DLA Piper LLP (US)
10/8/2023

Privacy, Cyber, and AI as Material Issues: Key Considerations for Companies

By Andrew Serwin and Hayley Curry

Cybersecurity (“cyber”), data/privacy, artificial intelligence (“AI”) and other technology matters are now material issues for many companies, and there are many implications of that—the main one being the application of disparate and complex non-privacy and security-based laws to privacy and security professionals.[1] These change how privacy and security professionals do their jobs, as well as their own personal liability. This article identifies why such changes are necessary, as well as key considerations for companies as they think about their data practices in this new light.

Take-Aways Regarding SEC and Delaware Obligations

For public companies, the Securities and Exchange Commission (“SEC”) has enacted rules (the “Final Rules”) that require disclosure of a company’s cyber risks, cyber incidents, and Board-level cyber governance, and that will also require cyber and privacy professionals to create new processes and information systems to enable them to escalate certain issues, including to the Board.[2] The Final Rules do not focus on AI but note that “developments in artificial intelligence may exacerbate cybersecurity threats.” The consequences of failing to meet these standards can result in legal consequences for the company, the Board members, as well as certain officers.

Many large companies are incorporated in Delaware and thus are subject to Delaware law. Due to the application of the “internal affairs doctrine,” Delaware law defines the duties that the Board and certain officers owe the company—things that privacy and security professionals are not used to doing. Delaware law has existing requirements for the Board and certain officers—the duty of care and the duty of oversight, and also a structure for “governance.” Focusing on the duty of oversight, Delaware law requires the Board to: (a) have appropriate information systems to allow the escalation of red flags; and (b) not consciously disregard red flags the Board is aware of. Officers must “identify red flags, report upward, and address them if they fall within the officer’s area of responsibility…”

Compliance is Not Enough

Most privacy and security professionals have a compliance focus, which of course is important. However, both the SEC Final Rules and Delaware requirements go beyond substantive controls/compliance issues—they also include (directly or indirectly) requirements to have appropriate internal systems in place to identify, categorize, and escalate risks in certain circumstances. In short,

[1] This article is based upon *Defining Governance in a Hybrid World*, originally published on September 30, 2022, and *Understanding Delaware Fiduciary Duties—Putting Governance and Risk in Context and Reducing Personal Liability*, published in August 2023, both of which can be found at https://laresinstitute.com/publications.

[2] See our recent article, *New SEC Cyber Rules – A Deep Dive into Cybersecurity Processes to Support Accurate and Complete Disclosures*, published in September 2023, which can be found at https://privacymatters.dlapiper.com/2023/09/us-new-sec-cyber-rules-a-deep-dive-into-cybersecurity-processes-to-support-accurate-and-complete-disclosures/?utm_source=linkedin&utm_medium=social&utm_campaign=cyber&utm_term=us-privacy-matters-blog&utm_content=blog

there are important process requirements, in addition to the substantive “compliance” requirements that privacy and security professionals are used to addressing. This means there may be changes to budgets, the topics compliance professionals are trained on, upskilling and training of existing resources, as well as reallocation of existing resources to meet these obligations.

Operational Resiliency and the Link between Data and Critical Business Processes

Another “compliance-centric” issue must be considered as well. Delaware law identifies two primary risks the Board and officers should be focused on—legal compliance and operational viability/resilience. In short, legal compliance is one, but only one, of the risks that privacy and cyber professionals need to focus on under Delaware law—having a program that makes the company operationally resilient is also important.[3] To illustrate this point, if you are a compliance professional and focus exclusively on “being compliant” but do not consider what mission-critical “red flags” may exist in your substantive area, your program may be “compliant,” but it may not meet the requirements of Delaware law.[4]

And to understand why privacy and cyber are so critical to resiliency today, we can consider the reason that companies exist—namely, to return value to shareholders (i.e., create profit.) They do that by creating business processes that allow them to provide goods and services in a way that (hopefully) generates more revenue than the cost of providing the goods and services. That provides an important take-away: business processes are critical to businesses, and a business needs to take steps to protect those processes (i.e., be operationally resilient). That is key to understanding the context of technology and data risk.

In our highly-connected modern world, data is the propellant (fuel) for our current line of communication. And not just personal data. While most companies have personal data in some form, and some have a lot of it, not all important data is personal, and personal data is not the only form of data that fuels commerce. By focusing on privacy, with its inherent focus on the individual, we could miss the broader point that data—including, but not limited to, data regarding an individual—fuels our line of communication and, consequently, is critical to business processes.

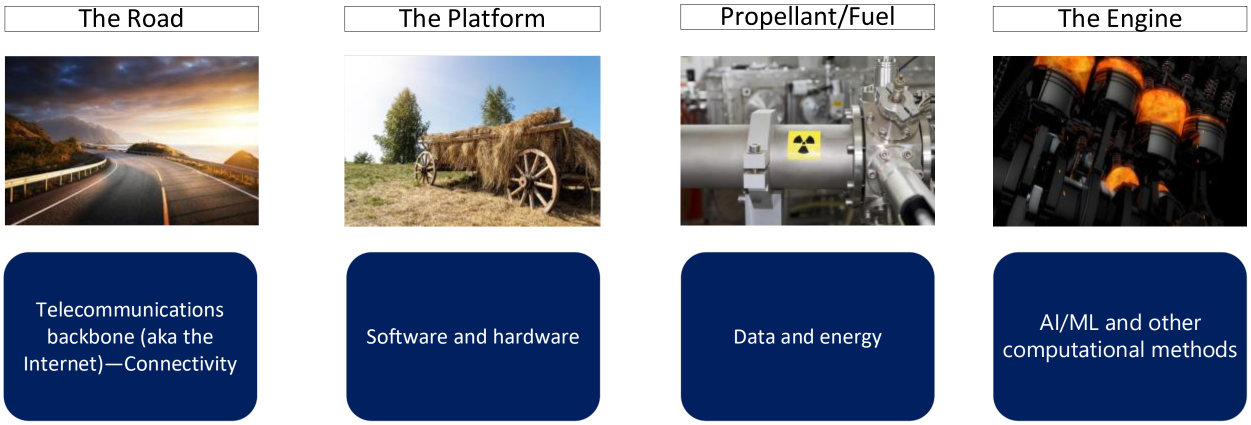
[3] Privacy professionals often try to broaden compliance to discuss terms like “brand” or trust. These terms have limited meaning in this context, but they are proxies for resiliency issues, and part of operating a key risk area like privacy is that privacy professionals will have to address resiliency risk in addition to compliance risk.

[4] As set out in *Marchand v. Barnhill*, “[T]he fact that Blue Bell nominally complied with FDA regulations does not imply that the *board* implemented a system to monitor food safety *at the board level*. Indeed, these types of routine regulatory requirements, although important, are not typically directed at the board. At best, Blue Bell’s compliance with these requirements shows only that management was following, in a nominal way, certain standard requirements of state and federal law. It does not rationally suggest that the board implemented a reporting system to monitor food safety or Blue Bell’s operational performance.” 212 A.3d 805, 824 (Del. 2019).

Components of a Line of Communication: Data = Fuel

What do we mean by a line of communication? To understand that, we must put into context the history of how society moves things over great expanses. Society has always looked for ways to connect itself, which required the creation of technology to do it, and understanding the core components to that process is important because there are certain consistencies in these methods of connecting—namely there is a medium that is used to connect (a "road"), a "platform" that travels along the road, an "engine" that propels that platform, and "propellant" or "fuel" that powers the engine. Over time, our ability to connect in a more efficient way has only increased, and not surprisingly the state—in many cases the military—created this technology.

Now, we connect in cyberspace via a web of networks that are linked via our current road, the telecommunications backbone, with myriad platforms, and the engines being computing power, including AI and machine learning, which is propelled by data. There are no natural or man-made borders, in most cases, with our current road, and the size of the engine keeps growing. And, as always, as the engine grows, so too does the need for the propellant—in this case data—making data and its related issues of privacy, cyber, and AI, vitally important to a company's business processes and operational resiliency.



The Road	The Platform	Propellant/Fuel	The Engine
Telecommunications backbone (aka the Internet)—Connectivity	Software and hardware	Data and energy	AI/ML and other computational methods

"Materiality," "Governance," and the Precision of Language

The precise terms we use are important here. Different stakeholders use different language; this is particularly true with technical Subject Matter Experts. Privacy, cyber and AI are no exception. As these are now "Board-level" issues, privacy and cyber professionals will need to learn the language of the Board, the SEC, and Delaware law, because gaps in language can lead to gaps in communication and understanding. Two examples illustrate the point.

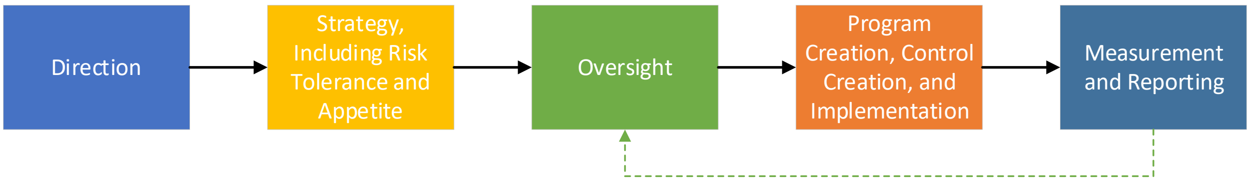
"Materiality" under SEC standards is very different than a cyber professional's definition of a "material" issue, or even how the Federal Trade Commission ("FTC") would define "materiality." So, when a privacy professional uses the word "material," is that under the FTC's deception authority, SEC requirements, or both? And is it a mission-critical red flag?

Another example is the use of the term "governance." Governance under Delaware law, and what the SEC is contemplating in the Final Rules, is very different than what a privacy or security professional typically means when they use this term. While this may seem like a pedantic point to raise—it is actually a substantive one. Both the SEC and Delaware law expect governance to have certain components that the typical privacy or security professional is likely not referencing and may not even be aware of. As the SEC Rule now has "governance" disclosure requirements, and since Delaware law provides substantive input on the topic, privacy and cyber professionals must use governance in the same way. And not just using the right word, but actually aligning how their program functions to these requirements and essentially "nesting" their governance structure into corporate governance models, so that they do not cause a material issue or red flag to not be addressed or escalated. In short, language gaps can cause other gaps, and those gaps can have consequences.

A Governance Process

The graphic below captures what governance is, including escalation, as represented by the green dashed line, coming from "Measurement and Reporting", which is essentially the information systems/information gathering capability of a company. It should be noted that governance obviously includes both oversight and operations concepts.

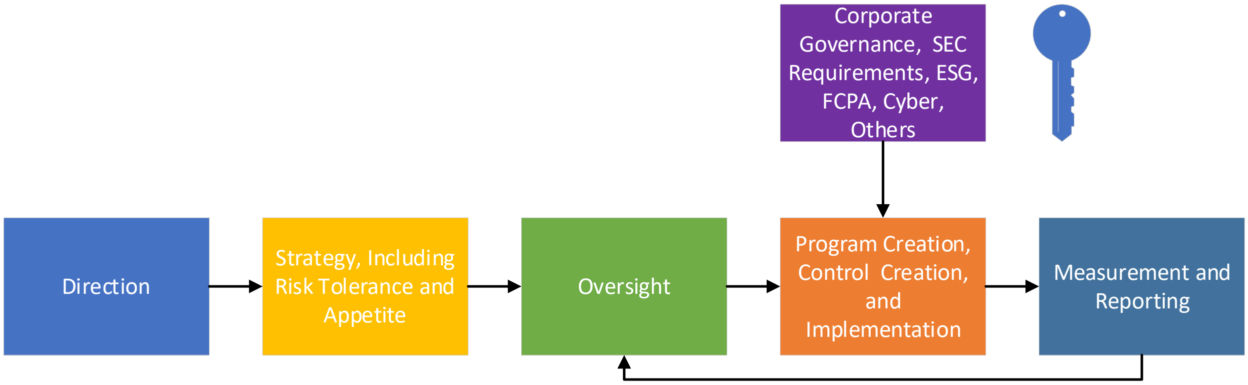
The Process


Direction
Strategy, Including Risk Tolerance and Appetite
Oversight
Program Creation, Control Creation, and Implementation
Measurement and Reporting

To help further differentiate these points, the direction that is set is a broad vision for a company. The strategy layer takes that direction and begins to tie it to actions. As an example, a company might have as its corporate direction to grow market share. Its strategy to accomplish that goal might be to acquire a number of different companies. If it desired to govern its growth process, it would then implement oversight, tie its operations to its direction and strategy, and measure and report on its progress towards its direction. Some companies differentiate direction and strategy by calling them corporate strategy versus business strategy, but the terms used are less important than the difference between the two—one is a broad vision, and the other takes that broad vision and begins to tie it to specific actions.

Turning to data risk, what many companies refer to as "privacy risk," we can look at the governance process a little more specifically. For many companies, strategy around data includes defining a risk appetite and risk tolerance, because many decisions about data use are driven by them. From an operations perspective, program and control creation and implementation are the critical points. As illustrated by the purple box below, the operations component can be "keyed" to any particular control framework, depending on what the company's direction and strategy are, and what laws or controls it wants to comply with.

The Process


Corporate Governance, SEC Requirements, ESG, FCPA, Cyber, Others
Direction
Strategy, Including Risk Tolerance and Appetite
Oversight
Program Creation, Control Creation, and Implementation
Measurement and Reporting

This process allows companies to have a structure to implement their direction and strategy in a governed way.

Substantive Controls are Just Part of the Equation

One final note related to what we are, and are not, saying. When we refer to “substantive” requirements, or “substantive controls”, we mean the ever-changing set of laws and enforcement that privacy and cyber professionals deal with daily. Those laws and actions provide a significant amount of the input for a program’s “controls”—what it should do to be legally compliant. Those are, and will remain, critical to address. In no way is this article saying that the FTC, federal and state privacy laws, the Attorneys General, or other key stakeholders in privacy or security are irrelevant. They all are still very relevant, and the “controls” should be part of the governance process.

Instead, this article illustrates that if all a privacy professional does is consider FTC opinions, or the latest state law—the “controls”—he or she will miss the rest of the structure, which is driven by non-privacy laws. Materiality requires us to look at issues not just through our area of substantive expertise, but to also consider other areas of law that impact the liability of the company, its directors, and privacy and cyber professionals. It also requires that we try and align our language to that of a company’s Board and Senior Leadership, and we have to do more than just focus on “compliance.” In other words, controls are part of a governance program, but merely having controls is not governance, at least under Delaware law, and likely also under the SEC’s expectations for governance disclosures.

And not making these changes and ignoring the requirements of the SEC and Delaware corporate law can come at a heavy price.