A Practitioner’s Perspective on Ops Risk in the Plumbing

OFR-FSOC Annual Conference

Caryl Athanasiu
Chief Operational Risk Officer and Head of Operational Risk
Wells Fargo & Company

© 2014 Wells Fargo Bank, N.A. All rights reserved.
“Operational risk is the risk of loss resulting from inadequate or failed internal processes, people or systems, or resulting from external events.”

– Basel II definition

“It is the kitchen sink of risk.”

– Caryl Athanasiu
Failures in operational risk can cause or amplify financial shocks and contagion

- Primary systemic players of interest are:
  - Financial market utilities (FMUs) involved in clearing and settlement for payments and securities
  - Financial institutions with dollar and/or transaction volume concentration

- Extent of systemic disruption will be most influenced by:
  - Which players are impacted and their relative roles in the whole
  - How long it takes to restore “business as usual”
  - Extent of the asymmetry created

- The most relevant operational risks are
  - Cyber / information security
  - Technology changes
  - Resiliency
  - Third party management
  - Orderly recovery
Who should keep you up at night?

- Focus on transaction volume and dollars
- Evaluate movement holistically -- direction, timing, concentrations, potential blockages
- Examples of FMUs include Fedwire, CHIPS, DTCC, CME, ICE, LCH
- Examples of institutions include BONY, State Street
What will make the biggest systemic mess?

- Partial disruption of clearing and settlement utility and/or of a concentrating institution
  - Entire system down hard impacts everyone equally; likely wait for business as usual provided the outage isn’t protracted.
  - Non-concentrating institution hard down results in limited impact
  - Partial disruption creates asymmetry, confusion and uncertainty; requires many decisions (often with limited information); and can lead to unpredictable outcomes and messy clean-up

- The longer the disruption, the greater the uncertainty and the more downstream impacts as everyone tries to protect their interests
  - 24 hours is manageable; beyond 48 hours decisions will become increasingly conservative

- Asymmetry will exacerbate already existing issues in counterparty management
How will it happen?

- **Info/cyber security breach**
  - Actors include hactivists, terrorists, nation-states
  - Threat vectors include malware, social engineering and internals (Snowden effect)
  - Data destruction is a real concern

- **Technology failure**
  - Poor design
  - Insufficiently robust testing (negative testing, regression testing)
  - Complex application inter-dependencies
  - Complex environments and environmental inter-dependencies
  - No clear owner, lack of end-to-end project management

- **Insufficient Resiliency**
  - Mirroring and hot back-up increases likelihood that malware will spread quickly.
  - BCP more important than ever – but needs to be faster
  - Fallback plan isn’t enough – must be executed well

- **Third Party surprise**

- **Poorly executed recovery**
Questions