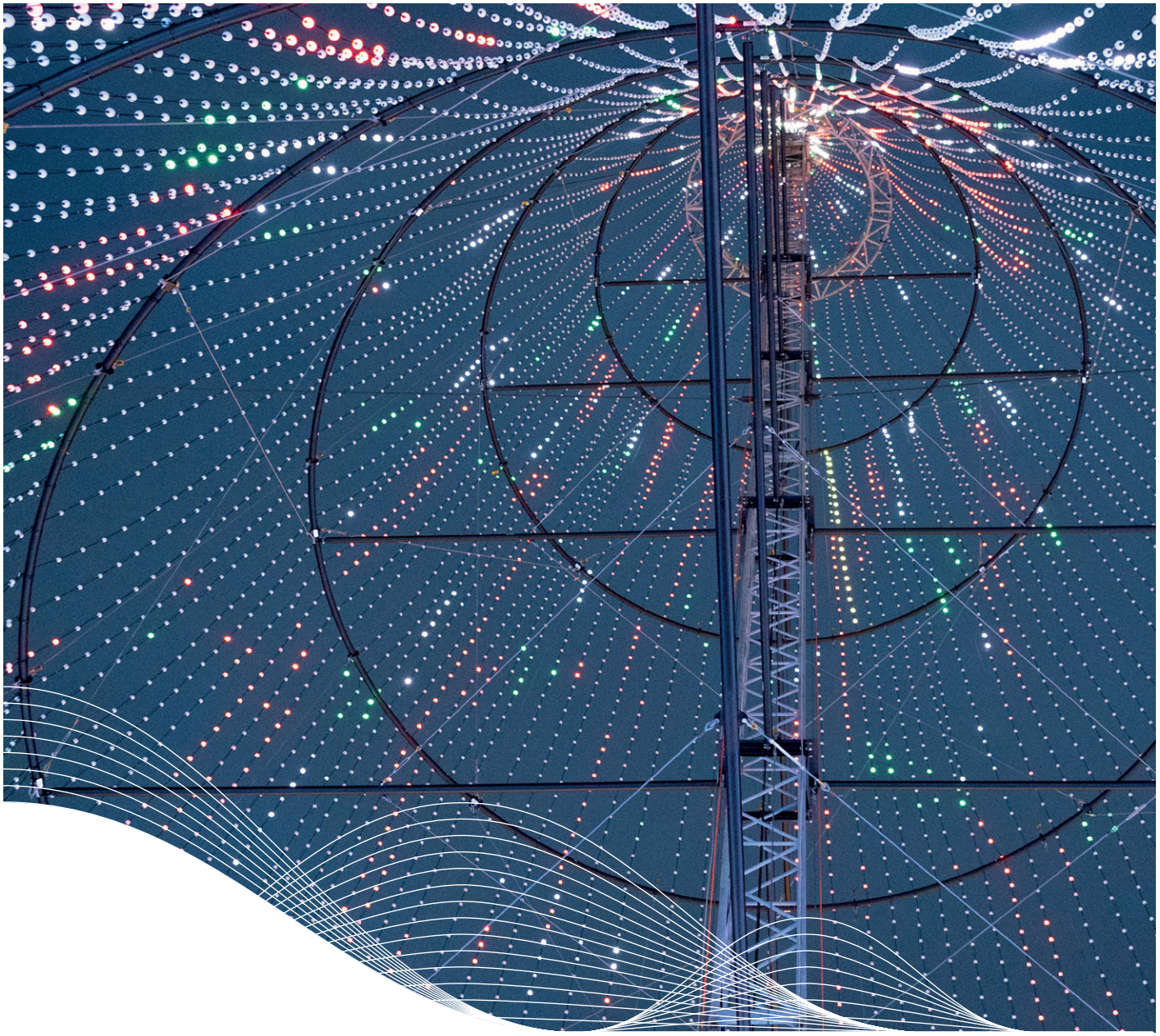


Putting governance and risk in context and reducing personal liability for the cyber and privacy professional

DLA PIPER

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"), data/privacy, artificial intelligence (AI) and other technology 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 rule does not focus on AI but notes 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. 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, 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 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 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.

The precise terms we use are important here. Different stakeholders use different language; this is particularly true with technical subject matter experts (SMEs). Privacy, cyber, and AI are no exception. As these 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 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 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 one. Both the SEC and Delaware law expect governance to have certain components that the typical privacy or security professional is likely not referencing 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 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 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.

One final note related to what this white paper is, and is not, saying. When we mention "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. 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 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.

Introduction

Privacy professionals have long touted the importance of their field, claiming that it should be a matter of concern for boards of directors and often citing potential FTC actions or the size of potential fines under the General Data Protection Regulation (GDPR), which in the case of GDPR overall have not materialized in the way they were predicted. Privacy is an important issue on any number of fronts, including for companies, and can be an issue for board oversight. The challenge with this approach – apart from the lack of large GDPR fines – is that the issue is viewed through 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 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, including that your personal liability has likely increased, and that your job has changed.

Who's who

To level set, it is helpful to clarify how roles are defined for the board, senior leadership, and management (or SMEs). If we summarize the roles of each, it is as follows:

THE BOARD	SENIOR LEADERSHIP	MANAGEMENT
• Fiduciaries who are not involved in operations • Express and implied duties of oversight – *ie,* governance – on issues including the company's operational viability, legal compliance, and financial performance • Input on, and in some cases a broader role in, business strategy	• With management, manages and operates the business, under the oversight of the Board. • Provides leadership and vision regarding strategy • Management of operations includes operational viability, legal compliance and financial performance, which includes defining including overall risk appetite and tolerance for the business on these issues • In the case of certain Senior Leaders, fiduciary duties	• Runs the operations of a business • Drives/implements the strategic objectives of business as well as operational viability, legal compliance and financial performance • Provides the information and input where needed to enable the Board and Senior Leadership to discharge their obligations/business roles

Why do for-profit companies exist?

For-profit corporations do not exist to protect privacy – they exist to return value to shareholders (*ie*, create profit). Businesses generate profit by providing goods or services via the creation of business processes that generate revenue over the cost of providing the good or service. That provides an important takeaway: business processes are critical to businesses, and a business needs to take steps to protect those processes (ie, be operationally resilient).

That is not to say companies 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.

The problem with privacy

Brand.	Values.	Notice and choice.
Trust.	Ethics.	The right to be let alone.
Digital risk.	The "creepy" factor.	Fundamental human right.

These and other words are the terms you hear when people talk about "privacy," or why companies should care about privacy. The challenge with these terms is not that they are not important, but rather that their importance is not always put in the right context so that companies can actually understand and take appropriate actions regarding data.

Privacy is a concept rooted in individual rights, usually enforced by the data subject or a regulator via some enforcement action. As was discussed above, a corporation's primary purpose is to return value to shareholders. To be clear, that is not the only thing corporations do, but it is the primary purpose, and certain issues are core to that primary purpose.

And that is one of the problems with privacy – by casting it in the terms above, we have created the perception that it is an issue not related to the primary purpose of a corporation, when in fact it is. The other problem with privacy is that it is underinclusive as a concept, which we will explore first.

As discussed in greater detail below, 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 the fuels commerce. By focusing on privacy, with its inherent focus on the individual, we are missing the broader point that data – including, but not limited to data regarding an individual – fuels our line of communication.

Turning to the perception issue, we must first focus on the primary purpose of corporations, and the core corporate governance principles. If we reduce corporate governance down to four points, it is a focus on strategy, operational resiliency, legal compliance, and financial performance. It is not that other issues do not matter to corporations, but the important point is that other issues matter the most when they impact those four principles.

Take brand as an example. For some companies, brand is a critical issue, and for others (such as your local energy utility) brand may not be as critical, which illustrates the issue with using concepts like brand – brand ultimately matters for some companies and not others because of how it interacts with the four corporate governance principles. Where brand impacts strategy, resiliency, and financial performance, it matters. Where it does not, it likely does not matter (or matter as much) for the company.

While one can have a debate about the importance and role of other concepts, such as ethics and values, and their independent value to companies in other contexts, that is a debate we do not need to have here. The reason is the importance of data to fuel our global economy, which means that how data is used, or not used, impacts companies' strategy, operational resilience, legal compliance, and financial performance. As illustrated by the brand example above, we are better off skipping the middle step of using terms like brand or privacy, and instead focusing on the impact on the four corporate governance principles.

So where does that leave us? It leaves us looking for a better concept to describe how companies should think of their data practices – particularly one that better integrates all of the corporate governance principles and that takes into account the role of data in our current line of communication. That concept is data sustainability.

What do we mean by that? We mean that data impacts all four principles, which is the concept that is missing from the vast majority of the discussions regarding privacy. We all write articles about the next new enforcement case, what the next privacy law is, or should be, and all of those things are important, but they are only really important to the legal compliance principle, and if one actually looks at how data is used today, the problem becomes clear. How companies use data has strategic implications, resiliency implications, and impact on financial performance, in addition to legal consequences.

To move more directly down this path, compliance systems all operate from a set of controls – sometimes that is a framework like the Payment Card Industry Data Security Standard (PCI DSS) requirements, and sometimes that is a law, a regulation, or even an enforcement action that identifies allegedly improper activities. There are consequences for non-compliance with those controls – usually monetary consequences, but as will be shown below, that can just be the beginning.

The concept of data sustainability is focused more upon the other three principles, particularly the operational resiliency component of corporate governance, again given the importance of data in our economy. This hits another core issue with how we describe data practices.

When a privacy professional says something is "creepy," what they are really saying is while it might be legal, it may not be perceived well by the data subject, a regulator, a policy-maker, the media, or other key stakeholders, and there may be non-legal consequences to the company or its executives (*eg*, a trip to Washington for Congressional testimony, a front-page story in the media, etc.), that in many cases get the company to stop the practice in question, even before the company is legally compelled to do so. In other words, these practices are not sustainable, and therefore are not resilient. To return to the brand example, a "creepy" data practice that is not sustainable will impact a brand-conscious company's image, which ultimately means that there is an impact, at minimum, on operational resilience and financial performance.

This becomes even clearer when one thinks about how people talk about cyber. Cyber focuses on protecting data and systems from third parties. Sometimes that is from data exfiltration, sometimes that is from modification, and sometimes that is from encryption/deletion. Security professionals refer to this as the CIA triad, "Confidentiality, Integrity, and Availability," and it is the last point that is important – data can be unavailable due to third-party activity, ransomware, or because the data practice itself ultimately is not sustainable and therefore is not an operationally resilient practice.

To address what some lawyers may be thinking – no we are not saying ignore the legal consequences of processing personal information – again, quite the opposite. And one need only look at some of the consequences from regulators to actually understand that the "legal" risks in many cases are actually operational resiliency risks. Under Section 5 of the FTC Act, the FTC does not have the ability to obtain civil penalties, and its ability to use Section 13(b) has been curtailed. So, what are the usual remedies for privacy violations? A consent decree that has a number of requirements that can include the deletion of data, conduct restrictions, and in some cases the deletion of algorithms generated from illegally collected data – algorithmic disgorgement. Turning to the European Union (EU), the most critical issue right now is data transfer, and while fines are certainly possible under GDPR, the main issue regulators are talking about is suspension of data flow. All of these consequences create more of an operational resiliency issue than a legal compliance issue.

Data sustainability is discussed in greater detail below, but the important point is that the concept is meant to be more inclusive of issues beyond legal consequences for the use of personal data, and also look at the risks and benefits of the use of data. To be clear, data sustainability includes the concept of privacy and factors in its importance, but it does not stop there. In short, having a road with nothing moving down it because there is no fuel is the same as having no road at all.

Understanding SEC and Delaware obligations

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 percent of the Fortune 500 are in fact incorporated in Delaware.

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 do not impact the privacy or cyber professional. The same cannot be said for other SEC requirements, however.

SEC OBLIGATIONS SUMMARIZED

Focus is on disclosure to investors

The key takeaways 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.[2]

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 – *ie*, the initial sale of securities. The Securities Act of 1934 imposes disclosure obligations upon companies on a periodic basis – and includes, for domestic companies, 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 while examining 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.

On July 26, 2023, the SEC adopted the final version of its much-anticipated enhanced disclosure requirements regarding cybersecurity risks and incidents for public companies (the Cyber Rule). The Cyber Rule adds additional disclosure obligations on public companies, including:

- New disclosure requirements on Form 8-K for cybersecurity incidents within four business days of determining that a cybersecurity incident is material. The Form 8-K must describe the material aspects of the nature, scope, and timing of the incident, as well as its material impact (or reasonably likely material impact) on the company. Public companies must also file an amendment to the initial 8-K to provide any information that was undetermined or unavailable at the time of the initial 8-K filing.
- New cyber risk management disclosures in Form 10-K, whereby companies must describe 1) their processes for assessing, identifying, and managing material risks from cybersecurity threats, and 2) whether any such risks have materially affected or are reasonably likely to materially affect the company.
- New cyber governance disclosure requirements 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.

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

The SEC's disclosure-based regulatory regime is centered around the idea that if investors have timely, accurate, and complete *material* information, they can make informed investment decisions. 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.[3]

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."[4]

In its adopting release of the Cyber Rule, the SEC reiterated that materiality determinations are to be based on both quantitative and qualitative factors, and clarified that qualitative factors include those such as harm to a company's reputation, customer or vendor relationships, or competitiveness, and the possibility of litigation or regulatory investigations or actions.[5] This complicates the analysis. In some ways, the qualitative analysis may be similar to an examination of resiliency risks under Delaware law (see below), but it will depend in some ways on how the SEC interprets and enforces this portion of the Cyber Rule.

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.[6]

To help ensure accurate and complete information required to be disclosed in reports filed with the SEC, pursuant to Exchange Act Rules 13a-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness.[7] "Disclosure controls and procedures" (or "DCPs") are defined as controls and procedures that are designed to ensure information required to be disclosed is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms.[8]

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 which 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 given its substantive focus.[9]

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 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 required to be disclosed to investors is recorded, processed, summarized and reported timely.[10] 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. Indeed, as SEC Chair Gary Gensler stated in the press release accompanying the final version of the much-anticipated enhanced disclosure requirements the Final Rules, "whether a company loses a factory in a fire – or millions of files in a cybersecurity incident – it may be material to investors." And a company's principal executive and financial officers must certify whether the company's DCPs are effective.[11] 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, 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 the California Consumer Privacy Act (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 does not absolve the company of 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.[12] 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 Section 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… "[13] 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.

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.[14]

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.[15]

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, cyber, and AI 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…"[16] 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 that both are applicable to officers and directors.[17] 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.

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.[18] 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 (fig. 1) 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.[19]

Most privacy professionals are in legal or compliance organization 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, but, 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 management, as well as third-party experts in certain cases.[20] 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.[21]

Where there is no breach of the duty of loyalty, the applicable standard for the duty of care is gross negligence.[22] This includes claims predicated upon the assertion that the directors did not review sufficient information before making a decision.[23]

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.[24]

The 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.

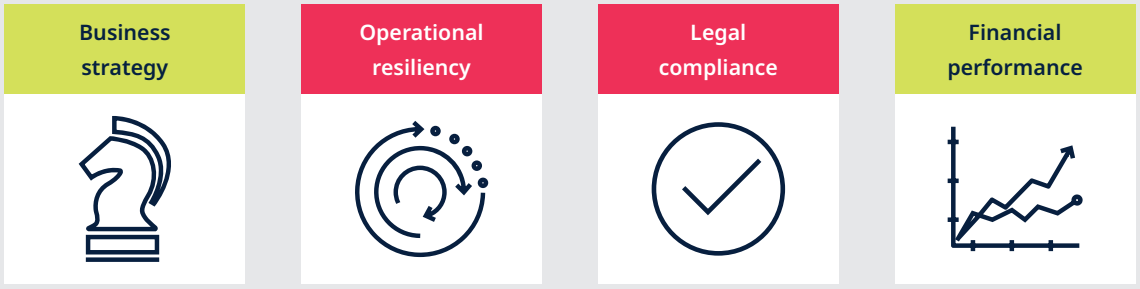
The duty of loyalty

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

> 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.[25]

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

Fig. 1.



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.[26]

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.[27]

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 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).[28]

KEY TAKEAWAYS 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.

AI risk and value

The "risks" of AI extend well beyond compliance to those enterprise risks that AI presents due to its ability to disintermediate or disrupt existing business models. If we pause and think about what has happened since we decided to connect to the Internet, the issues become clearer. The first wave of the Internet really caused massive disintermediation of companies based upon other companies using the advances in infrastructure to displace existing businesses, and we are now moving to a different phase in which advancements in computational methods will likely cause massive disintermediation as well. As noted in a post from 2012 entitled "Information Superiority – The CEO's Path to Improved Decision-Making" discussing the hot topic of the time, "Big Data":

> **Big Data Is Not the Answer – Information Superiority Provides a Solution for Your Company.**
>
> Discussions about Big Data are the rage these days, but Big Data is not the solution for executives, and at some level is part of the core problem for companies. Definitions of Big Data abound, but they all at some level focus on the volume and velocity of information, and how the information can help define business goals.
>
> Big data is a popular term used to describe the exponential growth, availability and use of information, both structured and unstructured. Much has been written on the big data trend and how it can serve as the basis for innovation, differentiation and growth.

According to IDC, it is imperative that organizations and IT leaders focus on the ever-increasing volume, variety and velocity of information that forms big data.

The ever-increasing volume and velocity of data is an issue that in context must be addressed, but this definition illustrates that Big Data is not the answer for the broader concern of executive decision-making. Indeed, the lessons of 9/11 illustrate that the problem wasn't having too little information, or having information drive decisions, but rather that there was a lack of leadership and clarity of goals that precluded the relevant people from *efficiently* identifying, drawing, gathering, and sharing the relevant information so that the information could be used in a superior way.

This is the same issue the private sector faces. Similar short-comings have caused some traditional businesses to fail because threats to business models were not perceived–think of big box video rental stores and the impact that online content distribution has had on this industry. Moreover, if you look again at the materials on executive decision-making discussed above, as well as the 9/11 Commission Report, the issue is apparent. Whether it is expressed as "exchanging information," learning "best practices and techniques for gathering data and making critical decisions with limited time and resources," identifying a "quarterback" to set goals and have accountability for the team, being "able to draw relevant intelligence from anywhere," or learning "what ingredients are necessary to make a good decision," the issue for the public and private sector is the same – *making behavioral and organizational changes that facilitate the goals of the organization to efficiently get the right information, to the right people, at the right time*.[29]

The main risk, and value, of AI is the same – the ability to disintermediate existing business models. Some companies will win, and some will lose, in this environment, but these risks are truly enterprise-level risks, and the value is also at the enterprise-level.

If we return to the corporate principles – business strategy, operational resiliency, legal compliance, and financial performance – how to frame the risk and value issues become clear. The discussion around who will "own" compliance fits in the legal compliance box, which is an important issue, but that is one of four issues to consider. Just as the use of advances in infrastructure in the early 2000's presented significant enterprise opportunities and risks, so too does AI. And those issues all go to the other three principles: business strategy, operational resilience, and financial performance. In short, some companies will become Blockbuster due to AI – those issues don't arise from compliance issues – they arise from all of the other issues listed above. In short, while we could frame these issues in terms of fiduciary duties, which are not unimportant, the issues go to the survival of businesses in many cases.

Just as AI risk is not synonymous with compliance risk, AI risk is also broader than data risk. AI is a disjunctive set of technologies spanning more than 60 years, linked more by the "what" (ability, complexity, autonomy, adaptability) than the "how" (any particular technology) – which helps explain why WIPO and others have observed that there "is no universal definition of artificial intelligence." Perhaps as a result, many privacy and cyber professionals revert to a view of AI as processing data, when in fact AI's impacts on financial, strategic, resiliency, and legal issues turn only in part on data and its governance.

All of which raises the core question – who should "govern" that? When framed in this way, the answer is clear. While framed in terms of information sharing in the context of Big Data, the answer remains the same:

A Non-Delegable Duty.

There has been discussion in the Information Age about who should help facilitate the use of information. Some believe that it is the CIO's responsibility, while others talk about creating a new role, such as a Chief Digital Officer. The reality is this is a duty that must fall to the CEO, as the "quarterback" of the company. This is not to say that other executives – indeed all other executives – are not critical to the success of Information Superiority in your organization, but the tone from the top must be set by the CEO so that the goals of the organization drive information gathering and sharing, not the other way around. This will help your harness the power of information in a way that will help drive your company's goals in an efficient way that promotes joint action among the key executives. Using other methods may drive some value, but they will not efficiently deliver the value that Information Superiority can. For today's CEO, anything less can lead to a waste of resources and future business opportunities.

There are any number of ways AI can be used by companies. The questions to ask aren't "Are you using AI?" but "Are you using it in a way that is strategic and drives financial performance, while protecting your business from resiliency issues – not at the program level, but at the enterprise-level?" Compliance is also of course a concern, but it is by no means the only concern, and not the one that is most likely to put your company out of business.

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 (fig. 2) captures what governance is, including escalation, as represented by the blue 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.

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

Fig. 2.

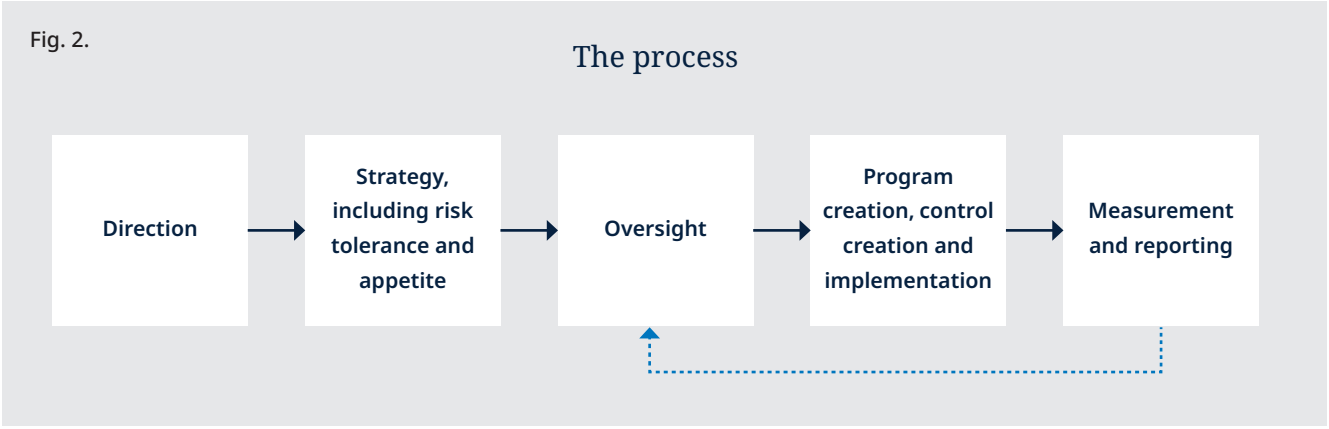
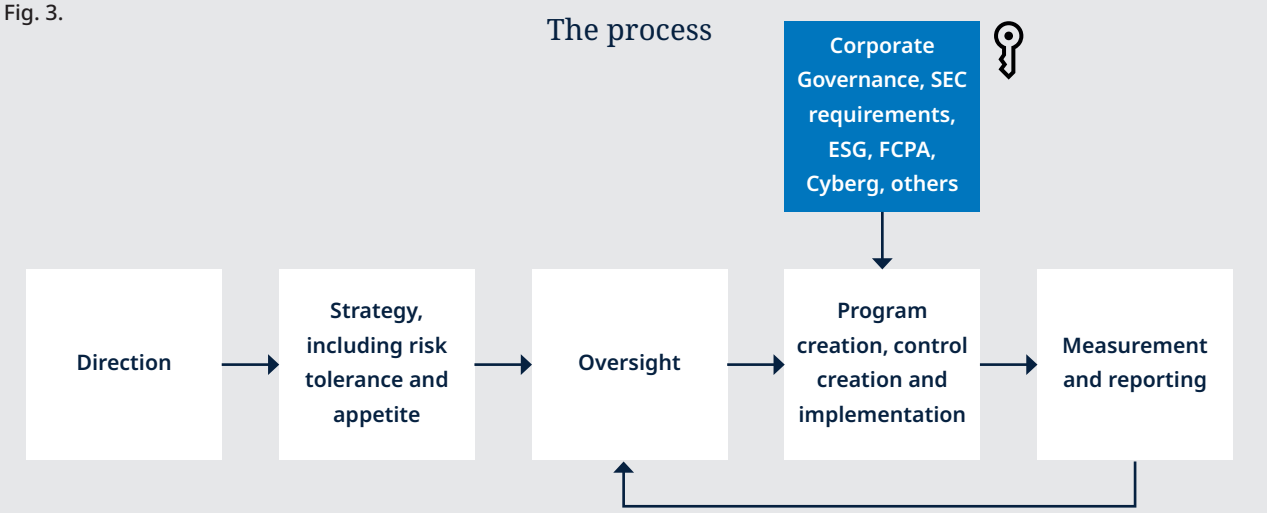


Fig. 3.



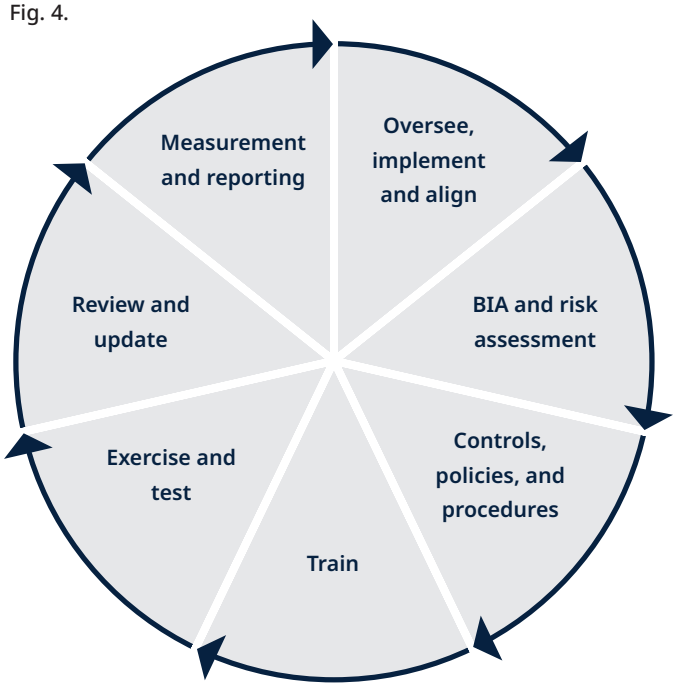
versus business strategy, but the terms used are less important than the difference between the two – one is a broad vision, and the other takes that broad vision and begins to tie it to specific actions.

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 blue box below (fig. 3), 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.

Having defined the first two boxes, we move to the rest of the process. It is perhaps easier to place this part of the process in a wheel, to illustrate the process that occurs (fig. 4).

The components of the wheel are largely self-explanatory. This process allows companies to have a structure to implement their direction and strategy in a governed way.

Fig. 4.



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 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."[30]

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.

CORPORATE GOVERNANCE

To create a corporate governance framework, we can simply take the four principles of risk and value for corporations, noted above, and combine them with the five steps of the governance process as represented below (fig. 5), with the black lines representing a process pushing down, and the green dashed line representing reporting up to oversight.

This defines corporate governance on an enterprise basis.

In most companies, oversight is provided by the board, and the company is operated by the senior leadership team (SLT) and management, which means that the SLT and management are responsible for much of the activity in corporate governance, though the board plays an important role as it oversees corporate governance.

The impact of SEC and other corporate legal issues is worth emphasizing here. While legal compliance is one of the four points, it is only one of the four points. Said differently, a legally compliant corporation with no business strategy, operational resiliency, or financial performance wouldn't seem to be a company one would want to be a shareholder in.

While this framework works for the directors and officers with company-wide responsibility, it does not 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.

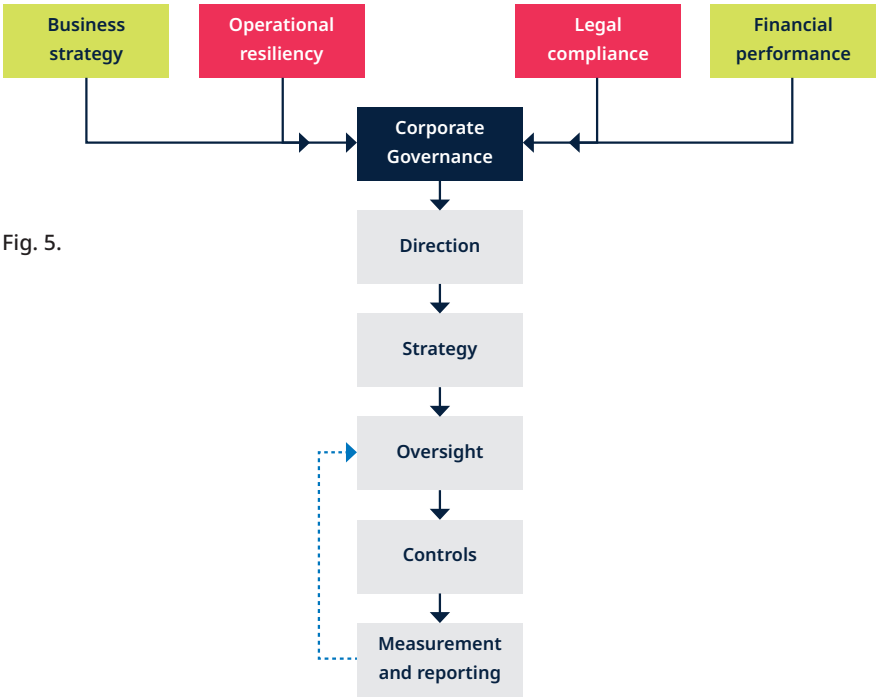


Fig. 5.

NESTED GOVERNANCE

Corporate governance sits above program governance, and when implemented in a "nested" way, program governance inherently aligns with, and is informed by, corporate governance. The concept of nested governance, then recognizes the fact that to actually achieve appropriate governance of the relevant subject areas, it is helpful to apply the same processes and standards of corporate governance in the individual subject areas that are material or mission-critical for a company. Indeed, the program governance layer should be informed, as relevant, by the company's business strategy, operational resilience, legal compliance, and financial performance.

Nested governance would look like this (fig. 6):

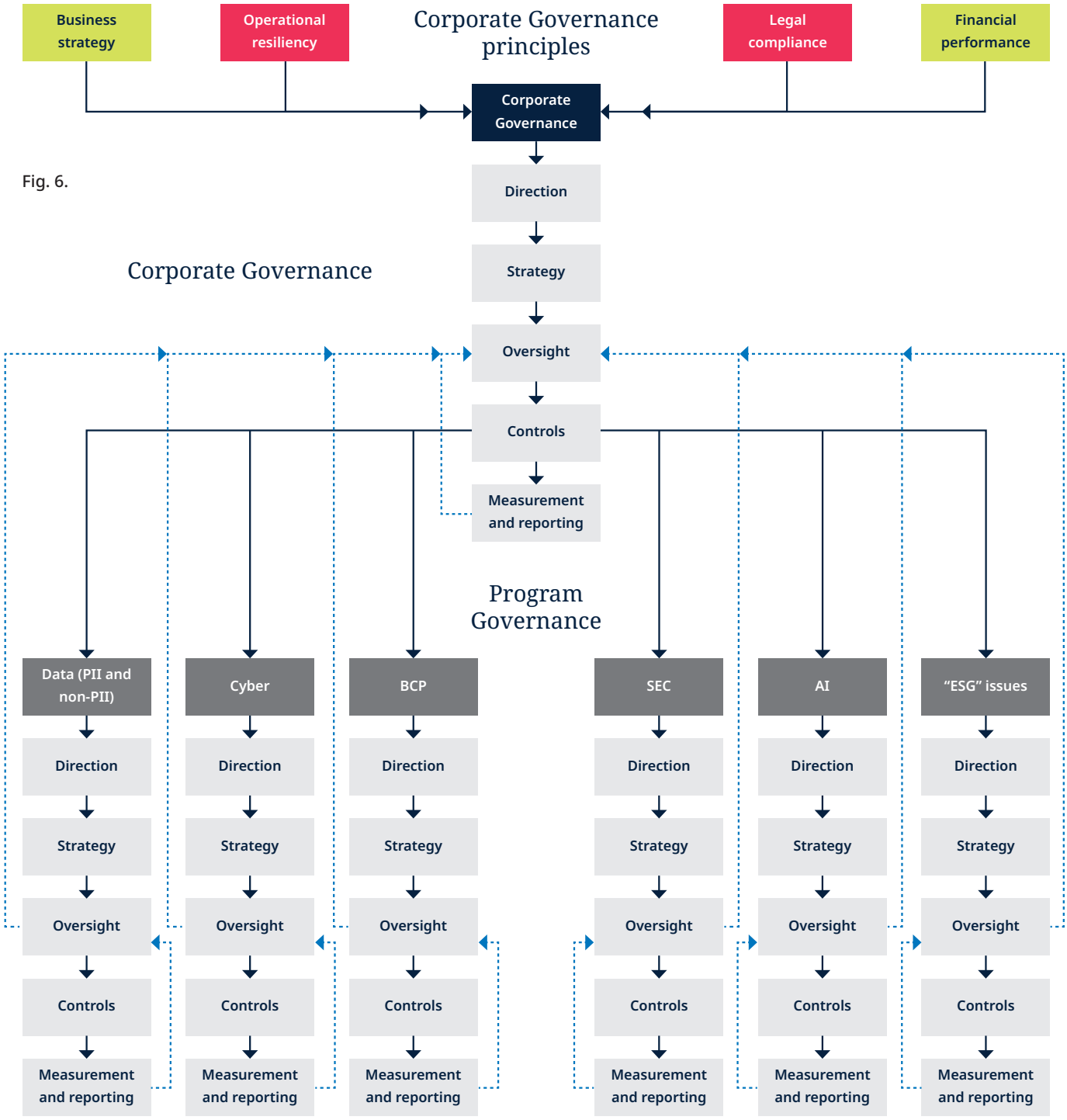


Fig. 6.

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, thout 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.

Looking closely at the structures above, some broader issues become clear when one thinks through the implications. First, it is obvious that direction, strategy, oversight, controls, and measurement and reporting are distinct functions with different owners. At the corporate governance level, the board engages in oversight, not day-to-day operations. Day-to-day operations such as the implementation of controls and measurement and reporting are the job of the SLT and management, as appropriate.

While that seems like an unremarkable statement, that delineation is not always recognized. That is not to say that a board should not have appropriate policies and procedures, but it is to say that the board should in general be making day-to-day operational decisions for the company.

Second, and this issue highlights another common misunderstanding, issues that are programmatic or control-based particularly are not directly corporate governance issues, and instead fall under the legal compliance principle. In other words, all for-profit corporations have to deal with those four principles, but not every for-profit corporation has to deal with the same programmatic or control-based issues.

Looking at the SEC requirements for public companies as a particular example, even if those requirements sound in governance, they are not truly corporate governance. While that certainly might make some lawyers perk up, one need only ask a question to illustrate the point: should non-publicly traded companies operate according to the four corporate governance principles? Given that those four principles implement the singular purpose of a corporation – providing benefit to its shareholders – the answer is clear: yes, non-publicly traded companies should operate consistent with those principles, even though the SEC requirements for public companies would be inapplicable. The point is that 1) corporate governance obligations exist independent of SEC public company requirements, not because of them, and 2) those requirements would have to fold into the four principles, not exist independent of them. In other words, public companies do not have a fifth corporate governance principle; instead, as shown in the nested governance model, SEC requirements would be governed by the broader corporate governance of the company.

This is not a point we raise to debate the role of SEC regulation – it is to make a broader point we will return to: things that are not one of the four corporate governance principles (strategy, operational resiliency, legal compliance, and financial performance) matter most for a corporation when they impact one of the four corporate governance principles. That is not to say that corporations will not do things that do not directly impact those four principles, but it is to say that corporations are not likely to spend significant resources on initiatives that do not advance the corporation's position relative to these four principles, and that if a corporation does not do things to positively enhance its position on these four principles, it could find itself out of business.

To illustrate again using our brand example, brand is not a corporate governance principle, and for companies that need to be conscious of their brand, we do not add a fifth principle. Like SEC requirements for publicly traded companies, brand may be highly relevant for some, and largely irrelevant for others. A good example is utilities: most electric utilities have a monopoly on a particular service area. While they do not want to damage their brand, if they can avoid it, it is not the same level of issue for a utility as it is for a company where brand is more critical – a hotel or resort chain as an example. Brand matters a lot where there are alternatives, or what the company is selling is really its brand but matters less when there are not easy alternatives for the consumer to move to.

That is the broader point. Brand matters to those companies not because of the brand itself – it is because a brand hit will cause an impact on the four corporate governance principles, financial performance being the main one, though others may be implicated as well, including strategy.

One final point which is clear from this example: "privacy" and security are not corporate governance principles and do not have the same importance for companies unless they implicate the four corporate governance principles. That is not to say "privacy" and security do not implicate corporate governance principles, or do not matter for the vast majority of companies, but it is to say that how those issues have traditionally been presented to boards and senior leaders is not the optimal way because the focus at times with privacy and security is not on corporate governance principles, but rather on privacy and security, or concepts such as brand.

Data sustainability

Circling back to where we began on data sustainability, we will now try to define the concept in more detail, which ultimately is based upon creating governance structures that actually account for the view of the many interdependent stakeholders that can impact a company's data practices.

Putting together our discussion of the four corporate governance principles (of which legal compliance is but one), our current line of communication (which is propelled by data), and the components of governance (which are not just limited to the creation of controls), it becomes clear that a broader concept than privacy is needed – one that recognizes that data creates both value and risk, and the resiliency component that is associated with data in our hybrid world. And in order to truly govern the resiliency issues, we must use governance concepts, which include creating a direction, a strategy, oversight, controls and measurement, and reporting (fig. 7).

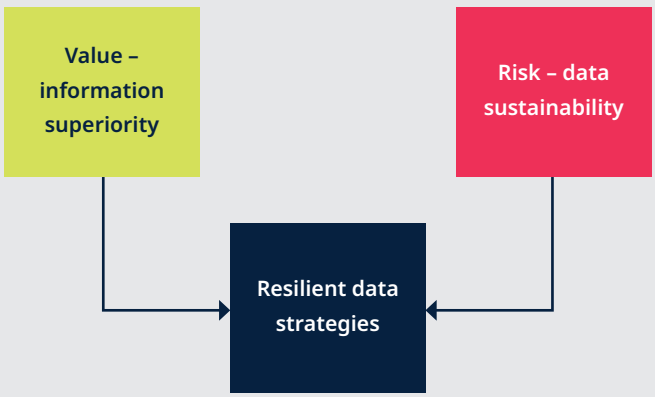
Here, we examine the risk, or sustainability, side.

If we are going to address an issue that is as important and complex as how we make the propellant for the current engine available in a way that does not result in the engine being shut down – for example algorithmic disgorgement or blocking of data transfer, we must begin to think of these issues in a different way, and a way that isn't rooted purely in statutory review or legal compliance – our current regime for assessing privacy.

This signals a shift from looking at the issue purely as a privacy issue, even under the more European regime of fundamental human rights, because, as we see from Schrems II, core to the enforcement of human rights in Europe is the ability to have legal redress – the perceived absence of which causes the EU to have concerns about data transfer to the US. Instead, it requires that we think about data in terms of risk and make risk decisions where we reduce the times that we make uninformed risk decisions, particularly on material risks.

Having factored in corporate governance concerns, including business strategy and operational viability, not just legal compliance or even financial performance (as viewed through brand impact), we also must factor in continuity and resiliency concepts because if we accept data is the propellant for our Hybrid World we must view data through a continuity lens, as well as a resiliency lens, in order to appropriately consider data practices under corporate governance concepts. We must also consider ESG and ERM concerns for similar reasons. Given the borderless world, our solution must factor in not just different legal regimes, but also differing cultural norms regarding data use where those are not necessarily contained in laws or regulations. In short, a rote examination of current laws and enforcement will not necessarily provide a full accounting of future risk, which creates the potential for legal issues to become operational viability issues.

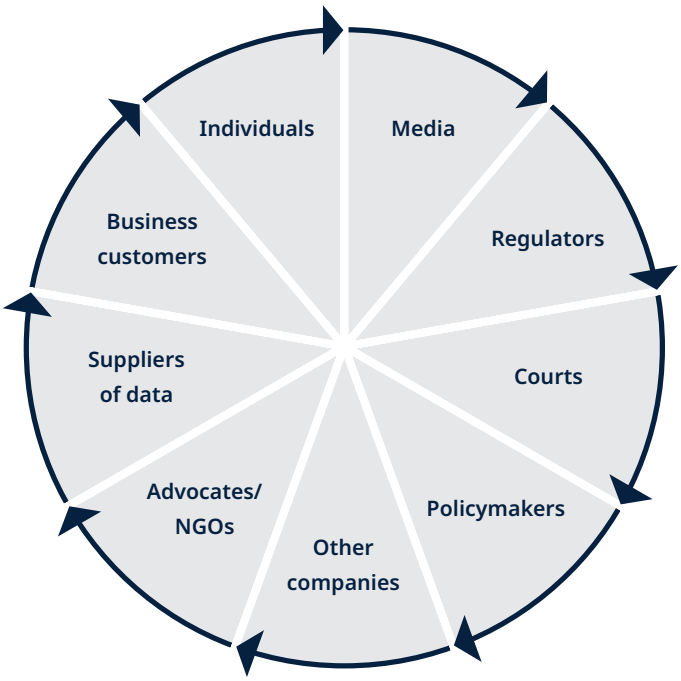
Fig. 7.



Many of these points are clear for cyber – the reason a business wants to have resilience around cyber isn't to avoid legal consequences – it is instead to make sure the business is operationally viable. What we need to realize is, as stated before, having a road with nothing moving down it because there is no fuel is the same as having no road at all.

What does that really mean? It means that while we need to continue to focus on current legal compliance regimes for the purposes of legal compliance, determining whether your data practices are actually sustainable requires more than that. At some level it involves trying to predict where the regulators are going, but it is broader than that.

Fig. 8.



It means that in order to actually make informed risk decisions regarding data, consideration should be given to thinking about different voices as you consider your data practices (fig. 8).

One voice is the voice of the individual when there may be data subjects in many parts of the world – currently privacy professionals will use terms like "creepy" for data practices that may be legal but which would not be perceived well by the data subject in different cultures. What we are truly saying there is that the adverse processing impact of such a practice is so high that it is in fact not a sustainable practice. That could be because the data subject might stop giving your company data, an advocate might discover the practice and bring it to light, or because a regulator might find it to be "unfair," which leads us to our next voices – that of the advocate, the media, the policy-maker, the courts, and the regulator.

There are countless examples of advocates focusing attention on company's data practices, which, in turn, results in data risk. The best example currently is Max Schrems who has brought attention to surveillance issues, and that attention has led to the invalidation of two different treaties between the EU and the US, and threatens to cut off data transfer between the EU and the US. Simply put, the voice of the privacy advocate can directly impact a company's ability to process data – ie, have sustainable data practices, and merely looking at the law as it stands, without factoring in the voice of the advocates creates data sustainability risk.

The voice of the media is another consideration – again not because of legal implications, but because of data sustainability concerns. The age-old question for companies in privacy – "Would we want to see this on the front page of the *Wall Street Journal*?" – is one that certainly in the end can result in legal consequences. But most reporters do not limit themselves to writing about data practices that are illegal. As a result, the core issue isn't whether the data practice in question is legal – it is whether the data practice in question can withstand public scrutiny – in other words whether it is sustainable.

The voice of the policymaker is another example. There are innumerable examples of CEOs being called to testify regarding data practices, as well as cyber incidents, and those requests are not in any way limited by Congress asserting there is a violation of data protection laws, so an exclusive focus on what is "legal" may not hear the voice of the policymaker.

The voice of the courts is also relevant. Particularly in the US, and increasingly in Europe, private litigation is used to seek redress for privacy violations. The long-running challenges for privacy plaintiffs in the US around Article III standing in the United States are well-documented and were part of the issues litigated in Schrems II. While this is a voice that is relevant, it again is not the only voice that is relevant, particularly given the standing challenges that plaintiffs face.

Finally, we turn to the voice of the regulator. While there certainly are aspects of managing the voice of the regulator that are strictly based upon statutory interpretation, or review of prior enforcement, you will not truly hear the voice of the regulator, particularly in the US, if that is all you do. UDAP authority is inherently flexible, and focused on harm to the consumer, balanced against consumer benefit, or benefit to competition, and ironically at some level these are core business issues and balancing of harm versus benefit.

If the goal is to build a program based upon compliance concerns, that certainly can be done via controls including people, process, and technology. However, as anyone who has built a privacy compliance program knows, the laws change frequently, and in many cases you are

constantly chasing new standards. In short, a compliance focus, at best, leads to compliance, but it does not lead to more than that, and it will not in most cases hear all of the voices noted above. The way to hear those voices in a more fulsome way is to create a governance structure that is geared to all of these different stakeholders so that you can create sustainable data practices.

Building a sustainable program starts with an understanding of the key business processes that utilize data to assess their importance to the company, with the added benefit that this process can also be used to unlock additional value from data. It also involves the setting of risk tolerance and risk appetite around data practices, so that the program that is created stays within those parameters. While legal compliance certainly is relevant to these points, these issues in many ways are more business focused and a broader team than just lawyers or compliance professionals can add valuable input. Ultimately, governing these issues and building sustainable data practices gives a company the best chance of hearing all of the relevant voices, rather than just hearing the legal or compliance-focused ones.

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 percent fines – which is why GDPR was always used as an example of a reason to invest in privacy. Resiliency – and we 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 in getting funding and people to actually understand the risks that privacy creates.[31]

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.

Who should govern AI?

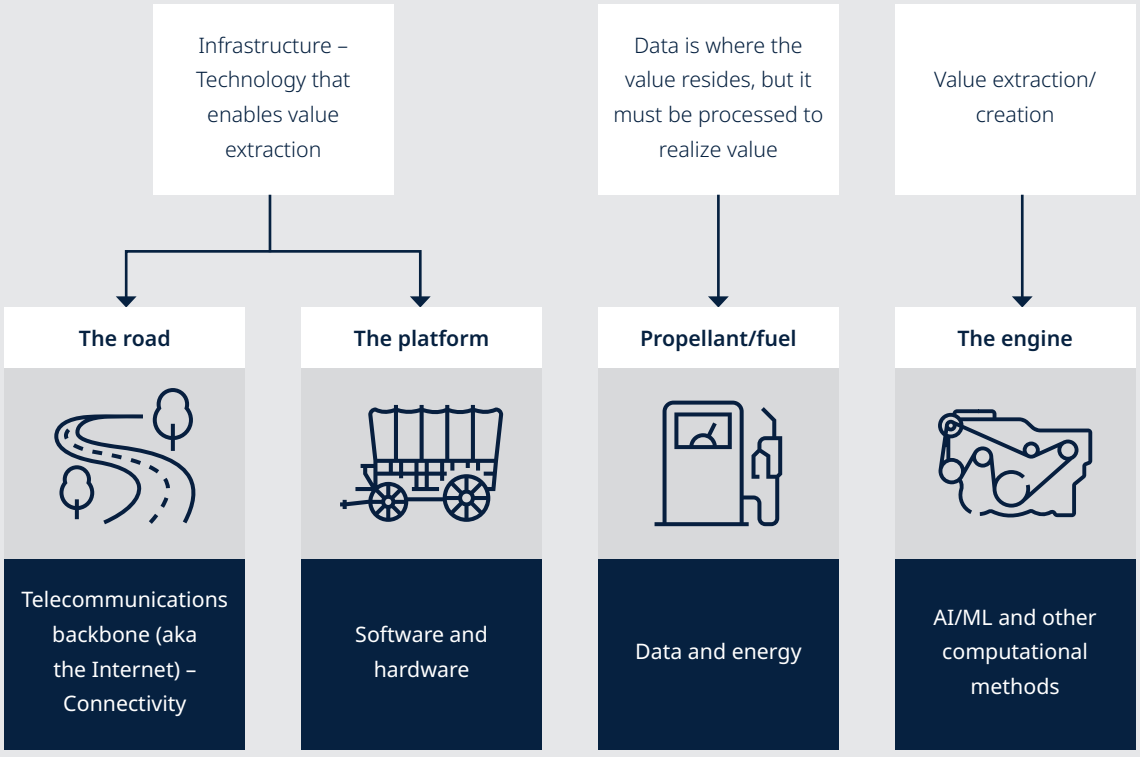
Many companies are struggling with how to define and where to place AI governance within organizations due to the recent global attention on AI and race toward adoption, and again it is helpful to place the use of AI into context of our use of the "Internet." As discussed further below, we currently use a line of communication that is hybrid – both virtual and physical – that we have become extremely dependent upon for things other than using what we think of as the traditional Internet. The issues presented by our use of the Internet can be put into three categories – infrastructure; data; and value extraction/creation, the latter of which are presented by the application of AI and other advanced computational methods (fig. 9).

This illustrates an obvious point – different professionals have different skillsets in different areas and those who are experts in protecting the infrastructure – "security" – are distinct from those who specialize in the computational methods used in AI, just as both are distinct from those who specialize in data.

In certain organizations, information security and privacy compliance functions have asserted interest in "governing" AI, and in others, those who focus on issues such as data science have asserted interest in governing AI. For privacy professionals, this is due to their historic role in managing data risk. Security/technology risk functions have done the same, given their understanding of security of systems and data, technical capabilities, software design lifecycles, and broader features of the AI engine. Those with a data science background have asserted governance primacy because their expertise is focused on the computational methods used by AI, alongside an understanding of the limitations and risks of those methods and their outputs.

While all of these voices are important, AI both potentiates and changes existing issues in security and data, and also presents unique issues that do not fit within existing compliance functions. The graphic below presents a summary of these issues and illustrates their complexity and that the issues around advanced computational methods and output that

Fig. 9.



are distinct from what security and privacy professionals do, or are generally qualified to do.

TECHNOLOGY (INFRASTRUCTURE)	DATA	COMPUTATIONAL METHODS	OUTPUT
• Confidentiality • Integrity • Availability • Use of AI to defend the network from existing and new attacks, including AI-enabled attacks	• Access • Rights/Ownership • Resiliency of data flows (including transfers issues) • Privacy • Data quality • Bias/Fairness • Purpose • Existing processing restrictions, including automated processing restrictions	• Bias/Fairness • Accountability • Transparency • Reliability • Safety • Honesty • Usefulness • Explainable and Interpretable	• Illegal/inappropriate uses • UDAP (including misrepresentations about using AI) • Discrimination • Credit decisions (FCRA) • Improper discrimination against employees (FEHA) • Bias/Fairness • Ownership • Contractual liability • Competition/Antitrust • Resiliency of process • Others

Simply put, in most organizations privacy and security are managed by different professionals with different skillsets. The CISO and CPO are different roles for a reason just as the issues and skillsets around the use of advanced computational methods and output are distinct.

An extended discussion of those issues is beyond the scope of this section, but it is important to note that these are all really independent compliance domains with different experts having different skills to address the issues. Ultimately, when we look at AI governance from a programmatic perspective, it means that multiple subject matter experts (SMEs) must be at the table if we are to actually manage these programmatic risks.

Recent guidance and practice have shown this. AI systems are rapidly being adopted, they are extremely complex, and the impact of the AI systems is far different, though related, to the impact of information security and privacy. As noted by NIST, "AI system scale and complexity (many systems contain billions or even trillions of decision points)" are such that "existing frameworks and guidance" on security and privacy "are unable to … confront the challenging risks related to generative AI," which can impact the "sustainability of the organizational as a whole" (NIST 2023).

NIST has promulgated the first major US framework for AI risk management,[32] which is separate from the existing frameworks for cybersecurity and privacy, and the AI framework was "directed by the National Artificial Intelligence Initiative Act of 2020 (P.L. 116-283)" in order to "help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems."[33] It is telling that, without reference to (or likely consideration of) Delaware law, NIST anchors AI risk management squarely to governance and situates it at the apex of the organization as addressing existential enterprise risk:

> Governance and Oversight tasks are assumed by AI actors with management, fiduciary, and legal authority and responsibility for the organization in which an AI system is designed, developed, and/or deployed. **Key AI actors responsible for AI governance include organizational management, senior leadership, and the Board of Directors.**[34]

NIST bases this on the scale of the endeavor and the potential impact to the organization: "These actors are parties that are concerned with the **impact and sustainability of the organization as a whole**."[35]

In other words, NIST has defined AI risk as one of operational resiliency,[36] which for certain companies, depending on the use case, can be a mission-critical risk. NIST also anchors AI oversight to the other corporate principles outlined above: legal compliance, business strategy, and financial performance. Indeed, the first role of Governance characterized by NIST (1.1 under *Govern*) is ensuring "[l]egal and regulatory requirements involving AI are understood, managed, and documented." NIST further guides organizations to address AI as a matter of business strategy and performance, tying it to "the organization's mission and relevant goals for AI technology," the "business value or context of business use," and "[o]rganizational risk tolerances."

Under NIST, AI governance is a precondition to operationalizing other AI-related functions within the organization: "**Assuming a governance structure is in place**, functions may be performed in any order across the AI lifecycle as deemed to add value by a user of the framework."[37] NIST situates compliance and ethics/policy functions as subcomponents of the larger AI governance model. Ethical norms are inputs balanced among "technical, societal, legal, and ethical standards or norms." And compliance is characterized, appropriately given Delaware law, as an aspect of governance rather than governance itself: "**Aspects** of GOVERN, especially those related to compliance or evaluation, should be integrated into each of the other functions."[38]

NIST identifies significant upskilling required for privacy and security professionals to contribute to AI management within their domains, and the opposite is also true – existing professionals that address computational methods and outputs must also gain skills to understand the risks around security and data given the rise of AI. Referencing its own prior security and privacy risk frameworks, NIST states:

> there are significant differences between these frameworks based on the domain addressed – and because AI risk management calls for addressing many other types of risks – frameworks like those mentioned above may inform security and privacy considerations…[but do] not comprehensively address many AI system risks.[39]

Current frameworks further cannot "comprehensively address security concerns related to evasion, model extraction, membership inference, availability, or other machine learning attacks; account for the complex attack surface of AI systems or other security abuses enabled by AI systems; and consider risks associated with third-party AI technologies, transfer learning, and offlabel use[.]"[40]

While security and privacy functions are plainly significant contributors to AI risk management, just as privacy is to information security and information security is to privacy, they do not address the risks around computational methods and output and cannot therefore subsume AI risk management any more than privacy subsumes information security. NIST lists 11 characteristics of trustworthy AI, two of which are "secure" and "privacy-enabled," but this doesn't mean that experts in computational processes or output are now suddenly security or privacy experts, any more than privacy and security experts are experts in the design and deployment of AI models. Indeed, NIST notes that within AI systems, these characteristics are often in tension with one another and require careful tuning and balancing at all stages of design and deployment to ensure the overall trustworthiness of the system. For instance, "in certain scenarios tradeoffs may emerge between optimizing for interpretability and achieving privacy. In other cases, organizations might face a tradeoff between predictive accuracy and interpretability. Or, under certain conditions such as data sparsity, privacy-enhancing techniques can result in a loss in accuracy, affecting decisions about fairness and other values in certain domains."[41]

These are not one-time tradeoffs that can be set by an executive team prospectively as a matter of business strategy. Rather they are contextual and case-dependent, meaning daily operators tasked with owning and managing AI must make these adjudications:

> Dealing with tradeoffs requires taking into account the **decision-making context**. These analyses can highlight the existence and extent of tradeoffs between different measures, but they do not answer questions about how to navigate the tradeoff. Those depend on the values at play **in the relevant context** and should be resolved in a manner that is both transparent and appropriately justifiable.[42]

As such, NIST demonstrates that no one domain, existing or new, can "own" AI, because responsible AI governance and oversight requires a cross-functional view that can neutrally adjudicate between these perspectives for the overall resilience of the organization: "Highly secure but unfair systems, accurate but opaque and uninterpretable systems, and inaccurate but secure, privacy-enhanced, and transparent systems are all undesirable."[43] Accordingly:

> A comprehensive approach to risk management calls for balancing tradeoffs among the trustworthiness characteristics. It is the joint

> responsibility of all AI actors to determine whether AI technology is an appropriate or necessary tool for a given context or purpose, and how to use it responsibly. The decision to commission or deploy an AI system should be based on a contextual assessment of trustworthiness characteristics and the relative risks, impacts, costs, and benefits, and **informed by a broad set of interested parties**.[44]

Because the "AI lifecycle consists of many interdependent activities involving a diverse set of actors," where those "in charge of one part of the process often do not have full visibility or control over other parts,"[45] this requires a top-down, AI-specific governing body. AI governance and oversight at the operational level thus requires a body that can balance "the relationships and tradeoffs among trustworthiness characteristics, socio-technical approaches, and AI risks," establish "policies, processes, practices, and procedures for improving organizational accountability efforts related to AI system risks," and administer the "explicit processes for making go/no-go system commissioning and deployment decisions."[46]

For now, in many organizations, this means the creation of a dedicated AI function, whether a cross-functional committee or stand-alone unit reporting up to senior management, with the expertise across the computational methods, output, technology and data domains to balance risks, impacts, costs, and benefits to the organization, and with stakeholder input from business, technology, security, privacy, and other functions. At the top of this process, and reflected in the expected output of this decision-making, is an AI function that ensures each AI use case deployed by companies is "**well-aligned with their goals, considers legal/regulatory requirements and best practices, and reflects risk management priorities**,"[47] as well as the value and disruption side of the equation, which is a distinct risk issue that is more related to traditional business-principles.

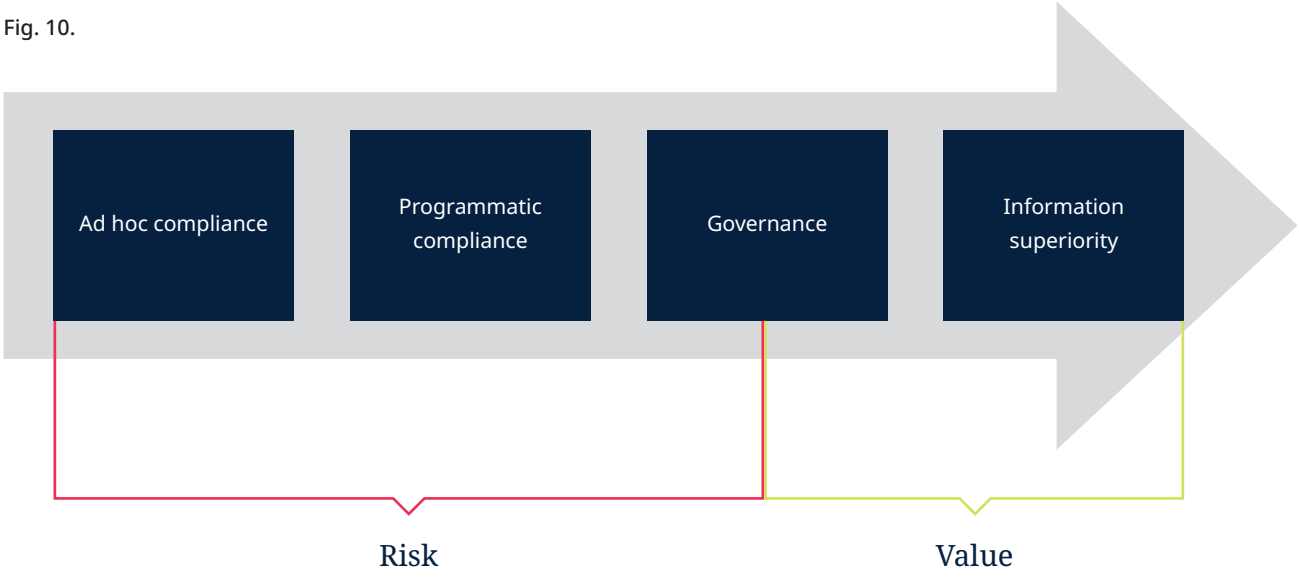
AI governance

Returning to the nested governance model, program governance of AI, like any other subject area, should have appropriate professionals involved, but the program has to be subordinate to the enterprise-level corporate governance program, with parallel and co-equal status to other top-line governance verticals, particularly where the risks and opportunities are this important.

Companies that realize this and align their oversight and operations to this reality will perform better than those that don't as we enter another period of business model disintermediation. Ultimately though, the risk of disintermediation isn't a program-level issue – it is an enterprise issue around strategy, financial performance and resiliency which isn't tied to a compliance framework like the NIST standards, which can mitigate risk but not set risk tolerance or business strategy nor derive positive value. (NIST itself makes this point). Instead, it comes down to how well a company runs its business and anticipates and in fact gets ahead of its competition and moves past programmatic compliance and governance and into Information Superiority (fig. 10).

Said differently, Blockbuster didn't have a "cyber" problem (the name we give to the risks around the technology that is the infrastructure for the Internet) – it had a business model problem that was created by the technology. Managing and overseeing those risks requires very different skillsets, which are rapidly becoming important for many companies.

Fig. 10.



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.

There has been much discussion about the impact of new technologies such as virtual reality (VR) and how they will change our society. The reality is that society has already changed, most of us just don't fully appreciate it. We are already living in a hybrid world where the "real" world and the "cyber" world are inextricably linked and impact each other. For those old enough to remember the time before the Internet, think about how differently you retained and searched for information before Google, how many "friends" you had that you and never actually met in person, how many times you bought an item from a store without a physical presence, or better yet, how many items you bought that weren't actually physical items, versus virtual goods such as NFTs. No, we don't all walk around with VR/AR headsets on, at least not yet, but we do live in an augmented reality nonetheless, using a screen and a keyboard on our phones, which are really portable computers with computing power that is millions of times larger than the guidance computer for Apollo 11. The only real difference is the interface we use (VR headset versus device screen) – but that is an interface issue only.

And by that, we mean this – whether everyone runs out tomorrow and buys a mansion in the Metaverse or not, we already live in a hybrid world with "real" and "virtual" hopelessly enmeshed. How much time we spend in each, and what mechanism we use to interact our hybrid world, matters not at all.

At this point, you may wonder why this followed a section about corporate governance, and what this has to do with companies and how they govern themselves. The answer is *everything*. The reason we have entered this hybrid world is that our predominant line of communication is, for the first time, virtual, and many things in the "physical" world now depend on the virtual world. One of many such examples is a connected medical device – is that a physical device or a "virtual" device? The answer is, it is a hybrid device. Given the dependence upon the "Internet" by businesses now, most business processes are at minimum hybrid, if not fully virtual.

What do we mean by a line of communication? To understand that, you have to 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 to move the platform. 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.

The components of our current line of communication are below (fig. 11):

Fig. 11.

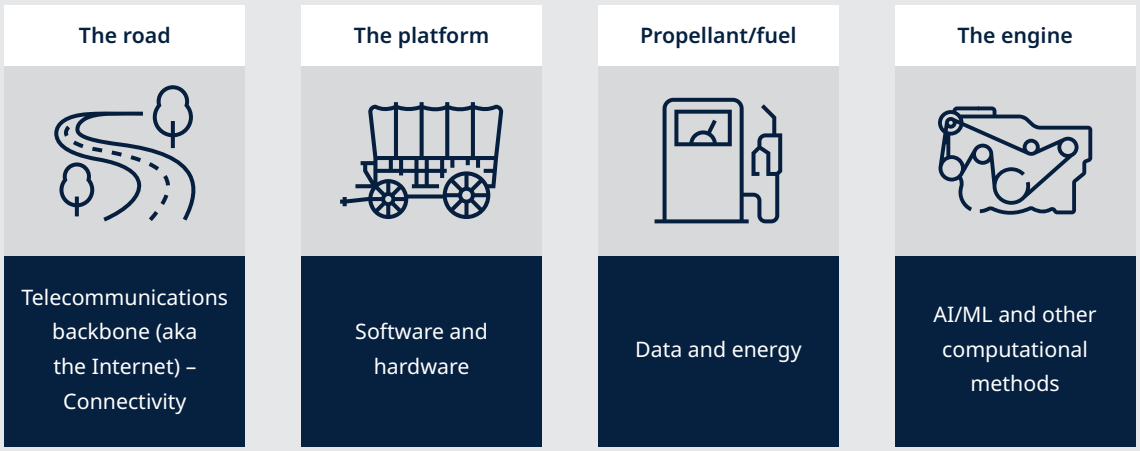


Fig. 12.

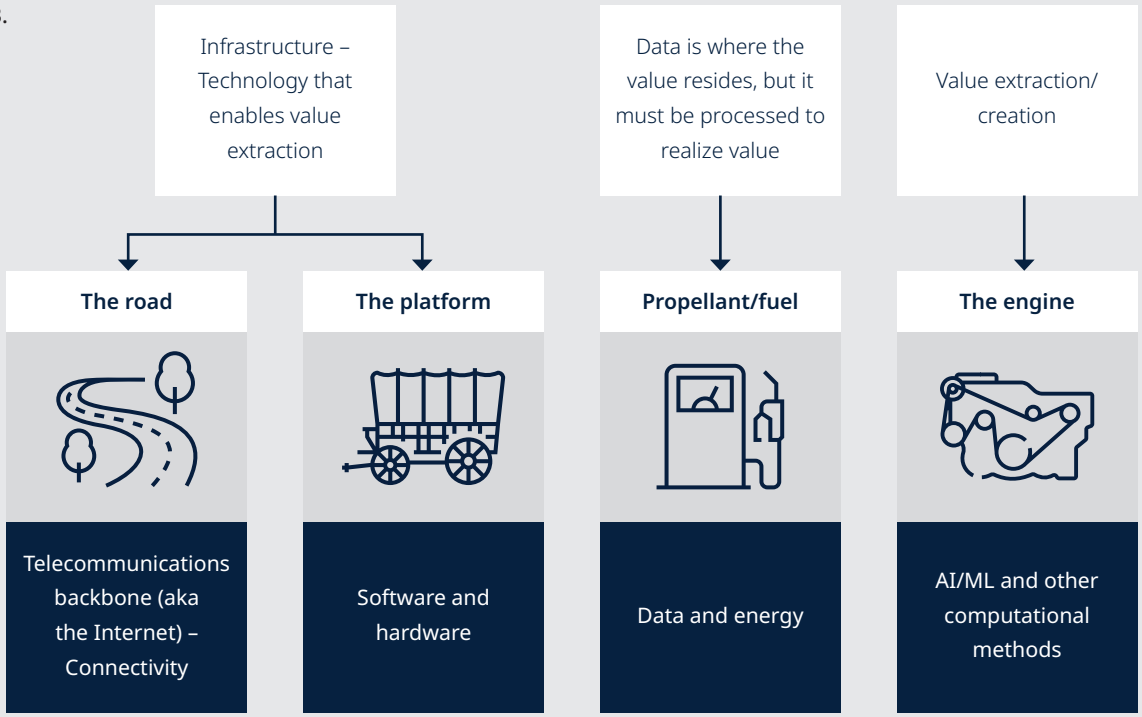
If one looks at the history in context (fig. 12), roads were used for centuries, with various carts serving as the platform, pack animals provided the engine, and food for the animals fueled the engines. Society eventually began using the ocean when ships were created that could travel long distances, and sails were the engine (before the creation of other engines for ships), and wind was the propellant. Eventually the skies became the "road," when the plane became a way to connect quickly after the advent of the jet engine, which ran on oil.

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/ML, which is propelled by information. And as with many of these prior roads, this one was funded by the military – in this case, what is now known as the Defense Advanced Research Projects Agency, or DARPA. 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.

A point is worth noting on the fuel/propellant point: while energy is needed to make the computers turn on, computers are equally dependent on data to propel the computing process. And to be clear, not just personal data. Data of all types fuels, or propels, computing power in our current line of communication.

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 (fig. 13).

Fig. 13.



One can look at all of the examples above of how the creation of technology enhanced the connectivity of our world, and a key point becomes clear—these lines of communication can be used to do four things that are generally helpful for societies, but they also can be used to do four things that are detrimental to society (fig. 14).

- Diplomacy v. war
- Information sharing v. propaganda
- Commerce v. crime/piracy
- Social connection v. espionage

Our core challenges in "privacy" and cyber result from our inability to see two things. First, from a "privacy" perspective, much of our society depends upon a DARPA-created line of communication that is propelled by, and inherently dependent upon, an ever-increasing amount of data. Second, from a cyber and national security perspective, our current line of communication is a borderless global road that permits these four sets of activities to occur, with few checkpoints along the way to regulate conduct.

Talking to the board about ~~privacy and cyber~~ floods

Lawyers love writing about talking to the board about privacy and cyber, but we are going to broaden that discussion and instead address how to talk to your board about risk – not just about root causes.

Starting from our corporate governance principles, we can illustrate how a corporation operates. The corporation creates business operations to operate itself consistent with its direction and strategy. Those operations are made up of sub-component business processes and other activities. These could include a payroll system, an accounts receivable system, a business process that facilities the manufacture of advanced semiconductors, or the software development process.

Which illustrates the point – companies operate through business processes, and the disruption or interruption of them is what creates risk for companies. To be clear here, when we talk about disruption and interruption, we are including alteration of the process as well (including potential theft of data). The point here is that those risks are the same independent of the root cause.

What do we mean by a root cause? The root cause is the reason that a business process has been interrupted or disrupted. For example, if a company has a business process that is dependent upon a data center, there is of course risk that the data center gets shut down due to ransomware, but there are other risks as well. What if the data center goes down due to a flood or other natural disaster? Isn't that the same risk, even though the root cause is different? The answer is clearly yes.

Fig. 14.

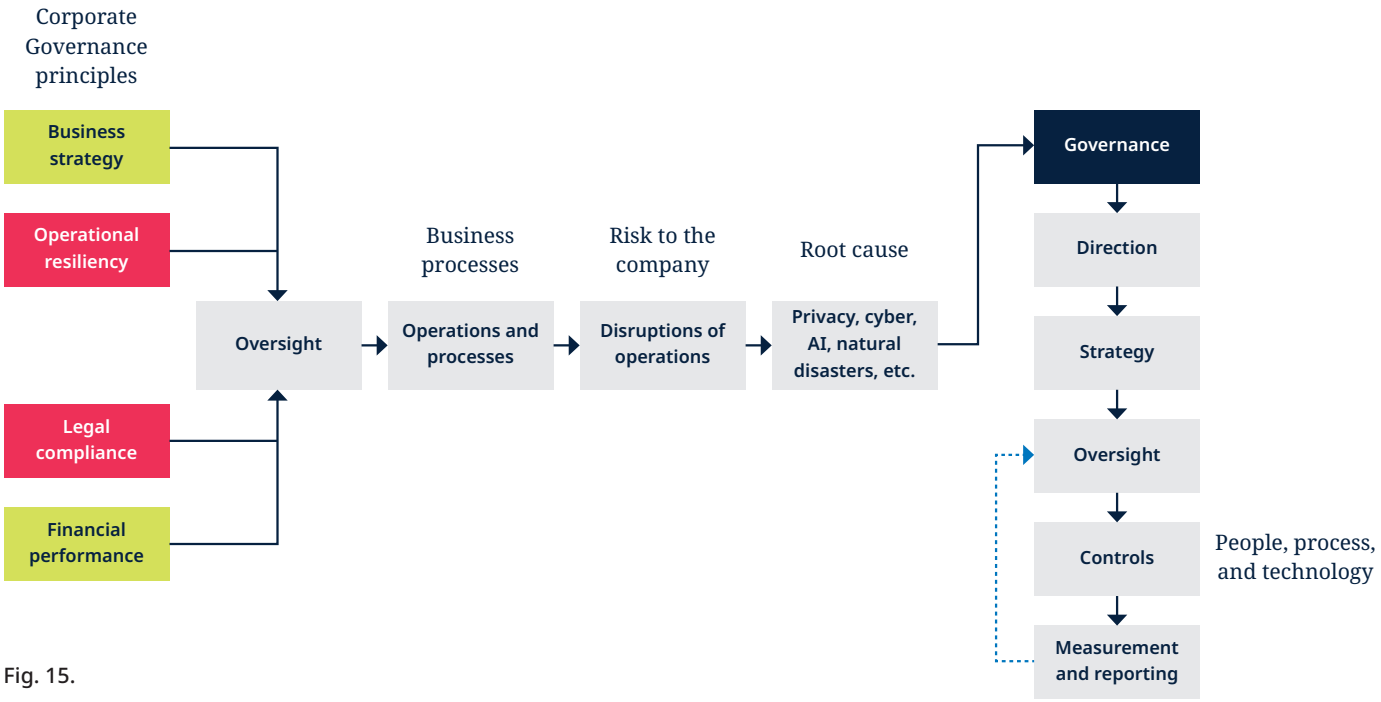


Fig. 15.

Without question, how different root causes are governed differs, and there will be different controls (though some will be the same – *eg*, off-site backups) put in place to deal with ransomware versus flood risk, which helps us illustrate this using our prior definition of governance (fig. 15).

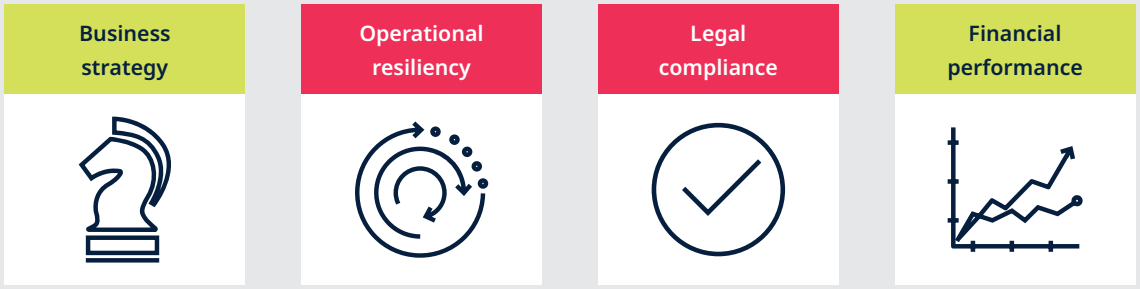
As previously noted, boards are fiduciaries that are generally not involved in the day-to-day operations of the company, while the SLT and management operate the company. Looking at this graphic in that light begins to help us define the problem with some of the thinking about how to talk to boards about privacy, cyber, and AI. It is not that we think that the most senior leaders in a company should be unaware of the control posture on critical issues, but at times there is almost an exclusive focus on the root causes – "talking to the board about privacy" – and the resulting control portion of the governance of the root cause.

We see this in any number of areas, not the least of which is defining escalation criteria for boards. Is "ransomware" an issue that should be escalated – maybe – but doesn't it really depend less on the root cause of a problem and more on the risk – namely the interruption of the business process? Said differently, wouldn't you escalate the issue of the loss of a critical data center to your board if it went down due to a flood, not just ransomware? And shouldn't we be at least considering how we deal with other root causes that aren't privacy, cyber, or AI to try and align how the company manages risk across different domains?

Changing our thinking here also begins to address the technical gap that can exist at times between the subject matter experts who operate the company, and the board (assuming there aren't privacy or cyber SMEs on the board). While the technical portions of privacy, cyber, and AI are very important – they are controls on the root cause – as illustrated above, they are part of the solution, but not the only part of the solution.

In sum, privacy, cyber, and AI are critical issues not because they are a particular type of root cause, but instead because of the criticality of connectivity and data to our current line of communication. In other words, a disruption to the road or the fuel or the engine may need to be escalated no matter the root cause, but not because of it. So instead of exclusively focusing on talking to the board about privacy, cyber, and AI , we need to consider talking to the board about data, technology, and connectivity, the risks that result from the interruption of critical business processes that are dependent upon them, and then putting the root causes that cause the interruption in the right context.

Fig. 16.



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 (fig. 16).

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 (eg, from manufacturing or payroll vendors) or provide goods or services (*ie*, to customers)
  - Loss of access to critical internal systems
  - Productivity loss resulting from inability to access vendor systems and services
  - Slowed communications (eg, related to email and other communications or infrastructure vendors)
  - Customer invoked restrictions on processing data (*eg*, 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 (*eg*, 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.

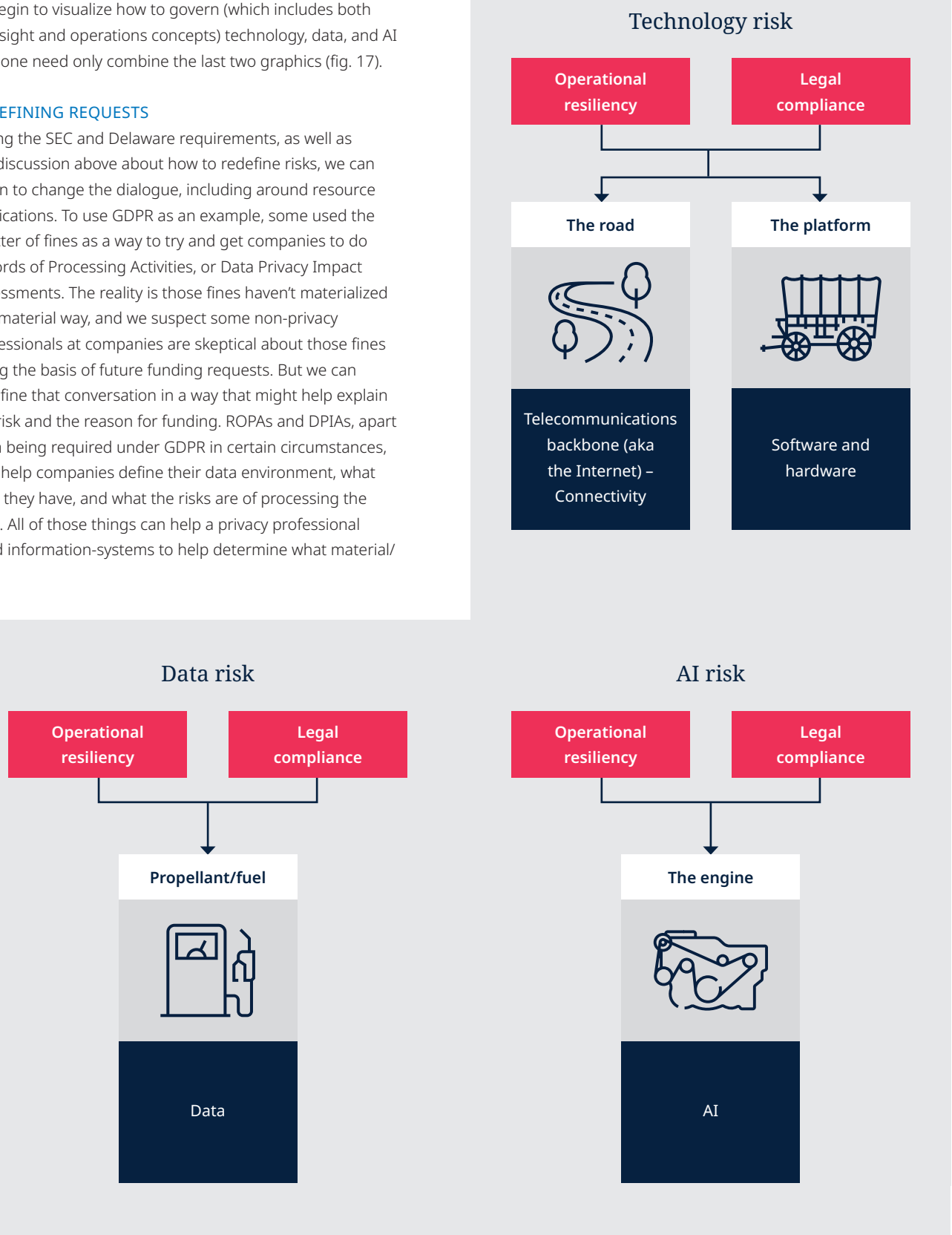
CREATING TECHNOLOGY, DATA, AND AI RISK GOVERNANCE

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 (fig. 17).

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 around 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 we 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/

Fig. 17.



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 we have framed it above.

Are we saying that companies shouldn't comply with GDPR? Of course not. What we are 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 takeaways

To summarize the key points:

- One key element of meeting obligations under SEC and Delaware law is having sufficient information reporting systems; 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, AI, and other 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.

Endnotes

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. With the exception at some level regarding internal control over financial reporting and disclosure controls, though the ultimate purpose of those requirements is still about ensuring accurate and complete public disclosure.

3. SEC Acting Chief Accountant Statement ("Assessing Materiality: Focusing on the Reasonable Investor When Evaluating Errors") available at https://www.sec.gov/news/statement/munter-statement-assessing-materiality-030922#_edn3.

4. *TSC Industries v. Northway, Inc*., 426 U.S. 438, 449 (1976).

5. SEC Adopting Release ("Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure"), Release Nos. 33-11216; 34-97989, available at https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

6. Staff Accounting Bulletin No. 99, Materiality (Aug. 12, 1999), available at https://www.sec.gov/interps/account/sab99.htm#body4.

7. 17 C.F.R. § 240.13a-15.

8. *Id*.

9. Though, public companies should still be cognizant of Exchange Act Sections 13(b)(2)(B)(i) and (iii), which require certain issuers to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurance that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization. In 2018, the SEC filed a report clarifying that these controls apply to cybersecurity risks. *See Report of Investigation… Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Control Requirements*, Exchange Act Release No. 84429 (Oct. 16, 2018), https://www.sec.gov/files/litigation/investreport/34-84429.pdf.

10. 17 C.F.R. § 240.13a-15.

11. *Id*.

12. 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.

13. Cal. Civ. Code § 1798.140.

14. *Edgar v. MITE Corp*., 457 U.S. 624, 645 (1982) (citing Restatement (Second) of Conflict of Laws § 302 cmt. b. (1971)). JUUL Labs, Inc. v. Grove, C.A. No. 2020-0005-JTL (Del. Ch. Aug. 13, 2020).

15. *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).

16. §141 DGCL.

17. *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.")

18. 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." The Delaware Way: Deference to the Business Judgment of Directors Who Act Loyally and Carefully, available at https://corplaw.delaware.gov/delaware-way-business-judgment/.

19. "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).

20. "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.

21. https://corplaw.delaware.gov/delaware-way-business-judgment/.

22. *Aronson v. Lewis*, 473 A.2d 805 (Del. 1984)

23. "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.

24. "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).

25. https://corplaw.delaware.gov/delaware-way-business-judgment/.

26. *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019).

27. *Id.* at 824.

28. *In re Mcdonald's Corporation Stockholder Derivative Litigation*, C.A. No. 2021-0324-JTL (2023).

29. https://laresinstitute.com/archives/4279.

30. *In re Mcdonald's Corporation Stockholder Derivative Litigation*, C.A. No. 2021-0324-JTL (2023).

31. 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 does not 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.

32. https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF.

33. https://www.nist.gov/itl/ai-risk-management-framework/roadmap-nist-artificial-intelligence-risk-management-framework-ai#:~:text=116%2D283)%2C%20the%20goal,and%20use%20of%20AI%20systems.

34. Appendix A, NIST AI Risk Management Framework.

35. *Id*.

36. In fact, NIST describes the scale of risk from organizational use as going beyond the organization, extending to harm to outside people and ecosystems. From an organizational perspective, this translates as risk to values and mission as well as business and legal risk (*eg*, mass tort).

37. NIST AI RMF Core.

38. NIST AI RMF Core.

39. Appendix B, NIST AI RMF.

40. Appendix B, NIST AI RMF.

41. NIST AI RMF AI Risks and Trustworthiness.

42. NIST AI RMF AI Risks and Trustworthiness.

43. NIST AI RMF AI Risks and Trustworthiness.

44. NIST AI RMF AI Risks and Trustworthiness.

45. NIST AI RMF Core.

46. NIST AI RMF.

47. NIST AI RMF Profiles.

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

For more information

To find out more about the topics covered in this report, please contact any of us:

Era Anagnosti
Partner
Co-Chair, Capital Markets and Public Company Advisory Practice
+1 202 799 4087
era.anagnosti@dlapiper.com

Ronald N. Brown III
Partner
+1 302 468 5665
ronald.brown@dlapiper.com

Hayley R. Curry
Associate
+1 214 743 4540
hayley.curry@dlapiper.com

Eric Forni
Partner
+1 617 406 6040
eric.forni@dlapiper.com

John Gevertz
Of Counsel
+1 212 335 4771
john.gevertz@dlapiper.com

Larry W. Nishnick
Partner
Chair, Southern California Corporate and Securities
+1 858 677 1414
larry.nishnick@dlapiper.com

Chelsea Rissmiller
Associate
+1 619 699 2630
chelsea.rissmiller@dlapiper.com

Andrew Serwin
Partner
Global Co-Chair and US Chair, Data Protection, Privacy and Security Practice
+1 858 677 1418
andrew.serwin@dlapiper.com

Danny Tobey M.D., J.D.
Partner
Global Co-Chair and US Chair, AI and Data Analytics Practice
+1 214 743 4538
danny.tobey@dlapiper.com

Jon Venick
Partner
+1 917 952 9737
jon.venick@dlapiper.com

Sept 14 2023 | MRKT0003281 v3IP