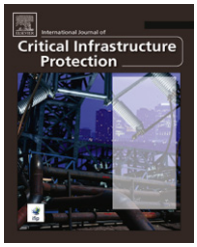
available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip



Assessing operational risk in the financial sector, using interdependency metrics

*Tyson Macaulay**

Bell Canada, 160 Elgin Street - 24th floor, Ottawa, K2P 2C4, Ontario, Canada

ARTICLE INFO

Article history:
Received 1 May 2008
Accepted 6 August 2008

Keywords:
Financial institutions
Interdependencies
Metrics
Operational risk

ABSTRACT

Alternatives are needed to using intuition as the dominant approach for assessing critical infrastructure interdependencies. Since there is no single, measurable unit that accurately reflects interdependencies between critical infrastructure sectors, an interdependency metric must be a composite of measurable elements related to the dependency of one sector on another. This paper defines and applies quantitative and qualitative metrics, derived from the US financial sector, to assess its interdependencies with other sectors. The quantitative metric engages econometric data about the value of goods and services flowing between the financial sector and other critical infrastructure sectors. The qualitative data dependency metric is derived from financial sector executives' opinions on the criticality of data and information flows between their companies and other sectors. The econometric and data dependency metrics are shown to possess strong correlations, and a composite interdependency metric is generated from the two metrics. The composite metric is then applied to understand the cascading impacts of disruptions in the financial sector.

1. Introduction

Intuition, if it were a person, would be Instinct's egghead cousin. Intuition is thought applied to instinct. Intuition is the path of least resistance when comprehending complex issues [11]. Instinct and intuition are certainly valuable when dealing with fire, snakes and heights, but using them to manage operational risk is a little different. Managing operational risk associated with critical infrastructure (CI) threats is largely based on intuition at this time.

This paper describes a metrics-based approach to understanding internal and external risks associated with critical infrastructures, and discusses possible vulnerabilities and threats to the US financial sector and financial institution assurance [9]. The metrics and methodology presented are useful for managing a variety of risks: operational risk based on supply chain, compliance and regulatory risks; market risk associated with reputation, brand, competitive differentiation and client support; and credit risk related to ratings and changes in the cost of capital.

Operational risks within, and between, the various CI sectors are complex issues. Grouped as ten sectors, these include financial services, telecommunications, energy, health, transportation, safety, food, water, manufacturing and government (regulatory and social services) [2]. Analytical approaches applied to CI interdependencies and the related operational risks engage methodologies such as threat risk assessment (TRA) that typically focus on discrete assets. For instance, what are the possible vulnerabilities, threats and risks associated with this IT application? This generator? This building? Such an assessment technique does not scale, because the resulting data set is usually incompatible for aggregating the results obtained for individual assets. Efforts to assess CI interdependencies through "close-up" TRAs stall and collapse under their own weight.

* Tel.: +1 613 292 9132.
E-mail address: tyson.macaulay@bell.ca.

1874-5482/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2008.08.008

A second approach to CI interdependency analysis is to use table-top exercises, where CI stakeholders walk through hypothetical disaster or crisis scenarios. These exercises are excellent for testing recovery plans and training staff, but they produce few metrics, and those that are derived are related to the specific threat/risk/crisis scenarios played out.

Using intuition to establish policy and plans around CI interdependency risk management is dangerous, because intuition is biased by one's frame of reference. Government, for instance, has a different frame of reference than the private sector, especially with regard to financial institutions. Government entities frequently consider financial services to be an infrastructure that has a lower priority than energy, transportation, telecommunications and health, especially when macro-level risk management decisions are made based on intuition. A government entity would consider energy to be crucial to remaining operational and transportation security as critical to personal safety. On the other hand, an executive with a private sector entity would argue that remaining profitable is just as important as being operational. There is little point in being operational if goods cannot be sold and services cannot be metered—it is not possible to simply give them away.

From the perspective of a financial institution, this gap between the intuition of government policy makers and empirical metrics represents a fundamental operational risk. Indeed, in some jurisdictions, policy may not support operational reality in times of crisis, and the impacts could be amplified, when they could have been dampened.

2. Operational risk metrics

Using input–output econometrics to assess relationships among industries (in our case, patterns of infrastructure interdependencies) has its roots in the work of Leontief [8]. Leontief was the first to show how a matrix representation in the input–output model of economics can be used to estimate the effect that changes in one industry can have on other industries, as well as changes introduced by consumers, government and foreign suppliers of the economy. Haimes and colleagues [7] have assessed CI interdependencies using input–output econometrics. However, their work focuses on specific industries, rather than infrastructure sectors, and does not attempt correlation with other independent variables related to interdependencies.

Data dependency is a second metric that can be applied to CI interdependency analysis. Using data dependency metrics associated with data and information flows to perform interdependency analysis has its roots in electronic warfare and information operations where resources are applied to gathering and assessing observed communications patterns among counterparties [5]. Information assurance, a subfield of the information operations discipline, deals with the properties that define communications among different entities and assets. By understanding these properties, an organization gains information superiority and is in a better position to defend its assets or exploit weaknesses in enemy defenses [3]:

"When it exists, the information available to commanders allows them to accurately visualize the situation, anticipate events and make appropriate, timely decisions more effectively than adversary decision makers. In essence, information superiority enhances commanders' freedom of action and allows them to execute decisions and maintain the initiative, while remaining inside the adversary's decision cycle. However, commanders recognize that without continuous information operations designed to achieve and maintain information superiority, adversaries may counter those advantages and possibly attain information superiority themselves."

Understanding data dependency is a fundamental component of information superiority for infrastructure owners and operators in the context of interdependencies, and the ability to prevent, detect, respond and recover from cascading impacts in CI sectors. The metrics discussed in this paper are representative of normal operating conditions by design. While metric sets that describe operating vulnerabilities and risks under crisis conditions are useful, a distinct metric set is required for each crisis or risk. Maintaining such metrics is not scalable. Instead, metrics under normal operating conditions can be applied to expose vulnerabilities that manifest varying degrees of risk under all-hazards risk management. Similarly, risk practitioners can apply metrics from normal operating conditions as a baseline, against which the risk associated with a specific event and organization can be assessed.

Applying metrics to critical infrastructures in this manner is new; however, much work remains to be done. The metrics discussed here are by no means definitive or flawless. Rather, they are intended to establish a starting point for assessing operational risks associated with critical infrastructures, where metrics are used in the assessment as opposed to intuition and guesswork.

3. Inbound and outbound metrics

CI metrics associated with operational risks can be categorized as "inbound" or "outbound". Inbound metrics indicate the level of assurance required in the goods and services consumed from other sectors. Outbound metrics indicate the level of assurance placed on goods and services produced by the sector for consuming sectors. Therefore, an "inbound dependency" captures the degree to which a CI sector needs other sectors' goods and services. An "outbound dependency", on the other hand, expresses the degree to which other sectors need a given sector's goods and services. Inbound metrics provide insights into a sector's possible supply chain vulnerabilities, while outbound metrics provide insight into the threats a sector may pose to other sectors.

4. Econometrics and operational risk

CI sectors in the United States consumed more than $4.7 trillion in intermediate inputs from a national GDP of $12.4 trillion in 2005, $2.6 trillion of this amount flowed between sectors via supply chain relationships [1]. Industries in the US