Transform.

Compete.
Council on Competitiveness

Resilience in the Age of COVID-19—An Update to the 2007 Report

Resilience in the Age of COVID-19—
An Update to the 2007 Report

THE COUNCIL is a nonprofit, 501 (c) (3) organization as recognized by the U.S. Internal Revenue Service. The Council's activities are funded by contributions from its members, foundations, and project contributions. To learn more about the Council on Competitiveness, visit Compete.org.

Printed in the United States of America.

Transform.

Compete.
Council on Competitiveness

Resilience in the Age of COVID-19—An Update to the 2007 Report

Table of Contents

Letter from the Board

We are pleased to share with policymakers and the public an important update to one of the Council on Competitiveness' (Council) seminal reports, *Transform*, which was first released in 2007. The result of a multi-year assessment of the synergy between competitiveness and security, *Transform* made the case for resilience in the face of a myriad of potential threats to businesses, government and U.S. critical infrastructure. While the nomenclature of resilience has since become commonplace, the decimating impact of the COVID-19 virus on the U.S. economy and the lack of preparedness by the public and private sectors is evidence that the warnings and recommendations in *Transform* remain relevant 13 years later. In short, the United States knew this was coming, and the country was not ready.

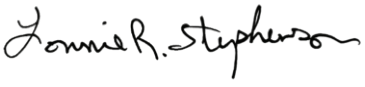
The Council is updating *Transform* in the hope that the country can refocus on resiliency, so that the standard against which future crises are measured is not how long the economy has to be shut down, but whether a shut down is necessary. Done right, resilience can help shape U.S. destiny and allow government to focus on a response to any crisis, not be controlled by it. There is no reason that the conventional wisdom of needing 12-18 months to recover from the COVID-19 pandemic needs to be standard operating procedure in the future.

Importantly, the response to the pandemic has highlighted many potential pathways to greater resilience in the future, including the ability to supplant or complement supply chains through 3D printing, the rapid re-skilling and deployment of workers, and the utilization of disruptive technologies from AI to automation to biotechnology to minimize the economic impact of the crisis and shorten the time frame to normalcy.

Dr. Mehmood Khan
Chief Executive Officer, Life Biosciences, Inc., and
Chairman, Council on Competitiveness

Dr. Michael M. Crow
President, Arizona State University, and
University Vice-chair, Council on Competitiveness

Mr. Brian T. Moynihan
Chairman and Chief Executive Officer, Bank of America, and
Industry Vice-chair, Council on Competitiveness

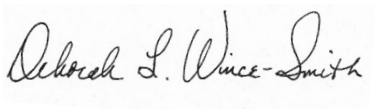


Mr. Lonnie Stephenson
International President, IBEW, and
Labor Vice-chair, Council on Competitiveness

What was true 13 years ago remains just as true today—resilience is a cornerstone of economic competitiveness and new value creation. There is unquestionably a business case for security and that, done right, security can be a productivity-driver, not a sunk cost. This realization is increasingly important in a global economy increasingly characterized by uncertainty, complexity, connectivity and speed. The Council described this risk landscape as an emerging competitiveness challenge in 2007. Today, it is reality and to prosper nations, businesses and organizations must have the capability to survive, adapt, evolve and grow in the face of change.

The Council is proud to offer this update, which reiterates a strategy of resilience for both the public and private sectors.

Mr. Samuel R. Allen
Chairman and Chief Executive Officer, Deere & Company,
and Chairman Emeritus, Council on Competitiveness



The Honorable Deborah L. Wince Smith
President
Council on Competitiveness

Executive Summary—This Should All Sound Familiar

In 2007, the Council on Competitiveness (Council) released *Transform,* making the case that resilience could be a competitive advantage enabling businesses, higher education and the public sector to recover from crises more quickly. There was a recognition that globalization, technological complexity, interdependence, terrorism, climate and energy volatility, and pandemic potential were increasing the level of risk that societies and organizations faced. And that risks were increasingly interrelated. Therefore, the ability to manage emerging risks, anticipate the interactions between different types of risk, and bounce back from disruption would be a competitive differentiator for companies and countries alike in the 21st century. That was the conclusion 13 years ago.

With more than 188,500 Americans dead,[1] at least 13.6 million Americans unemployed,[2] GDP growth at -31.7 percent,[3] colleges and universities struggling to reopen, and no congressional infrastructure in place to enable remote legislating—it is fair to ask: did anyone listen? The COVID-19 pandemic that has shaken the global economy may have been unexpected, but it was not unanticipated. Yet, policymakers and other stakeholders are treating the pandemic like a once-in-a-lifetime occurrence that could not have been planned for and that will require 12-18 months at least from which to recover. That is not resilience. That is capitulation.

To drive home the point that a focus on resilience should have been standard operating procedure for the public and private sectors by now, the following insights and recommendations from the original *Transform* report are included below. That they remain relevant is both a testament to the foresight of the Council and its members and to the lack of urgency and implementation by critical stakeholders.

What Policymakers Should Know

The national objective is not just homeland protection, but economic resilience—the ability to mitigate and recover quickly from disruption.

There are an infinite number of disruption scenarios, but only a finite number of outcomes. Leading organizations do not manage specific scenarios, rather they create the agility and flexibility to cope with turbulent situations.

Government regulations tend to stovepipe different types of risk, which impedes companies' abilities to manage risk in an integrated way. Policies to strengthen risk management capabilities would serve both security and competitiveness goals.

What Business Should Know

Businesses must root the case for investment in resilience strategies to manage a spectrum of risks, not just catastrophic ones.

1 https://covid.cdc.gov/covid-data-tracker/#cases.

2 https://www.bls.gov/news.release/empsit.nr0.htm.

3 https://www.bea.gov/news/2020/gross-domestic-product-2nd-quarter-2020-second-estimate-corporate-profits-2nd-quarter.

Making a business case for investment in defenses against low-probability events (even those with high impact) is difficult. However, making a business case for investments that assure business continuity and shareholder value is not a heavy lift.

The investments and contingency plans these leading companies make to manage a spectrum of risk create a capability to respond to high-impact disasters as well.

Operational risks are growing rapidly and outpacing many companies' abilities to manage them.

Corporate leadership has historically viewed operational risk management as a back office control function. But managing operational risks increasingly affects real-time financial performance.

Lack of collaboration between risk specialties, and lack of consistent and "leading" metrics to anticipate emerging or interacting risks, are important gaps in the risk management process.

What Policymakers Should Do

Lead by Incentive
- Include resilience criteria in procurement and research and development processes

Reinforce Market Mechanisms
- Explore expanded U.S. Securities and Exchange Commission (SEC) disclosure requirements on non-financial material risks

Reduce Risk and Cost for Resilience Solutions
- Leverage computational capabilities of universities and national laboratories to strengthen modeling and simulation of operational risks
- Catalyze regional networks for crisis management and information exchange
- Expand technology test beds to demonstrate the cost effectiveness of resilience solutions

What Business Should Do

Walk the Talk at the Top
- Inspire cultural transformation

Link Operational Risk to Revenues
- Organize risk management processes as a continuum

Take a Systems Approach
- Identify critical vulnerabilities across business assets and operations

Manage with Metrics
- Benchmark risk management performance on the operational side

Harness New Technologies
- Apply technology solutions, that create early warning and tracking capabilities, as well as coordination across the organization

Create Adaptive Capacity
- Develop capabilities to mitigate a variety of outcomes from disruptions

What Universities Should Do

Learning to Change
- Create cutting-edge, cross-disciplinary resilience curricula and research centers

Invest in Training and Education to Change the Culture:
- Create a Resilience Curriculum Fund to embed resilience in undergraduate and professional education
- Stimulate cross-disciplinary research centers on resilience

The Competitiveness and Security Conundrum: IT'S ALL ABOUT RESILIENCE

Key Findings

After the shock of 9/11, the Council on Competitiveness introduced the concept that America's security is also a national competitiveness challenge.
Our economy—the engine of jobs and prosperity—could be brought to its knees by a well-placed terrorist attack. And, for the first time in our nation's history, its economic assets and infrastructure were on the front lines of a battlefield: key targets and even pathways for attack. By the same token, however, the economy could suffer an equally damaging blow from excessive security measures that stifled productivity and slowed commerce.

What we learned is that the challenge is not security, it is resilience.

What Policymakers Should Know

It's a Whole New Ball Game for Risk (Irrespective of Terrorism)

Globalization, technological complexity, interdependence, and speed are fundamentally changing the kind of risks and competitive challenges that companies—and countries—face. Failure, whether by attack or accident, can spread quickly and cascade across networks, borders and societies. Increasingly, disruptions can come from unforeseen directions with unanticipated effects. Global information and transportation networks create interdependencies that magnify the impact of individual incidents. These new types of risk demand new methods of risk management.

What is Resilience?

Definition adopted from Center for Resilience, The Ohio State University.

Resilience is the capacity for complex systems to survive, adapt, evolve and grow in the face of turbulent change. The Resilient Enterprise is risk intelligent, flexible and agile.

Resilience Trumps Protection

Homeland security is often seen as a protective, even defensive, posture. But Maginot lines are inherently flawed. Fences and firewalls can always be breached. Rather, the national focus should be on risk management and resilience, not security and protection. Resilience—the capability to anticipate risk, limit impact and bounce back rapidly—is the ultimate objective of both economic security and corporate competitiveness.

The Business Case Begins with Business Risks

The business case for investment in resilience has to be rooted in meeting a spectrum of business risks. It cannot be based solely on the possibility of disaster. In fact, most of the investments that lead-

ing organizations are making—investments that can run in the hundreds of millions of dollars—are aimed at managing the risks they face on a day-to-day basis. For example, the supply chain flexibility that Wal-Mart pioneered—a capability that enabled the company to operate despite the devastation wrought by Hurricane Katrina—was not specifically created to cope with catastrophe. Rather, Wal-Mart's significant investments in RFID tags, software, and staging centers were intended to meet the day-to-day complexities of customer demand. But in the process, Wal-Mart's supply chain resilience also created extraordinary disaster management capabilities.

Regulatory Solutions Often Reinforce Risk Silos

For companies, there are an infinite number of disruption scenarios, but only a finite number of outcomes. In the end, it does not matter whether power failures, floods, strikes or terrorist attacks cause the down time. Causes count less than creating the agility and flexibility to mitigate risks and manage outcomes.

Government, however, tends to see different categories of risk—terrorism and natural disaster, climate change, worker safety, governance—as different problems requiring separate sets of regulatory solutions. In today's risk environment, that creates three potential problems:

- First, it often results in a "check the box" response that is at odds with the need to create value by managing risk on an enterprisewide basis.

Causes count less than creating the agility and flexibility to mitigate risks and manage outcomes.

- Second, because risks cascade across networks and private enterprises in complex ways, risk silos may actually increase risk exposure.
- Third, it sets up the potential for inconsistent and often overlapping sets of regulatory requirements, which raise cost and complexity without actually improving outcomes.

What CEOs and Boards Should Know

Enterprise Risk Management is a Competitive Advantage

Businesses make money by taking risks, but lose money by failing to manage them. A study by Deloitte Research indicated that many of the largest losses in value among the world's largest global companies were a result of a failure to manage risk effectively and systematically. The study found that most firms were exposed to more than one type of risk—whether strategic, operational, market or financial—and failed to manage the relationships among these different types of risk. Actions taken to address one type of risk had the potential to increase exposure to other types of risk.

1. Operational Risk Identified as Most Important Risk Facing Executives Today

Source: Tillinghast. "A Changing Risk Landscape." New York: Towers Perrin, November 2006.

The failure to manage risk on an enterprise basis takes a huge toll. The study found that almost half of the 1000 largest global companies suffered declines in share prices of more than 20 percent in a one-month period between 1994 and 2003, relative to the Morgan Stanley Capital International (MSCI) World Index. And the value losses were often long-standing. By the end of 2003, share prices for one-quarter of the companies had not recovered to their original levels.[1]

Managing Operational Risks is Key

The business equivalent to homeland security and critical infrastructure protection is operational risk management—a domain that many executives see as the most important emerging area of risk for their firms (see Chart 1, above).

Increasingly, failure to plan for operational resilience can have "bet the firm" results.

- Research on supply chain resilience demonstrated that the 835 companies that announced a supply chain disruption between 1989 and 2000 experienced 33 percent to 40 percent lower stock returns than their industry peers, regardless[2] of industry, cause of disruption or time period. Such firms experienced 7 percent lower sales growth and 11 percent higher costs. Changes in operating income, sales, total costs and inventories remained negative in the two years after the problems were disclosed.[3]

1 Deloitte Research. "Disarming the Value Killers." Deloitte, February 2006.

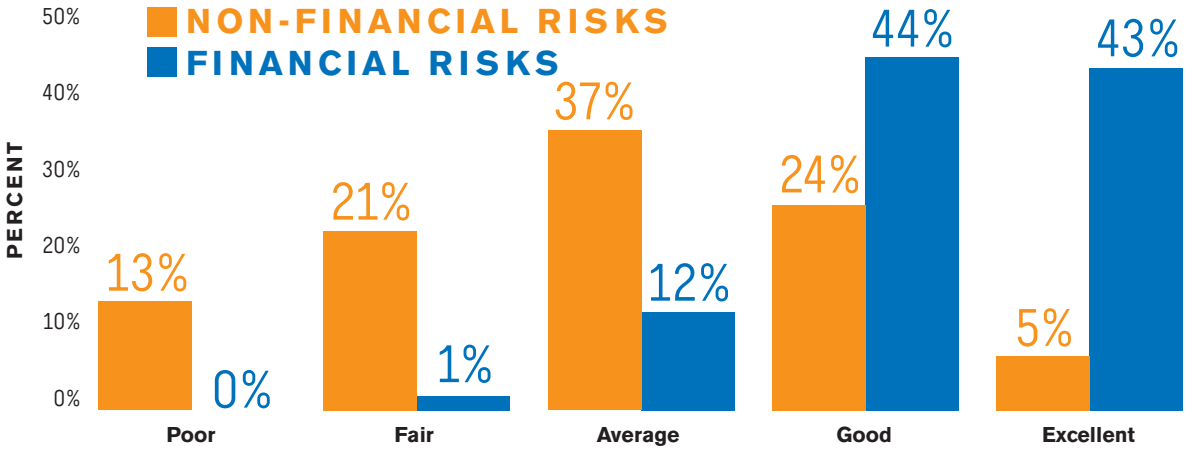
2 ibid.

3 K.B. Hendricks & V. R. Singhal. "An Empirical Analysis of the Effect of Supply-Chain Disruptions on Long-Run Stock Price Performance and Risk of the Firm." Productions and Operations Management. 14 (2005) 35-52. In FM Global, "The New Supply Chain Challenge: Risk Management in a Global Economy." (April, 2006).

2. Boards Are Less Confident in Non-financial Risk Management

Source: Deloitte. "In the Dark II." Deloitte, 2007.

How would you rate your organization's record of measuring and monitoring financial and non-financial aspects of performance?



- 25 percent of companies that experienced an IT outage of two to six days went bankrupt immediately. Ninety-three percent of companies that lost their data center for 10 days or more filed for bankruptcy within a year.[4]

Operational Risks Remain Stove piped and Under-measured

Different aspects of operational risk—physical and employee security, environmental health and safety, IT security, business continuity, disaster management, supply chain security, energy supply and quality—are frequently separated from one another within the organization, and sometimes de-linked from overall corporate risk management.

On the financial side, there are increasingly sophisticated systems that measure market and credit risk—often using sophisticated algorithms and supercomputers to model risk exposure. By contrast, although operational risks are arguably at least as complex, operational risk exposure tends to be measured by checklists, which are often based on experience and instinct. In fact, as Chart 2 (above) indicates, boards are not as comfortable with their non-financial as their financial risk management.

In 2020, almost all respondents considered their institution to be extremely or very effective in managing traditional financial risks. In contract, roughly half said the same about non-financial risks.[5]

4 Economist Intelligence Unit. "Business Resilience: Ensuring Continuity in a Volatile Environment." The Economist. 2007. Citing a U.S. National Archives study.

5 https://www2.deloitte.com/content/dam/insights/us/articles/4222_Global-risk-management-survey/DI_global-risk-management-survey.pdf.

Industry Continues to Face a Risk of Reactive Regulation

Given that six years have passed since 9/11, it is tempting to believe that the danger of a major attack on the United States has abated. Unfortunately, a successful and devastating attack on U.S. soil remains the gold standard for global terrorism. To date, efforts to regulate security have been incremental and sector-specific. But regulatory incrementalism could become a regulatory tsunami if a major attack occurs and industry has not taken the necessary steps to ensure its resilience.

Executive Priorities

Priorities for CEOs and Boards

Corporate executives need to transform current risk management practices with a vision and strategy to implement enterprisewide approaches, and build in the flexibility, agility and adaptability that are characteristic of resilient systems.

Walk the Talk at the Top Inspire cultural transformation by creating a vision for the enterprisewide resilience approach, connect the organizational silos, and engage the entire workforce in risk management.

Link Operational Risk to Revenues Organize risk management processes as a continuum—from prevention to profit—to enable consideration of financial trade-offs among different approaches.

Take a Systems Approach Identify critical vulnerabilities across business assets and operations, including competitive context, and analyze how disruptions might unfold.

Manage with Metrics Benchmark risk management performance on the operational side, identify leading rather than lagging indicators, and quantify the effectiveness of alternative risk management strategies.

Harness New Technologies Apply technology solutions that create early warning and tracking capabilities, as well as coordination across the organization.

Create Adaptive Capacity Develop capabilities to mitigate a variety of outcomes from disruptions, regardless of cause, rather than planning for specific scenarios.

Priorities for Universities

Universities should position themselves to drive new research, knowledge creation and educational curricula that will build the theoretical and practical groundwork for a resilient economy.

- Create cutting-edge, cross-disciplinary resilience curricula that prepare students for a turbulent, interdependent work environment.
- Develop interdisciplinary research centers that help government and industry respond to the challenges of building resilience.
- Galvanize local and regional efforts to enhance infrastructure resilience and preparedness along with economic development.

- Communicate the importance of aligning security and competitiveness to policy-makers, business leaders, and the public.

Priorities for Public Policymakers
Public policy should strive to reduce uncertainty and inconsistency, lead by incentive where possible, use market mechanisms more creatively and public-private partnerships more effectively, and support education and training programs that change cultures.

Lead By Incentive
- Leverage the government's buying clout to embed resilience criteria in the procurement selection processes and supply chains.
- Leverage the government's investments in technology to embed resilience criteria in the evaluation and selection process for emerging technologies.

Leverage Market Incentives More Creatively
- Expand guidance on disclosure of non-financial material risks in SEC filings.
- Support policies that incentivize risk management through the market rather than through prescriptive regulation.

Effective Partnerships: Reduce Risk and Cost
- Fund additional research to develop sophisticated computational modeling of operational risk and quantitative measures of effectiveness in risk management processes.
- Create regional networks to exchange information on infrastructure or system risk management, crisis planning and preparedness, non-proprietary best practices, and intelligence-sharing between the public and private sectors.
- Expand the program of technology test beds, such as the U.S. Department of Energy National SCADA Test Bed, which helps companies test how their current operating systems would interface with innovative security solutions.

Education and Training: Change the Culture
- Establish a Resilience Curriculum Fund under which universities and other education/training providers could apply for competitively awarded grants to develop resilience curricula and training programs, either stand-alone or embedded in existing curricula.
- Stimulate cross-disciplinary synthesis of resilience and research at a system level.

Seeking the Upside of Cross-Sectoral Truths

The Council's core insight immediately following the events of 9/11 was that the attacks not only had critical security repercussions, they also had major competitiveness implications. With so much of the economic infrastructure owned or operated by the private sector, any solution for addressing homeland security threats and scalable responses would have to come from within business, not imposed from the outside.

If integrated quality and safety management systems could become business drivers and pathways for productivity growth, why couldn't the same be true for integrated security management (see "We've Been Here Before" at right)?

Chart 3 (page 13) lays out a framework of the prospective business benefits from security.

Why Companies May Not Recognize the Business Benefits of Security

Despite the prospective bottom-line benefits from security, most companies have not moved creatively to capture them. Many continue to see security as a necessary function, but not a core business value. Organizationally, the security function is often disconnected from business continuity and business drivers. Few companies have developed consistent metrics to quantify cost, benefits or performance.

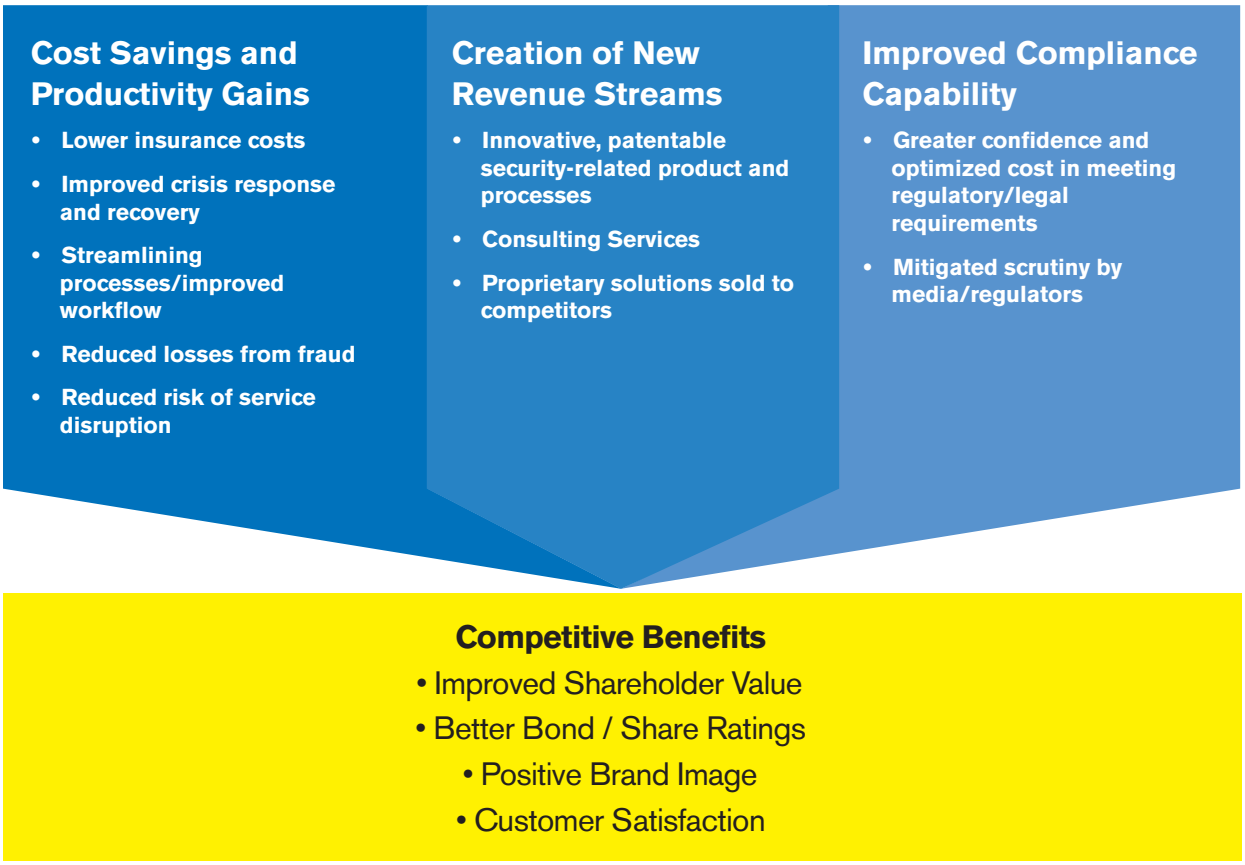
We've Been Here Before

It is instructive to remember that 30 years ago, America's business leaders thought that quality was a luxury they couldn't afford until the Japanese demonstrated that building quality into processes and production, rather than inspecting out the rejects, was a better formula for success. In fact, the Council on Competitiveness was born as part of America's response to the total quality management challenge from Japan.

In the same way, the chemical industry created a new framework for integrated safety management after the disaster in Bhopal, India. Today, the industry calculates that the savings from its safety program are five times greater than the direct cost of injuries—which includes the avoided costs of lost production, process interruptions, equipment replacement, litigation and damage to employee confidence, customer relations and public image. The drive toward zero accidents was not just the right thing to do; it became a best business practice.

3. Business Benefits of Security RESILIENCE

Source: Council on Competitiveness



The barriers to the business case are often organizational and cultural—a product of the way in which companies have historically positioned security. Looking across sectors, there are common patterns that capture some of these critical barriers.

Security Is Not Linked to Strategic Planning and Risk Management

Security in many of the sectors was not aligned with business strategy and not integrated into strategic planning, product development, engineering risk management or supply chain management. Indeed, the security function often does not report at the same level as other senior managers, resulting in what one executive called "security by obscurity".

MIA: Metrics for Success

In most companies, metrics to capture the value of the security function to the enterprise are unavailable, anecdotal or inconsistent. The lack of a framework to demonstrate efficiency gains, reduced theft or fraud, new business opportunities or new markets is a critical barrier. The inability to measure value reinforces the conventional perception that security is an overhead cost rather than a core business enabler. And, it impedes the ability to develop market-based standards by which ratings agencies or the insurance companies could assess different types of security risks.

Security Functions Are Stove Piped
In a number of companies, different aspects of security are siloed by function: physical and employee security; supply chain security; IT security; and IP security. The practical consequences of security silos is that companies within a sector find it difficult to agree on cross-cutting best practices. Between sectors, the existence of different organizational silos bogs down efforts to reduce the risks that stem from infrastructure interdependencies. Lack of a common lingo makes it harder to partner effectively with each other or with federal, state, and local governments—or even to demonstrate to Congress and the American public that companies are exercising due diligence.

Security Executives: Company Cops or Global Risk Managers?
Unlike most other C-Suite positions, the roles and responsibilities of chief security officers are not well defined. They can range from company cop (viewed with suspicion) to global risk manager (where no business decision is made without a security sign-off). Reporting often goes through the Office of the General Counsel (where the focus is on compliance) or through Human Relations (where the focus is on guards with guns).

Culture Wars: Linking Security to the Language of Risk and Reward
Many chief security executives come out of law enforcement, often with distinguished 30-year careers. That makes them exceedingly well equipped to catch crooks, but often less conversant with how to demonstrate the value of security to the overall enterprise. And they need to be able to speak the language of risk and reward when they're competing for investment capital. By the same token, business executives do not typically speak the language of security.

Lack of Worker Training as the First Line of Defense
Integrating security across the enterprise requires a culture that includes workers as a first line of defense. But few of the companies in the studies had taken steps to engage workers in securing the enterprise. Incidents were not always formally reported. In some cases, it took days before security executives were even aware that an incident had occurred. Given advances in IT and software, automated tracking systems are relatively simple to institute, create a valuable learning tool and could be a key component in developing the quantitative models to measure security risk and performance. Similarly, many companies lack the training programs to achieve a cultural transformation. In leader organizations, training is detailed, role-specific, automated and required at regular intervals. But this is the exception rather than the rule.

Learning to Change: Education and Research
Professional curricula largely ignore security as part of risk management and resilience. Business schools do not include security as part of the standard CEO education. Although engineering schools have embraced the principles of designing for quality, safety and more recently sustainability, they often lack a "design for security" focus.

In the same way, academic research centers study many aspects of many industry sectors—from organization and management to supply chain and product design—but only a handful embed concepts of security or risk management into the research agenda. They represent a large—and largely untapped—potential to create the intellectual content (and metrics) that will drive a paradigm shift toward resilience.

Looking Ahead

Challenge for Companies

The challenge for companies is to overcome a historical perspective that views security as static defenses—whether fences or firewalls—and security executives as company cops. To the contrary, security must be integrated into the risk management continuum, not only for loss avoidance, but also for value creation. (see "Transforming Security into a Strategy for Resilience" below)

Challenge for Government

The dilemma for public policy is that the "security" in homeland security does not necessarily match up to the corporate security function. Arguably, homeland security missions are as much about economic resilience as they are about protection. And the functional equivalents to the economic resilience mission in the private sector are business continuity, disaster management and risk management functions, not just security.

Yet, the focus of much of the government's efforts has been to create public-private partnerships that reach out principally to security executives. From a resilience perspective, this may not be the logical partnership focus. Moreover, government attempts to create a regulatory structure to assure private sector preparedness may actually reinforce risk silos, rather than strengthen private sector risk management and response capabilities.

Transforming Security into a Strategy for Resilience

Old Think

- Passive Private Sector/Wait for Regulation
- Security = Static Defences (fences and firewalls)
- Security = Compliance-driven
- Security = Sunk Cost

New Think

- Dynamic Leadership Vision
- Security = Agility/Adaptability
- Security = Core Business Value
- Security = Strategic Opportunity

Warning: Turbulence Ahead IS HERE

The risk environment has changed dramatically for countries and companies alike. Added to the threat of global terrorism are new technical, operational and strategic risks: extended supply chains; technological interdependencies; IT vulnerabilities; mutating viruses; even weather phenomena. These combine to create the potential for disruptions that propagate quickly across technological networks and geographic borders.

In fact, many of these emerging trends not only create new homeland security challenges, they exacerbate operational risks for companies as well—risks that not all companies are well-prepared to meet. Silos in security are characteristic of many aspects of operational risk management. Just as security functions (physical and employee, IT, supply chain security) are siloed, so too are business continuity; safety, environment and health; disaster management.

Within these risk specialties, there are, to be sure, very sophisticated management processes. The problem is that risks do not respect silos. An IT data breach is not just a problem for the IT security executive; it can rapidly evolve into a reputation risk, a litigation risk and a financial risk that can engage the entire company.[7]

Given some of the turbulence ahead, the lack of an integrated approach to risk management is itself becoming a potential risk factor. Some of the trends that change the risk that companies face include:

- The Emergence of Global Enterprises
- New Technology and Infrastructure Risks
- Evolving Legal and Regulatory Risks
- Over the Horizon Risks: Energy Volatility and **Pandemics**

Emergence of Global Enterprises

Global enterprises of the 21st century are very different from the multinationals of the last century. Where multinational companies typically transplanted themselves as self-contained businesses on foreign shores, global enterprises disperse pieces of their business operations across different geographies, which are networked to each other through voice and data IT systems and supply chains.

From a corporate risk perspective, globalization of companies cuts two ways. On one hand, companies are able to leverage geography to disperse risk. Indeed, rather than creating static backup sites (that often gather dust until a disruption occurs), some of the leading companies are rolling out plans to automatically shift operations among global hubs, should one site go down. They are creating shadow seats in each of their locations and cross-training employees in different geographies to assure business continuity for critical functions in case of an emergency.

On the other hand, the diffusion of interconnected operations also increases a company's exposure: to infrastructure disruptions—in transportation, communications, information—that enable the enterprise

to operate seamlessly across different geographies, to the rapid spread of contagious diseases among employees who are traveling between sites, and to geo-political instabilities and terrorism.

New Technology and Infrastructure Risks

Infrastructure risks continue to mount as disruptions across networks and catastrophic losses escalates.

Electric power outages and power quality problems already cost the private sector and the nation about $80 billion every year in lost productivity and downtime. But when an outage cascaded across multiple transmission systems in the August blackout of 2003, the losses escalated to between $6–10 billion for a single incident.[6]

The Internet is creating an entirely new set of vulnerabilities and risks that many companies have not mastered. A recent study indicated that almost seven out of 10 companies were losing sensitive data or having it stolen out from under them as many as six times a year. It turns out that losing data is expensive. Companies that publicly reported a data loss or breach had an average of 8 percent loss of revenue.[7]

The recent Internet attack in Estonia ushered in a new kind of threat. The attackers used a giant network of bots—perhaps as many as one million computers in places as far away as the United States and Vietnam—to amplify the impact of their assault.[8]

One cybersecurity expert noted:

> "Everything you have seen in hacking up until now has been a Beta Test of what is possible. This was a multi-pronged attack against several asset classes and financial institutions. What was not widely reported were the digital ripples globally: shutdowns of central banks; processing centers; parts of the U.S. and EU Treasuries; and other financial elements."[9]

Even without data breaches or cyber-attacks, the cost of computer systems going down is enormous. The last published analysis of the cost of these kinds of events appears to have been conducted seven years ago. In 2000, it was estimated that the cost of an hour of downtime for e-Bay was $225,000, for Amazon.com $180,000, and for brokerage companies $6,450,000. (These numbers are not only dated, they do not include the cost of lost productivity.)[10]

The text box below estimates loss per hour by sector.

2020 UPDATE: IT DISRUPTIONS CAN CRIPPLE THE BOTTOM LINE

98% of organizations say a single hour of downtime costs more than **$100,000**.

81% of respondents indicated that 60 minutes of downtime costs their business more than **$300,000**.

33% of those enterprises reported that one hour of downtime costs their firms **$1-5 million**.

https://www.randgroup.com/insights/cost-of-business-downtime/, accessed 5/28/20.

6 Lawrence Berkley National Laboratory: Kristina Hamachi-LaCommare and Joe Eto. "Understanding the Cost of Power Interruptions to U.S. Electricity Consumers." Berkley: U.S. Department of Energy's Office of Electric Transmission and Distribution.

7 Lisa Vasas. "Some Companies Lose Data Six Times a Year." EWeek. March 7 2007. June 6, 1995. http://www.eweek.com/article2/0,1895,2101683,00.asp.

8 Landler and John Markoff. "After Computer Siege in Estonia, War Turns to Cyberspace." New York Times. May 29, 2007, Final, Technology. June 5, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html.

9 Stephen Spoonamore. Cybrinth:CEO. May 29, 2007.

10 David A. Patterson. "A Simple Way to Estimate the Cost of Downtime." The Proceedings of LISA 2002: Sixteenth Systems Administration Conference. Berkley: Berkley USENIX Association, 2002. Pp. 185-188.

Over the Horizon Risks: Energy Volatility and Pandemics

Energy could become a significant risk factor. The rapid growth in demand from developing economies, such as China and India, is putting pressure on both prices and supply. Indeed, the recent volatility in oil, natural gas and electric power has shaved a percentage point off U.S. GDP growth, increased the costs of energy for U.S. companies, and reduced discretionary income for most Americans.[11]

Daniel Yergin, chairman of the Cambridge Energy Research Associates, notes that the twin energy challenges—the need for energy to drive growth and the need to manage the consequences of energy use—will be dominant challenges in the decades ahead.

On the demand side, the magnitude is daunting. Every day, the global economy requires 86 million barrels of oil, and that is only 40 percent of the total daily world energy consumption.[12] The supply side risks are growing as well. Investments in low carbon alternatives by major financial institutions, energy companies and technology developers could be put at risk if governments around the world fail to agree on an equitable framework for allocating carbon emissions.[13]

Similarly, public health officials have been warning that a future pandemic is not a matter of "if" but "when". The risk of an avian flu outbreak is growing, according to the Congressional Budget Office assessment, because of the way the virus is evolving.

- It is entrenched among the domestic ducks in rural areas of Asia—a permanent ecological niche.
- It is more robust than a weaker 1997 strain; able to survive longer under a broader range of environmental conditions.
- It has increased the range of species it can infect, including cats and captive tigers.
- It has become resistant to one of the two classes of antiflu drugs.[14]

Estimates of the cost of such a pandemic run into the trillions of dollars—costs that could be mitigated by advance planning. Yet a recent survey by Deloitte highlighted that although 73 percent of businesses are aware of the pandemic flu threat and 68 percent are very concerned about the avian flu, only half believe that they have adequately planned to protect themselves from an event—and less than half feel confident about the plan.[15]

11 Council on Competitiveness. "Energy Security, Innovation and Sustainability Initiative" Washington D.C.: Council on Competitiveness, May 2007.

12 Daniel Yergin. "Energy's Challenges." Forbes.com. April 23, 2007. June 5, 2007. http://www.forbes.com/opinions/2007/04/23/solutions-energy-yergin-opinion-cx_lm_0423yergin.html.

13 CERA Insights. "Carbon Markets: Globally Warming." CERA, April 2007.

14 Congressional Budget Office. "A Potential Influenza Pandemic: Possible Macroeconomic Effects and Policy Issues." Washington D.C.: U.S. Congress, July 2006.

15 K.B. Hendricks & V. R. Singhal. "An Empirical Analysis of the Effect of Supply-Chain Disruptions on Long-Run Stock Price Performance and Risk of the Firm." Productions and Operations Management. 14 (2005) 35-52. In FM Global, "The New Supply Chain Challenge: Risk Management in a Global Economy." (April, 2006).

Managing Risk on an Enterprise Basis

Enterprise Risk Management appears to be more popular on paper than in practice. Consider that:

- Only 25 percent of directors of non-financial companies report that the board considers all major risks to the company versus 55 percent of financial industry directors.[16]
- Most companies give themselves high marks in financial risk management, but only 29 percent describe their ability to track non-financial performance as excellent or good, and more than a third describe it as fair or poor.[17]
- During the past 12 months, one in five companies surveyed had suffered significant damage from a failure to manage risk and more than half had experienced at least one near miss. As many as 10 percent reported three near misses during the past year.[18]

One of the missing links in moving toward an enterprise view of risk is the lack of a disciplined approach to operational risk. Notes Joe Sabatini, JP Morgan Chase Managing Director and Head of Corporate Operational Risk: "The industry loses money every day in credit and market risk. We're not bothered by that when we take those risks and incur those losses on an informed basis. The key is to create the same disciplined approach to operational risk."[19]

In fact, the lack of a disciplined approach to operational risk increases the potential for what Harvard Business School professors Max Bazerman and Michael Watkins call "predictable surprise—the disasters you should have seen coming."[20] One example might be in the energy area. Most executives recognize that energy is becoming a risk factor, but few companies appear to have integrated energy planning into risk management. A recent survey from Hill & Knowlton found that, although 82 percent of senior technology leaders from around the globe said they "closely monitor" global warming news, only 35 percent have a concrete energy strategy to deal with it.[21] Similarly, in each of the five sectors studied, senior executives clearly understood that the risk dynamic in their industry was changing, but few had integrated that knowledge into the company's risk management operations.

Why The Markets Are Not Driving Enterprise Risk Management

Given the evidence that integrated risk management is a shareholder value and bottom-line issue, as well as an asset protection strategy, why aren't the markets creating new standards and best practices that capture management attention though lower risk premiums or stronger market valuations? One barrier might be the lack of a common set of priorities among the key stakeholders or any commonly accepted metrics.

"Whose Risk?" on page 21 dramatically highlights widely divergent views of risk between corporate CEOs and insurance executives. Corporate risk managers are most concerned about risks to reputation or continuity that are often uninsurable, while insurance executives are primarily concerned with physical damage and losses. This could make communication about managing risk relatively more difficult.

But the lack of metrics impedes the creation of even a baseline for discussion about transformational approaches to risk and resilience. The lack of risk metrics, particularly operational risk metrics, is a show stopper. Insurance companies accept and price risk based on actuarial data. But for many types of operational risk, there are no actuarial data. Similarly, although Wall Street ratings analysts are increasingly

16 Conference Board. CEO Challenge, 2006.

17 Deloitte Research. "In the Dark II" Deloitte, 2007.

18 Lloyd's, In Association with the Economic Intelligence Unit. "Taking Risk On Board." London: Lloyd's, 2006.

19 Neil Davey. "Operational Risk: A Disciplined Approach." First Services Technology. June 5, 2007.

20 Max. H. Bazerman and Michael D. Watkins. Predictable Surprises: The Disasters You Should Have Seen Coming, and How to Prevent Them. Cambridge: Harvard Business School Press, 2004.

21 Hill and Knowlton. "Return on Environment" New York: Hill and Knowlton, April, 2007. June 5, 2007 http://www.greenbiz.com/news/news_third. cfm?NewsID=35038.

GROWTH IN TORT COSTS

	Growth in Tort Costs Percent Average Annual Increase	Growth in GDP Percent Average Annual Increase
1951–60	11.6	6
1961–1970	9.8	7
1971–1980	11.9	10.4
1981–1990	11.8	7.6
1991–2000	3.2	5.4
2001	14.7	3.2
2002	13.4	3.4
2003	5.5	4.7
2004	5.7	6.9
2005	0.5	6.3
55 Year Average:	**9.5**	**7.1**

Tillinghast. "2006 Update on U.S. Tort Cost Trends." New York: Towers Perrin, 2006.

homing in on risk management capabilities, they are struggling to come up with appropriate metrics and methodologies to assess risk management systems or to value resilience. For its part, while the government has a vested interest in creating more robust risk management capabilities in the private sector, homeland security generally views risk through the lens of catastrophic events and not as part of a risk continuum.

The increasing turbulence of the business environment is partially at fault for the slowness of response to mounting risks. When a ceaseless array of day-to-day pressures and unexpected crisis bombard executives, it is difficult to step back and develop an integrated strategy. In a simpler time, companies were able to achieve operating efficiency by establishing stable business models with repeatable, uniform processes. Today, stability is elusive, and companies must learn new skills—agility, adaptability, and resilience—in order to deliver consistently high performance and shareholder value.

2020 Update: Supply Chain Risk Remains a Challenge [22]

- Seventy-four percent of survey respondents have faced at least one third-party related incident in the last three years.
- More than 50 percent of respondents reported "some" or a "significant" increase in their level of dependence on third parties in the last year.
- Only 20 percent of respondents have integrated or optimized their extended enterprise risk management mechanisms.
- Just 11 percent of respondents are "fully prepared" to deal with the increased uncertainty in the external environment.

22 https://www2.deloitte.com/us/en/pages/risk/articles/extended-enterprise-risk-management-global-survey.html, webpage accessed 5/28/2020.

WHOSE RISK? Top 10 Risk Priorities

Corporate Executives	Insurance Executives	Hometown Security
Reputation	Hurricane	Chemical Threats
Business Interruption	Flood	Biological Threats
Third Party Liability	Oil Spill	Crime
Supply Chain Failure	Terrorism	Fire
Market Environment	Blackout	Cyber-attack
Regulation/Legislation	Wildfires	Tornado
Talent	Industrial Accident	Nuclear Threats
Market Risk	Cyber-attack	Earthquake
Physical Damage	Pandemic	Hurricane
Merger & Acquisition	Earthquake	Flooding

Executive Risk Rankings: Aon, 2007 Global Risk Management Survey.

Insurance Risk Rankings: Risk and Insurance, Top 10 Risks, April 15, 2007.

Mayors' Risk Rankings: Key survey findings, conducted by the U.S. Conference of Mayors and DuPont through their Cities United for Science Progress partnership.

Where Do We Go from Here?

The numbers are staggering. 6.26 million known cases[1] of COVID-19 in the United States. A death toll as of September 7 of 188,513.[2] 13.6 million workers unemployed.[3] Thousands of business shuttered, many to never reopen. GDP growth likely to drop by more than 20 percent. Hundreds of thousands of students forced to seek degrees online and uncertainty about when campuses will reopen. Supply chains in numerous industries have been disrupted or stretched near the breaking point, impacting thousands of products, creating spot shortages of products in high demand and production slowdowns. Demand in some markets has tanked leading to massive layoffs, while a few others have soared leaving firms scrambling to rapidly scale their workforces.

Hope for a vaccine remains high, but how quickly one can be developed, mass produced and made available remains unknown. States are beginning to experiment with various plans to reopen their economies and schools. Businesses are making plans to return to the office, but the reality is that the office environment is likely to be vastly different than what is was before the pandemic. The implications for transit, real estate, and even urban/rural divide are tremendous.

In short, the COVID-19 pandemic has disrupted the U.S. economy in ways we are only beginning to grasp. It seems likely that many aspects of the way people learn, work, and recreate are changed irrevocably. Yet, this crisis also has spawned tremendous innovation and creativity that coupled with greater resilience could signal a better outcome when the next crisis hits.

For it was no small accomplishment that colleges and universities successfully transitioned their entire curriculum online in a matter of days. New consortiums to tackle treatments and potential vaccines sprung up quickly, including one bringing together the awesome power of high-performance computing across the public and private sectors to include universities, national labs and leading U.S. businesses. Many workers are being retrained in real time to fill gaps in the workforce from virus contact tracing to processing unemployment claims.

Looking to the next economy that will rise from the depths of the COVID-19 crisis, one “ace-in-the-hole” that could bridge resilience and innovation is the rapid advancement in technology. As the unfolding and accelerating revolutions in science and technology—such as biotechnology, digital technology, big data, artificial intelligence, nanotechnology, advanced materials, and autonomous systems—collide and converge on the global economy, enterprises, and society simultaneously, they have numerous and potential future applications that can contribute to building a

1 https://covid.cdc.gov/covid-data-tracker/#cases.

2 ibid.

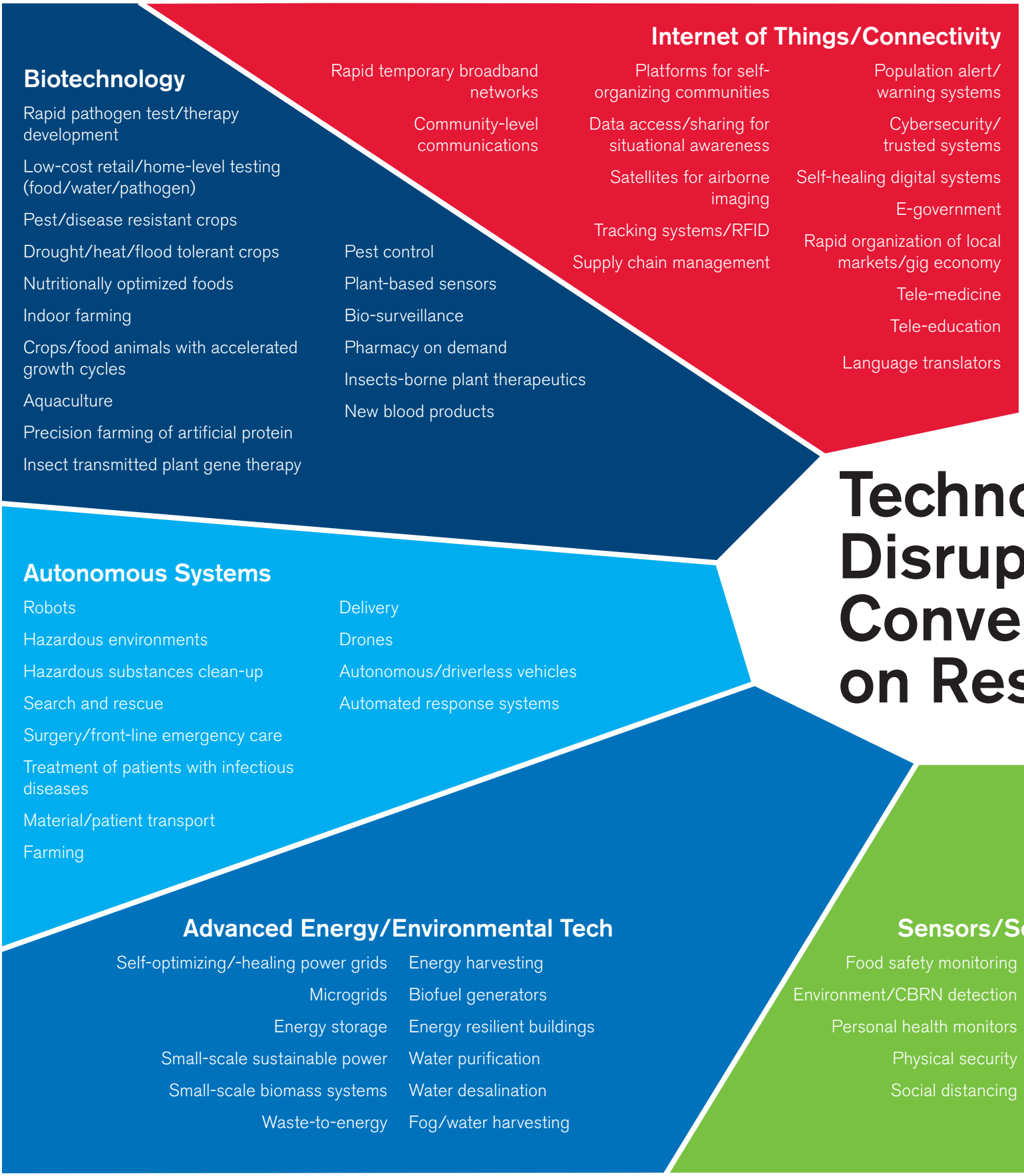
3 https://www.bls.gov/news.release/empsit.nr0.htm.

Prepare for What?

- Climate change
- Earthquake/tsunami
- Flood/dam failure
- Hurricane/tornado/severe storm
- Heat wave
- Severe winter weather
- Volcano
- Wild fire
- Drought
- Chemical/toxic substance release
- Terrorist attack
- CBRN release
- Contagious disease outbreak
- Plant/animal disease outbreak
- Cyber-attack/computer virus
- Power blackout
- Transportation system failure
- IT/telecom outage
- Port or trucking strike/labor unrest
- Protest/civil unrest
- Geopolitical instability
- Product tampering/ contamination
- Water contamination
- Supply chain breakdown
- Energy supply disruption
- Food supply disruption
- Critical material supply disruption

broad capacity for resiliency at every level of society and its systems (see illustration for examples). To leverage these disruptive technologies to achieve this outcome, a multidisciplinary development and deployment effort carried out across numerous societal dimensions at different levels and scales will be needed. Governments at all levels, the private sector, other sectors such as health care, communities, and households all have roles to play.

What should be clear from this updated report is that the United States has the tools to both prepare and respond to crisis. Leaders in the public and private sectors must embrace the dual mandates of resilience and innovation. Chad Holliday, Chairman, Royal Dutch Shell, who co-chaired the development of the original *Transform* report, stated it best back in 2007, when he said, "Our country can be competitive in light of threats either natural or manmade, if we do three things: develop fundamentally resilient systems; stick with them year after year; and do not become complacent."


Biotechnology
Rapid pathogen test/therapy development
Low-cost retail/home-level testing (food/water/pathogen)
Pest/disease resistant crops
Drought/heat/flood tolerant crops
Nutritionally optimized foods
Indoor farming
Crops/food animals with accelerated growth cycles
Aquaculture
Precision farming of artificial protein
Insect transmitted plant gene therapy
Pest control
Plant-based sensors
Bio-surveillance
Pharmacy on demand
Insects-borne plant therapeutics
New blood products
Internet of Things/Connectivity
Rapid temporary broadband networks
Community-level communications
Platforms for self-organizing communities
Data access/sharing for situational awareness
Satellites for airborne imaging
Tracking systems/RFID
Supply chain management
Population alert/ warning systems
Cybersecurity/ trusted systems
Self-healing digital systems
E-government
Rapid organization of local markets/gig economy
Tele-medicine
Tele-education
Language translators
Techno
Disrup
Conve
on Res
Autonomous Systems
Robots
Hazardous environments
Hazardous substances clean-up
Search and rescue
Surgery/front-line emergency care
Treatment of patients with infectious diseases
Material/patient transport
Farming
Delivery
Drones
Autonomous/driverless vehicles
Automated response systems
Advanced Energy/Environmental Tech
Self-optimizing/-healing power grids
Microgrids
Energy storage
Small-scale sustainable power
Small-scale biomass systems
Waste-to-energy
Energy harvesting
Biofuel generators
Energy resilient buildings
Water purification
Water desalination
Fog/water harvesting
Sensors/S
Food safety monitoring
Environment/CBRN detection
Personal health monitors
Physical security
Social distancing

Nanotechnology/Advanced Materials

- CBRN protection
- Self-healing materials
- Antimicrobial surfaces/ coatings
- Nano-based vaccines/ immunotherapies
- Critical materials substitutes/ reduction
- Wound healing monitors
- Filters/membranes
- Infrastructure/structure hardening
- Engineered living materials
- Multi-functional materials
- Functional fabrics/ electro-textiles

Advanced Engineering/ Manufacturing

- Mobile infrastructure
- Rapid laboratory infrastructure establishment
- 3-D printing
- Disaster-resilient design/materials
- Flexible manufacturing/ rapid set-up
- Smart structures respond to changing conditions
- Rapid construction methods
- Chemical process intensification
- Structures on demand/ temporary structures
- Smart/novel packaging

ology tors rge siliency

Artificial Intelligence

- Patient screening/triage
- Knowledge/skill enhancing agents for "para" workers
- Image analysis
- Data analytics
- Tele-medicine/diagnostics
- Chat bots/service agents

ensorization

- Anti-tamper
- Alarms
- Thermal imaging
- Geolocation/GPS
- Persistent observation/data collection/remote sensing

Computing/Big Data/Data Analytics

- Modeling/simulation/visualization
- Early detection of disease outbreak
- Epidemic Response
- GIS
- Risk assessment
- Rapid personnel identification/ mobilization/ management
- Source identification (food poisoning/ contagious disease/tampering)
- Supply chain modeling/reconfiguration
- Decision-support systems
- Digital twins

2007 Competitiveness and Security Steering Committee

CO-CHAIRS

Charles O. Holliday, Jr.
Chairman and CEO
DuPont

Jared Cohon
President
Carnegie Mellon University

DISTINGUISHED FELLOW

Thomas Ridge
Former Secretary U.S. Department
of Homeland Security

MEMBERS

Morton Bahr
Former President
Communications Workers of America

John T. Casteen III
President
University of Virginia

Ruth David
President and CEO
Analytic Services Inc.

John Menzer
Vice Chairman
Wal-Mart Stores, Inc.

John A. Edwardson
Chairman and CEO
CDW Corporation

Shirley Ann Jackson
President
Rensselaer Polytechnic Institute

Douglas McCarron
General President
United Brotherhood of Carpenters & Joiners of America

John Morgridge
Chairman
Cisco Systems, Inc.

Clayton Daniel Mote, Jr.
President
University of Maryland

Kenan Sahin
President and Founder
TIAX, LLC

Andrew L. Stern
President
Service Employees International Union

Paul Yarossi
President
HNTB Companies

William D. Zollars
Chairman, President & CEO
Yellow Roadway Corporation

2007 Competitiveness and Security Advisory Committee

ADVISORY COMMITTEE CO-CHAIRS

Catherine Allen
Former CEO
BITS Financial Services Roundtable

Robert Moore
Executive Director, Global Security Group
Merck & Co., Inc.

MEMBERS

Don Anthony
President
Council for Chemical Research

David Barron
AVP, Federal Relations and National Security
BellSouth

Roger Bowers
Vice President, Government Affairs
HNTB Companies

Ed Casey
Director, Corporate Security
Procter and Gamble

Cheryl Charles
Senior Vice President
BITS Financial Services Roundtable

Jerry Cox
Chairman and CEO
Potomac Energy Associates

Alex de Alvarez
Director, Office of Energy Security and Assurance
U.S. Department of Energy

Steven Flynn
Senior Fellow, National Security Studies
Council on Foreign Relations

Mildred Hastbacka
Director
TIAX, LLC

Christopher Heinz
Political and Legislative Director
Brotherhood of Carpenters & Joiners

Michael Hickey
Vice President for Homeland Security
Verizon

Connie Hughes
Commissioner
New Jersey Board of Public Utilities

Mike Kelley
Vice President, Government Affairs
Yellow Roadway Corporation

Henry Kenchington
Program Manager
U.S. Department of Energy

Ben Levitan
President and CEO
EnvoyWorldWide

Timothy McNulty
Special Assistant for Strategic Technology Initiatives
Carnegie Mellon University

Mark P. Mills
Chairman, CTO
ICx Technologies

James B. Porter, Jr.
Vice President, Engineering and Operations
DuPont

Rob Quartel
CEO and Chairman
Freight Desk Technologies

Harvey Rubin
Professor of Medicine, Division of Infectious Diseases
University of Pennsylvania

John Ryan
Director of Corporate Security
Constellation Energy

John Sullivan
Vice President, British Petroleum Group Security
British Petroleum, Plc.

Denise Swink
Formerly Director, Office of Energy Assurance
U.S. Department of Energy

Robert Weber
Director
TIAX, LLC

Margaret Welsh
Senior Vice President
Energetics

Chelsea White, III
IsyE Chair, Transportation and Logistics
Georgia Institute of Technology

Martin Wilhelm
President
M.C. Wilhelm Associates, LLC

About the Council on Competitiveness

For more than three decades, the Council on Competitiveness (Council) has championed a competitiveness agenda for the United States to attract investment and talent and spur the commercialization of new ideas.

While the players may have changed since its founding in 1986, the mission remains as vital as ever—to enhance U.S. productivity and raise the standard of living for all Americans.

The members of the Council—CEOs, university presidents, labor leaders and national laboratory directors—represent a powerful, nonpartisan voice that sets aside politics and seeks results. By providing real-world perspective to Washington policymakers, the Council's private sector network makes an impact on decision-making across a broad spectrum of issues—from the cutting edge of science and technology, to the democratization of innovation, to the shift from energy weakness to strength that supports the growing renaissance in U.S. manufacturing.

The Council's leadership group firmly believes that with the right policies, the strengths and potential of the U.S. economy far outweigh the current challenges the nation faces on the path to higher growth and greater opportunity for all Americans.

Council on Competitiveness
900 17th Street, NW, Suite 700
Washington, D.C. 20006
202 682 4292
Compete.org

Council on Competitiveness Members, Fellows and Staff

BOARD

Chairman
Dr. Mehmood Khan
Chief Executive Officer
Life Biosciences, Inc.

Industry Vice-chair
Mr. Brian T. Moynihan
Chairman and Chief Executive Officer
Bank of America

University Vice-chair
Dr. Michael M. Crow
President
Arizona State University

Labor Vice-chair
Mr. Lonnie Stephenson
International President
IBEW

Chairman Emeritus
Mr. Samuel R. Allen
Chairman
Deere & Company

President & CEO
The Honorable Deborah L. Wince-Smith
Council on Competitiveness

FOUNDER

Mr. John Young
Former Chief Executive Officer
Hewlett Packard Company

EXECUTIVE COMMITTEE

Mr. Jim Balsillie
Co-founder
Institute for New Economic Thinking

Mr. Thomas R. Baruch
Managing Director
Baruch Future Ventures

Dr. Gene D. Block
Chancellor
University of California, Los Angeles

Mr. William H. Bohnett
President
Whitecap Investments, LLC

Dr. James P. Clements
President
Clemson University

Mr. Jim Clifton
Chairman and CEO
Gallup

Mr. Mark A. Crosswhite
Chairman, President & CEO
Alabama Power Company

Dr. John J. DeGioia
President
Georgetown University

Mr. George Fischer
Senior Vice President and President, Global Enterprise
Verizon Business Group

Ms. Janet Foutty
Chair of the Board
Deloitte LLP

Dr. William H. Goldstein
Director
Lawrence Livermore National Laboratory

Mr. James S. Hagedorn
Chairman and CEO
The Scotts Miracle-Gro Company

Dr. Sheryl Handler
President and CEO
Ab Initio

Mr. Charles O. Holliday, Jr.
Chairman
Royal Dutch Shell, plc

Ms. Jacqueline Hunt
Member of the Board of Management
Allianz, SE

The Honorable Shirley Ann Jackson
President
Rensselaer Polytechnic Institute

Dr. Farnam Jahanian
President
Carnegie Mellon University

Dr. Pradeep K. Khosla
Chancellor
University of California, San Diego

Mr. James B. Milliken
Chancellor
The University of Texas System

Gen. Richard B. Myers
President
Kansas State University

The Honorable Janet Napolitano
President
The University of California System —Regents

Mr. Nicholas T. Pinchuk
Chairman and CEO
Snap-on Incorporated

Professor Michael E. Porter
Bishop William Lawrence University Professor
Harvard Business School

Dr. Mark S. Schlissel
President
University of Michigan

Mr. Steve Stevanovich
Chairman and Chief Executive Officer
SGS Global Holdings

Ms. Randi Weingarten
President
American Federation of Teachers, AFL-CIO

Dr. W. Randolph Woodson
Chancellor
North Carolina State University

Mr. Paul A. Yarossi
President
HNTB Holdings Ltd.

Dr. Robert J. Zimmer
President
The University of Chicago

GENERAL MEMBERS

Mr. Jonathan R. Alger
President
James Madison University

Dr. Michael Amiridis
Chancellor
University of Illinois at Chicago

Dr. Joseph E. Aoun
President
Northeastern University

Dr. Aziz Asphahani
Chief Executive Officer
QuesTek Innovations, LLC

Dr. Dennis Assanis
President
University of Delaware

Dr. Eric Barron
President
The Pennsylvania State University

The Honorable Sandy K. Baruah
President and Chief Executive Officer
Detroit Regional Chamber

Dr. Mark P. Becker
President
Georgia State University

Dr. Richard Benson
President
The University of Texas at Dallas

The Honorable Rebecca M. Blank
Chancellor
University of Wisconsin—Madison

Dr. Lee C. Bollinger
President
Columbia University

Dr. Robert A. Brown
President
Boston University

Mr. Al Bunshaft
Senior Vice President, Global Affairs
Dassault Systèmes Americas

The Honorable Sylvia M. Burwell
President
American University

Mr. Bill Cave
CEO
Prediction Systems

Mr. John Chachas
Manging Partner
Methuselah Advisors

Mr. John Chisholm
Chief Executive Officer
John Chisholm Ventures

Dr. Steven Currall
President
University of South Florida

The Honorable Mitchell E. Daniels, Jr.
President
Purdue University

Mr. Ernest J. Dianastasis
CEO
The Precisionists, Inc.

Dr. Michael V. Drake
President
The Ohio State University

Dr. Taylor Eighmy
President
The University of Texas at San Antonio

Mr. Robert Ford
President and Chief Operating Officer
Abbott

Mr. Kenneth C. Frazier
Chairman and Chief Executive Officer
Merck & Co., Inc.

Dr. Wayne A. I. Frederick
President
Howard University

Dr. Julio Frenk
President
University of Miami

Dr. W. Kent Fuchs
President
University of Florida

Ms. Joan T. A. Gabel
President
University of Minnesota

The Honorable Patrick D. Gallagher
Chancellor
University of Pittsburgh

Dr. E. Gordon Gee
President
West Virginia University

Dr. Amy Gutmann
President
University of Pennsylvania

Ms. Marillyn A. Hewson
Chairman, President and CEO
Lockheed Martin

Mr. G. Michael Hoover
Chief Executive Officer
Sundt Construction

The Honorable Steven J. Isakowitz
President and Chief Executive Officer
The Aerospace Corporation

Rev. John I. Jenkins
President
University of Notre Dame

Dr. James R. Johnsen
System President
University of Alaska

Dr. Paul Johnson
President
Colorado School of Mines

Dr. Robert E. Johnson
Chancellor
University of Massachusetts Dartmouth

Mr. Edward Jung
Founder and CEO
Xinova, LLC

The Honorable Alexander A. Karsner
Managing Partner
Emerson Collective

The Honorable Mark Kennedy
President
University of Colorado

Mr. Shahal Khan
Chief Executive Officer (Interim)
Economic Transformation Technologies

Dr. Timothy L. Killeen
President
University of Illinois System

Dr. Laurie A. Leshin
President
Worcester Polytechnic Institute

Dr. Michael R. Lovell
President
Marquette University

Dr. Larry R. Marshall
Chief Executive
CSIRO

Dr. Gary S. May
Chancellor
University of California, Davis

Mr. Sean McGarvey
President
North America's Building Trades Unions

Dr. Jonathan McIntyre
Chief Executive Officer
Motif FoodWorks, Inc.

Brig. Gen. John Michel
Director, Executive Committee
Skyworks Global

Mr. Jere W. Morehead
President
University of Georgia

Mr. Christopher Musselman
Head, U.S. Commercial Business
Palantir Technologies, Inc.

Mr. Eloy Ortiz Oakley
Chancellor
California Community Colleges

Dr. Christina Hull Paxson
President
Brown University

Dr. Neville Pinto
President
University of Cincinnati

Mr. John Pyrovolakis
CEO
Innovation Accelerator Foundation

Dr. Edward Ray
President
Oregon State University

Dr. L. Rafael Reif
President
Massachusetts Institute of Technology

Mr. Rory Riggs
Managing Member
Balfour, LLC

Mr. John Rogers
President and CEO
Local Motors

Dr. Rodney Rogers
President
Bowling Green State University

Mr. Clayton Rose
President
Bowdoin College

Mr. Douglas Rothwell
President and Chief Executive Officer
Business Leaders for Michigan

Dr. David Rudd
President
University of Memphis

Vice Admiral John R. Ryan
President and Chief Executive Officer
Center for Creative Leadership

Dr. Cathy Sandeen
Chancellor
University of Alaska Anchorage

Dr. Timothy D. Sands
President
Virginia Polytechnic Institute and State University

Dr. Kirk Schulz
President
Washington State University

Mr. Frederick W. Smith
Chairman and Chief Executive Officer
FedEx

Dr. Joseph E. Steinmetz
Chancellor
University of Arkansas

Dr. Elisa Stephens
President
Academy of Art University

Dr. Claire Sterk
President
Emory University

Dr. Elizabeth Stroble
President
Webster University

Dr. Kumble R. Subbaswamy
Chancellor
University of Massachusetts Amherst

Dr. Satish K. Tripathi
President
University at Buffalo

Dr. Marty Vanderploeg
Chief Executive Officer and President
Workiva

Dr. Ruth Watkins
President
University of Utah

Dr. Adam S. Weinberg
President
Denison University

Dr. Kim A. Wilcox
Chancellor
University of California, Riverside

Dr. Wendy Wintersteen
President
Iowa State University

NATIONAL LABORATORY PARTNERS

Dr. Steven F. Ashby
Director
Pacific Northwest National Laboratory

Dr. Paul Kearns
Director
Argonne National Laboratory

Dr. Martin Keller
Director
National Renewable Energy Laboratory

Dr. Thomas Mason
Director
Los Alamos National Laboratory

Dr. Mark Peters
Director
Idaho National Laboratory

Dr. Michael Witherell
Director
Lawrence Berkeley National Laboratory

Dr. Thomas Zacharia
Director
Oak Ridge National Laboratory

CORPORATE PARTNERS

HP Federal

Intel Corporation

PepsiCo, Inc

Philip Morris International

SparkCognition, Inc.

UNIVERSITY PARTNERS

The Texas A&M University System

University of California, Irvine

NATIONAL AFFILIATES

Dr. Dean Bartles
President & CEO
National Center for Defense Manufacturing and Machining

Mr. Jeffrey Finkle
President and CEO
International Economic Development Council

Ms. Sherry Lundeen
President
ARCS Foundation Inc.

Dr. David W. Oxtoby
President
American Academy of Arts and Sciences

FELLOWS

Mr. Bray Barnes, Senior Fellow
Director, Global Security & Innovative Strategies, Washington, DC

Ms. Jennifer S. Bond, Senior Fellow
Former Director, Science & Engineering Indicators Program, National Science Foundation

Dr. Thomas A. Campbell, Senior Fellow
Former National Intelligence Officer for Technology, Office of the Director of National Intelligence

Ms. Dona L. Crawford, Senior Fellow
President, Livermore Lab Foundation; and Former Associate Director, Computation, Lawrence Livermore National Laboratory

The Honorable Bart J. Gordon, Distinguished Fellow
Partner, K&L Gates LLP; and Former United States Representative (TN)

Mr. Thomas Hicks, Distinguished Fellow
Principal, The Mabus Group; and Former Undersecretary of the Navy, U.S. Department of Defense

Dr. Paul J. Hommert, Distinguished Fellow
Former Director, Sandia National Laboratories; and Former President, Sandia Corporation

Dr. Lloyd A. Jacobs, Distinguished Fellow
President Emeritus, The University of Toledo

Dr. Ray O. Johnson, Distinguished Fellow
Executive in Residence, Bessemer Venture Partners; and Former Senior Vice President and Chief Technology Officer, Lockheed Martin

The Honorable Martha Kanter, Distinguished Fellow
Executive Director, College Promise Campaign

Mr. Dominik Knoll, Senior Fellow
Former Chief Executive Officer
World Trade Center of New Orleans

The Honorable Steven E. Koonin, Distinguished Fellow
Director, Center for Urban Science and Progress, and Professor, Information, Operations & Management Sciences, Leonard N. Stern School of Business, New York University; and Former Second Under Secretary of Energy for Science, U.S. Department of Energy

Mr. R. Brad Lane, Distinguished Fellow
Co-Founder & Chief Executive Officer
RIDGE-LANE Limited

The Honorable Alan P. Larson, Distinguished Fellow
Senior International Policy Advisor, Covington & Burling LLP; and Former Under Secretary of State for Economics, U.S. Department of State

Mr. Alex R. Larzelere, Senior Fellow
President, Larzelere & Associates LLC; and Former Director, Modeling and Simulation Energy Innovation Hub, Office of Nuclear Energy, U.S. Department of Energy

Mr. Abbott Lipsky, Senior Fellow
Former Partner, Latham & Watkins LLP

Mr. Edward J. McElroy, Distinguished Fellow
Former Chief Executive Officer, Ullico, Inc.

The Honorable Julie Meier Wright, Senior Fellow
Former Chief Executive, San Diego Regional Economic Development Corporation; and Former First Secretary of Trade & Commerce, State of California

Mr. Mark Minevich, Senior Fellow
President, Going Global Ventures

Ms. Michelle Moore, Senior Fellow
Chief Executive Officer, Groundswell; and Former Senior Advisor to the Director, Office of Management and Budget, Executive Office of the President of the United States

Dr. Luis M. Proenza, Distinguished Fellow
President Emeritus, The University of Akron

Ms. Jody Ruth, Senior Fellow
CEO, Redstones

Mr. Reuben Sarkar, Senior Fellow
Former Deputy Assistant Secretary for Transportation, U.S. Department of Energy

Mr. Allen Shapard, Senior Fellow
Senior Director, Chair of Public Engagement Strategies
APCO Worldwide

Dr. Branko Terzic, Distinguished Fellow
Managing Director, Berkeley Research Group, LLC

Dr. Anthony J. Tether, Distinguished Fellow
Former Director, Defense Advanced Research Projects Agency, U.S. Department of Defense

Ms. Maria-Elena Tierno, Senior Fellow
Senior Business Development Manager, Constellation Energy

Dr. Thomas M. Uhlman, Distinguished Fellow
Founder and Managing Partner, New Venture Partners LLC

Dr. William Wescott, Senior Fellow
Managing Partner, BrainOxygen, LLC.

Dr. Mohammad A. Zaidi, Distinguished Fellow
Member, Strategic Advisory Board, Braemer Energy Ventures; and Former Executive Vice President and Chief Technology Officer, Alcoa, Inc.

STAFF

Mr. William Bates
Executive Vice President

Mr. Chad Evans
Executive Vice President

Ms. Marcy Jones
Special Assistant to the President & CEO and Office Manager

Ms. Patricia Hennig
Vice President for Finance

Ms. Kathy Trimble
Vice President

Mr. Gourang Wakade
Vice President

Ms. Yasmin Hilpert
Senior Policy Director

Mr. Christopher Reigelsperger
Director for Information Technology and Services

Mr. Joshua Oswalt
Policy Analyst

Mr. Timothy Planert
Policy Analyst

Council on Competitiveness
900 17th Street, NW, Suite 700, Washington, D.C. 20006, T 202 682 4292
Compete.org

@CompeteNow
facebook.com/USCouncilonCompetitiveness
linkedin.com/company/council-on-competitiveness/

Compete.
Council on Competitiveness