George Mason University

Macroprudential Policy in the Information Technology Sector

Managing emergent systemic risks in the Information Technology industry

Paul Andrew Kavitz
paul@kavitz.com
4/10/2011

Executive Summary

In the midst of the U.S. subprime contagion (Dodd, 2008) and the largest economic crisis since the Great Depression, attendees of the 2008 Plenary Session of the Critical Infrastructure Protection Advisory Council reviewed risks to the seventeen infrastructure sectors identified as critical to national security, national economic security, public health and safety (Office of the Press Secretary, The White House, 2003). In the concluding remarks for the banking and finance sector, in spite of the global financial meltdown, sector leadership advised of no significant unmitigated risks (Critical Infrastructure Partnership Advisory Council, 2008).

This claim epitomizes the current perspective towards critical infrastructure protection in the US Federal government. This perspective is a reaction to national threat categories freshest in political memory: concern with intentional terrorist threats following the attacks on September 11, 2001, and with natural disasters following Hurricanes Katrina and Rita of 2005. The subprime mortgage crisis of 2008 showcases a new category of system-wide risks that emerge from the collective behavior of individual institutions. This new category of threats should be included within national infrastructure assurance plans.

A key response to the subprime contagion within the banking sector is in the form of macroprudential policy: policy seeking to improve resilience of the entire system, not just the institutions within that system. The need for macroprudential policy is not confined to banking and finance however; it applies to all system-based infrastructure sectors including communications, energy, food and agriculture, and information technology. This paper demonstrates the existence of systemic risks to information technology to justify extension of macroprudential policy approaches to this sector. This risk described here arises from an aggregate decline in backup power capacity across U.S. data centers, yielding increased vulnerability year-on-year to sustained power outages.

In light of the recent global financial crisis and the evidence that systemic risks exist also in the information technology sector, critical infrastructure stakeholders should re-focus efforts to develop macroprudential policy approaches that manage system-wide risks not just risks to individual enterprises. By taking action now, Federal authorities may help our nation better survive further systemic shocks.

Problem Statement

Information Technology (IT) is a complex and dynamic infrastructure enabling operations in the modern enterprise across all sectors deemed critical for our national and economic security. The pervasive public policy focus on risk in this sector focuses upon the intentional theft or misue of information.

According to the Government Accountability Office (Langevin, 2008) , over 70% of the enforceable private-sector IT regulations pertained to information access control and privacy, with the balance requiring general risk management or protective security measures within the private-sector enterprise. The GAO review showcases a microprudential orientation to regulation (mitigating risks to individual enterprises) and an emphasis upon intentional mailicious acts of information theft or sabotage. This orientation also pervades the National Infrastructure Protection Plan (NIPP) framework which tends to focus upon asset protection and typically excludes visibility into how enterprises keep essential systems functioning (La Porte, 2006).

This paper identfies one particular systemic risk to operational continuity within the US information technology infrastructure as an illustration of the blind spot created by the prevailing cybersecurity microprudential policy focus upon prevention of intentional criminal acts. Following an analysis of this case study, policy options are explored and a recommendation is made to remediate this risk and position critical infrastructure culture to develop macroprudential policy for information technology.

An Emergent Systemic Risk within the Information Technology Sector

Data centers are facilities housing computer servers required to support the complex transactions of the modern enterprise. Airline reservation and scheduling systems, supply chain logistics operations, market exchanges, and government services are but a few examples of processes which depend upon data centers to manage activity at scale.

Between 2000 and 2005, the aggregate power consumption of data centers in the United States doubled (Koomey, 2007). While economic factors also contributed to this growth, the prevailing identified cause is significant demand for large quantities of commodity servers and their supporting cooling and

auxiliary equiement. This growth trend in data center power consumption magnifies the IT sector's dependence upon, and sensitivity to service disruptions within, the electricity sector.

Data centers have always been dependent upon electricity, and local power outages are a regular occurance across the U.S., often due to weather. To mitigate this systemic risk, large data centers are typically constructed with an on-site generator capable of handling the power demands of the computer infrastructure, with enough local fuel storage to last 48-72 hours, and with fuel contracts to provide replacement fuel. Historically, this has provided sufficient buffer capacity to sustain operations in the event of regional power failures.

However, in light of the growth trends noted earlier, the buffer capacity of on-site fuel storage will have reduced in direct proportion to the increase in power conumsption at each facility. Fuel storage sufficient to last 72 hours a decade ago may last less than 48 hours today. Since facility fuel storage infrastructure has a significantly longer investment payback period than server technology, upgrades to this backup power capability are on a far longer refresh cycle than the computer server technology housed within the facility. It is reasonable to anticipate that without intervention, the aggregate trend across all US IT infrastructure is towards a reduced power buffer capacity. In civil engineering terms, facilities designed to survive the '100-year storm' will eventually only withstand a 10-year storm event.

With the complexity of modern enterprises, the presence and consequences of this trend are likely invisible to most IT executives. Even if the executive were aware of this trend and the potential incremental increased risk to failure, it is unclear whether organizational incentives are sufficiently strong to justify risk remediation. Many companies struggle to adopt a risk management approach to identify and prioritize risk mitigation measures for IT security, and those that do may not easily or accurately estimate probability or duration of outages within the electricity grid outside of their direct control. Net result: the individual enterprise typically does not address this issue.

Describing this using an interdependence analytic framework (Rinaldi, 2001), we can say the backup power buffer intervenes a tight coupling that continues to tighten. Failure of the dependent electricity infrastructure and this buffer reserve would create an instantaneous cascade of a regional power failure to business operations in any other critical sector dependent upon the impacted data centers, which would likely escalate the failure beyond the regional scale of impact caused by the initial outage.

A service failure within the energy/electricity sector may exceed in duration the threshold of tolerance of numerous data centers simultaneously as a result of the annual decline in backup power capacity. This simultaneous trend across numerous individual actors creates an emergent endogenous risk to the system overall. This risk category that 'emerges from within' stands in stark contrast with the prevailing cybersecurity focus upon deterring exogenous risk.

Policy Options

Business as Ususal Option

There is always uncertainty of a significant failure in a particular time frame. If no policy action is taken, a regional failure in the power grid may not endure long enough to overwhelm the dwindling buffer capacity of data centers. 'Green' efforts to improve energy efficiency of data centers may temper or even reverse this growth trend over time (Kavitz, 2009), though evidence of this is not yet seen. Nevertheless, unmanaged emergent systemic risks in the IT sector will eventually transpire, resulting in a significant economic impact and leaving government and private-sector institutions to respond to the aftermath.

Tactical Response: Introduce mandatory standard for data center vulnerability

The US Federal Government could respond tactically to the data center vulnerability described within this paper through the introduction of mandatory standards. IT data center power efficiency standards to reverse the growth trend would be the most advantageous in terms of cost and long-term benefit, however these are problematic to develop and enforce. A more feasible approach would be to impose a mandatory on-site fuel reserve requirement for a specified number of hours. This requirement could be tiered based on criticality or size of the data center operation.

While development of the standard would be relatively straightforward and simple to audit, the creation and funding of a regulatory body to monitor this trend would be very costly for a single standard. Leveraging existing compliance bodies would be more feasible, but would not be comprehensive, as suggested by the absence of mandatory standards or regulation of IT in eight of the eighteen critical infrastructure sectors (Langevin, 2008).

Strategic Response: Develop macroprudential policy for systemic risks

Calls have emerged in the aftermath of the global financial crisis of 2008 to re-orient the regulatory framework within the banking sector towards a system-wide focus (Clement, 2010). This macroprudential policy approach addresses risks that may seem small to the individual enterprise, but that are large when considered in aggregate (Bank of England, 2009).

In the next iteration of National Infrastructure Protection Plan (NIPP), emphasis could be placed upon macroprudential policy for all system-based infrastructures including banking and finance, communications, energy, food and agriculture, and information technology. The sector-specific plans (SSPs) for these industries should extend beyond the microprudential recommendations for risk management of individual enterprises and include macroprudential analyses and policies to improve system-wide resilience.

Since adherence to the NIPP and SSPs is purely voluntary, invigoration of these plans serves mainly to raise awareness of these risks across the public-private partnership stakeholders. Legislation should also be introduced in parallel that empowers system-based sector regulatory authorities to develop and enforce macroprudential regulations within their sectors. These authorties would include the Department of Treasury for banking and finance, the Department of Agriculture for food and agriculture, the Department of Energy for energy, and the Department of Homeland Security for IT and communications.

This option would have a larger financial cost to implement, which would be difficult in the current climate of austerity, but this has the highest risk mitigation benefit. The public attention generated by the subprime mortgage crisis may allow lawmakers to leverage this interest to stabilize the economy and extend macroprudential legislation to prevent similar systemic risks in other key sectors such as IT.

Policy Recommendation

As shown in the example of systemic risks to IT data centers, the need for a macroprudential approach is not limited to banking. The communications, energy, food and agriculture, and information technology sectors should leverage the policy approach being developed for the banking and finance sector. So that we might avoid systemic failures within the information technology sector, the author recommends adopting the strategic policy option outlined above.

Bibliography

Bank of England. (2009). *The role of macroprudential policy.* London: Bank of England.

Clement, P. (2010, March). The term "macroprudential": origins and evolution. *Bank for International Settlements Quarterly Review* , 59-67.

Critical Infrastructure Partnership Advisory Council. (2008, July 30). 2008 Plenary Session. Washington DC.

Dodd, R. a. (2008). Outbreak: U.S. Subprime Contagion. *Finance and Development , 45* (2).

Kavitz, P. K. (2009). *Green Energy for Information Technology Data Centers.* Arlington: New Voices in Public Policy.

Koomey, J. G. (2007). *Estimating Total Power Consumption by Servers in the U.S. and the World.*

La Porte, T. M. (2006). Managing For the Unexpected: Reliability and Organizational Resilience. In P. E. Auerswald, *Seeds of Disaster, Roots of Response* (pp. 71-76). New York: Cambridge University Press.

Langevin, J. R.-L. (2008). *Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors.* Washington DC: U.S. Government Accountability Office.

Office of the Press Secretary, The White House. (2003, December 17). *Homeland Security Presidential Directive 7.* Retrieved April 9, 2011, from Department of Homeland Security: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

Rinaldi, S. M. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine , 21* (6), 11-25.

U.S. Department of Homeland Security. (2009). National Infrastructure Protection Plan (NIPP). Washington DC: US Department of Homeland Security.