On May 9th, 2007, President George W. Bush issued National Security Presidential Directive 51. The order provided for “continuity of government” and for the country’s “effective response to and recovery from a national emergency.” It was a call to national “resilience.”

The directive recognized the reality that the Cold War’s end had ushered in a different and far more complex security environment—one featuring an expanding array of asymmetric threats, when crisis can arise with little warning and devastating effect. This reality hit home in 2001 when al Qaeda terrorists hijacked four commercial jumbo jets to attack strategically selected targets in New York City and Washington, D.C.

The nation was shocked, civil society was shaken, and the economy reeled from the assault; but as we have done throughout our history, America rallied. In keeping with our fundamental character we got back on our feet to carry on the work of freedom and in so doing deprived our adversaries of their strategic aim—which was not only to kill Americans but to inflict permanent damage on the American system and trigger national retreat.

The attack roused deep within America’s nature a source of strength we have always called upon in times of crisis: the will to overcome. This celebration of the human spirit was personified by a very special colleague with whom I served on the 9/11
Commission staff. Then a young Navy Lieutenant, he was serving in the Pentagon’s Naval Operations when on the morning of September 11, 2001, American Airlines Flight 77 crashed through its walls. He suffered severe injuries. The attending EMTs lost his heartbeat several times, but he survived and recovered, and today he flourishes. He fortified us then, as he does now, by his inspirational example and with the constant exhortation: “Never Forget.”

Those words are among 9/11’s most poignant legacies. They continue to inspire the nation to remember faithfully our fallen and to honor the heroism demonstrated that day and in its aftermath. Yet the words also serve as a warning to heed the compelling lessons of this seminal chapter in our nation’s history. They yield critical insights into the nature of risk and the dynamics of resilience in the 21st century—revelations germane to preserving the well-being of our communal, business, familial, and personal systems in a complex and hazardous world. Protecting America’s national security in this way means transforming “Never Forget” into “Never Again.”

Grasping not just how the events unfolded that day and the nature of our ill-preparedness but garnering lessons learned was among the 9/11 Commission’s primary charges.

As one of the Commission’s staffers, my colleagues and I were asked to examine the facts and analyze the policy and executional flaws responsible for the many failings in evidence. The scope of the investigation underscored the complex and multi-faceted nature of risk today with elements of the commission looking at our intelligence, the national aviation security system, the national air defense system, and our emergency response capability. This required asking tough questions of what decision makers and operators did and why—retrospective questions that are far easier to ask “what shall we do” but essential to carry away lessons learned. The Commission was asked to consider the latter question and provide its final recommendations. What we learned about ourselves prior to 9/11 was still in evidence afterward. Neither the public nor private sectors were ready for the tough, brutal reality of the post-9/11 world. Getting ready would require some tough analysis and action.

RISK IN THE 21ST CENTURY

To begin we needed to adjust our perception of risk. As the events of 9/11 demonstrated, risk in the 21st century is far more dynamic and variable than in the bi-polar context of the Cold War. Threats emerge more swiftly and manifest themselves more unpredictably. Small groups of people, even individuals, now have access to a growing range of tools and wider opportunity to inflict monumental damage. It was at first shocking, but eventually paradigm-shifting that such a small group of people could plan and execute so destructive an attack with such far reaching effects.

America has always been a bulwark against the haters, fanatics, and would-be dictators who conspire to impede human advancement. We know and love the value of freedom. We understand that mankind reaps tremendous rewards from the interconnectivity, freedom, transparency, and cooperation that are the moorings of today’s trade-based global economy.

Our times feature marvelous, life-changing architecture such as a worldwide transportation system, universal ICT and mobile telephone networks, fertile shared cyberspace, borderless economic engagement, and expansive new economic, social, and political interactions and interdependencies. These systems have improved the lives of millions and yielded wondrous results. Each is an essential
cog in the global economic system that is vital to America’s interests and mankind’s prospects for peace and prosperity.

Yet these transformational benefits come with bigger risks that can spread more quickly and are harder to identify and anticipate. 9/11 made clear that the fundamental openness and accessibility of our society and its systems—an interconnectedness that is expanding with economic and social globalization—is also an enormous vulnerability. The commission was chartered to explore these vulnerabilities, understand how the plot was developed and executed, and investigate why we were so ill-prepared to defend the homeland.

While we have made significant improvements in our homeland defenses and resilience in the past decade, the challenges are dynamic and many of the lessons of 9/11 still go unheeded. Malefactors still seek to exploit open transportation networks to commit atrocity. Human pathogens can spread swiftly across borders threatening millions of people. Malicious code is deployed at the speed of light to attack our critical systems from infinite points around the globe.

Moreover, increasing international economic competition can beget new commercial and competitive threats. Poor decisions made in distant board rooms, union halls, financial institutions, legislative chambers, and governmental bureaucracies can imperil our savings, our job, and our enterprise. Insecurity in remote parts of the world can disrupt global supply chains and grind operations to a halt imperiling the health of our economy. Our systems, though miracles of human ingenuity and strength, can also be exceedingly fragile.

Indeed, risks abound and as 9/11 demonstrated, modern threats are more random and unpredictable than ever.

**RISK ASSESSMENT**

A long-held security risk-assessment formula in vogue prior to 9/11 illustrates the point that times have changed. Two seemingly rational and elegant equations were intended to identify where to place our homeland security attention and direct limited resources for protecting ourselves; these were “intent plus capability equals threat” and its companion “threat plus vulnerability equals risk.”

When I first came across this calculus during the commission’s investigation, it seemed rational. Yet when matching it up against the attacks and the posture of our nation’s intelligence, aviation security, and national air defense systems that day, it was clearly a dated and deficient formula.

**WHEN WE EXCESSIVELY DEPEND ON FOREKNOWLEDGE, WE DO SO AT OUR OWN PERIL.**

The primary flaw in this equation was that the identification of a threat depended on perfect knowledge of others’ intentions and abilities, something no person, business, or country in the world has, even when it possesses the finest intelligence system. Perhaps 9/11 was, at least in part, a failure of intelligence, but expectations of advanced warning whether by government or business is unrealistic in a fast-paced, multi-polar world featuring a wider array of actors and malefactors. When we excessively depend on foreknowledge, we do so at our own peril.

Others have observed that 9/11 was also a failure of “imagination.” The fact is that elements of our intelligence community had indeed imagined that people could use commercial aircraft as weapons of mass destruction on strategic targets. We simply did not believe that such an attack would occur. First, we had
no intelligence that such an attack was in the offing and, second, such an attack had not occurred in just that way before. Such a “tombstone” approach to security was, as it remains—a recipe for fighting previous battles rather than preparing for those to come. It ensures that leaders are one step behind when the key to managing risk in a complex, dynamic environment is staying one step ahead.

We can’t begin to comprehend our true vulnerabilities if we assess ourselves only in terms of threats about which we are forewarned or those we determine that adversaries have in mind, rather than taking into consideration the full spectrum of imaginable threat. I’m not sure either our public or private sector has adopted this new and necessary approach.

Another major flaw in the formula became clear. It didn’t properly account for “consequences.” It brooked little consideration for guarding against a highly consequential attack in the absence of actionable intelligence or a preceding event. The lives lost, ensuing economic damage, and our subsequent involvement in two wars amply testify as to the cost and consequence of demanding precedent in order to take preventative action against the imaginable, feasible, and disastrous.

Prior to 9/11 we had not endeavored to fully consider every conceivable way that adversaries could attack our civil aviation system. We had not measured the consequences of a successful attack across the spectrum of possibilities. Nor had we honestly assessed the efficacy of our countermeasures against the feasible. Had we done so, perhaps we would have erroneously concluded that existing measures were sufficient or that the cost and unintended consequences of taking preventative steps to stop people from hijacking a commercial aircraft and using it as a weapon of mass destruction would not justify action.

Still we never had in place the procedures and framework necessary to make such a calculus—one that would enable to us to account for the full range of possibilities and rationally decide what requirements were in order. Therein is the cautionary tale for today—to ensure we have in place the processes to assess disruptive risks that are imaginable not just imminent, evident, or probable; and to measure them against systemic vulnerability and the consequences should they manifest themselves.

Without disciplined approaches for identifying and assessing risk then government, businesses, and communities can’t hope to achieve the “resilience” necessary to survive and thrive in today’s extremely hazardous environment and competitive economy.

RESILIENCE

The events of 9/11 and other natural disasters teach us that “resilience” is not defined merely by the quality of a response when disruption or disaster strikes. Rather, “resilience” is a proactive cycle of preparedness with a set of mutually reinforcing processes.

It begins with the prevention of emergencies by proactively deterring hazard and establishing proper defenses as far
from the core of operations as possible—an imperative requiring effective early warning mechanisms. Two, it encompasses the mitigation and containment of damage and cascading ill-effects from the onset of a problem through resolution. Three, it includes fostering the ability to maintain continuity of operations and to recover swiftly and fully. Finally, it demands constantly capturing lessons learned and feeding them back into the system in a virtuous cycle of continuous improvement. Here again we ask ourselves the tough question, the answer to which is dubious. Are we applying the lessons of 9/11 to dynamic threats materializing before us such as cyberattack, bioattack, commercial espionage, state capitalism, the conditions which foster radicalism, and so forth.

Successfully performing each duty in the cycle requires checking the box on a set of common fundamentals. Obvious though they might be, they were lacking in the lead-up to the 9/11 attacks and its uncertain how well we have fully incorporated lessons learned across society:

**SYSTEMIC KNOWLEDGE** Those responsible for the “resilience” of a system (whether it’s national, governmental, commercial, or other) must intimately know each of the organization’s discrete human, infrastructural, and process elements. This entails having a keen understanding of each discrete element’s function; its significance to the whole; how it might fail, become obsolete, gamed, disrupted, or destroyed; and the systemic consequences of component failure. Gaining such insight requires rigorous systems analysis, independent testing of vulnerability (often referred to as “red teaming”), continuous evaluation of the operating environment, and gaming internal and external threats.

**PLANNING** Each aspect of the cycle must be supported by intelligent planning. This means establishing well-conceived strategic, operational, and tactical priorities, policies, procedures, and protocols that build resilience. The failure to plan whether for threat prevention, system defense, or response and recovery is a gamble with potentially existential consequences.

**RESOURCING** Of course, if planning is to bear fruit then the measures it proposes must be sufficiently resourced. In austere times proper resourcing presents an enormous challenge but as Thomas Edison tells us, “vision without resources is hallucination.” Priorities must be set. This requires risk-assessment that takes into account more than the probability and our vulnerability to a threat. Consequences must be considered. Prioritizing in times when public budgets are overstretched and private margins are thin is essential. It implies a new line in the formula previously mentioned to guide decision making—risk multiplied by consequence equals priority.

Protecting ourselves against highly probable but low consequence risks at the expense of those that are less probable but highly consequential is out of step in an environment when adversaries are more ruthless, their imaginations are more fertile, and their capabilities expand by the day.
Finally, in building resilience against dynamic modern threats, organizations must realize that there is strength in numbers. In most cases, risk exposure is broadly shared, and the effectiveness of successful prevention, mitigation, and recovery is significantly enhanced by robust partnerships that yield efficient economies of scale. Internal and external teaming is mandatory for bridging dangerous stovepipes, ensuring the regular sharing of critical information, and collaborating to remain strong and bounce back fast when emergency strikes. This reality is very much at the heart of NSPD 51.

The attack on America’s civil aviation security system and the cascading effects of the catastrophe point not only to the strategic prerequisites above but to operational imperatives as well. Four stand out:

- Security measures must be layered so that a threat must defeat multiple lines of protection, exponentially reducing the probability it can harm.
- Critical functions must have redundancy so that single point failure of an operational element or security measure can’t induce systemic failure.
- A system’s critical components must be isolable so, where possible, damage can be firewalled.
- Resiliency plans, methodologies, and measures must be agile and adaptive so that systems can cope with a dynamic environment in which circumstances, threats, opportunities, and countermeasures are constantly changing.

CONCLUSION

Each of these strategies and requirements are necessary to our security. Every leader in the public and private sector needs to survey the checklist to see how the systems for which they are responsible match up and apply the lessons learned, lest we be required to relearn them by harsh new experience.

In doing so, our society mustn’t lose sight of the fact that we will never live in a riskless world. We wouldn’t want to, because it will mean we have lost our freedom; but there is much we can and must do to reduce the probabilities of catastrophic events and bolster our capacity to carry on no matter the circumstances. This requires we learn another lesson of 9/11—perhaps its most critical and enduring—that the heart of resilience is character. That is, the unyielding personal and communal resolve to survive and thrive regardless of the circumstance or obstacles. This indispensable element is our most potent preventative. The more adversaries and competitors perceive our resilience to threats—in our systems but most of all in our spirit—the less likely they are to challenge us or to succeed.

We have much work to do in enhancing the resilience of our country, communities, enterprises, and ourselves. The core of that capability will remain our unbreakable will. It’s the heart and soul behind the responsibility to “Never Forget.” We haven’t. We mustn’t. We won’t.

John Raidt serves as a Scholar at the U.S. Chamber Foundation, the Advisor to the Chairman of the U.S. Chamber of Commerce, and as a Senior Fellow at the Atlantic Council. Raidt has over 21 years of public policy experience, including national and homeland security, energy, the environment, and natural resource management issues. He has served as a professional staff member of three national commissions, including the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), the Commission on the National Guard and Reserves, and the Independent Commission on the Security Forces of Iraq. In 2008, Raidt served as Deputy to General James L. Jones (USMC-Ret.), Special Envoy for Middle East Regional Security, focusing on resolution of the Israeli-Palestinian dispute. He has also worked as a senior staff member in the U.S. Senate, including as the Legislative Director for U.S. Senator John McCain and Chief of Staff of the U.S. Senate Committee on Commerce, Science and Transportation.