Measuring and Managing Systemic Resiliency

by J. Michael Barrett[1]

Choosing where to focus limited resources is never easy but it is nonetheless necessary. While in the past decade we have gotten better at managing routine risks, we cannot lose sight of the fact that certain key nodes of our economy are ultimately more important than others. Identifying and ensuring the survivability of the systems these nodes support is the essence of a focus on resiliency, and it remains today perhaps the least well managed form of risk we face.

Background

The United States thrives on global trade, economic opportunity and extremely high levels of consumption. Consider that with less than 5% of the world's population the U.S. consumes some 25-30% of total resources. While that may not be equitable, it is an undeniable part of our relative per capita wealth. Protecting the American way of life therefore means ensuring the interdependent critical infrastructure (CI) systems that enable global trade are able to continue operating, come what may. It therefore follows that the homeland security community's most important job in today's resource-constrained environment is to find effective and efficient ways to reduce, manage, or otherwise deal with the potential impacts of catastrophic events upon those systems that ensure the secure and free flow of commerce both domestically and internationally.

Simply put, *we should focus first on addressing catastrophic failure and ensuring we survive worst-case scenarios and unforeseeable "black swan" disruptions.* Recent work in this area centers on creating practical approaches to protecting CI and promoting overall systemic security by protecting what matters most. It takes a bottom-line approach to ensuring the survival and operation of the system – and as such compliments and completes traditional risk management approaches by ensuring the ability to enact pre-event safeguards that help manage catastrophic events and minimize CI impacts.

Where Current Risk Models Fall Short

Risk models used in homeland security are almost uniformly *probabilistic* in their approach, meaning they emphasize estimated likelihood (or 'probability') as their first step in examining adverse events and how to allocate resources to minimize overall impacts. When it comes to today's hyper-complex systems, however, *by design these models are forced to use assumptions with a degree of precision that is illusory at best*. This is because most modelers believe that through an alchemy of estimation, historical analysis, and complex *Monte Carlo* and other simulations they can divine a number close enough to be, for all practical purposes, 'exactly correct'. In turn, these models are believed to produce answers that are 'exactly correct'. This approach works well enough where immutable laws of physics dictate cause and effect or where linear changes are phased in over time and historical precedents adjusted to reflect today's reality. Yet probability-based risk models are of much less value in today's environment of radical changes across the global system.

---

[1] A former Fulbright Scholar, Naval Intelligence Officer and Director of Strategy and Resources for the White House Homeland Security Council, Mike is a risk and resiliency expert with the Washington, DC-based consultancy Diligent Innovations. He may be reached at mbarrett@diligentinnovations.com.

Why Resiliency Works Better

It is becoming clear that there is a need to complement traditional risk models with "resiliency models", or models examining not the likelihood and severity of an event but rather how best to minimize the cascading impacts of an event and ensure that the Critical Infrastructure system continues to operate at a minimally acceptable level. This approach maps out the interconnectedness and cascading effects of the loss of any given system upon the rest of the CI systems.

This approach to measuring and managing resiliency is comprised of three sequential phases. The first examines CI systems in terms of vulnerability, criticality, and interdependence. Often conducted at the regional level, this process uses scenarios and expert elicitation to model the role of various CI systems in that specific location. Phase two of the process is to establish *minimally acceptable throughputs* for specific CI systems and identify where bottlenecks occur not only during normal operations but also during a given type of disruption. Finally, in the third phase experts assess gaps and seams by focusing on four main thrusts: Decreasing an event's likelihood of occurrence; Increasing the given CI sector's overall redundancy/capacity; Addressing regulatory and governance issues that limit flexibility and resiliency; and Improving substitute systems that can provide similar services if the primary system falters.

Of note, this approach enables rational resource allocation in terms of small pre-event investments that minimize the down side of a future catastrophic event. While many of the solutions will impose small routine costs, these costs are akin to insurance premiums where daily costs are balanced against how well pre-event investments enable better post-event operations. Furthermore, this resiliency model relies less on elegant mathematical formulas and more on expert elicitation about experiences in having worked with disrupted systems and which ones are most important at specific levels of functional capacity (i.e., is electricity disruption a problem if there are adequate back-up generators, or can alternative routes be used for transporting certain hazardous materials, etc). While this qualitative approach makes some mathematicians uncomfortable, it allows for clarity of assumptions and also for real-world practitioners to more readily follow their inputs and the transparent process by which systems are evaluated and ranked, and it also forces reality into the models.

Conclusion

Without actively measuring and managing resiliency the only option when allocating resources is to draw out discrete, singular risks and protect against either or both the most likely and the worst of them. However, such approaches require a precision which is just not possible in today's world of rapid change and broad-ranging threats where it is not sufficient merely to strengthen the weakest points or to spread resources thinly across every possible point of attack or failure. Instead, we must determine what is critical to ensuring the interconnected CI systems are flexible and durable enough to continue to operate at acceptable levels and then take measures to implement solutions that address current gaps. We can do this by using new models that enable us to better measure and manage systemic resiliency.