appropriate metrics such as number of customers affected, sensitivity of data exposed, etc. It also focuses on incident response which requires directors to focus on business continuity and disaster recovery plans.

New Standards and Frameworks

The ISO/IEC 27000 family of standards handles IT security, cybersecurity, and privacy protection; and ISO 27001, the most common standard for information security management systems, vetting people, processes, and technology for confidentiality, integrity, and availability, was updated in 2022 to expand the handling of information security and data protection. Other references such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework can also help improve cybersecurity practices by providing benchmarks for companies to measure their cyber maturity.

Secure by Design is becoming a requirement for many supply chains and thus should be a point of vigilance for directors. "Secure by Design products are those where the security of the customers is a core business requirement, not just a technical feature." (Secure by Design: CISA driving safer tech - LinkedIn) It has been embraced by more and more sectors, i.e.:

- guidelines published by The National Elevator Industry Inc to improve cybersecurity control systems for elevators and escalators
- ISA 62443, released in late 2021 by the International Electrotechnical Commission, to safeguard critical infrastructure and industrial control systems and processes from cyber attacks

As with the SEC rule, a strict calendar of reporting is a must; four business days after companies become aware of a cyber incident is a short turnaround, but it is also becoming the norm for successful insurance claims.

THE INFLATION OF LAWS, REGULATIONS AND STANDARDS RAMPS UP COMPLIANCE AND ACCOUNTABILITY

The new laws and trends reflect a few common attributes, all pointing in the direction of better preparation and vigilance from boards across three areas:

Speed of Implementation: The usual time span between enactment and enforcement of new cybersecurity laws used to be around two years. Today, there is usually not that much time to prepare for implementation after a law is passed.

Extraterritoriality: It is not new, SOX already in 2002 had an extra territorial reach. But now it is the norm and should be a point of vigilance for directors involved with international activities.

Risk Approach: Adoption of a multi-risk approach is encouraged, with proportionate technical, operational, and organizational security measures, underscoring the importance of risk mapping and business continuity, as well as board's preparedness.

Measure of Materiality

Just as the concept of materiality made inroads in ESG accounting, for the first time in the US, the new SEC cyber disclosure rules are based not on data privacy breach but on materiality to investors; directors need to put in place or approve KPIs and thresholds to measure materiality, such as number of clients impacted, duration, geographic spread, and criticality of services affected. The board also must decide on who has the authority to declare materiality, and at what level it gets engaged.

Speed of Reporting

As with the SEC rule, a strict calendar of reporting is a must; four business days after companies become aware of a cyber incident is a short turnaround, but it is also becoming the norm for successful insurance claims. It also begs the question of disclosure: a specific plan to disclose a disruption and effectiveness of incident response needs to be established to be transparent to investors and create trust without sharing too much information.

Heavy Fines

Catching up with heavy European fines, cyber penalties in the US have become heavier. The FTC has dealt heavy fines, just like the SEC for inadequate and misleading disclosures. States have also joined in the trend, as in the recent cases of California fining Google[5] or Kaiser[6], and Illinois[7] and Texas[8] imposing heavy fines on META for violation of biometric laws.

Accountability

The SEC raised the "cyber" bar for the market in general by requiring directors of public companies to have the knowledge and skills necessary to assess cybersecurity risks and establish liability of top management and board members for gross negligence in case of security incidents.

Directors and officers (D&O) liability insurance typically covers claims alleging breach of fiduciary duty, including those related to cybersecurity oversight. However, coverage may be limited if the directors are found to have acted recklessly or in bad faith. The eventuality of lawsuits against directors if investors believe that they failed to adequately oversee cybersecurity risks, or disclose material cybersecurity events, should be of concern to business leaders. Board meeting minutes, for example, are an easy tool for documenting what was discussed (and when), which could make a difference between a painful lawsuit or an easier resolution.

Data privacy and cyber safety have evolved from mere regulatory compliance to a customer trust imperative and thus a strategic opportunity for directors.

Digital risk is often treated as an IT-only issue, despite the fact that such risk is manifested across entire organizations and supply chains.

NEW ACCOUNTABILITY REQUIRES RAMPED UP PREPAREDNESS AND VIGILANCE

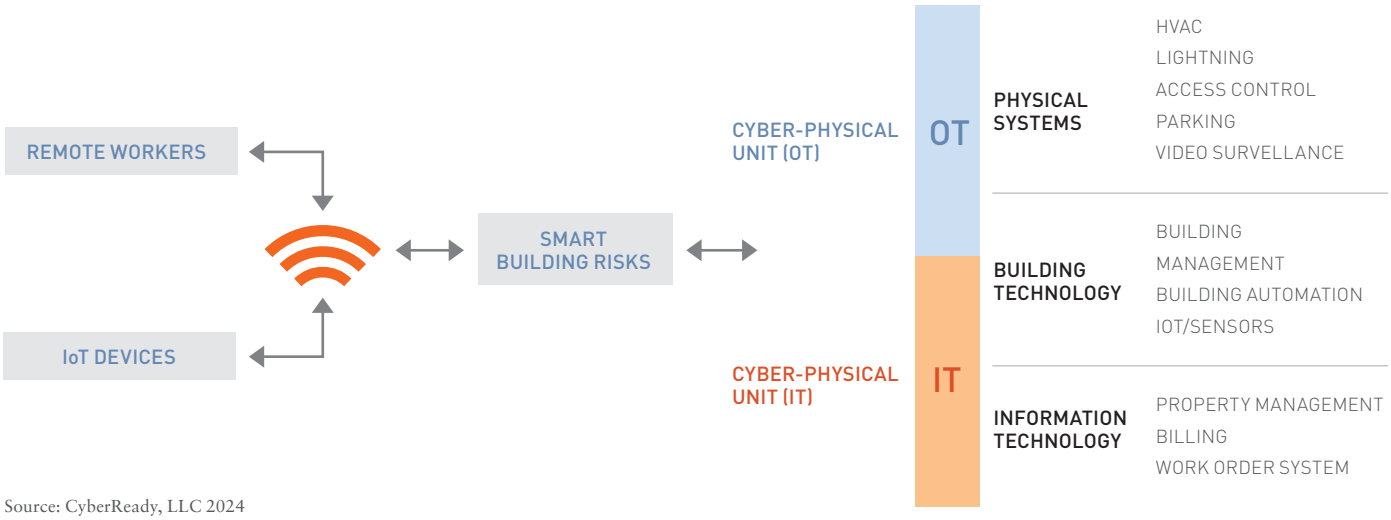
The business world is hyperconnected. The value chain of data ownership can be very complicated, because it often involves aggregation from many sources. A set of controls and audit procedures must be in place to ensure ongoing compliance with internal data policies and external government regulations. Data governance should extend to third parties as well. The same data issues raised and resolved internally should be addressed in interactions with external entities.

The Role of the Board

With today's interconnectivity, it is imperative that the board take a holistic risk management view *(Exhibit 4)*. Here, leaders gain a full view of how their organization's risks impact objectives, strategies, and business operations. Successful integrated risk management (IRM) programs take into account events that might take place outside of the identified risk, contributing to a healthy analysis of the landscape and the board's position in all areas of the company's operations.

In addition to integrating operational, enterprise, and cybersecurity risk management functions, a mature IRM program could also integrate ESG risk management and reporting into the umbrella, getting ahead of pending regulatory requirements.

EXHIBIT 3: DATA SHARING IN A HYPER-CONNECTED WORLD



Source: CyberReady, LLC 2024

EXHIBIT 4: HOLISTIC RISK MANAGEMENT

Source: CyberReady, LLC, 2024

Business Continuity and Disaster Recovery

Strong data governance is also increasingly critical for business continuity and crisis management.

Modern cyber risk management must address physical, behavioral, technical security and data privacy.

- **Physical Security:** Are buildings and building operations secure from intruders? Is sensitive data protected from prying eyes (e.g., intentional, accidental, or even remote through video conferencing)?
- **Behavioral Security:** Do personnel understand and practice safe data management practices? Do employees understand how to spot a phishing attack? Are safe protocols followed when entering and exiting spaces containing sensitive data? Is line-of-sight checked when participating in video calls?
- **Technical Security:** Is the network secure? This seems a simple question, but with the addition of generative AI, remote workers, IoT devices, and cloud storage, the network is no longer limited to the office. Technical security must focus on protecting the data wherever it is flowing.
- **Data Privacy:** Who has access to the data? Who controls and tracks this access? Is the board aware of what third-parties do with data provided them by the organization? How are breaches reported/responded to?

Modern cyber risk management must address physical, behavioral, technical security and data privacy.

Finally, it is not enough to merely protect each of these areas. Good cyber risk management must address the interaction between them. As an example, many companies require employees to use a passkey to access the office. That is good physical security. However, if a package delivery person is standing outside the door with an arm full of packages, most employees will hold the door and allow them to enter. While this is common courtesy, it creates a breach that could allow a malicious actor to enter the facility. Proper policy and training on how to handle this situation is part of behavioral security. Both physical and behavioral security are required in this instance to maximize the protection to the company.

Now more than ever boards need to treat cyber risk as a business risk. Whether it is a smart building, interconnected devices, remote workers logging on to office networks with personal devices, or third parties accessing corporate information, private data is within easier reach and more vulnerable to attack.

ABOUT THE AUTHORS

Marie-Noëlle Brisson, FRICS, MAI, and Michael Savoie, PhD, are Co-Founders of CyberReady, LLC, which provides cyber risk management, and state-of-the-art online and in-person training and assessments of the cyber risk profile of an organization's physical, behavioral and technical assets.

NOTES

1 https://cloud.google.com/learn/what-is-artificial-intelligence

2 (https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act)

3 https://sarbanes-oxley-act.com/#:~:text=Under%20the%20Sarbanes%2DOxley%20Act,that%20system%20of%20internal%20controls)

4 https://iapp.org/media/pdf/resource_center/us_state_ai_governance_legislation_tracker.pdf

5 https://oag.ca.gov/privacy/privacy-enforcement-actions

6 https://dmhc.ca.gov/Resources/Newsroom/PressReleases/June15,2023.aspx

7 https://www.legaldive.com/news/class-action-lawsuits-illinois-biometric-data-law-privacy-corporate-counsel-law-arent-fox-freeman/699258/

8 https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture