The Lares Institute

Defining Governance in a Hybrid World

September 30, 2022

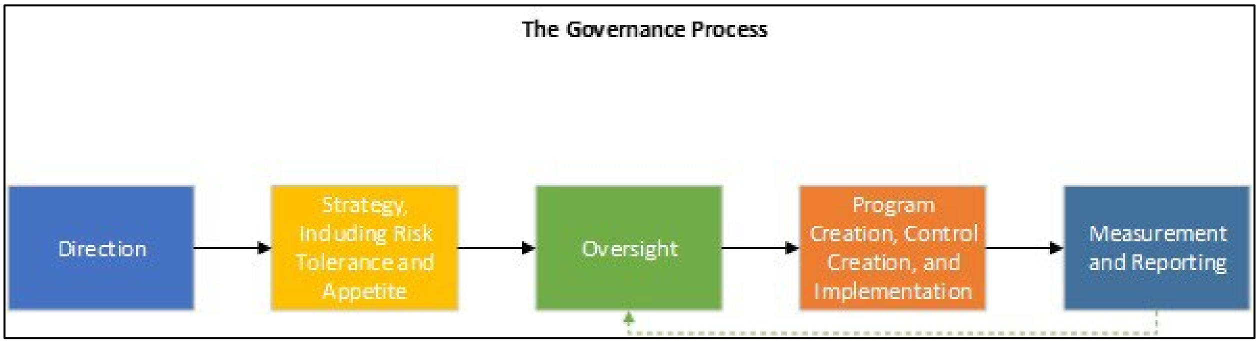
Table of Contents

Defining Governance

Governance is perhaps one of the most often used, but misunderstood, concepts by business people and compliance professionals. The goal of this article is to identify what goverance is, how it can be implemented, and how it can be utilitzed in different contexts—"keyed" to different control frameworks, so that business people and compliance professionals can better understand how goverance can be used as a tool to enhance outcomes across organizations.

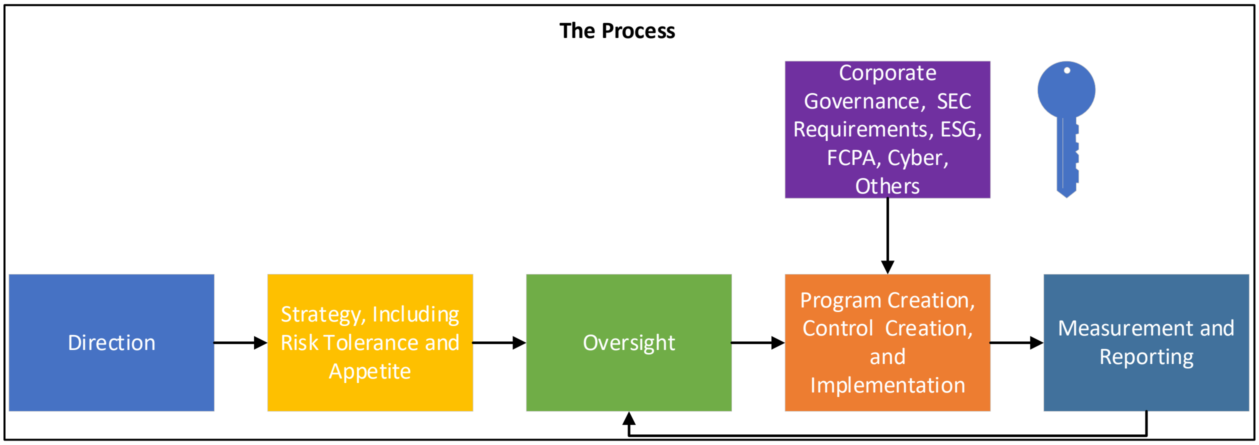
If you raise the concept of goverance, people immediately think of a specific type of "governance" and assume that is what you are talking about. Sometimes that means they are focused on controls (operations), or sometimes it means they are focused on a particular type of governance—corporate goverance, governance of a particular program, privacy, cyber, or BCP are good examples, but it in most cases doesn't actually focus on what goverance actually is.

Goverance is a process, not tied to any particular substantive area, that does five things. It sets a direction, develops a strategy, create an oversight structure, establishes operations to implement the strategy, and provide a framework for measuring progress and reporting back to the oversight layer on an ongoing basis.

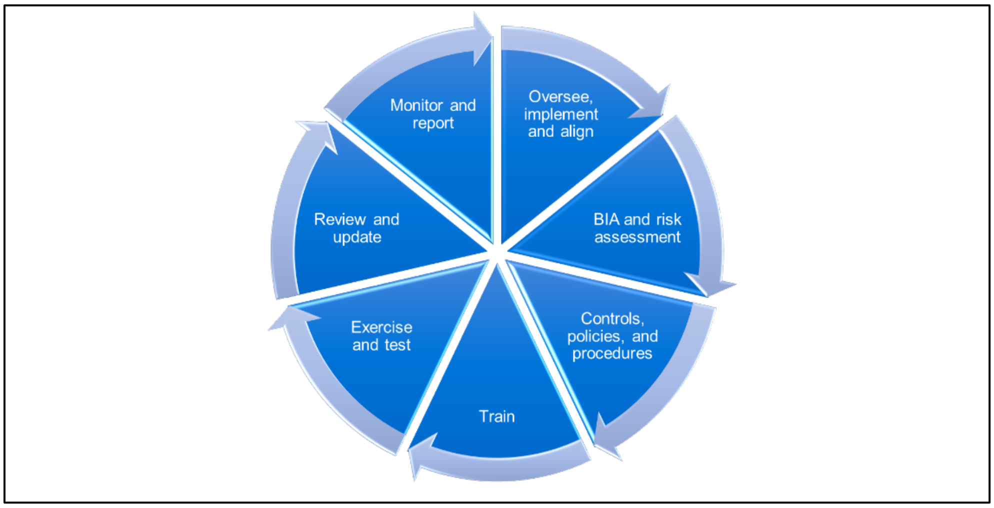

The Governance Process
Direction
Strategy, Including Risk Tolerance and Appetite
Oversight
Program Creation, Control Creation, and Implementation
Measurement and Reporting

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

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


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

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.



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.

Mission Statements and “Primary Purpose”

Corporations and other entities frequently create mission statements, values, or other similar statements regarding the entity’s primary purpose, including what the entity does, in order to help orient themselves, as well as those that interact with them. As we think more about governance, as well as how to begin to solve some of the issues that have been identified, it is important to understand what these different statements are, and how they help us potentially solve some of these issues, but also how they tie into governance frameworks, particularly at the corporate governance level. If we were to stack these concepts, it would look something like this:

- Primary purpose
- Mission statement/direction
- Strategy
- Values
- Ethics

An entity’s primary purpose is essentially a statement about why the entity exists. For most for-profit corporations, that is to return value to shareholders. That does not mean that an entity’s primary purpose is the only thing it does, but it does mean that in most scenarios, an entity will choose its primary purpose over a different purpose, if there is a choice to be made, though that choice will never be unrestricted. A good example of this is a statement from Google’s values/philosophy page:

> Google is a business. The revenue we generate is derived from offering search technology to companies and from the sale of advertising displayed on our site and on other sites across the web. Hundreds of thousands of advertisers worldwide use AdWords to promote their products; hundreds of thousands of publishers take advantage of our AdSense program to deliver ads relevant to their site content. To ensure that we’re ultimately serving all our users (whether they are advertisers or not), we have a set of guiding principles for our advertising programs and practices:
>
> https://about.google/philosophy/

Does that mean all Google does is focus on generating revenue from search? As you can see above, no, but the statement above helps orient us to how for-profit entities orient and align their primary purpose with other priorities—serving users which ultimately results in a set of principles that guide Google’s advertising program.

With other entities, particularly government agencies, returning value to shareholders isn’t the primary purpose of the entity, and there will be different purposes for different entities.

Where things begin to diverge for most entities is at the mission statement level. At this level, the overall direction of the entity is set as part of defining its mission, and this direction informs the strategy, corporate values, ethics, as well as a number of other processes. At their core, for private companies, these statements begin to define how a company returns value to shareholders. To use an example from a corporation—Meta:

> Meta’s mission is to give people the power to build community and bring the world closer together. https://investor.fb.com/resources/default.aspx

Google provides another example:

> Google's mission is to organize the world's information and make it universally accessible and useful. https://about.google/

Turning to strategy, a strategy focuses on, at a high-level, how an entity will achieve its mission statement. That might be focused on certain revenue or sales objectives, cost reduction, increasing or maintaining profit, other corporate growth activities, or in some cases, other objectives. These statements can, and probably should, be short and focused on specific achievements, and be specific enough to allow measurement of progress. For companies like Meta and Google, their strategies inherently would have to be intertwined with data and connectivity. This also may be true for many companies, even those in different industries, because using data and connectivity might be critical to achieving the strategy (creating products that rely upon research data, or implementing cost reductions as an examples), even if not explicitly referenced.

Next, we turn to values, which can be expressed as corporate values, area-specific values, or in other ways. Again, we can look at Meta as an example:

- Move Fast
- Focus on Long-Term Impact
- Build Awesome Things
- Live in the Future
- Be Direct and Respect Your Colleagues
- Meta, Metamates, Me

Google uses a different format, but expresses its values in a list called, "Ten things we know to be true."

1. Focus on the user and all else will follow.
2. It's best to do one thing really, really well.
3. Fast is better than slow.
4. Democracy on the web works.
5. You don't need to be at your desk to need an answer.
6. You can make money without doing evil.
7. There's always more information out there.
8. The need for information crosses all borders.
9. You can be serious without a suit.
10. Great just isn't good enough.

Corporations and other entities also create codes of conduct and ethics statements that are based upon the entity's mission, strategy, and values. Google again provides a good example. The main headings are below, with the full conclusion, as there is a significant amount of detail in Google's code of conduct:

> I. Serve Our Users
>
> II. Support and Respect Each Other
>
> III. Avoid Conflicts of Interest
>
> IV. Preserve Confidentiality

> V. Protect Google’s Assets
>
> VI. Ensure Financial Integrity and Responsibility
>
> VII. Obey the Law
>
> VIII. Conclusion
>
> Google aspires to be a different kind of company. It’s impossible to spell out every possible ethical scenario we might face. Instead, we rely on one another’s good judgment to uphold a high standard of integrity for ourselves and our company. We expect all Googlers to be guided by both the letter and the spirit of this Code. Sometimes, identifying the right thing to do isn’t an easy call. If you aren’t sure, don’t be afraid to ask questions of your manager, Legal or Ethics & Business Integrity.
>
> And remember... don’t be evil, and if you see something that you think isn’t right – speak up! https://abc.xyz/investor/other/google-code-of-conduct/

For a company like Google, issues regarding data and privacy are intertwined in a number of ways with their code of conduct, but again given the Hybrid World in which we now live, data and connectivity are frequently part of the mission or strategy of a company, and as a result may be covered in codes of conduct.

So why does this matter for people focused on “privacy”, cybersecurity or governance? The answer is three-fold. First, entities do a much better job achieving their goals when their goals are understood and are aligned with operations, and privacy and cyber are still seen as compliance issues rather than issues that are core to a company’s mission statement. It is hard to imagine the use of data, personal data or not, and connectivity not being critical to a company’s primary purpose, mission statement, and strategy, and that is one of the issues with focusing on issues involving data as being “privacy” issues, such as when we focus on “talking to the Board about privacy.”

As noted in other posts, privacy is a concept focused on individual rights, usually enforced through legal means. While that is a critical issue for the individual, enforcing individual privacy rights isn’t an issue that will be part of a company’s strategy or mission, because it does not relate directly to the company’s primary purpose. However, that in no way means the issue is irrelevant—quite the opposite in many cases--but the issues regarding use of personal data must be put in terms related to what the company does, not vindication of individual rights for the company to truly be able to understand and govern “privacy.”

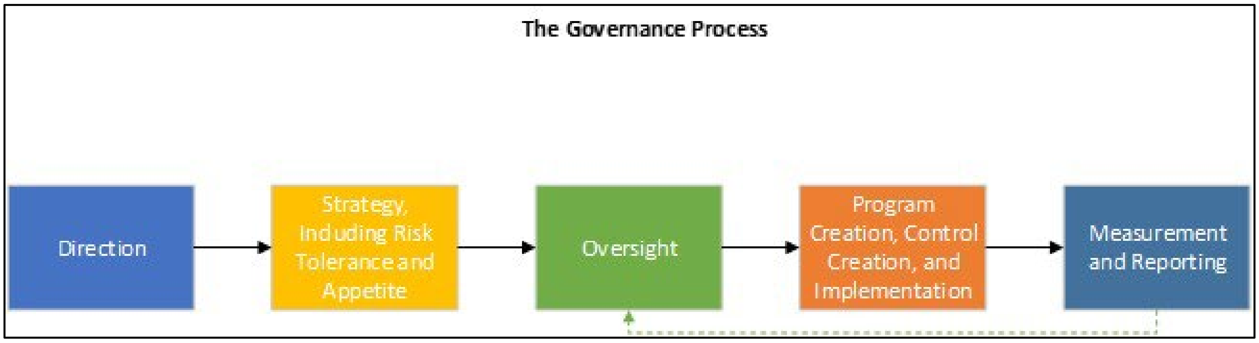
Second, regarding cybersecurity, as will become clear in future posts, one of the core challenges in the US right now is that we do not have an agency with a primary purpose of disruption of cyberattacks, or other similar critical issues related to cyber.

Third, regarding governance, direction and strategy are critical components of establishing governance, and whether that is corporate governance, based upon the four corporate governance principles, or programmatic governance, making sure that those overseeing the governance process in question understand the mission, strategy, values and ethics of the company is important, because otherwise the governance process devolves into an empty set of controls with no real direction. While that can provide some control around particular issues, that will not truly provide governance of issues, and it will not ensure that the governance model is horizontally integrated.

Future posts will examine how data, including “privacy” fits into the mission and strategy of corporations, as well as provide some thoughts on how we begin to solve the cyber challenges we face as a nation.

Corporate Governance

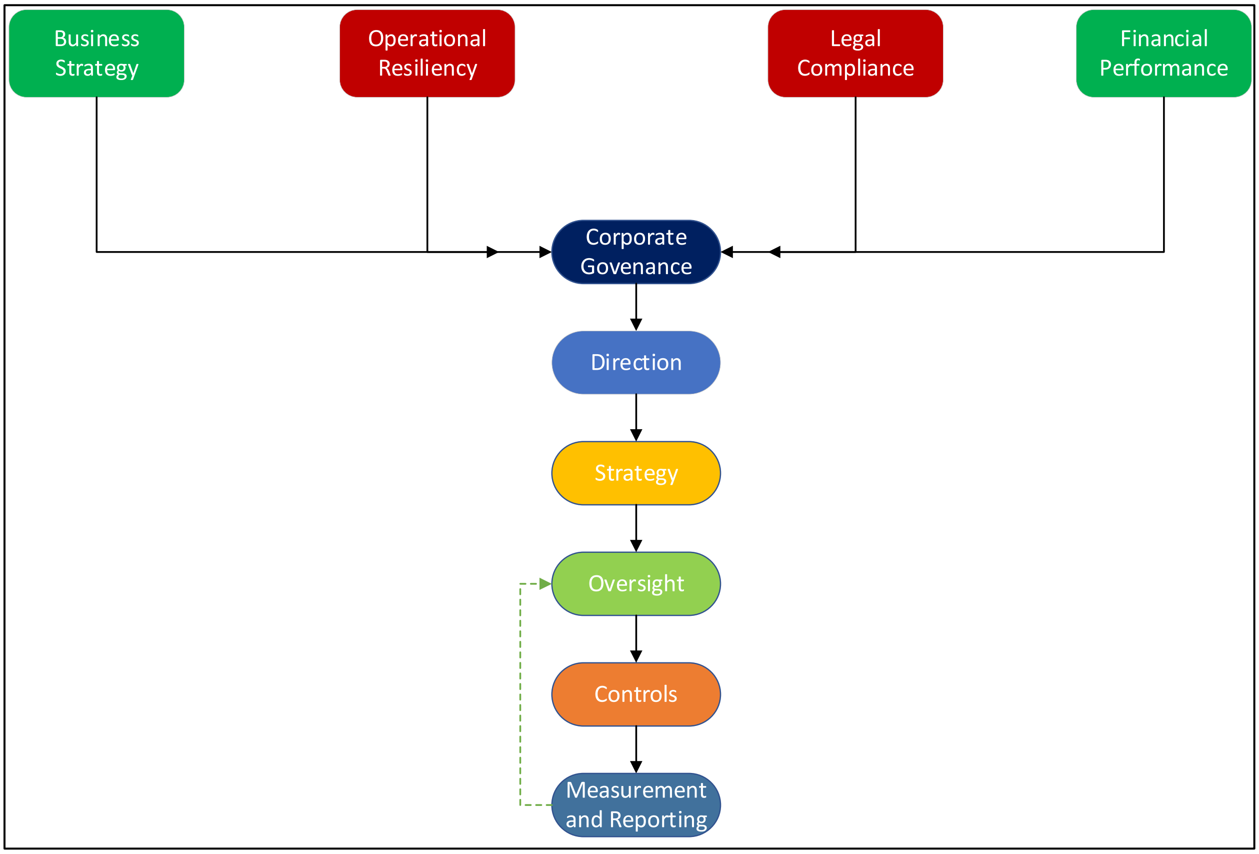
The first step in our journey was to define governance, which is summarized by the process below, where a direction for the issue governed is created, as well as a strategy, and then oversight, operations and measurement and reporting follow, and the second step is to define corporate governance, as well as program governance. In this image, as with the ones that follow, the black lines represent a process pushing down through the governance structure, and the dashed green line represents reporting up to the oversight function.


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

Since governance is an empty process until it is keyed to a particular issue, it raises the question of what corporate governance is, and perhaps what it is not. To address the second issue first, corporate governance isn’t exclusively tied to an examination of SEC issues or Delaware law—not all companies are subject to SEC or Delaware jurisdiction--though those issues become important for many companies in a programmatic governance sense. What corporate governance is relates back to the core of why corporation exist.

Corporations exist to provide benefit to its shareholders, and for most corporations, at least for-profit corporations, that means providing a return on the shareholder’s investment. Corporate governance is therefore directly informed by this singular purpose. Much has been written about how corporations can and should provide benefit to shareholders, but ultimately what a corporation must focus on to do this can be summarized in four points that corporations should focus on:

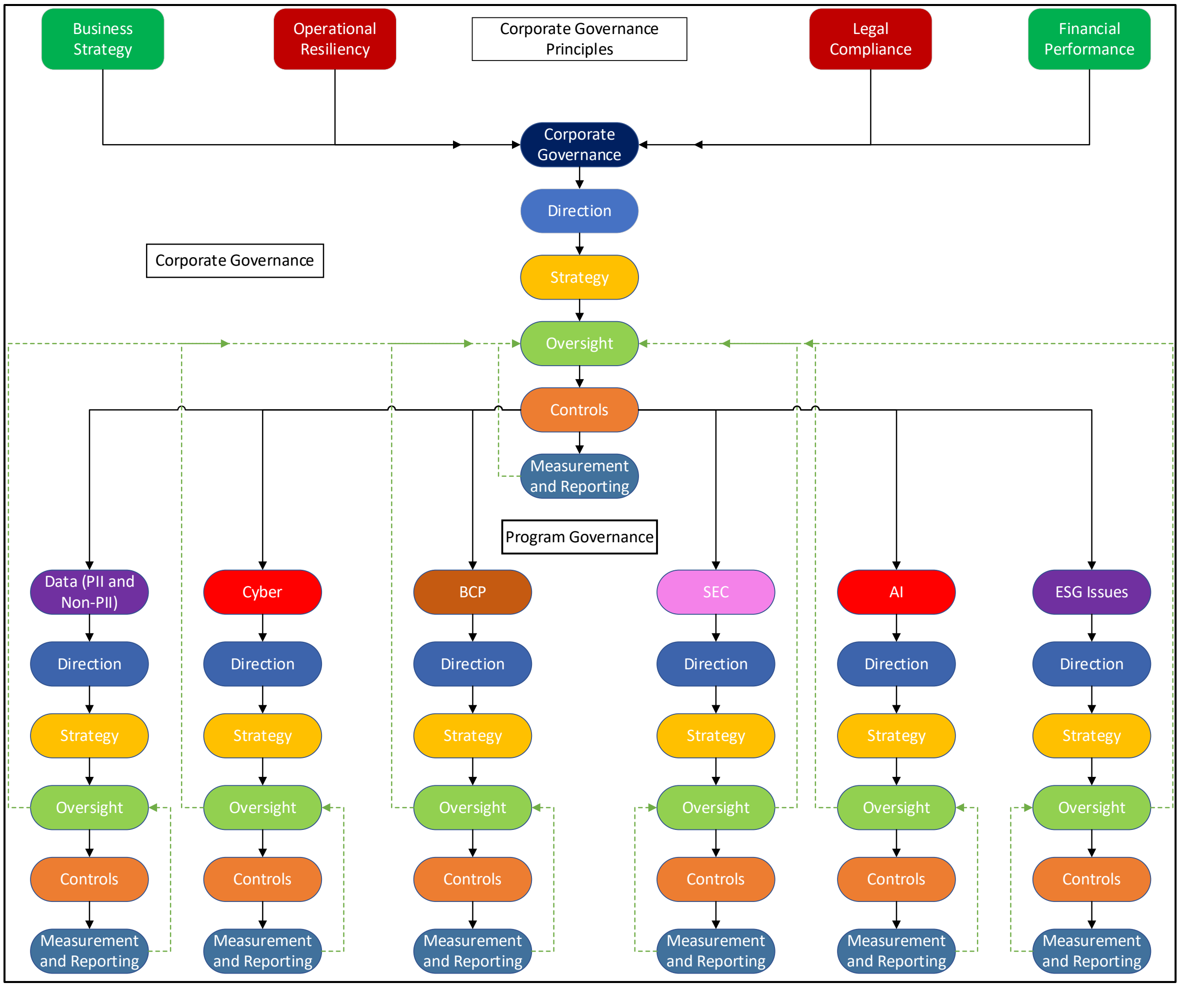
While this may seem like an oversimplification, the truth is that a focus on business strategy (as opposed to a strategy to implement governance), operational resiliency, legal compliance, and financial performance will significantly help a company provide benefit to its shareholders. So what does that really mean? It means that one can now define corporate governance using these four points, as well as the governance process, and that combined process is represented below, again with the black lines representing a process pushing down, and the dashed green line representing reporting up to oversight:



This is corporate governance. In most companies, oversight is provided by the Board, and the company is operated by the Senior Leadership Team 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 noting now. 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.

Now that we have defined the governance process, as well as corporate governance, the distinction between corporate governance and governance of a program becomes clearer.



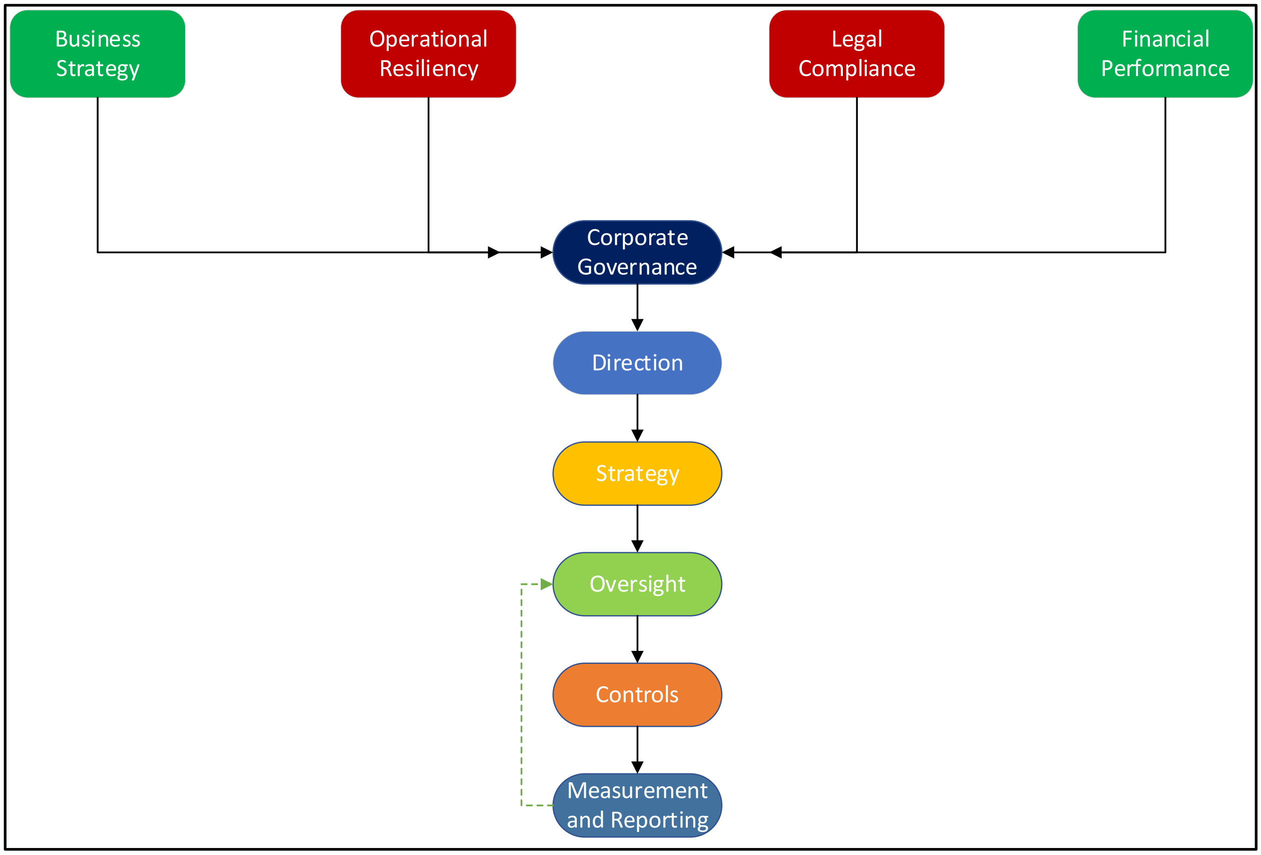
Corporate governance sits above program governance, and when implemented in a "nested" way, program governance inherently aligns with, and is informed by, corporate governance, and while both layers set direction and strategy, the direction and strategy at the program governance layer should be informed, as relevant, by the company's business strategy, operational resilience, legal compliance, and financial performance, which is pushed down by the corporate governance process. The advantages of this model will be discussed in future posts, but the critical point is that by nesting governance in this way, companies can horizontally integrate business issues and risks in a much better way.

One final note regarding the programs selected for governance in the nested model. Those topics are important for many companies, which is why they were chosen, but it is important to note that I did not choose privacy quite intentionally. As will be discussed in future posts, privacy, while important for many companies, as well as for the data subjects themselves, shouldn't be the exclusive focus in a program governed by corporate governance principles. Instead, it is a critical component of governance of the use of data by the company, which can be personally identifiable data, or data that in no way relates to an individual.

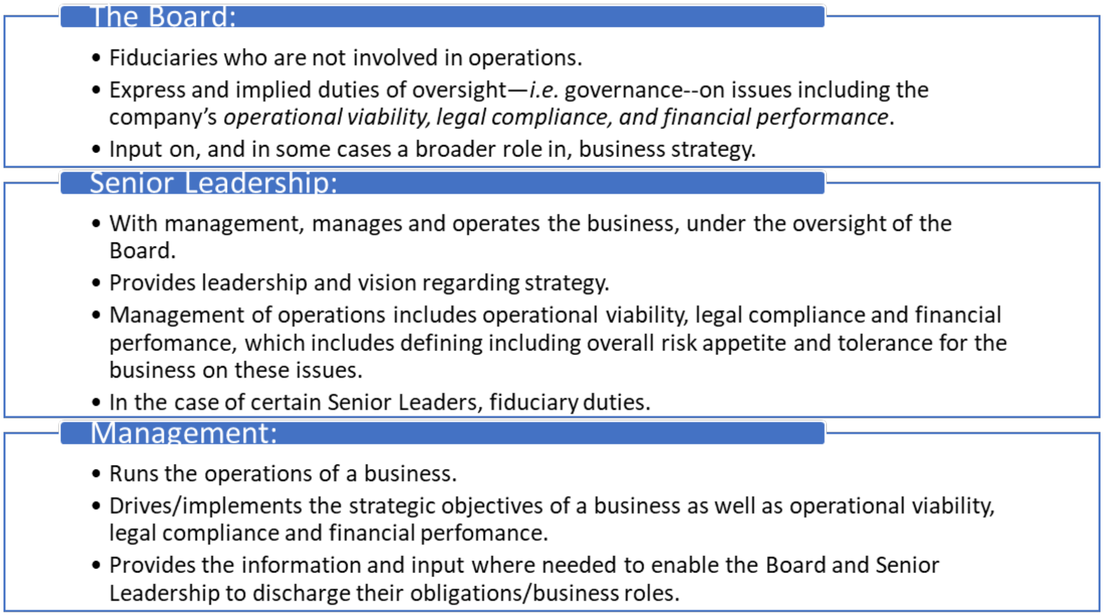
Applying Corporate Governance

In my last article, I covered corporate governance and defined what it was, and most importantly what it was "keyed" to. In this article we will address how the governance structures can "nest" to implement governance, as well as begin to discuss how to address issues that are not the four corporate governance principles, but instead impact those principles.

To recap corporate governance, it can be expressed as a process as follows:



Turning to how most companies implement corporate governance, it is helpful to recognize that there are four key issues, three key groups, and two key functions. The four key issues have been previously identified, and they are the corporate governance principles—strategy, operational resiliency, legal compliance, and financial performance. The three key groups are the Board (fiduciaries of the corporation), Senior Leadership (who if they are officers of the company, also owe fiduciary duties), and Management. The two key functions, which are an important distinction, are oversight versus operations. If we summarize the roles of each, it is as follows:



The Board:

- Fiduciaries who are not involved in operations.
- Express and implied duties of oversight—*i.e.* 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.

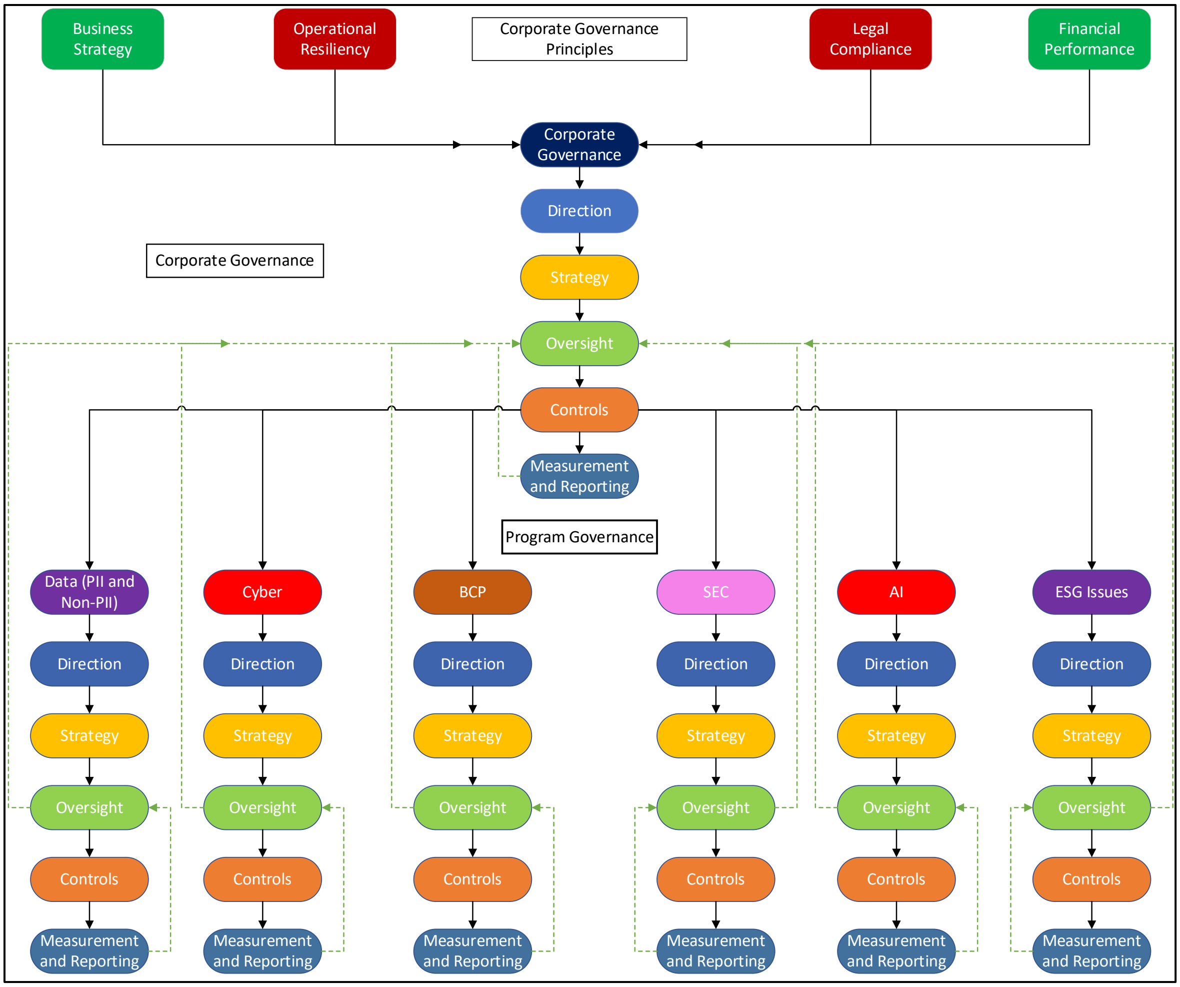
Senior Leadership:

- 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 perfomance, which includes defining including overall risk appetite and tolerance for the business on these issues.
- In the case of certain Senior Leaders, fiduciary duties.

Management:

- Runs the operations of a business.
- Drives/implements the strategic objectives of a business as well as operational viability, legal compliance and financial perfomance.
- Provides the information and input where needed to enable the Board and Senior Leadership to discharge their obligations/business roles.

Turning back to our corporate and program governance structures, some broader issues become clear when one thinks through the implications.



First, when one looks at the governance process, 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 Senior Leadership Team and Management, as appropriate.

While that seems like an unremarkable statement, that delineation isn't 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 not 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.

To pick an example that is very common, SEC requirements for public companies. 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 corporate governance obligations exist independent of SEC public company requirements, not because of them, and that 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—as shown in the nested governance model, SEC requirements would be governed by the broader corporate governance of the company.

This isn't a point I 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 won't 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 use another common example one hears when one works with companies and their privacy and security programs—brand. Brand is not a corporate governance principle, and for companies that have 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 damage done to 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 and will be the subject of future articles—"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 don't implicate corporate governance principles, or don't 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 isn't the optimal way because the focus at times with privacy and security isn't on corporate governance principles, but rather on privacy and security, or concepts such as brand.

There is an alternative path that we will be exploring, but we will first have to actually understand the role of data and connectivity in our world to truly understand how to govern "privacy" and security.

The Hybrid World

> "born from the ashes of a world at war…..
>
> warfare is evolving…..
>
> everything we touch is a weapon…."
>
> 4th PSYOP Group – Ghosts in the Machine (May 2022)

There has been much discussion about the impact of new technologies such as VR and how they will change our society. The reality is that it 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 headsets on, at least yet, we use 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.

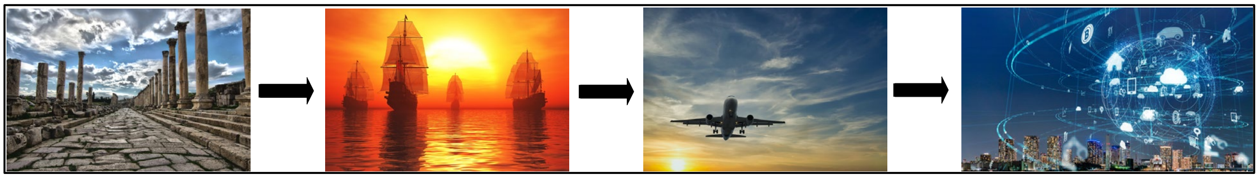
And by that I mean this—whether we all run out tomorrow and buy a mansion in the Metaverse or not, we already live in a hybrid world with "real" and virtual hopelessly enmeshed—how much time we spend in each, and what mechanism we use to interact our hybrid world, matters exactly not at all.

While you may wonder why I followed a series of articles about corporate governance with this one, 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 a hybrid device. Given the dependence upon the "Internet" by businesses now, most business processes are at minimum hybrid, if not fully virtual.

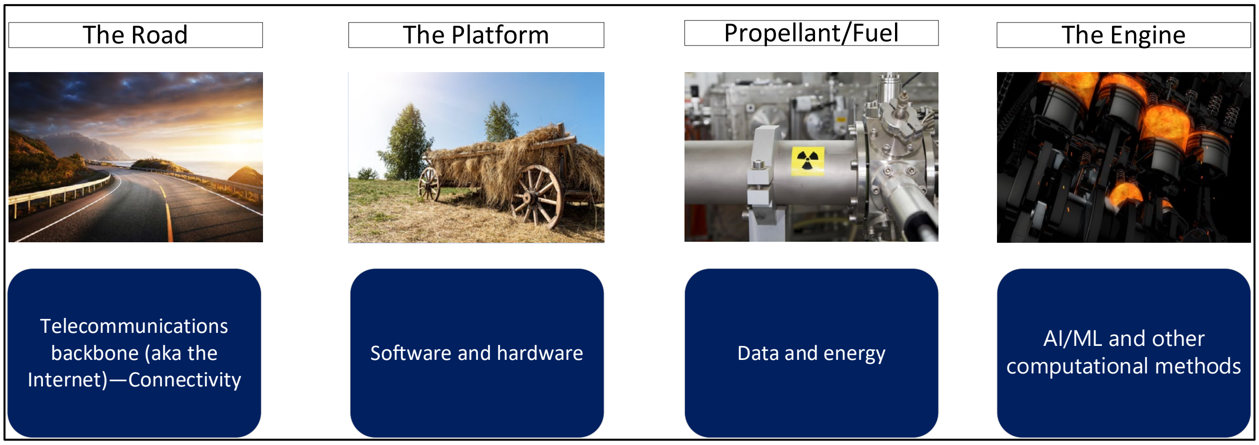
What do I mean by a line of communication? To understand that, you have to put into context the history of how society moves things over great expanses. Society has always looked for ways to connect itself, which required the creation of technology to do it, and understanding the core components to that 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.

If one looks at the history in context, 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.



The Road

The Platform

Propellant/Fuel

The Engine

Telecommunications backbone (aka the Internet)—Connectivity

Software and hardware

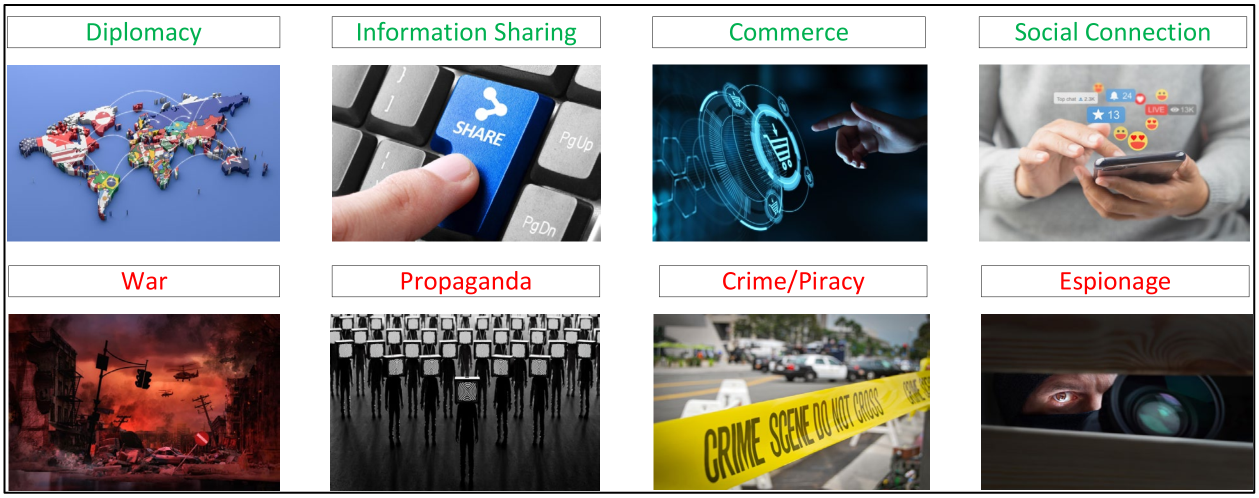
Data and energy

AI/ML and other computational methods

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

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.

- 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.

You cannot solve complex problems without first identifying what the problems actually are. It is past time to do that with “privacy” and cyber. Future articles will link these issues more directly to how companies should rethink these issues, as well as how we all should rethink “privacy” and cyber to help improve our Hybrid World. Until we do that, we will continue to provide the same answers to the same questions, and get the same results.

Talking to the Board About ~~Privacy and Cyber~~ Floods

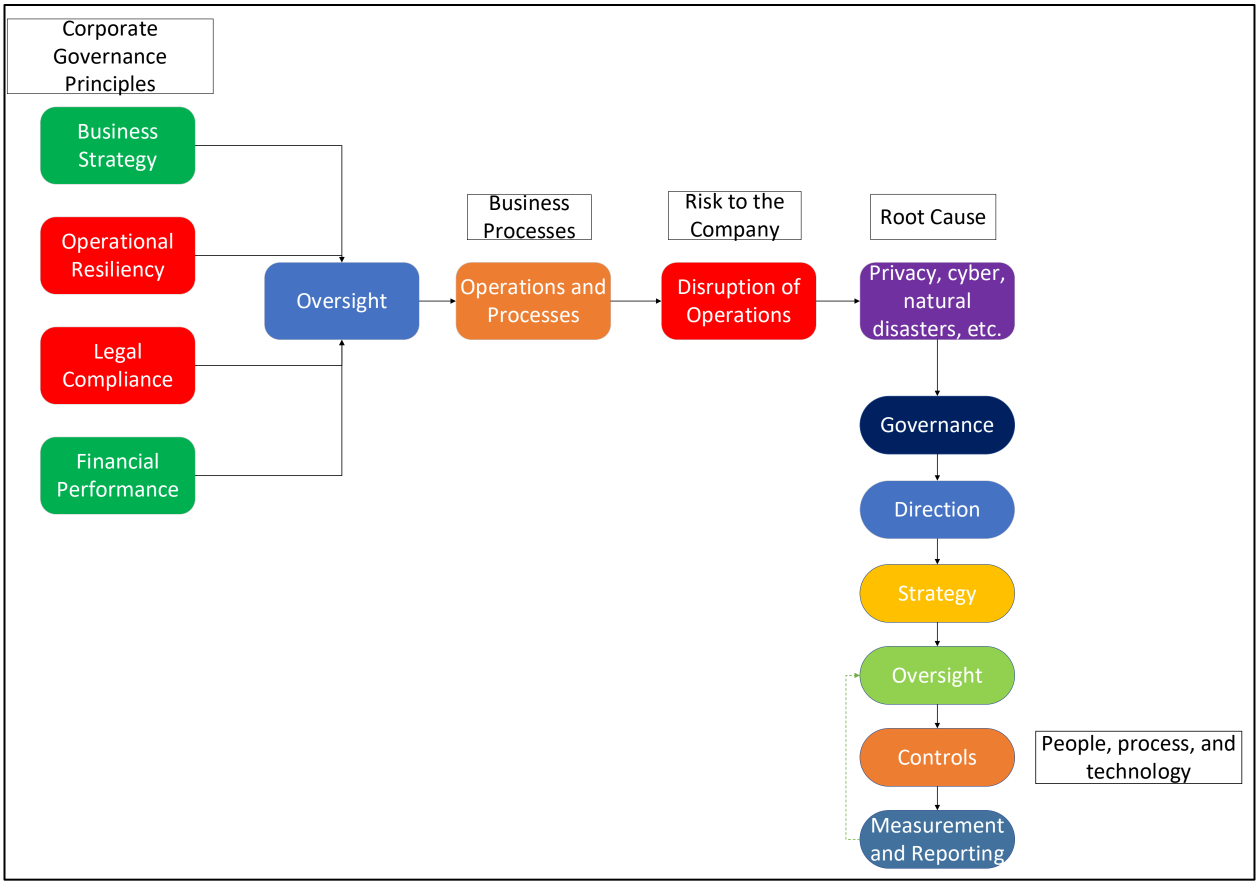
Lawyers love writing about talking to the Board about privacy and cyber, and I could add yet another article to that mix—but I won't. Instead I'm going to write about how to talk to your Board about risk, not just about root causes.

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. That could be 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, and to be clear here when I am talking about disruption and interuption, I am including alteration of the process as well (including potentially theft of data). The point here is that those risks are the same independent of the root cause.

What do I mean by a root cause—the root cause is the reason that a business process has been interrupted or disrupted. An example makes this clear. 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.

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



As previously noted, Boards are fiduciaries who are generally not involved in the day-to-day operations of the company, while the SLT and management operate the company, and 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 and cyber. It is not that I think that the most senior leaders in a company should be unaware of the control posture on critical issues, but I think that 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 and cyber 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 and cyber 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.

Privacy and cyber 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 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 and cyber, we need to consider talking to the Board about data 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.

The Problem With Privacy.

Brand.

Trust.

Digital Risk.

Values.

Ethics.

The “creepy” factor.

Notice and choice.

The right to be let alone.

Fundamental human right.

These and other words are terms you hear to talk about “privacy”, or why companies should care about privacy. The challenge of these terms isn’t that they aren’t important, but rather that their importance isn’t 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 in the earlier article on corporate governance, a corporation’s primary purpose is to return value to shareholders. To be clear, that is not the only thing corporations do, as we see from many of the stands that corporations are taking on a variety of issues, but it is to say that the primary purpose is the primary purpose, and that 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 made it be perceived as 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.

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. It would be hard to estimate the ratio of personal data to non-personal data that companies use, in no small part because it will vary company to company, but no matter the percentage, the point is 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. Again, 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 don’t matter to corporations, but the important point is that other issues matter the most when they impact those four principles. To pick an example—brand. For some companies, brand is a critical issue, and for others, think of 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 doesn't, it likely doesn't matter (or matter as much) for the company.

While one can have a debate about the importance and role of these 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. The importance of data in our global economy inherently means that how data is used, or not used, impacts companies' strategy, operational resilience, legal compliance, and financial performance, and as illustrated by the brand example above, we are better off skipping the middle step of using terms like brand, 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. That concept is data sustainability.

What do I mean by that? I mean that all four principles means just that, which is what 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 the use of data in our Hybrid World, 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 PCI requirements, and sometimes that is a law, a regulation, or even an enforcement action that identifies allegedly improper activities. There are then 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, which 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—a trip to Washington for Congressional testimony, a front-page story in the media, other things 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 isn't sustainable will impact a brand-conscious company's brand, 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 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 isn't sustainable, and therefore isn't an operationally resilient practice.

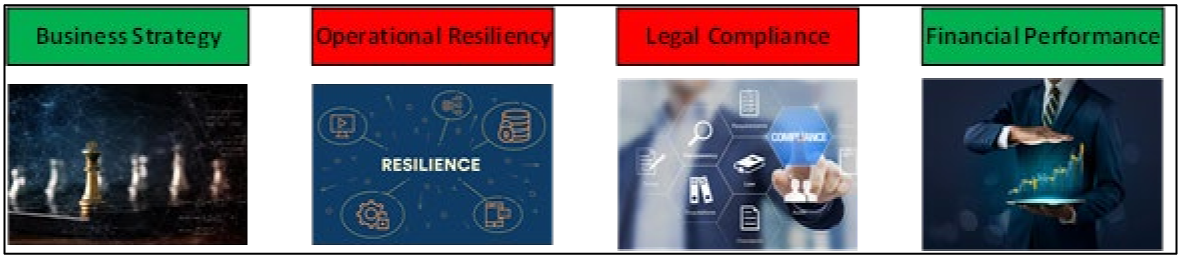
To address what some lawyers may be thinking—no I am not saying ignore the legal consequences of processing personal information—again quite the opposite. And one need only look at some of the consequences from regulators to actually understand that the "legal" risks in many cases are actually operational resiliency risks. Under Section 5, the FTC does not have the ability to obtain civil penalties, and its ability to use 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 EU, the most critical issue right now is data transfer, and while fines are certainly possible under GDPR, the main issue being talked about by regulators is suspension of data flow. All of these consequences create more of an operational resiliency issue than a legal issue.

Future articles will help further define data sustainability, 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 doesn't 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.

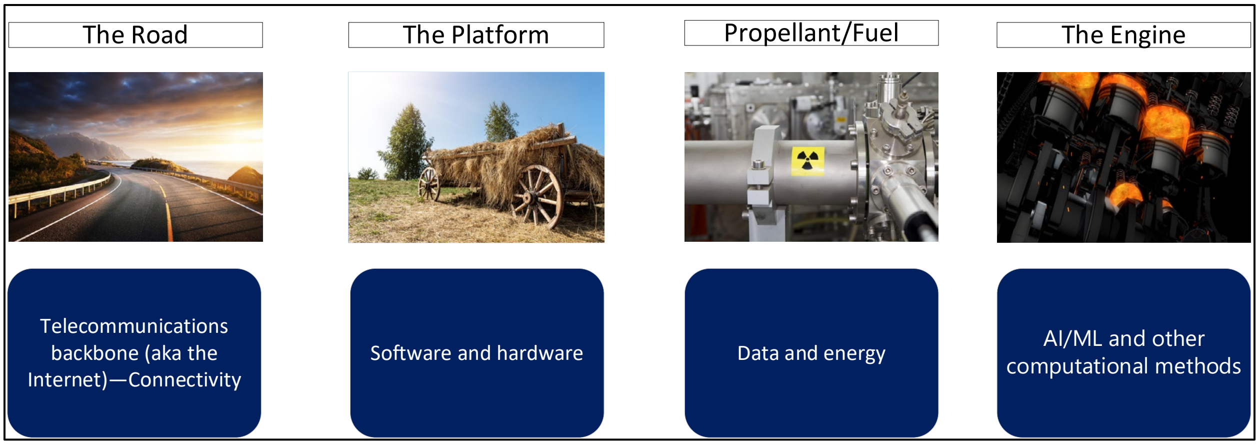
Data Sustainability

Having taken what seems like a detour down the path of "primary purpose" after having identified the problems with privacy, we return to data and will try to define the concept of data sustainability 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.

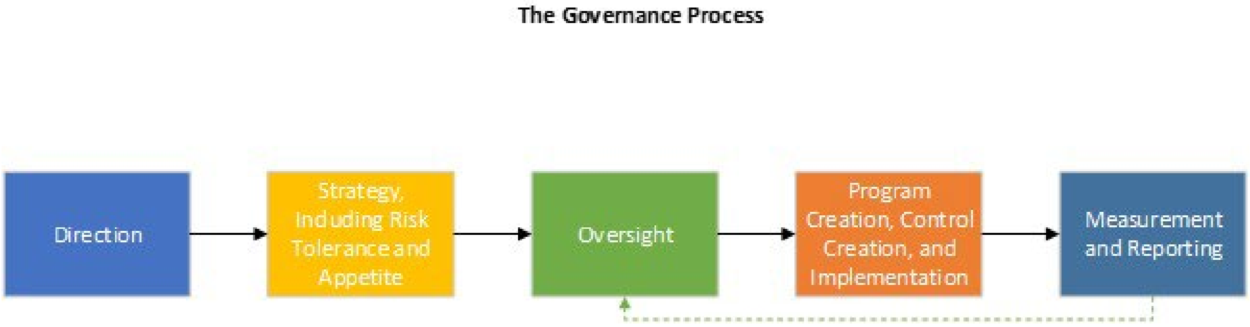
To do that, it is helpful to recall the four corporate governance principles, so that we recognize that legal compliance is one, but only one, of the four principles.



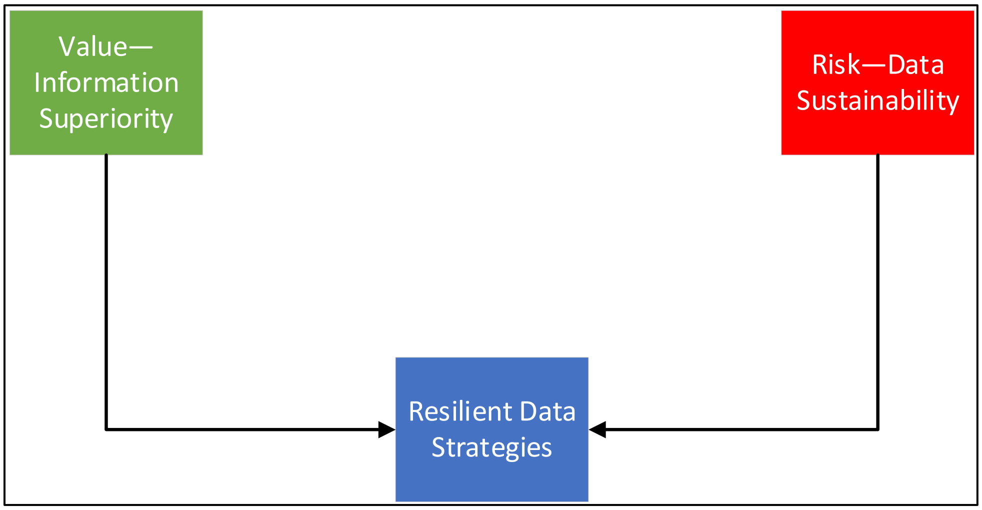
It is also helpful to recall the components of our current line of communication, which is propelled by data.


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

Finally, it is also helpful to recall the components of governance, which are not just limited to the creation of controls.


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

Putting these ideas together, 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.



This post will examine the risk, or sustainability side.

If we are going to address an issue that is as important and complex as how to 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 making risk decisions where we reduce the times that we make uninformed risk decisions, particularly on material risks.

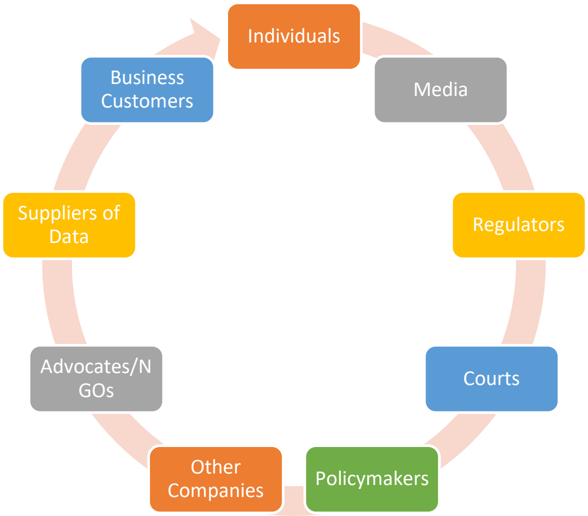
Having factored in corporate governance concerns, including business strategy and operational viability, not just legal compliance or even financial performance (as viewed through brand impact), we also must factor in continuity and resiliency concepts because if we accept data is the propellant for 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.

This is all the more true when one considers the four positive and negative points that any line of communication can be used for—simply put legal-based approaches, including a law enforcement centric approach inherently cannot address all of the potential issues, because the potential issues are all not based upon law.

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.

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.



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 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 lead to the invalidation of two different treaties between the EU and the US, and threatens 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—i.e. 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 policy-maker.

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.

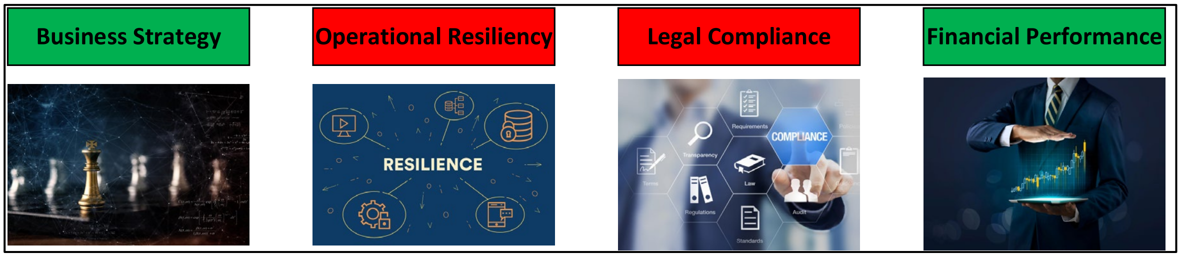
If the goal is to build a program based upon compliance concerns, that certainly can be done via controls including people, process, and technology. However, as anyone who has built a privacy compliance program knows, the laws change frequently, and in many cases you are constantly chasing new standards.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

Defining Value and Risk in Corporate Governance, and the Limits on Privacy

As we continue to explore new strategies for governance around data and cyber, it is helpful to return to our corporate governance principles and begin to view them through value and risk, and the prior discussion of primary purpose again is a helpful reference point.

Each one of the principles has a primary purpose, and ultimately that boils down to whether the principle is focused on creating value, or focused on controlling risk. The graphic below tries to illustrate that, with value creators in green, and risk controls in red.



🟩 Business Strategy

🟥 Operational Resiliency

🟥 Legal Compliance

🟩 Financial Performance

To head off one argument, am I saying that companies don't have strategic or financial risk? Of course not, but what I am saying is that the primary purpose of a business strategy and focusing on financial performance isn't to avoid a negative (risk), but rather to create a positive (value). Similarly, most companies do not set resilience and compliance goals with a focus around creating a positive (value), but rather to avoid a negative outcome around processes failing or a negative legal consequence (risks). Said differently, there is no value created from being legally complaint past a certain point, though legal compliance programs can in certain cases create value, but would be expressed in the realm of strategy or financial performance, not compliance.

In short, the primary purpose of strategy and financial performance is to create value, and the primary purpose of resiliency and compliance is to avoid risk.

Turning to data and the limits on privacy, it is important to focus on the types of data that companies use, which is certainly not limited to personal data. A few examples include:

- Financial information;
- Information regarding individuals (including employees and customers);
- Proprietary/confidential information;
- Undisclosed M&A activity;
- Business and marketing plans;
- Pricing;
- IP;
- Information regarding businesses processes, including process improvements;
- Information regarding business trends;

- Social data/user-generated content;
- Machine data; and
- De-identified data.

Privacy, given that its primary purpose is the protection of individual rights regarding data, with a corresponding focus on legal compliance as the consequence for non-compliance, simply cannot be the basis of governance for data, because it is simply to limited a concept for our Hybrid World. In short, if you want to focus on one of the corporate governance principles, and on one set of data out of a number of critical data sets, a focus on privacy is the answer.

At some level, this illustrates the difference in the role of a Chief Data Officer, and a Chief Privacy Officer. A data officer is concerned about data in all forms that matter to the company—a CPO's primary purpose is to manage privacy risk, which means a lot of forms of data are not truly in scope. Do CPOs help companies create value at times, and also focus on data other than personal data, yes. Is it their primary purpose. No.

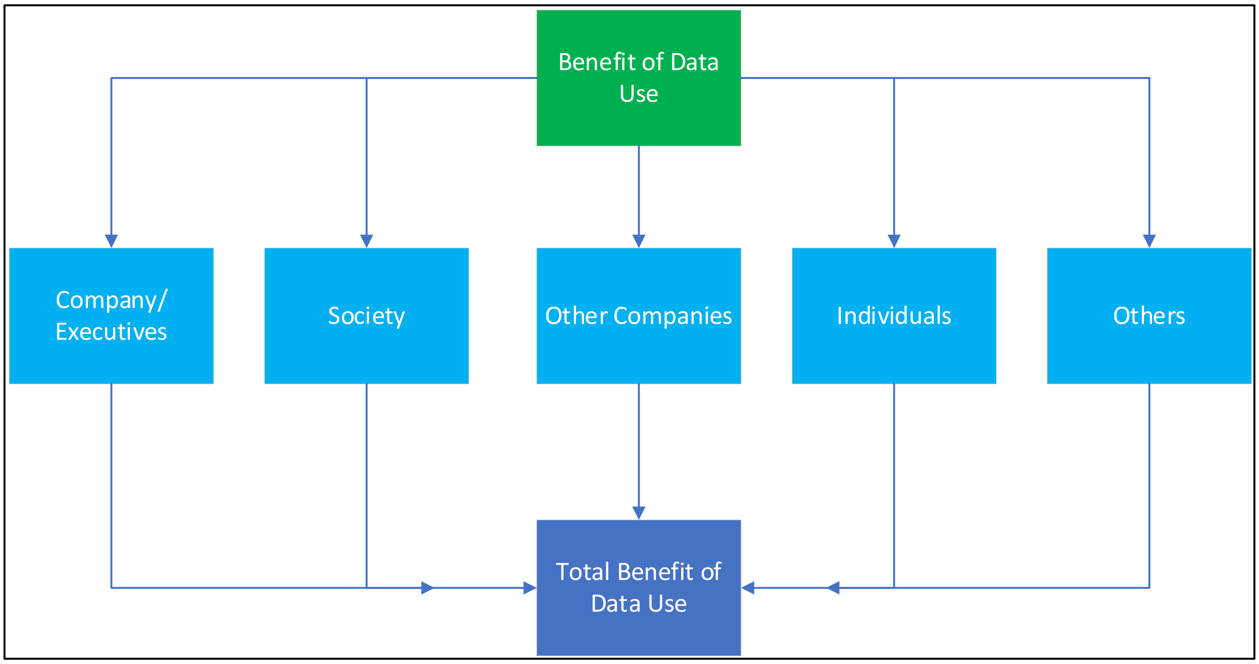
So what is the point? As we now inhabit a world where data is the propellant, and we move into a world where data sustainability is a more workable concept, we need to start thinking about data of all types, and examining the value and risk of what we do with data, and stop viewing how we use data through the lens of risk to the individual only, including because there are risks to using data that go beyond the risk to the individual, and given data's central role in our world, we can no longer ignore the value side of data use, by only focusing on individual risk.

Value and Data

Picking up on the last post regarding value, risk and data, it is helpful to again return to the types of data that companies use to create value. These include:

- Company financial information;
- Information regarding individuals (including employees and customers);
- Proprietary/confidential information;
- Undisclosed M&A activity;
- Business and marketing plans;
- Pricing;
- IP;
- Information regarding businesses processes, including process improvements;
- Information regarding business trends;
- Social data/user-generated content;
- Machine data; and
- De-identified data.

Having tried to define categories of data, it is also helpful to look at the individuals and entities that can benefit from data use, and these are just broad categories of key stakeholders—there are many more examples that can be provided.



The point here is two-fold. First, in our Hybrid World, the use of data creates value, sometimes to the company using it, sometimes to an individual, sometimes to other companies or entities, and there have been any number of studies on this topic. Examples include:

- Public health, including the creation of treatments, disease management, and improved diagnostics, including through AI;
- Process improvement and cost reductions for the public and private sector;
- National security;
- Crime reduction;
- Environmental issues, including traffic reduction; and
- Increased revenue and personalization of advertising and products.

That list is hardly exclusive, and ultimately we do return to the four positives and negatives of a line of communication.

While all of those are important, there is a broader point to be made about the use of data, which is that increasing the use of the right data will improve all decisions, because using data in inherent to making any decision, whether that is in the public or privacy sector. Executives have many roles in a company, but as illustrated by a Harvard Business Review Article on executive decision-making, there is one key distinction between executives and non-executives in organizations:

> The job of a manager is, above all, to make decisions. At any moment in any day, most executives are engaged in some aspect of decision making: exchanging information, reviewing data, coming up with ideas, evaluating alternatives, implementing directives, following up.
>
> …

> To climb the corporate ladder and be effective in new roles, managers need to learn new skills and behaviors—to change the way they use information and the way they create and evaluate options.[1]

There are also examples from the public sector that emphasize the importance of executive decision-making and the key role of information, including from the Naval War College in a text entitled "Executive Decision Making":

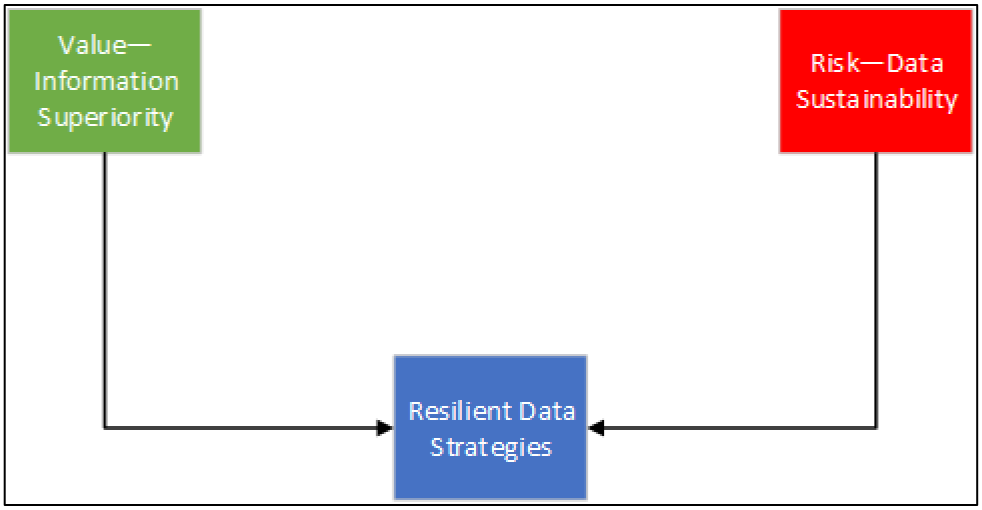
> Making high-level defense decisions is a large part of being a senior military officer or career defense civilian.
>
> …
>
> These kinds of choices will push you into new, unfamiliar circumstances in which procedure and experience are no longer sufficient unto themselves. How do you decide whether to advocate producing a next-generation weapon or to push instead for a complete technological leap forward? This text will help you answer that kind of question by providing a structured approach to problem solving and decision making. It will help you identify and bound not only what is known and unknown, but also what ingredients are necessary to make a good decision.
>
> …
>
> The key is to treat experience and lessons-learned as one source of data or evidence to bring to bear on a decision, along with all other useful information from other sources.[2]

There are two key points to focus on from these examples—(1) the executive's job, whether public or private sector, is to make decisions, and (2) efficiently getting the right, not just more, information is a critical part of executive decision-making.

Ultimately what this means is that if your company wants to make better decisions, and have resilient data strategies, it can't simply focus on risk around data (let alone on privacy—a risk that is only related to one of the data sets), and instead has to focus on both the value side of the equation, as well as the risk side.

[1] The Seasoned Executive's Decision-Making Style, Kenneth R. Brousseau, Michael J. Driver, Gary Hourihan, Rikard Larsson, Harvard Business Review, February 2006.

[2] http://www.au.af.mil/au/awc/awcgate/navy/edm/exc-dm.pdf

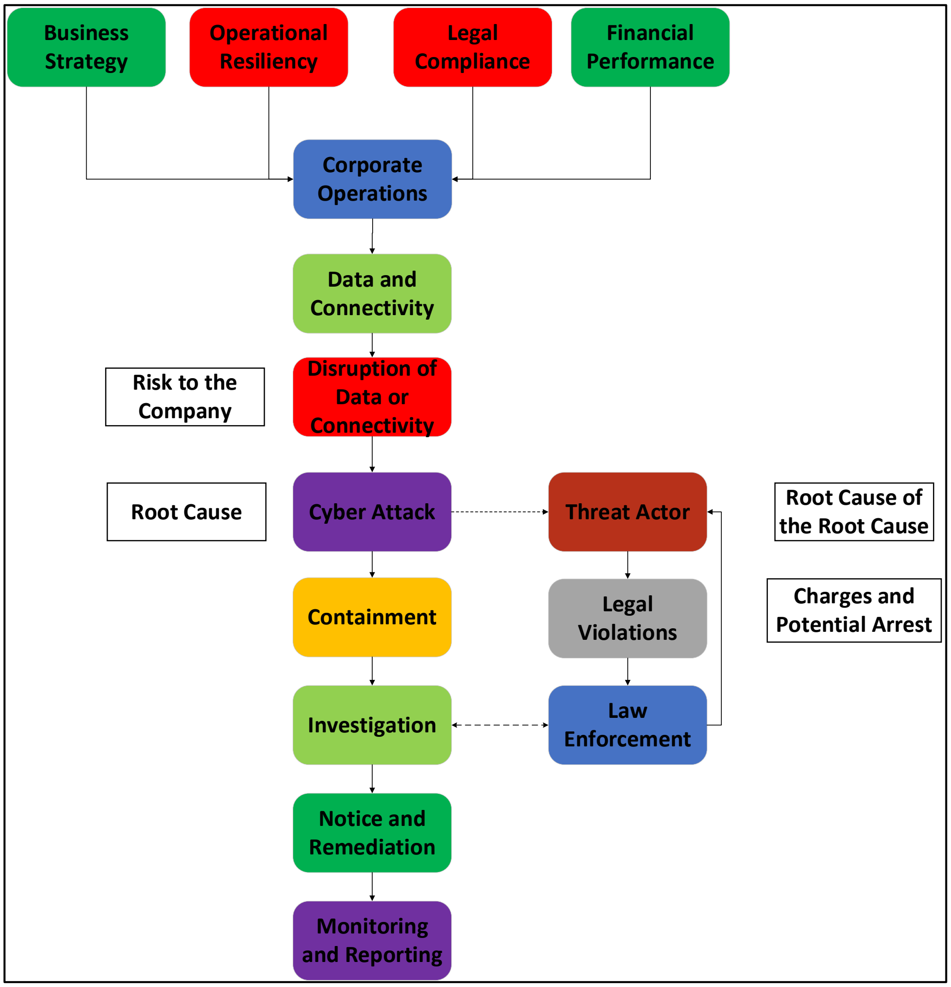


In short, risk governance focuses on risk, but corporate governance focuses on both risk and value, and given the importance of data in the Hybrid World, any governance of data inherently has to account for both sides of the equation.

Cybersecurity and the Hybrid World

Having just examined privacy and data and shown that how we look at "privacy" isn't perhaps the best way, I will not make the same arguments regarding cyber, because how we think of cyber isn't the issue--it is perceived as a resiliency issue. The issue instead is related to how we believe we "solve" cybersecurity, because while we recognize the problem is resiliency, we don't try to solve it through resiliency, at least from a public sector perspective. In short, we are focused on agencies and activities that address what happens to the "root cause of the root cause", and not on the risk to the company, which is a loss of connectivity and data, and resiliency, which is a core corporate governance principle. The graphic below illustrates how corporate governance principles feed into a company's operations, then that data and connectivity are core to those operations (which is true for almost every company), then that as previously discussed, risk to the company is the disruption of data or connectivity, not "cyber" which is a root cause of the risk.

The graphic then adds the process of responding to a cyber attack—specifically containment, investigation, notice and remediation, and monitoring and reporting. It also illustrates the issue with a law enforcement-centric response—as discussed below, law enforcement has as its primary purpose to charge, arrest, and prosecute people, which in the case of cyber goes to what happens to the "root cause of the root cause." While not an unimportant consideration, for most companies it is not the primary consideration—resiliency is. It is also important to note that there can be fusion between law enforcement and an attacked company around the investigation—information sharing—but information sharing during an event isn't the primary purpose of law enforcement.



In short, the consequences to the "Root Cause of the Root Cause" don't in the end make companies more resilient, and in most cases they do not help a company disrupt an event while it is happening. While I know the response at some level will be that by disrupting threat actors we reduce the threat, I think the last 10 years have shown there is always a new threat actor waiting to take over.

In the United States, and at some level globally, the non-regulatory government entities that are part of the cyber ecosystem fall into a few broad categories. Generally there are risk mitigation entities, intelligence gathering entities, and law enforcement. Military groups, particularly from certain nation-states also operate in the cyber domain, but in many cases (at least in the US and Europe), there is not a direct fusion between the private sector and military units.

A good example in the US of a risk mitigation entity is the Cybersecurity & Infrastructure Security Agency, or CISA, which is part of DHS. CISA's stated mission is that it, "…works with partners to defend against today's threats and collaborates to build a more secure and resilient infrastructure for the future." https://www.cisa.gov/about-cisa The U.K., among other countries, have similar entities performing these types of activities—which are primarily risk mitigation activities, such as NCSC.

There are also a variety of entities that gather intelligence, including around cyber. If one looks at the US, it is helpful to define what the Intelligence Community (IC) is, and what it does. According to the Office of the Director of National Intelligence, "The IC is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States." https://www.dni.gov/index.php/about/faq?start=2

There are a variety of entities that are part of the IC—some of which have gathering intelligence as their primary mission, while others have intelligence activities as a secondary mission.

There are also law enforcement agencies involved in cyber. Most front-and-center are the Department of Justice and the Federal Bureau of Investigation. DOJ's stated mission is, "To enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans." https://www.justice.gov/about

The FBI's stated mission leans into cybersecurity and being ahead of the threat, but ultimately the FBI's role and jurisdiction is not unlimited, and it does not have the resources to address every issue. When it determined its priorities, it asked three questions:

- What are those realities that most threaten the security of the United States?
- What are the threats to our way of life that the American people need the FBI to address first?
- To what degree do the threats fall most exclusively within the FBI's jurisdiction and competencies? https://www.fbi.gov/about/mission/fbi-strategy

The FBI is the premier law enforcement agency in the world. It is also an important part of the IC in the United States, and has a presence in other countries to help protect Americans, but the FBI does not have jurisdiction in those other countries. And while the FBI certainly does more in cyber than just indict people, it's primary mission is a law enforcement role, which is inherently focused on indictments and arrests, and it is, in essence, an entity focused on issues under Title 18 of the United States Code, a code entitled "Crimes and Criminal Procedure." Other entities, including some in the IC, operate under Title 50, which is entitled "War and National Defense."

Going back to the four primary things that can be done on any line of communication, as well as prior thoughts on mission statements and primary purpose of entities, the issue becomes clear.

While some malicious activities are crimes, others are clearly related to war and national defense. And you would no more send a solider to arrest someone in the US than you would send a police officer to fight a foreign war. They are different jobs, with different tools, and different outcomes. The same is true of a risk manager as well.

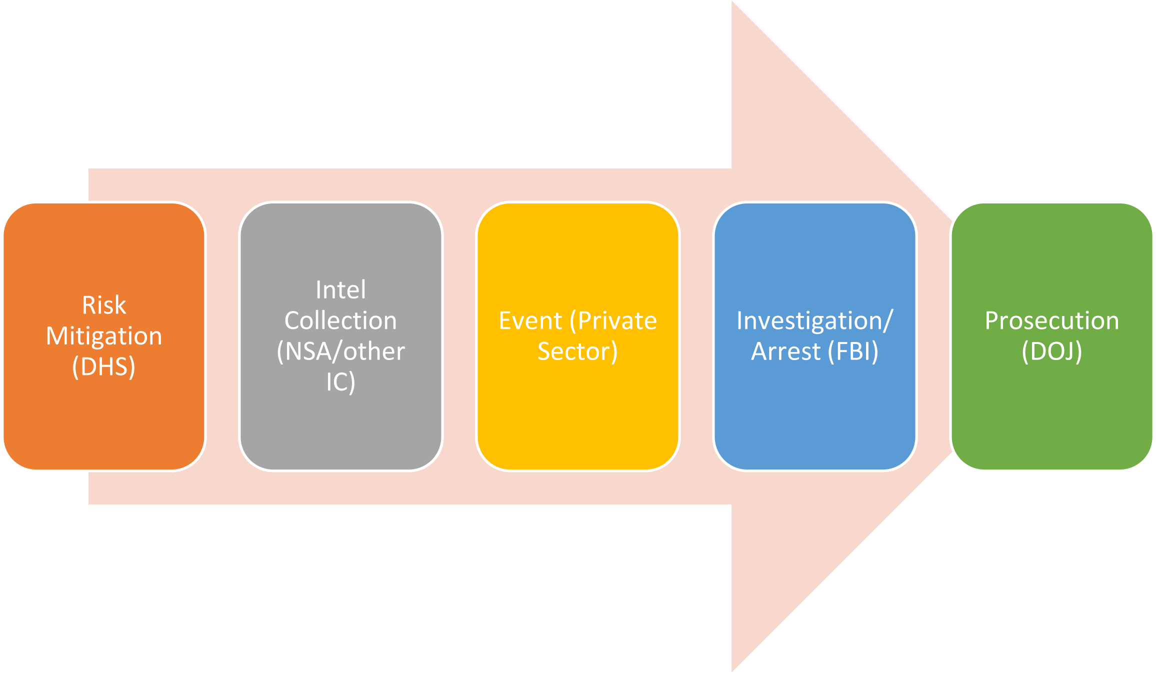
This is the challenge with cybersecurity in the US today—in the borderless hybrid world we have a multitude of entities all doing cybersecurity in different (and somewhat coordinated ways), but due to limitations on Title 50 entities operating in the United States, some entities that are more focused on national defense, with the ability to operate internationally, are limited in their ability to protect the United States, and the DOJ and FBI are similarly limited in their ability to operate in foreign countries, for obvious reasons.

The mission of the FBI and DOJ also makes information sharing harder at times, though both agencies do make strong efforts to share intelligence with other agencies, as well as the private sector. But again, the agencies' primary mission is building a criminal case against defendants, which inherently means they must protect their information. This is not exclusive to law enforcement—the IC also has similar legitimate concerns about protecting information, as well as sources and methods that can at times restrict information sharing.

The misunderstanding of the true issues with cybersecurity, as well as the role of information sharing, is not limited to the public sector.

To pick up on the point made above, from a policy perspective, we need to start re-imagining cyber and the government's response. This means that we need to start rethinking how private/private information sharing works, as well as how closely the public and private sector work to solve the cyber problems.

It also means we need to think through "who is who and what do they do." If we look at the chart below, it illustrates the point.



All of the entities listed above do a great job achieving their primary mission, but it is notable that the one entry that doesn't truly have a government agency associated with it is the event itself, and this illustrates the gap that is exploited by threat actors. There isn't a public sector entity in the US whose primary mission is disruption of cyber events, or direct support to a private sector entity when an event happens. While risk mitigators help try and mitigate risks before they happen, the intelligence community gathers intelligence, and law enforcement and prosecutors build cases, arrest perpetrators, and then prosecute them, there isn't an entity in the United States that is specifically tasked with this form of private sector support, and more specifically with disruption of cyber events. I am not suggesting that the entities listed in the chart, as well as entities that are not listed, do not provide some level of support during cyber events, but as shown above, disruption and private sector support during an event is not their primary mission. Given the true nature of the threats on our current line of communication, it is perhaps time this was rethought.

This is not to say that there are not agencies that address these concerns, https://www.thedrive.com/the-war-zone/43776/cyber-command-task-force-conducted-its-first-offensive-operation-as-defense-secretary-watched, but the reality is that those agencies in most cases don't have a private sector interface that most companies can engage with in the time of crisis. It is perhaps time to rethink that structure in some way, which we will do in future posts.

Links:

[Defining Governance]

[Corporate Governance]

[Applying Corporate Governance]

[The Hybrid World]

[Boards and Risk]

[The Problem with Privacy]

[Mission Statements, Strategy, Values and Ethics--How They Relate to Governance, Data and Connectivity]

[Data Sustainability]

[Defining Value and Risk in Corporate Governance, and the Limits on Privacy]

[Value and Data]

[Cybersecurity and the Hybrid World]