The Lares Institute

Understanding Delaware Fiduciary Duties—Putting Governance and Risk in Context and Reducing Personal Liability

August 2023

Contents

Executive Summary

This white paper is less about the "what" than the "why," which has been and will be covered in other articles and white papers. The core problem is this—cybersecurity ("cyber"), privacy, and other data issues are now material issues for many companies, and there are a number of implications of that, but the main issue is the application of non-privacy and security-based laws to privacy and security professionals. This changes how privacy and security professionals do their jobs, as well as their own personal liability.

For public companies, the Securities and Exchange Commission ("SEC") has now enacted a new rule that requires disclosure of a company's cyber risks, cyber events, and Board-level cyber governance, and that will require cyber and privacy professionals to create new processes and information systems to enable them to escalate certain issues, including to the Board. The consequences of failing to meet these standards can result in legal consequences for the company, the Board members, as well as for certain officers.

Many large companies are incorporated in Delaware. Due to the application of the internal affairs doctrine Delaware law defines the duties that the Board and certain officers owe the company—something 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…"

Most privacy and security professionals have a compliance focus, which of course is important. However, both the SEC Rule 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, there are important process requirements that, 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.

Another "compliance-centric" issue must be considered as well. As noted below, Delaware law identifies two primary main 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. To illustrate this point, if you are a compliance professional and focus exclusively on "being compliant", but don't 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.

the precise terms we use are important here. Different stakeholders use different language; this is particularly true with technical Subject Matter Experts (SMEs). Privacy a cyber are no exception. As privacy and cyber are "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 cause communication and understanding gaps. 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 new Cyber Rule 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 point. 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. Not just to use the right word, but to align how their program functions to these requirements, and essentially "nest" their governance structure into corporate governance models, so that they don't 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.

One final note related to what this white paper is, and is not, saying. When it refers to "substantive" requirements, or "substantive control requirements", that refers to 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. Also, in no way is this white paper 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 fit into the orange "control" box on page 13 under "data", "cyber" or another subject area as appropriate.

Instead, this white paper illustrates that if all a privacy professional does is consider FTC opinions, or the latest state law—the "control" box--they 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." This white paper identifies why we need to make these and other changes to what we currently do. In other words, controls are part of a governance program, but merely having controls isn't governance, at least under Delaware law, and likely 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.

Introduction

Privacy professionals for years have long touted the importance of their field, claiming that it should be a matter of concern for Boards of Directors, , often citing potential FTC actions or the size of the potential for GDPR fines, which in the case of GDPR overall haven't materialized in the way that was predicted. Privacy is an important issue on any number of fronts, including for companies, and can be an issue for the Board oversight. The challenge with this approach, apart from the relative rarity of FTC actions or the lack of large GDPR fines, is that the issue is viewed though the wrong lens. Laws outside privacy and data protection help guide what is, and is not, a Board level issue.

This can be seen by considering the answers to a series of questions:

> Do you think privacy or cyber is a "Board-level" issue for your company?
>
> Do you think privacy or cyber is a material issue for your company?
>
> Do you think privacy or cyber is a mission-critical issue for your company?

Many privacy and cyber professionals would say yes to all of these questions, without fully appreciating the implications of their answers—namely the application of a disparate and complex set of legal and business requirements that impact the ways in which privacy or cyber professionals manage their responsibilities, as well as their personal liability. These requirements also change how these professionals should interact with their leadership, the language they should use to communicate risk and value, as well as nature and the volume of information the professional escalates and expects other corporate leaders to assimilate and understand. It also requires us to understand the "Internet" in context so that we can appropriately assess materiality from both a quantitative and qualitative perspective, as well as resiliency.

In short, when your area of responsibility is material to a company, that has consequences and, including that your personal liability has likely increased, and that your job has changed.

Understanding SEC and Delaware Obligations

Why Do For-Profit Companies Exist?

For-profit corporations do not exist to protect privacy—they exist to return value to shareholders. That is not to say they only focus on profit in every decision, but it is to say that when the conduct of the officers and directors is measured and assessed, it is assessed by the shareholders against this metric. Not surprisingly, the Board of Directors for a public company is elected by the shareholders to protect the interests of the shareholders.[1] And ultimately that is returning value to the shareholders.

Publicly traded companies are subject to a variety of obligations imposed by the SEC, as well as Delaware law, if the company is incorporated in Delaware, and many are—over 60% of the Fortune 500 are in fact incorporated in Delaware.[2]

[1] https://www.finra.org/investors/insights/get-board-understanding-role-corporate-directors#:~:text=In%20general%2C%20the%20role%20of,impact%20on%20a%20company's%20profitability.

[2] https://www.cnbc.com/2023/03/13/why-more-than-60percent-of-fortune-500-companies-incorporated-in-delaware.html

A key distinction to understand up front is that with the exception of areas such as Sarbanes-Oxley (SOX), SEC requirements are not substantive control requirements—they are instead disclosure requirements, which in turn necessitate the implementation of appropriate procedures. The substantive law regarding duties to the corporation are generally covered in state law. To perhaps deal with SOX up-front, so we can move past it, SOX was passed in reaction to some high-profile accounting scandals and mandated a series of accounting controls and record keeping around financial data. There are certification requirements by certain officers, internal controls requirements, record keeping requirements, as well as some IT requirements around certain systems in a company. While the mandates go beyond disclosure requirements, ultimately these reforms were passed to try to restore investor confidence in the financial disclosures of public companies. While relevant for public companies generally, these requirements don't impact the privacy or cyber professional. The same cannot be said for other SEC requirements however.

SEC Obligations Summarized

The key take-aways here are: SEC obligations apply only to publicly traded companies in the US (with some limited exceptions); and the focus is on disclosure of information to the investing public, not on the quality of controls in any particular risk area, with the exception at some level regarding disclosure controls, though the ultimate purpose of those is public disclosure.

The focus of the SEC requirements is disclosure to the investing public, and there are two acts that are relevant, as well as the new Cyber Rule. The Securities Act of 1933 imposes disclosure obligations upon companies when they file their initial registration forms to go public—i.e. the initial sale of securities. The Securities Act of 1934 imposes disclosure obligations upon companies on a periodic basis, and includes the 10-K, 10-Q, and 8-K filings, and these are disclosures that are required related to the secondary market for securities, which is why they are ongoing past the initial sale of securities. It is important to keep that in mind as one examines these requirements, because the purpose of both requirements is to keep investors appropriately informed at the initial sale of securities, and on an ongoing basis, about certain information.

Both acts essentially prohibit false or misleading statements about "material" facts, and that includes risks the company faces, as well as events that could impact the company. It is important to note that both affirmative misstatements are prohibited, as well as the omission of facts, if either are material.

The SEC just enacted a new Cyber Rule which adds additional disclosure obligations on public companies. There are new 8-K requirements for cyber security events, including around updating an 8-K if certain conditions are met; new cyber risk management disclosures in Form 10-K mandating that companies describe their processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any such risks have materially affected or are reasonably likely to materially affect the company; new cyber governance disclosure requirements[3] that require the company to describe the board's oversight of material risks from cybersecurity threats and management's role and expertise in assessing and managing such risks; as well as certain other requirements.

[3] While not every large company is incorporated in Delaware, it is quite possible that the SEC will expect cyber governance to track the structure that Delaware sets forth given the prominence and prevalence of Delaware-centric governance models in the Fortune 500.

In short—there are requirements to disclose cyber risks, cyber incidents, and cyber governance.

Another common SEC issue is insider trading under Rule 10b-5. While companies will implement controls to try and prevent insider trading, the core issue is the same—the public being at an information disadvantage when they trade securities—at least as it relates to material, non-public information.

Materiality is a challenging concept which has been summarized as follows:

> The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.
>
> This formulation in the accounting literature is in substance identical to the formulation used by the courts in interpreting the federal securities laws. The Supreme Court has held that a fact is material if there is –
>
> a substantial likelihood that the . . . fact would have been viewed by the reasonable investor as having significantly altered the "total mix" of information made available.
>
> Under the governing principles, an assessment of materiality requires that one views the facts in the context of the "surrounding circumstances," as the accounting literature puts it, or the "total mix" of information, in the words of the Supreme Court.[4]

In summary, the SEC requirements prohibit false or misleading statements regarding material facts, and those statements can relate to the disclosure of the company's risk posture, as well as events that impact the company. They do not, however, impose substantive "control" obligations in the context that we are examining the SEC requirements. That instead falls to other regulators such as the FTC, as well as other laws at the federal and state level that impose substantive requirements that a company must meet to be "compliant" with privacy and security laws. In other words, a company could have poor privacy or cyber risk controls, and as long as those were adequately disclosed, it might not violate the disclosure provisions of the federal securities laws, though that approach obviously would not work with the FTC with its substantive focus.

One important thing to note is that the new Cyber Rule also requires an examination of both quantitative and qualitative issues for disclosure purposes, which complicates the analysis. In some ways, the qualitative analysis may be similar to an examination of resiliency risks under Delaware law, but it will depend in some ways on how the SEC interprets and enforces this portion of the Rule.

So how does this impact a privacy or cyber risk professional? The risk professional must be able to not just create a program that is substantively "compliant", but also assess, and escalate, both material risks the company faces, as well as material events because the company needs to have appropriate information gathering, escalation and disclosure controls and procedures (DCPs) to ensure that the public disclosures are not false or misleading. Specifically, one of the provisions of the federal securities laws requires publicly traded companies to have DCPs designed to ensure that information that is

[4] https://www.sec.gov/interps/account/sab99.htm#body4

required to be disclosed to investors is recorded, processed, summarized and reported timely.[5] As referenced above, the SEC expects that a company's DCPs will cover a broader range of conduct than SOX-related controls, such as non-financial risks related to the company's business. And a company's principal executive and financial officers must certify whether the company's DCPs are effective.[6] Ultimately, many of these issues relate to information sharing—sharing within the company, as well as sharing with key stakeholders externally. Sharing externally will help companies understand context for qualitative risks, including risks that may relate to national security issues around cyber.

In short, where issues are material to a company, that means that the risk professional's job now includes assessment of risk under federal securities laws, as well as the creation of systems for information gathering, escalation and input into the disclosure control process. None of this has anything to do with the substantive or other control requirements of CCPA, GDPR, the NIST framework, or any other privacy or cyber-centric set of control requirements—it has everything to do with the SEC requirements, and as noted above, the quality of controls isn't the focus in these areas—the appropriate disclosure of risk posture and events is the focus.

While the lack of substantive control requirements under the SEC Rule might provide some comfort (recognizing that this doesn't absolve the company of its existing substantive compliance obligations), the application of state law complicates that answer even more, particularly around governance.

Delaware Law Summarized

Why Does Delaware Law Matter?

There is some irony in the application of Delaware law to privacy, and while it is likely not intuitive for most privacy professionals, it should be.[7] If we examine Article 3 of GDPR, GDPR will apply to processing of data by a controller or processor in the context of the activities of an establishment in the EU, regardless of whether the processing takes place in the Union or not. GDPR can also apply, at least in certain circumstances, where there is no establishment in the EU, but the data subject resides in the EU. In short, residency matters.

Data protection laws at the state level follow a similar pattern. Using California law as an example, the data breach law applies to breaches involving the data of a California resident under Cal. Civ. Code § 1798.82(a), and that answer is true on a state-by-state basis across the US for data breach laws. Similarly, we see the same concept in the new state privacy laws, like CCPA—the individuals that have rights under CCPA are "consumers", defined as "a natural person who is a California resident…" Cal. Civ. Code § 1798.140, and this tracks through other state privacy laws. In short, residency matters.

Corporations are formed under state law in the US, and that is, no matter what, a place where the corporation "resides", and is always subject to jurisdiction. In GDPR parlance, it is where the corporation is "established." Welcome to the internal affairs doctrine, and it provides that ultimately one state law is the only one that matters for the internal affairs of a corporation.

---

[5] 17 C.F.R. § 240.13a-15.

[6] *Id.*

[7] While we use different terms for the internal affairs doctrine, it essentially, like GDPR, imposes substantive requirements on companies due to an "establishment" in a particular state—Delaware in most cases for large companies.

The Internal Affairs Doctrine

Delaware law, as well as holdings by the Supreme Court, make clear the importance of state law regarding how the relationships and duties of shareholders, the company, directors, and officers, are defined:

> The internal affairs doctrine is a conflict of laws principle which recognizes that only one State should have the authority to regulate a corporation's internal affairs—matters peculiar to the relationships among or between the corporation and its current officers, directors, and shareholders—because otherwise a corporation could be faced with conflicting demands. *Edgar v. MITE Corp.*, 457 U.S. 624, 645 (1982) (citing Restatement (Second) of Conflict of Laws § 302 cut. b. (1971)). *JUUL Labs, Inc. v. Grove*, C.A. No. 2020-0005-JTL (Del. Ch. Aug. 13, 2020).

The Supreme Court has also been explicit about the role of state law and the reliance of investors on it, even over federal law, absent specific circumstances:

> Corporations are creatures of state law, and investors commit their funds to corporate directors on the understanding that, except where federal law expressly requires certain responsibilities of directors with respect to stockholders, state law will govern the internal affairs of the corporation. *Cort v. Ash*, 422 U.S. 66, 84 (1975), abrogated on other grounds by *Act Transamerica Mortg. Advisors, Inc. (TAMA) v. Lewis*, 444 U.S. 11, 15 (1979).

In short, it is important to understand the scope of Delaware law (or other applicable state laws depending upon the state of incorporation) because those laws are without question applicable to the directors and officers, and in fact define the duties they owe to the company. Said differently, if governance is defined by one body of law, it is defined by state corporate law. As a result, for a privacy or cyber professional, it is critical to understand at some level the structure and requirements of Delaware law, at least if you believe that privacy and cyber are "mission-critical" for your company.

Operations Versus Oversight

Under Delaware law, companies "shall be managed by or under the direction of a board of directors…"[8] Most Boards delegate the management of the corporation to a management team, and instead the Board assumes an oversight role—the "under the direction of the board of directors" prong. This is an important distinction and illustrates the difference between operating a company, and overseeing a company, and most Boards of public companies are in an oversight role, with certain limited exceptions.

The Two Main Duties

It is important to note the two fiduciary duties under Delaware law—the duty of care and the duty of loyalty, and both are applicable to officers and directors. [9] The duty of loyalty includes good faith, which is central to oversight claims under *Caremark*, which has always been applicable to directors, and was recently extended to officers.

[8] §141 DGCL.

[9] *Gantler v. Stephens*, 965 A.2d 695, 708-9 (Del. 2009) ("In the past, we have implied that officers of Delaware corporations, like directors, owe fiduciary duties of care and loyalty, and that the fiduciary duties of officers are the same as those of directors. We now explicitly so hold.")

Corporate Principles

Before we examine the duties of care and loyalty, it is important to note that there are multiple issues that directors and officers should consider in discharging their duties. It is beyond question that directors and officers must consider business strategy issues when discharging their duties. [10] In addition, as illustrated in *Marchand*, the duty of oversight includes more than just legal compliance:

> Under *Caremark* and this Court's opinion in *Stone v. Ritter*, directors have a duty "to exercise oversight" and to monitor the corporation's operational viability, legal compliance, and financial performance.

That leads us to the use of the graphic below and illustrates the point the operational resilience and legal compliance are both risks that must be considered by officers and directors, and as *Marchand*, illustrates resiliency and legal compliance are not the same risk.[11]

Most privacy professionals are in legal or compliance organizations in companies, and compliance is their focus. However, as shown above, compliance is only one of the risks that Delaware law looks at when assessing oversight. Privacy professionals often try to broaden compliance to discuss terms like "brand" or trust. These terms have limited meaning in this context. However, as discussed below, 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; and learn and use the language of Delaware law and the Board on these points.

The Duty of Care

The duty of care, at its core, requires informed, deliberative decision-making based upon all material reasonably available. Boards can, in good faith, rely upon information they are provided by

[10] **Business judgment rule**: Although some major transactions require the consent of stockholders as well as the approval of the board, the board generally has the power and duty to make business decisions for the corporation. These decisions include establishing and overseeing the corporation's long-term business plans and strategies, and the hiring and firing of executive officers. https://corplaw.delaware.gov/delaware-way-business-judgment/

[11] "But the 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." *Marchand v. Barnhill*, 212 A.3d 805, 824 (Del. 2019).

management, as well as third-party experts in certain cases. [12] The duty has been summarized as follows:

> **Duty of care**: In managing and overseeing a corporation's business and affairs, directors must both make decisions and rely on subordinates. The duty of care requires directors to make informed business decisions but recognizes that directors must make decisions constantly and cannot spend forever on each one. Thus, directors are not required to review all information in making their decisions—only the information that is material to the decision before them. Nevertheless, in evaluating information provided to them by management, directors are expected to review the information critically and not accept it blindly.[13]

Where there is no breach of the duty of loyalty, the applicable standard for the duty of care is gross negligence. [14] This includes claims predicated upon the assertion that the directors did not review sufficient information before making a decision. [15] Officers owe a duty of care to the company also, subject to the same standards. Ultimately, these issues will be examined through the business judgment rule.[16]

One key takeaway here for privacy professionals—one thing that is discussed at times is whether Boards should review a significant amount of regulation/information about privacy, cyber, or other similar topics. That is not what Delaware law really contemplates, as shown above, and it is the privacy professional's job to help the Board understand what is, and is not, material to their oversight responsibilities or to a particular decision. Whatever that is, it is not thousands of pages of regulation.

The Duty of Loyalty

There are several components to the duty of loyalty, and it is summarized as follows:

---

[12] "A member of the board of directors, or a member of any committee designated by the board of directors, shall, in the performance of such member's duties, be fully protected in relying in good faith upon the records of the corporation and upon such information, opinions, reports or statements presented to the corporation by any of the corporation's officers or employees, or committees of the board of directors, or by any other person as to matters the member reasonably believes are within such other person's professional or expert competence and who has been selected with reasonable care by or on behalf of the corporation." §141(e) DGCL.

[13] https://corplaw.delaware.gov/delaware-way-business-judgment/

[14] *Aronson v. Lewis*, 473 A.2d 805 (Del. 1984)

[15] "We think the concept of gross negligence is also the proper standard for determining whether a business judgment reached by a board of directors was an informed one." https://casetext.com/case/smith-v-van-gorkom

[16] "Under Delaware law, the business judgment rule is the offspring of the fundamental principle, codified in 8 Del. C. § 141(a), that the business and affairs of a Delaware corporation are managed by or under its board of directors. In carrying out their managerial roles, directors are charged with an unyielding fiduciary duty to the corporation and its shareholders. … Under the business judgment rule there is no protection for directors who have made 'an unintelligent or unadvised judgment.' A director's duty to inform himself in preparation for a decision derives from the fiduciary capacity in which he serves the corporation and its stockholders. Since a director is vested with the responsibility for the management of the affairs of the corporation, he must execute that duty with the recognition that he acts on behalf of others." (citations omitted). *Smith v. Van Gorkom*, 488 A.2d 858 (1985).

> Broadly stated, the duty of loyalty requires directors to act in good faith to advance the best interests of the corporation and, similarly, to refrain from conduct that injures the corporation.[17]

Of particular note is the duty of loyalty includes the duty of oversight under *Caremark*.

Caremark

There are two prongs to potential *Caremark* liability—Directors or officers cannot:

- consciously fail to implement a board-level system to monitor reasonably company compliance with applicable law and related company protocols (an "Information-Systems" Claim); or
- having implemented such a system, consciously ignore red flags signaling material company noncompliance with such law and protocols (a "Red Flags" Claim).

A recent case involving an ice cream manufacturer illustrates the first prong of the *Caremark* test for "mission critical" risks. In *Marchand v. Barnhill*, (Blue Bell) the plaintiff alleged that the board failed to have systems in place for monitoring or reporting on food safety—a "mission critical" issue for a food company.

> Although *Caremark* may not require as much as some commentators wish, it does require that a board make a good faith effort to put in place a reasonable system of monitoring and reporting about the corporation's central compliance risks. In Blue Bell's case, food safety was essential and mission critical. The complaint pled facts supporting a fair inference that no board-level system of monitoring or reporting on food safety existed.[18]

Caremark and Officer Liability

In a recent case, the Court of Chancery held that officers also have oversight duties under *Caremark*.

> The foregoing authorities all indicate that officers owe oversight duties. A contrary holding would create a gap in the ability of directors to hold officers accountable. Reasonable minds can disagree about whether, as a matter of policy, stockholders should be able to sue to hold an officer accountable for a failure to exercise oversight. *But wherever one might stand on that issue, it is hard to argue that a board of directors should not be able to hold an officer accountable for a failure of oversight. As the preceding discussion shows, an indispensable part of an officer's job is to gather information and provide timely reports to the board about the officer's area of responsibility.* Pause for a moment and envision an officer telling a board that the officer did not have any obligation to gather information and provide timely reports to the board. The directors would quickly disabuse the officer of that notion, and an officer who did not get with the program would not hold that position for long.
>
> …
>
> *Another critical part of an officer's job is to identify red flags, report upward, and address them if they fall within the officer's area of responsibility*. Once again, pause and envision an officer

[17] https://corplaw.delaware.gov/delaware-way-business-judgment/
[18] *Marchand v. Barnhill*, 212 A.3d 805, 824 (Del. 2019).

> telling the board that their job did not include any obligation to report on red flags or to address them. A similar learning opportunity would result. (Emphasis added).[19]

Key Take-Aways Regarding SEC and Delaware Law

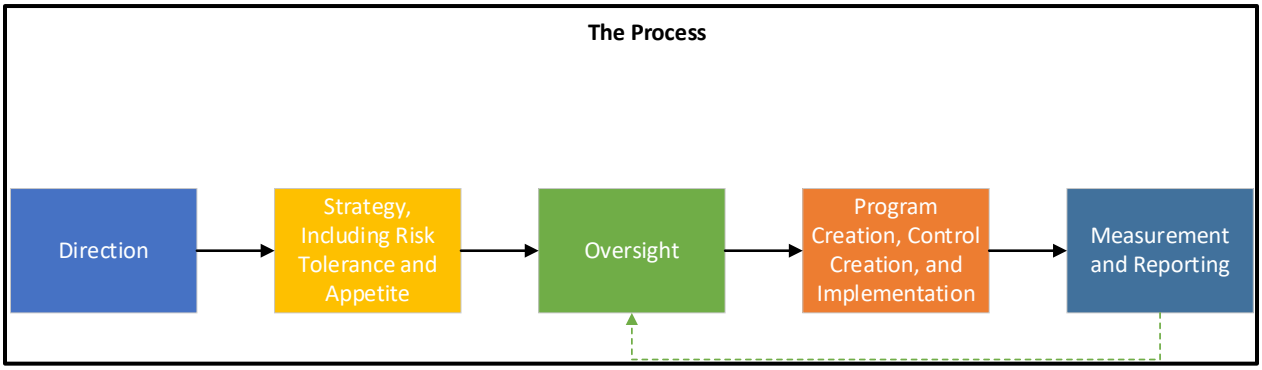
The SEC requirements in this context focus almost exclusively on disclosure of material facts regarding risks and events, but do not contain substantive requirements as state law does. However, adequately disclosing risks and events requires that companies have appropriate information systems in material areas, as well as escalation policies to ensure that the disclosure process works appropriately.

Delaware law imposes general substantive requirements upon fiduciaries—they owe duties of care and loyalty. Directors may be found liable under *Caremark* if they consciously fail to implement certain information systems, or consciously ignore "red flags." In the case of officers, they are obligated to identify, escalate, and address, red flags, if they fall within the officer's area of responsibility.

Governance

Implicit within Delaware law, and now explicit in the SEC Cyber Rule, is the concept of adequate governance. It is not what the FTC just said on a particular topic, what the NIST framework provides, or a set of controls in any particular subject area regarding privacy or cyber. Governance of a corporation is purely a matter of internal affairs, and while individual programs may be managed or "governed", that is not governance under Delaware law. And now that the SEC has added a specific disclosure requirement regarding cyber governance, it is all the more important to have a consistent definition and approach.

The graphic below captures what governance is, including escalation, as represented by the green 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.



Differing Governance Obligations

While the Board and certain senior officers have company-wide remits, not all officers do, and in fact most privacy or cyber professionals would not have company-wide remits:

> Although the duty of oversight applies equally to officers, its context-driven application will differ. Some officers, like the CEO, have a company-wide remit. Other officers have particular areas of responsibility, and the officer's duty to make a good faith effort to establish an

[19] *IN RE MCDONALD'S CORPORATION STOCKHOLDER DERIVATIVE LITIGATION*, C.A. No. 2021-0324-JTL (2023).

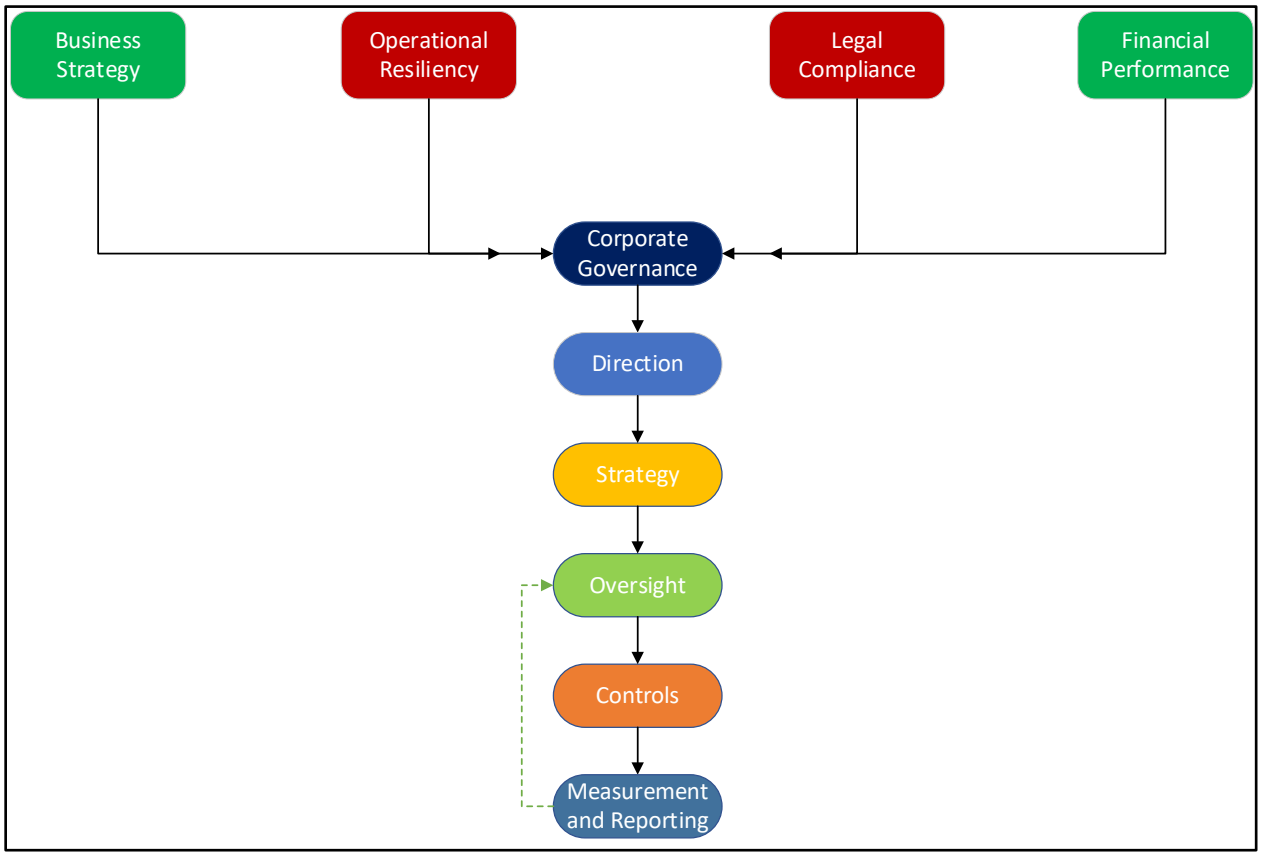
> information system only applies within that area. An officer's duty to address and report upward about red flags also generally applies within the officer's area, although a particularly egregious red flag might require an officer to say something even if it fell outside the officer's domain. As with the director's duty of oversight, establishing a breach of the officer's duty of oversight requires pleading and later proving disloyal conduct that takes the form of bad faith.
>
> …
>
> Most notably, directors are charged with plenary authority over the business and affairs of the corporation. *See* 8 Del. C. § 141(a). That means that "the buck stops with the Board." *In re Del Monte Foods Co. S'holders Litig.*, 25 A.3d 813, 835 (Del. Ch. 2011). It also means that the board has oversight duties regarding the corporation as a whole. Although the CEO and Chief Compliance Officer likely will have company-wide oversight portfolios, other officers generally have a more constrained area of authority. With a constrained area of responsibility comes a constrained version of the duty that supports an Information-Systems Claim.
>
> …
>
> For similar reasons, officers generally only will be responsible for addressing or reporting red flags within their areas of responsibility, although one can imagine possible exceptions. If a red flag is sufficiently prominent, for example, then any officer might have a duty to report upward about it. An officer who receives credible information indicating that the corporation is violating the law cannot turn a blind eye and dismiss the issue as "not in my area."[20]

This, in essence, illustrates the concept of "nested governance", and the difference between program governance and corporate governance within nested governance. However, given the importance of consistency in escalation and disclosure, it is important for companies to try and have similar processes in each subject area. Nested governance is discussed below.

[20] *IN RE MCDONALD'S CORPORATION STOCKHOLDER DERIVATIVE LITIGATION*, C.A. No. 2021-0324-JTL (2023).

Corporate Governance

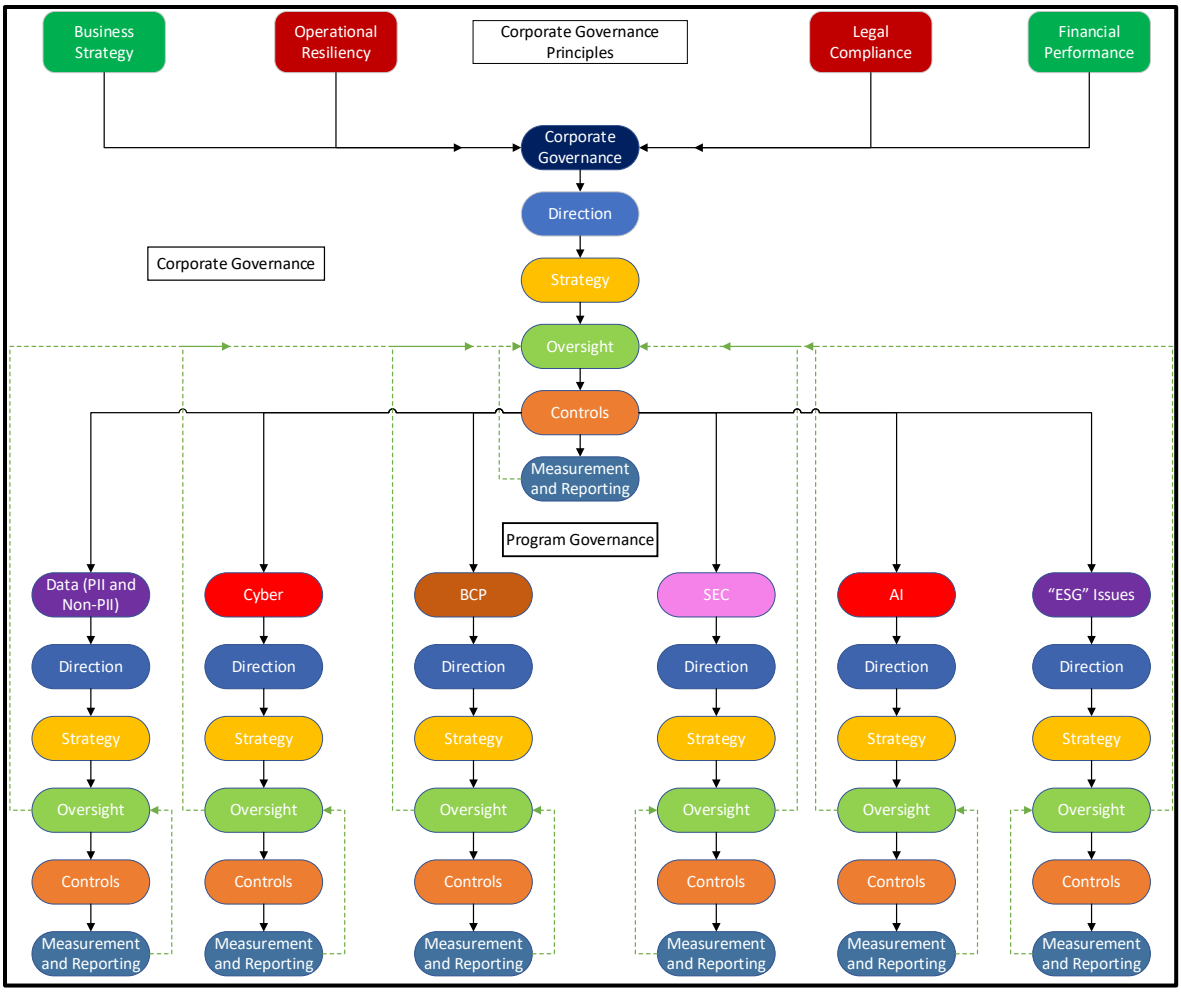
To create a corporate governance framework, we can simply take the 4 principles of risk and value for corporations, noted above, and combine them with the 5 steps of the governance process. This defines corporate governance on an enterprise basis.



While that works for the directors and officers with company-wide responsibility, that doesn't address how officers would handle governance in a narrower area, recognizing however that they do have responsibilities to escalate red flags outside of their particular subject area.

Nested Governance

The concept of "nested governance" recognizes the fact that to actually achieve appropriate governance of the relevant subject areas, it is helpful to apply the same processes and standards in the individual subject areas that are material or "mission-critical" for a company. Nested governance would look like this:



In short, what this creates is an integrated system of governance that is consistent with Delaware law and facilitates the escalation of red flags. Where these stacks will differ the most is around the control area—technology risk controls are different than data risk controls, without question. However, by using the same processes and criteria to govern the effectiveness of those different controls, as well as the escalation of red flags, you make everyone's job easier, and make it easier for the C-Suite and the Board, who have enterprise-wide responsibility, to understand and act upon these issues.

The Materiality Fallacy—An Over-Emphasis on Legal Risk

Privacy and security professionals are not alone in wanting others to understand and appreciate the importance of what we do. In many cases, privacy, or at least data risk, is a material issue for companies, but not always. Even where privacy issues aren't material, that doesn't mean companies won't address and fund privacy initiatives, and part of that is having the right infrastructure to assess the risks, even if the risks aren't always Board-level issues.

There are any number of issues and business processes that aren't material or "Board-level" that are well-funded by companies because the company doesn't want to deal with the loss of a business process, or litigation, even if it isn't material. So what does this mean—it means that privacy professionals need to be clear about the "why" here—a Fortune 500 company having to settle a case for a significant amount of money is still something the company will not want to do. Losing a business

process that may not be "material", but is still important, is also something a company will want to avoid, but the cost-benefit analysis has to be based upon the actual risk versus the cost, and that cost isn't always a fine—it can be the breakage of a business process.

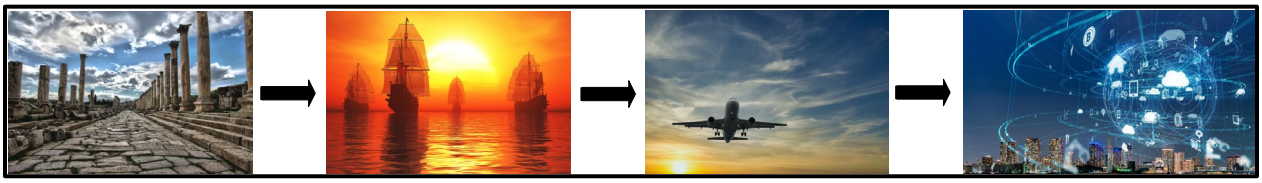
In other words, the emphasis has always been skewed to the legal compliance risk in privacy—remember the 4% fines--which is why GDPR was always used as an example of a reason to invest in privacy. Resiliency---and I would include issues such as "brand" and "trust" are resiliency impacts and frequently justify spend on privacy, but if they aren't put in the context of what the Board and Senior Leaders understand, the reason for the request may not be fully understood. The point here is that putting "privacy" into context that the Board and Senior Leaders are used to will help funding and people to actually understand the risks that privacy creates.[21]

Whether it is due to the SEC's qualitative risk disclosures, or to assess resiliency risk, context matters. In order to understand the risks in context, and that requires us to re-examine how we think of traditional roles in companies, what "privacy" and "cyber" risk really are, as well as what we actually did when we started using the Internet, and we will examine that now.

Putting Technology, Data, and AI Risk in Context

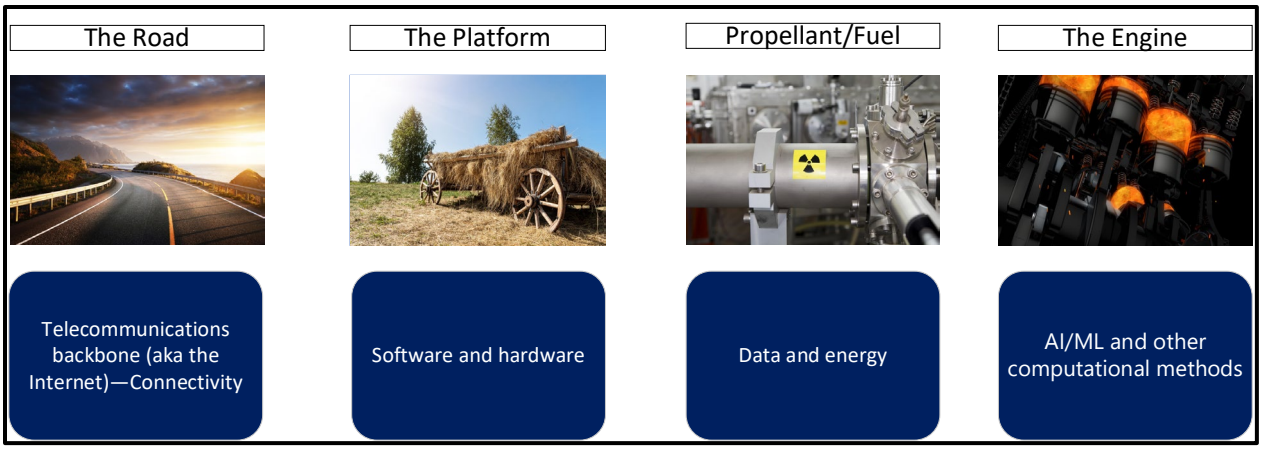
To put technology, data, and AI risk in context requires us to return to where we started—the reason that companies exist. Companies exist to return value to shareholders. They do that by creating business processes that allow them to provide goods and services in a way that (hopefully) generates more revenue than the cost of providing the goods and services. That is critical to understanding the context of technology, data, and AI risk.

An easy way to rethink these risks is to realize that society always creates "Lines of Communication" to engage in commerce, communicate, and do a variety of other things. Examples over time include, roads, ships, planes, and now the Internet:

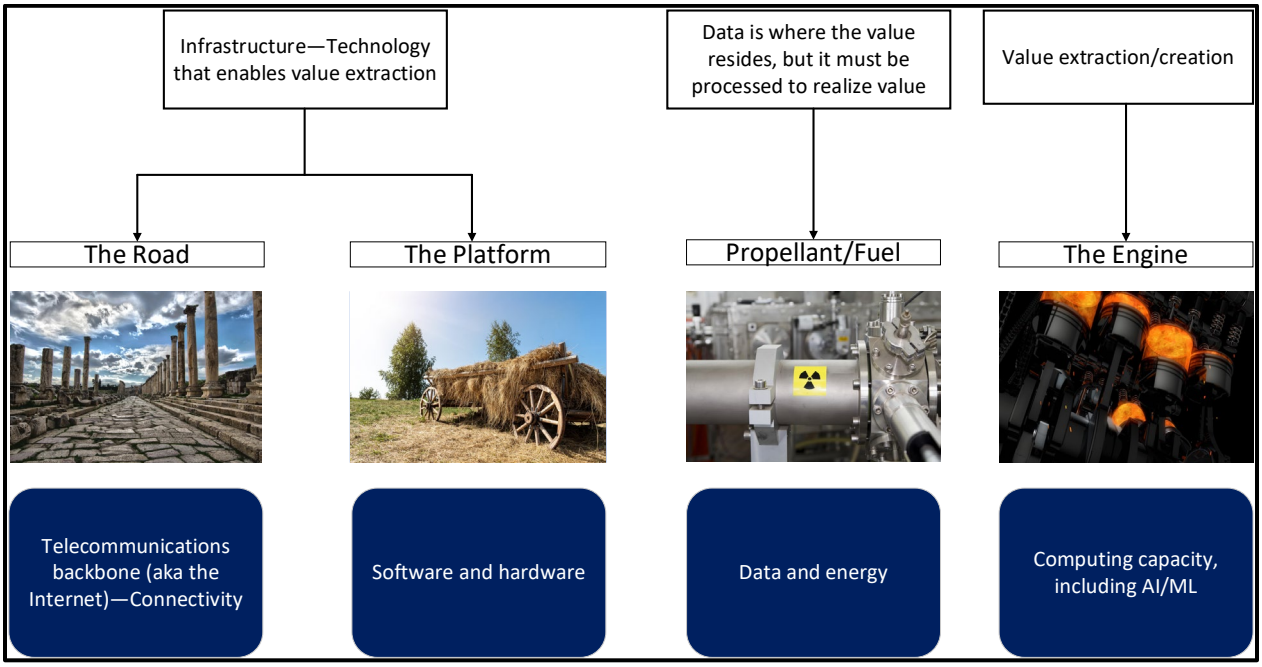


Each line of communication has 4 components that make it function—a road, a platform, fuel, and an engine, and the components of our current Line of Communication are below:

[21] At times DOJ guidance is used to assess a program's effectiveness. While that analysis can be helpful to assess whether the program of controls you have implemented have been adequately resourced, that guidance doesn't speak to how to create governance as Delaware law does. The distinction here is controls versus governance, with controls being a necessary, but not sufficient, condition for governance.



If we combine the road and the platform—which are both infrastructure issues, we have a category of technology risk. We then have data risk, as well as AI risk accounted for as well.



Combining Delaware Corporate Principles and Technology, Data, and AI Risk

To take the final step, and to illustrate where some companies struggle with these risks, we return to the 4 corporate principles, and note again the statement in *Marchand* regarding the distinction between legal compliance and operational resiliency:

Examples of Resiliency and Legal Compliance Impacts

It is also perhaps helpful to provide additional context on these risks with examples of issues that they present. To illustrate the point, the examples below are based upon data risk.

Examples of operational resilience risk impacts include:

- **Business interruption to company & its customers**
    - Slowed or total inability to send or receive goods or services (e.g., from manufacturing or payroll vendors) or provide goods or services (i.e., to customers)
    - Loss of access to critical internal systems
    - Productivity loss resulting from inability to access vendor systems and services
    - Slowed communications (e.g., related to email and other communications or infrastructure vendors)
    - Customer invoked restrictions on processing data (e.g., Client requests all its data be deleted, or access to systems be turned off)
    - Deletion or loss of learnings/algorithms and data
    - Impact on M&A activity
    - Brand/reputational harm and other PR-related issues
    - Distraction from the company's core purpose, including significant impact on senior executive's time
    - Limitation of strategic initiatives due to conduct restrictions or data and algorithm restrictions
- **Financial impact**
    - Customer churn/loss of revenue
    - Reduction in shareholder value (erosion of stock price and/or dividends)
- **Increased costs**

Examples of legal compliance risk impacts include:

- **Breach of customer contract or indemnity claims**

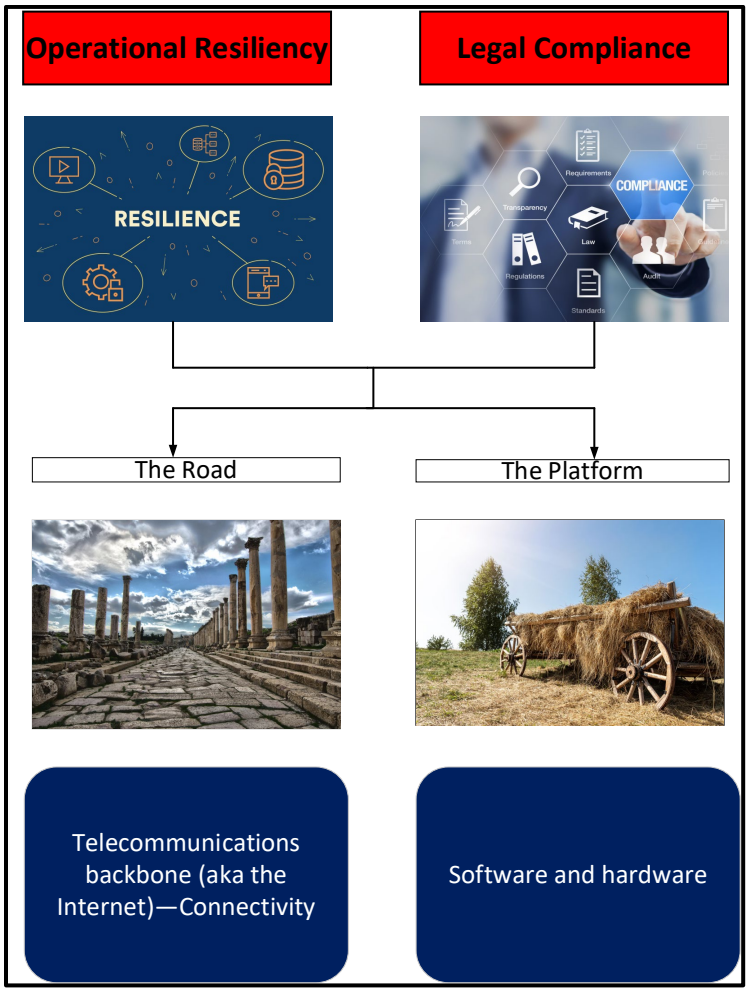
    - Failure to meet SLAs
    - Inability to comply with incident notification timing or content requirements in customer contracts
    - Failure to adequately protect customer data shared with third parties
    - Penalties
    - Increased customer demands for controls leading to higher costs
- **Regulatory, investigations and/or enforcement for mishandling incidents**
    - Fines, injunctions, consent orders
    - Regulator mandated restrictions on processing data (e.g., regulator limits permitted data uses)
    - Blocking of transfers, deletion of algorithms and learnings, as well as data
    - Increased compliance requirements that drive up costs
- **Class-action, or other litigation resulting from failure to adequately protect information**

There are other issues to consider that are part of a broader information sharing strategy that is both internal and external, and includes private/private and public/private sharing. This is particularly true where the threat actors create national security risk through their activities.

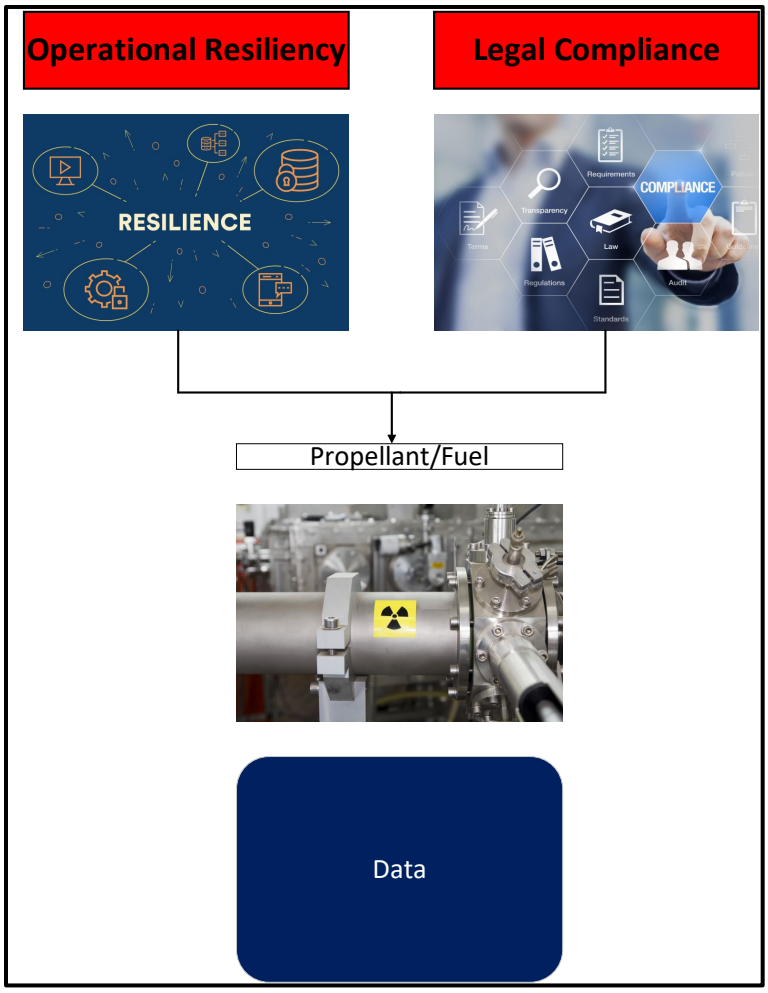
Creating Technology, Data, and AI Risk Governance

To begin to visualize how to govern (which includes both oversight and operations concepts) technology, data, and AI risk, one need only combine the last two graphics.

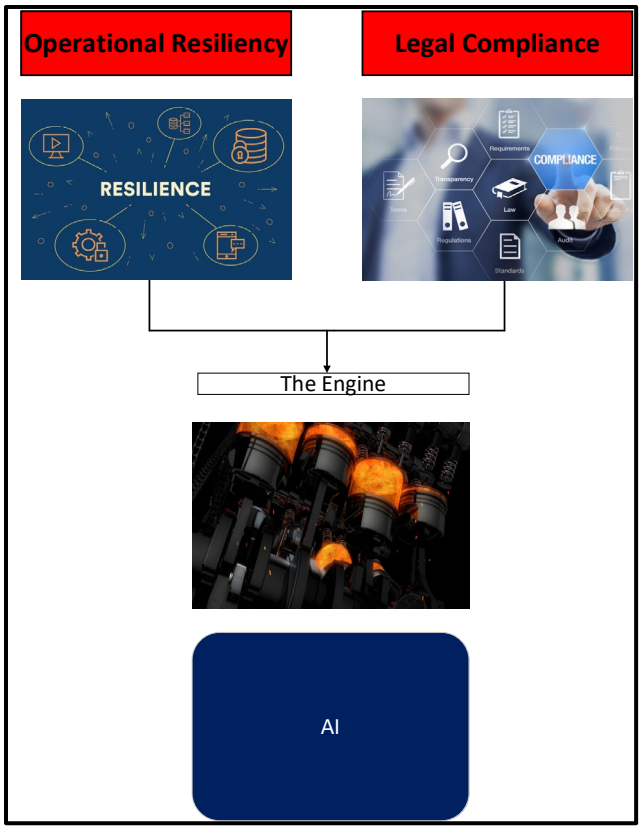
Technology risk:



Data risk:



AI risk:



Redefining Requests

Taking the SEC and Delaware requirements, as well as the discussion above about how to redefine risks, we can begin to change the dialogue, including resource implications. To use GDPR as an example, some used the specter of fines as a way to try and get companies to do Records of Processing Activities, or Data Privacy Impact Assessments. The reality is those fines haven't materialized in a material way, and I suspect some non-privacy professionals at companies are skeptical about those fines being the basis of future funding requests. But we can redefine that conversation in a way that might help explain the risk and the reason for funding. ROPAs and DPIAs, apart from being required under GDPR in certain circumstances, also help companies define their data environment, what data they have, and what the risks are of processing the data. All of those things can help a privacy professional build information-systems to help determine what material/mission-critical data risks companies have, which are of course part of what one must do under applicable SEC and Delaware requirements. It also makes the company more compliant, and that of course helps from a legal compliance, but also from an operational resilience perspective.

That isn't to say they necessarily need to be done on every system, and that there aren't other ways to map data flows, but the conversation is a different one when it is explicitly tied to SEC and Delaware law, including resiliency. While some privacy professionals do this, most, both inside companies and at firms, tend to frame the reason to do ROPAs and DPIAs in the context of fines for non-compliance, and not the way I have framed it above.

Am I saying that companies shouldn't comply with GDPR? Of course not. What I am saying is that many of the things that drive legal compliance with privacy laws also help privacy professionals meet other obligations that exist that are not privacy or cyber-specific, as well as make the company more resilient around its data flows. Framing the issues that way can only help drive awareness and funding in companies. The same is true in the cyber domain, and not just in privacy—the reasons to spend money on cyber aren't always compliance issues, and cyber has to be viewed in the same way by officers in charge of it, the enterprise-level executives, and the Board.

And there is another consideration as well beyond budgeting or information systems—it is the existing team. The existing team will have to gain skills and knowledge around these issues, which are beyond their substantive expertise. Understanding what the escalation obligations are, their priority, and thinking about and communicating the context for issues when they occur will also be important. There will be other changes as well that will likely have to occur to the existing team and resource allocation, and one way to help address that is training and education outside the compliance professional's "substantive" area around the issues and obligations identified in this white paper. Building systems that facilitate information sharing within the company, as well as with key external stakeholders also can be helpful.

Conclusions and Take-Aways

To try and summarize the key points:

- One key element of meeting obligations under SEC and Delaware law is having sufficient information reporting systems, and without these escalation and disclosure, as well as resolving risks, can be difficult;
- SEC obligations focus on external disclosures, while Delaware law imposes broader obligations, including on officers;
- Under Delaware law, officers have a duty of oversight, including a duty to escalate red flags, as well as to address red flags that are within their purview;
- Particularly where boards are in an oversight role and relying upon officers, company records, and relevant third-parties, they should not be expected to do "deep dives" into the particular compliance requirements of any one area. Instead they should focus on material or "mission-critical" issues with the appropriate context;
- SMEs should provide the board complete information in context, which includes not just facts and gaps in compliance, but also context around the type of risk (resiliency or legal compliance), and the level of risk;
- Information sharing is important and that should occur both internally, and externally, as relevant;
- SMEs should try and help boards understand that context by mapping concepts like "brand" or "trust" to resiliency, or legal compliance, as appropriate;
- Resiliency risk, as illustrated by *Marchand*, can be an overlooked risk, and operational control and oversight of this risk may not be well-defined;
- The CISO role is more accurately described as the Chief Technology Risk Officer;
- The CPO role is more accurately described as the Chief Data Risk Officer.

Ultimately, the more we use data and technology, the more important the issues become and the more that Senior Leaders and the Board will be involved. That means that the profession must evolve to meet that reality, as well as the reality that the adoption of AI will drive more scrutiny and emphasis on data practices. AI Governance is a topic that will be covered in future white papers, including who should be "in charge of AI", but the mere existence of AI changes how privacy and cyber professionals will have to do their existing jobs.