WHITE PAPER

CORPORATE GOVERNANCE

Systemic Digital Risk: Understanding And Overseeing Complex Digital Environments With The DiRECTOR™ And RISCX™ Frameworks

Bob Zukis
CEO, DDN
Adjunct Professor, USC Marshall School of Business[1]

The DiRECTOR™ and RISCX™ frameworks support the ability of corporate directors to identify systemic risk issues across complex digital environments to identify threats within the overall business system. This paper introduces an integrated framework to enable a greater understanding of the systemic risk issues in digitally enabled and driven business systems.

INTRODUCTION: Digital Success Starts At The Top

Boardroom ability to effectively govern digital and cybersecurity risk is evolving slowly — digital disruption and cybersecurity threats are not.

This has created an urgent need for a new paradigm that provides corporate directors with the ability to understand systemic risk and govern it across the complex digital systems that their companies depend upon. This paper introduces an integrated framework based upon the critical domains responsible for enabling and regulating the functioning of a complex digital business system along with the elements that are causing systemic risk.

Systemic risk is the threat that component failure in a complex system will cascade and jeopardize the much larger system. Systemic risk is inherent in almost all modern digital business environments and becoming more prevalent as digital disruption and transformation advance throughout business and society.

The World Economic Forum estimates that 60% of global GDP will be digitized by 2022. The final frontier in enabling and protecting the digital future will be navigated by the corporate boardroom.

Like the systemic financial sector contagion that took down Lehman Brothers and others during the financial market meltdowns of 2008, systemic risk in digital and cybersecurity risk oversight is a new, yet critical perspective in risk management. It's an issue that requires a much greater degree of understanding and leadership from business executives to reach the promise of the digital future.

Given the rapid advancements in technology and the far-reaching impacts of digital transformation, corporate director and leadership effectiveness in understanding and overseeing these issues has become much more difficult, yet significantly more vital.

For many corporate boards around the world, the practice of digital and cybersecurity governance is fairly immature or even non-existent. However, every corporate board and its directors have a responsibility to understand and oversee these issues.

[1] Special thanks to DDN Executive Founding Members Andrew Chrostowski, Tom Bennett and Jerry Nowicki for their input and assistance with this paper.

These issues materially impact business value in both the short and long-term. The ability of the organization to create, capture and preserve value in a rapidly changing digital world makes them priority corporate boardroom issues.

About This Paper

Business value, the key digital domains that drive it and the elements that cause systemic risk comprise the foundation of the overall integrated framework introduced in this paper.

Business value relates to shareholder value, and/or stakeholder value and the many components that go into producing it. Value is the ultimate duty of the corporate board and its directors. Ensuring that the organization creates it and preserves it is the universal corporate director mandate as the proxy for all corporate stakeholders.

The DiRECTOR™ framework identifies eight digital domains that work together across complex digital systems to produce and preserve value. These domains individually and collectively drive or degrade the ability of the digital system to drive, produce and protect business value.

Systemic risk in complex digital environments is primarily caused by five key elements that impact these domains. These elements are addressed within the RISCX™ framework introduced by this paper.

The application of the overall model can reveal significant gaps in understanding component and systemic risk throughout the digital business system. The model is intended to be applied at any level within an organization including project, objective, functional or enterprise.

The model is designed to be applicable to any organization or industry to enable a deeper understanding of how systemic digital risk exists and threatens the ability to support and deliver business value.

The integrated framework is illustrated with this diagram:

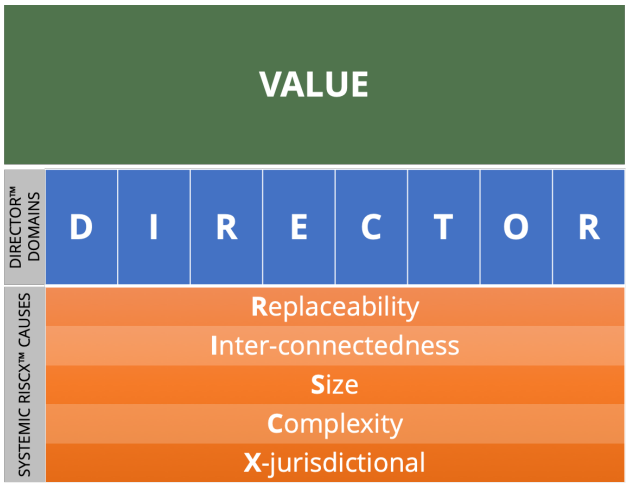

Figure 1 – The integration of business value, eight key digital domains and core systemic risk causes.
© DDN LLC

Frameworks are structured ways to understand a problem or issue. They are not prescriptive solutions for resolving the concerns that they may uncover.

Only once risk is understood, can it then be managed and mitigated. These models are designed to offer a way to reframe how executives and corporate directors comprehend complex systemic risks in digital business ecosystems. They are also intended to be a blueprint or "Rosetta Stone" for how technology executives communicate the complex issues they manage to the boardroom in a way that resonates with a corporate director's responsibilities and mindset.

Our approach reflects a desire to effectively approach both the upside and the downside of digital transformation. The downside is becoming readily identifiable as cybersecurity risks. The upside is somewhat less discernible but no less critical to the role of the corporate director. The upside focuses on competitive or opportunity risk.

That is, how organizations use digital tools to create and capture value over time. Two sides of the same coin, the framework addresses both, as it must.

Assumptions

This paper has been written to introduce these concepts to business leadership and the corporate boardroom community. It is not an implementation guide.

The paper is relevant to the corporate director or executive who does not have a deep understanding of technology issues. It is also for the growing group of board qualified technology experts (QTE's) who are working with their boards or becoming corporate directors themselves. It is our goal to help these business leaders understand, communicate and mitigate systemic risk in the complex environments that they govern and manage.

We wanted these concepts and models to be quickly consumable. So, this text is as brief as it needs to be. Good frameworks are simple, but not simplistic.

By reframing the risk management approach surrounding digital disruption through a systemic risk approach we can take a large step forward in addressing the digital leadership crisis facing companies around the world. Enabling corporate directors and their organizations to fulfill the promise of the digital future is our key learning objective with this work.

What The Models Look Like And How They Work

Corporate governance is an evolving practice globally. Its origins go back hundreds of years as the corporate form evolved as a means to pool and deploy capital around the world.

The role of the corporate board and its directors has been shaped over time by the laws, economics, politics, social practices, technologies and the history of the realms that have given rise to the corporate form. This makes every corporation and every corporate board a product of its unique circumstances.

Boards need to be comprised of corporate directors who have the skills and capabilities to effectively oversee the companies and the environments that they operate within today and in the future. Corporate directors must exercise insight and judgment that influences business outcomes in both the short and long-term.

Many forces are converging anew that are disrupting the corporation, the corporate board, and its directors. Local and global instability in the political, economic, social, technological, environmental, and legal environments are remaking corporations and challenging corporate leadership in new ways.

The common denominator across all of these challenges is the influence of digital disruption. For corporate governance and boardroom directors this presents an unprecedented challenge, and an extraordinary opportunity.

Navigating this future starts with understanding value, how it is changing, created, captured and preserved and how the digital system serves that purpose. This is the starting point of the integrated framework.

Value

Value encompasses all the component aspects of how companies create, capture and protect value. It includes the common corporate objectives of producing and growing revenue, profitability, and competing in competitive markets. Risk management and corporate governance serve these core purposes.

Different countries, legal jurisdictions and regulatory bodies impose different rules and

requirements that drive a range of corporate governance practices and approaches globally. These differences and subtleties are not our focus. Our focus is on the universal need for all corporate boards to improve digital and cybersecurity risk oversight to drive and preserve business value.

As such, the model serves the fundamental corporate director responsibility as steward of the long-term health and well-being of the firm.

Many factors contribute to the concept of business value, some tangible and measurable, some not. What's valued, and what creates value is also dynamic. A company's unique value proposition is its own and delivering on it is the unique challenge that all business leaders face.

While shareholders are principally concerned with stock price, revenue growth and profitability, other corporate stakeholders can define value differently. While corporate directors will usually see their responsibilities through the lens of shareholder value, that's not always their singular mandate. In the United States, Delaware law emphasizes shareholder primacy as the key responsibility of the corporate director. But in Europe, a broader stakeholder view is more common. This view is also beginning to emerge in the U.S.

A corporation has many stakeholders from shareholders, employees, customers, suppliers to the communities that they operate within. Price and convenience may define value for customers while wages, working conditions, and job security may be the primary value drivers for employees.

Every company is a collection of value components that collectively drive an overall value proposition. That value proposition is a unique system in its own right; one that is directly enabled and/or created by the digital system.

Each of these individual value drivers can be dependent upon the complex digital system in addition to contributing to the greater whole. Digital systems are not only core value enablers but are increasingly becoming a core producer of the value proposition.

This hasn't always been the case.

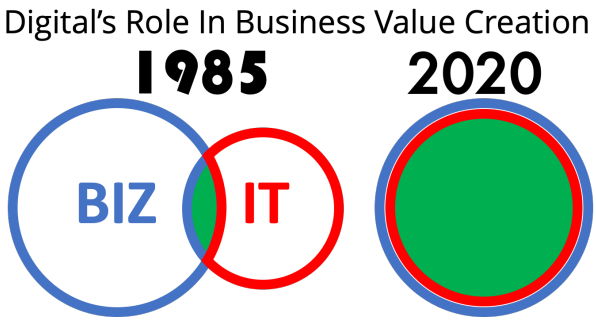

Figure 2 – Digital's role in business value creation.
© DDN LLC

While there is a renewed debate about the purpose of the corporation and who it serves in the U.S., most of America's boardrooms remain legally bound to the purpose of shareholder primacy. Whether that objective gets achieved with a different approach encompassing all corporate stakeholders remains a work in progress.

Regardless of who the corporation serves, the result of an organization's effort to create value manifests itself most commonly in the value created for its shareholders. Measured by share price, revenue and profitability these are the most commonly recognized value measures that digital systems serve. Most corporate directors will relate to issues in this context whether legally required to do so, or intuitively

To serve all stakeholder interests, the core economic motivations of free-market businesses must first fulfill the ambitions of the company's owners. Expanding the economic pie to enable larger slices for all and equitably distributing those pieces is also a boardroom issue. While America's boardrooms remain tethered to first creating shareholder value, the models in this paper also embrace all stakeholders.

Business value is the measure of total value output that the digital system both serves and

creates for all of its stakeholders. Our model begins with the core language of business value as the reference and anchor points for this primary service obligation of the complex digital system.

This approach makes the model universally relevant to all for-profit enterprises. It also focuses directors to help them understand how the complex digital system serves the ability of the organization to create, capture and preserve value over time across its entire ecosystem.

KEY POINTS:

- A director's role serves shareholder and stakeholder value and understanding how the digital system supports and drives it.
- Value can come from many different component elements that make up a business system. Value can change and it is increasingly enabled and delivered through the digital system.
- The common language of the boardroom is built upon value creation and preservation.

The DiRECTOR™ Framework And It's Eight Domains

The DiRECTOR™ framework covers eight key domains that enable complex digital systems. From a corporate director's vantage point these domains represent the key risk areas within the digital system. These domains are co-dependent and regulate the functioning and health of the digital system and how it supports business value.

Many digital issues and initiatives span several, if not most of these eight core domains. Corporate oversight needs to view and comprehend risk within each domain, while simultaneously understanding the systemic dependencies and contagion risks throughout the entire system.

The eight-core domains that comprise complex digital systems include:

Data — Digital oversight starts with data and how digital systems and business environments convert data into knowledge, insight, and action. Data can directly drive a value proposition, is vital to operating a business and is actively targeted by hackers for its intrinsic value.

iArchitecture — Information architecture is the technology design and backbone of the digital system and how it interacts with the business system. Digital systems embody the software, network, people, business processes and hardware components that enable any business system.

The DiRECTOR™ ontology and it's eight domains can be illustrated with this diagram.

Figure 3 – The eight domains in the DiRECTOR™ ontology. © DDN LLC

Risk Communications — Crisis communication gets the headlines. But leadership communication around the digital and business systems spans strategic and tactical communications that need to reach every stakeholder internally and externally. These communications play a key inter-dependent role with all of the DiRECTOR™ domains.

Emerging Technology — New digital tools are constantly emerging that can enable, threaten or redefine existing value drivers. These tools also layer on new complexities across the existing system. They can also exploit or alter fundamental economic concepts and principles in new ways making them an essential concern in digital risk oversight.

Cybersecurity — Where there's business value, there's risk. Hackers find and hack the weakest digital link. The non-stop threat to every digital system and the business supported by it, creates significant value protection and preservation challenges from people to technology; both from internal threats and external. Cybersecurity is not an afterthought. It's an integrated component of every digital environment from start to finish.

Third-Party — Business ecosystems have never been more connected. Systemic risk compounds across an extended business network that is constantly connected and in motion. Every third-party interacting with a digital system creates inter-dependencies and compound contagion risks across all systems.

Operation of IT — The pace of change in digital and IT is constant. The ability of an organization and its digital operations to effectively adapt to this type of dynamic environment plays a critical role in the sustainability and resiliency of the entire system.

Regulation — Digital regulation is accelerating and expanding. Fines, penalties and rules imposed by regulators directly influence business and shape corporate governance practice and policy. Every organization also has the opportunity to engage in public-private dialog on digital legislation. Compliance is a boardroom staple and understanding how this emerging regulatory world impacts digital risk and engaging in shaping responsible digital policy requires boardroom involvement.

Issues, risk or failure in any one of these domains can destabilize and put the entire digital system at risk. Complex systems science is focused on understanding the relationships and interactions between elements.

For example, new digital technologies, e.g., IoT, that support revenue growth or a profitability objective can introduce a new cybersecurity risk profile into a company. Those risks can jeopardize that specific business objective and others across a business system.

Those new technologies may also create new data types and sources that fall under a specific regulatory or policy directive such as supporting a service level agreement (SLA). The new digital technology may also be provided and supported by a third-party service provider which introduces a new information architecture element that creates a critical third-party risk.

That new technology may also require interfaces into other systems creating vulnerabilities and compounding complexity and risk across the entire digital environment.

The implementation and operation of this new technology may also impact a large number of users or customers across the enterprise and require a long and complicated design, build and launch process.

All of these component considerations have dependencies that contribute to creating another layer of complexity across a digital system already embedded with systemic risk.

Component risk and failure of any one element of this complex system could endanger the entire system. Introducing a systemic risk model is imperative to understanding how, and why, and to managing these risks to business value.

KEY POINTS:

- Systemic digital risk is the threat that a component failure or weakness will jeopardize the larger digital and business system through contagion effects.
- Digital risk oversight spans eight complex domains that are individually material and inextricably linked.
- Every company has a digital footprint specific to its organization and the value proposition that it is delivering.

RISCX™ And The Causes Of Systemic Risk

Existing risk management approaches fall short in their ability to accommodate complex systems and the inherent levels of systemic risk in today's digital systems. This requires a new paradigm in how to design, manage and control these new frontiers of digital complexity in business.

Systemic risk models are emerging in other domains globally to comprehend our complex world, e.g., planetary health, financial services, healthcare, etc.

> **"The whole is greater than the sum of its parts." -Aristotle**

Adapting and applying these emerging bodies of work from these other fields to the practice of complex digital systems oversight gives us a leveraged starting point.

Scientists have identified nine core elements that work together to contribute to the health of the earth system that enables a stable planetary environment ideal for human life. Climate change, ozone depletion, ocean acidification, and freshwater use are five of the nine critical processes that combine to effectively regulate the entire earth system.

Scientists created this systemic model to identify the critical causes or processes critical to planetary health. From here, they can understand where the risk lies within each element to comprehend the threats to the complex system critical to supporting life on this planet. Having this model and perspective can then lead to more targeted steps to begin to relieve the issues contributing to risk within and across the entire system.

Systemic risk and its contagion effects were also exposed during the financial crisis of 2007-2008 across the financial services sector. BASEL III is the third part of the BASEL international regulatory accords focused on banking sector risk, transparency, and resiliency. BASEL III has started to identify the contagion risks and their causes that were experienced during the financial crisis to understand what happened and to prevent them from happening again.

This body of work has provided insight into our approach to understanding systemic digital risk. Several concepts have been adapted into the DiRECTOR™ and RISCX™ frameworks.

Systemic risk can create a domino effect where one component failure cascades across a much larger system, putting the entire system at risk.

Automobiles are complex systems comprised of multiple intricate and inter-dependent domains. A combustion automobile is comprised of fuel systems, electrical systems, suspension, air conditioning, lubrication and exhaust systems that all work together to move a 4,000-pound mass of plastic and steel; while safely protecting the passengers inside. A flat tire on a car jeopardizes the entire system of the automobile that can render the larger system useless.

A simple fix to this catastrophic systemic risk is a spare tire. An innovation such as run-flat tires enables the system to continue to operate at a reduced functional level despite a component failure. Both are risk management tactics but very different approaches to the issue, with different results.

Replaceability of a key component in a systemic risk environment is one critical cause of systemic risk failure in complex systems. The RISCX™ framework starts here.

While the DiRECTOR™ model identifies the eight-core domains from a corporate director's perspective that regulate the health and vitality of a digital system, the RISCX™ model identifies the five key causes of systemic risk within and across these domains.

Together they form an integrated framework for understanding systemic risk issues and levels in complex digital systems.

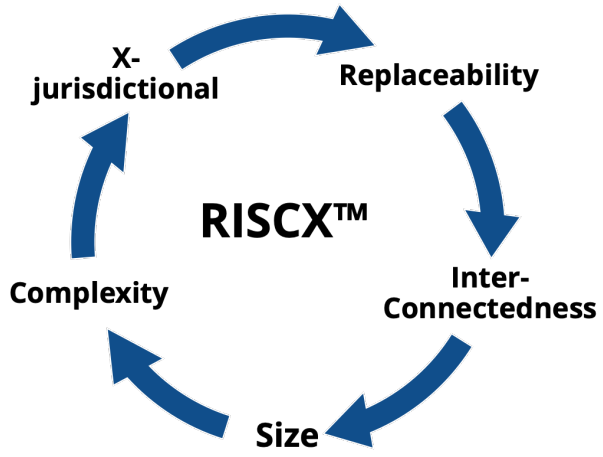

Figure 4 – RISCX™ and the key causes of digital systemic risk. © DDN LLC

Replaceability — How rare, irreplaceable and important is a component within the system? Critical, hard to replace components create significant risk and brittleness in a complex system. The more dependent the system is on the component and the harder it is to replace, the greater the level of risk to the larger system.

Interconnectedness — Businesses and the world have never been more interconnected. Digital environments can be highly connected both internally and externally. The more connection points across the system, the greater the risk of contagion, both inbound and outbound and the greater the risk that the failure can spread and cascade.

Size — Size impacts total exposure across the system. The larger the data universe that is being enabled, the more risk there can be within that data and across the system. Size factors from multiple perspectives including end-users, third-parties, software systems, etc. Scale creates more points of vulnerability, adds to digital complexity and contributes to systemic risk.

Complexity — Complexity in any environment makes it more difficult to understand how the environment functions and how it can be controlled. Digital complexity develops from multiple areas including the number of component elements and heterogeneity within the system and operation. Complex digital environments and operations cause systemic risk to increase.

X-jurisdictional — Companies and networks that span the globe create vulnerabilities from anywhere that can travel rapidly to everywhere. The more regulatory environments a digital system is exposed to the more difficult it is to oversee and manage regulatory risk. Jurisdictions include regulatory bodies and other policy jurisdictions such as rules imposed by third parties.

KEY POINTS:

- Systemic risk in digital environments creates contagion effects that jeopardize the larger business system.
- Systemic risk is inherent in complex digital systems and is caused by five core elements inherent to the system.
- Once risk is understood it can be managed.

Applying The DIRECTOR™ And RISCX™ Models

Digital transformation and cybersecurity risk are transforming the world around us and will

continue to do so. Cybersecurity has been declared an "existential risk" by the World Economic Forum and Warren Buffett. Digital disruption and transformation and their impact on business and society put these issues at the top of the global boardroom agenda.

The lag in boardroom capability development around digital and cybersecurity risk understanding and oversight has created a leadership crisis for many companies around the world. Business leaders are struggling to evolve their company's ability to adapt to the business benefits of digital transformation while simultaneously mitigating the cybersecurity risks that come along with these very same opportunities. The rapid pace of development and adoption of new digital approaches and technologies will only continue to exacerbate this problem.

This challenge puts corporate directors in the middle of these issues. Directors around the world have a duty to oversee how the companies they govern use all of the tools at their disposal to drive and preserve value for their organization's stakeholders.

While there are different jurisdictions and laws that govern the purpose of the corporation and who it serves, there is a universal objective for every corporation to create and preserve value and to survive into perpetuity. Corporate directors are the stewards of these goals which makes them the guardians of our digital present and future.

New perspectives can often yield new insights. The integrated framework we've introduced in this paper creates a starting point for analyzing, understanding and communicating systemic digital risk.

Our objective is to develop the ability of business leaders to have a deeper understanding of the systemic digital risks underpinning their business. The framework is also intended for technology executives to convey the complexities of their management efforts in a way that corporate directors can relate to, bridging the communications gap on these issues.

Once risk is understood, steps can be taken to manage it. This increases the value of business outcomes. That's the fundamental role of the corporate director.

These models can be applied at a detail level to understand the specific issues underlying systemic digital risk. They can also be applied through a high-level walkthrough to yield value as it will force a corporate board or leadership team to think through their digital environment and business differently.

Figure 5 – The integrated DIRECTOR™ AND RISCX™ frameworks. © DDN LLC

Directors and leaders who view their oversight responsibilities through this framework will shine a light on the inherent complexity of their digital system and the dependency their business value proposition has on it.

Our work is expanding to develop a reference guide across many different digital scenarios that will help apply the model. We will also be creating

reporting templates to help summarize the information and insights that can be gathered during the implementation of the models.

Managing and overseeing complex digital systems is a multidimensional process and practice. Doing it effectively is critical to realizing the digital future.

Acceptable Use

Digital Directors Network (DDN) is committed to providing thought leadership through the development of frameworks, methodologies and knowledge to help corporate boards and directors effectively govern systemic digital and cybersecurity risk. All of the DDN materials, images, content and concepts are protected by copyright.

We are building an industry consortium of leading firms working together to advance the practice and profession of systemic digital risk oversight. We invite you to join and to work with the network to shape and secure the digital future. More information on our mission can be found at www.digitaldirectors.network.

Individuals, corporate boards and organizations have limited rights to apply these concepts within their organizations. Contact us to learn more.

A license is required for the incorporation of any of these concepts or principles into any software sold or given to third parties or used for internal use.

A license is required to apply these concepts and principles in consulting or advisory engagements by any third parties.

We consider unauthorized uses to include publicly displaying any of the concepts or images either online or otherwise; copying; distributing; teaching with them or applying them in any educational context online or off; creating derivative works or inserting them into, processing with, or displaying them through any commercial or non-commercial product, including software.

These uses will constitute copyright infringement and a violation of DDN's intellectual property rights.

Contact us at info@digitaldirectors.network to join DDN, for information on licensing the frameworks and for help in applying them.