CAPCO

Operational

Safety in Numbers: Toward a New Methodology for Quantifying Cyber Risk

Sidhartha Dash, Peyman Mestchian

Journal

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

APEX 2016 AWARD WINNER

FINANCIAL TECHNOLOGY

Download the full version of The Journal available at CAPCO.COM/INSTITUTE

#44
11.2016

EMPOWERING THE [FINANCIAL] WORLD

Pushing the pace of Financial Technology, together we'll help our clients solve technology challenges for their business – whether it's capital markets in Mumbai or community banking in Macon.

We leverage knowledge and insights from our clients around the world:

20,000 clients in towns everywhere are becoming more efficient, modern and scalable.

27 billion transactions processed help solve clients' challenges — big and small.

$9 trillion moved across the globe in a single year empowers our clients' communities to build storefronts, homes and careers.

55,000 hearts and minds have joined forces to bring you greater capabilities in even the smallest places.

Empowering the Financial World

FISGLOBAL.COM

FIS

Journal

The Capco Institute Journal of Financial Transformation

Recipient of the Apex Award for Publication Excellence

WHAT ARE THE DRIVERS AND DISRUPTIONS THAT DETERMINE INNOVATION AND PROSPERITY?

CAN EVERY PROBLEM BE SOLVED WITH A QUESTION? YES, BUT NOT EVERY QUESTION HAS A SINGLE ANSWER.

The Munk School's Master of Global Affairs program is developing a new class of innovators and problem solvers tackling the world's most pressing challenges.

> Tailor-made, inter-disciplinary curriculum delivering the best of both an academic and a professional degree.

> Access to world-leading research in innovation, economic policy and global affairs.

> International internships with top-tier institutions, agencies and companies that ensure students gain essential global experience.

COME EXPLORE WITH US

BE A MASTER OF GLOBAL AFFAIRS

MUNKSCHOOL.UTORONTO.CA
MGA@UTORONTO.CA

MUNK SCHOOL OF GLOBAL AFFAIRS

UNIVERSITY OF TORONTO

Financial Technology

Operational

Transformational

Safety in Numbers: Toward a New Methodology for Quantifying Cyber Risk

Sidhartha Dash – Research Director, Chartis Research
Peyman Mestchian – Managing Director, Chartis Research

Abstract
For financial institutions, safeguarding against cyber attack is now about more than just protection – increasingly it means managing cyber risk effectively across the organization. In modern, diffuse networks, such as those in most large banks, allocating risk across multiple network nodes (defined here as IT infrastructure, assets, and points of access) is vital to developing comprehensive strategies for managing cyber risk. Central to this is quantifying the risk. We believe that current scoring and statistically oriented models for cyber risk quantification are based on flawed assumptions, and fail to answer several key questions. We propose a methodology for quantifying cyber risk that incorporates the physical network in the organization, and the behavior and characteristics of individuals and processes in that network – including the actions they take to mitigate cyber risks. In addition, as allocating and attributing risk are central to modifying the behavior of institutions and individuals, enabling organizations to easily attribute and allocate risk to specific nodes and edges of the network is central to our method. This paper provides a high-level summary of the approach, and highlights how it differs from, and improves on, existing models of cyber risk quantification.

INTRODUCTION: BEYOND PROTECTION

Financial institutions (FIs) are waking up to cyber risk, but often treat it as less important than other types of risk. They tend to concentrate on cybersecurity, or protection: safeguarding information by preventing, detecting, and responding to cyber attacks, and identifying, assessing, and prioritizing potential threats. But to protect against the growing number of cyber attacks worldwide, they now have to manage their cyber risk.

FIs have standards[1] for dealing with cyber risk, and often apply them widely. But these standards, most of which are fairly basic, are really only a starting point. By focusing largely on cybersecurity, FIs are neglecting several vital elements of managing cyber risk: locating areas of high risk (systems, processes, and so on), identifying the cause of that risk, quantifying the risk, and developing proper insurance and capital adequacy strategies to cope with it. Being able to accurately allocate and attribute cyber risk is essential if FIs and individuals are to change the way they deal with it.

We define "cyber risk" as the risk of losses due to the failure or lack of cybersecurity systems. Crucially, cyber risk is complex – multidimensional, dynamic, and often hard to manage.

This is distinct from cybersecurity. As with many terms in risk management, definitions of cybersecurity vary. At a basic level, cybersecurity is the technology and processes used by an organization to protect its IT systems from malicious cyber attacks. Many definitions go further, to include protecting systems from any damage or unauthorized data access, whether it is malicious or the result of errors and system failures.

The National Institute of Standards and Technology (NIST) defines cybersecurity as "the process of protecting information by preventing, detecting and responding to attacks." We have expanded on this definition, by building on concepts developed by the Federal Financial Institutions Examination Council (FFIEC). In our definition of cybersecurity, we broaden the concept to consider issues around data privacy and breaches that disrupt an FI's operations, business, and reputation.

Box 1 – Cybersecurity and cyber risk

MEASURING THE THREAT IN MODERN NETWORKS

Diffusion is a central feature of modern networks: how people behave in the digital world is no longer just about them. A data breach at a credit card company does not just affect the company, but its customers, its vendors, and its customers' vendors. Similarly, when a hacker or cyber criminal targets a network or individual's computing assets for a distributed denial-of-service (DDoS) attack, the breach does not just affect the owner of the hijacked asset. Individuals and targets with little connection to the victim can suffer too, simply because they were unfortunate enough to be on the same network. Cyber risk is shaped by the behavioral and commercial characteristics of all the components in an organization, across increasingly complex networks and architectures of "nodes," which include the FI's assets and its network access points.

To manage cyber risk effectively, organizations must first be able to measure it. Existing methods for quantifying cyber risk tend to calculate a value for cyber risk across an FI's entire organization. They also often rely on small amounts of data about infrequent cyber events, which not only increases the risk that datasets are skewed by a single extreme event, it also relies on past events to calculate future losses.

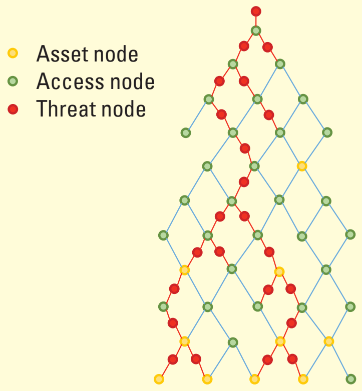
By quantifying cyber risk at a more in-depth level, FIs can manage it in a more optimal and flexible way, targeting specific areas, processes, and people. The data they gather can also help in stress-testing IT systems, and in meeting regulators' demands for information about cyber and data security.

[1] Among them the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Technology 27001 and 27002 framework (collectively ISO 27001/27002); and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (the "NIST Framework").

A NEW APPROACH

To address the limitations of current approaches, we have developed a new methodology for quantifying cyber risk. It uses an FI's physical IT network as a base to create "exposure network," via which cyber risks can be attributed to specific network locations. The methodology enables FIs to develop a customized approach to assessing and quantifying cyber risk. It scales well, and can be used to calculate cyber risk for networks of any size.

It employs tree-like structures to represent attacks on a system (see Figure 1). "Attack trees," which consist of multiple levels of connected nodes, are combined to create an exposure network. The overall network structure we use is derived from network monitoring and analysis systems (such as NetFlow), and takes into account IT infrastructure, threats, mitigating factors (such as antivirus and malware detection software), and assets (such as confidential records and customer data).



Note: A "threat node" is a node with a resident threat that could be transmitted to other nodes.
Source: Chartis Research

Figure 1 – A simple attack tree, showing the route of a potential cyber threat through a network of assets and access points

EFFECTIVE CYBER RISK MANAGEMENT: COVERING ALL THE ELEMENTS

For most firms, suffering a cyber breach is not a question of if, but when; or even how often. To operate effectively and stay stable – a state now increasingly demanded by law – they must manage their cyber risk. Table 1 summarizes the key elements of cyber risk management.

By considering all aspects of cyber risk, firms can:

- Identify potential system weaknesses (and evaluate them).
- Identify the specific areas most affected by cyber risk.
- Quantify risk in various locations.
- Use insurance (where relevant) to cover high-risk areas.
- Select and design appropriate strategies for managing cyber risk.
- Include cyber risk management in broader strategies and frameworks linked to wider operational risk (including financial crime, reputational risk, and customer relationship management), liquidity and credit risk, enterprise stress testing, and capital adequacy.

The current approach taken by most FIs is shown in the shaded areas of Table 1. So while they identify potential threats, and assign an overall value to them, they neglect the crucial elements of attribution, insurance, strategy, and quantification.

Cyber risk management strategy and framework	**Risk identification**	**Risk assessment and evaluation**	**Attribution**	**Quantification**	**Insurance**	**Ongoing monitoring and auditing**
			(locating areas of high cyber risk and identifying the cause of that risk)	(measuring risk)	(insuring against losses from cyber attacks; mitigating the cost, if not the event)	

Note: the shaded areas show most firms' current approaches, which focus more on identifying and evaluating risk, rather than managing it.

Source: Chartis Research

Table 1 – The key elements of cyber risk management

QUANTIFYING CYBER RISK: WHY AND HOW

Quantification is a key pillar of cyber risk management – put simply, you can't manage what you don't measure. And not only does quantifying cyber risk accurately help FIs manage it, it also enables them to answer some key business questions:

- How can we persuade the board to spend money on cyber risk management before it is too late, rather than waiting till after we suffer a catastrophic cyber attack?
- Where should we spend our budget for cyber risk management (software, hardware, training)?
- Cyber risk management is an expanding industry, but how do we know we have spent our money wisely?
- How do we ensure that employees and other stakeholders take cyber risk management seriously?
- How do we ensure that once risks are identified, they are attributed to the correct cause?
- How do we stress-test IT systems?
- How do we accurately calculate the impact of cyber risk on our operational risk capital?

VULNERABLE TO ATTACK: THE PROBLEM WITH EXISTING APPROACHES

Standard cyber risk quantification models share a problem that is common to general operational risk frameworks: they tend to be statistical methods with a very high dimensional fit and a very high sensitivity to initial conditions. Most "valuation" models provide a statistical analysis of the whole organization to give a single, firm-wide value for cyber risk. A finer level of scrutiny is either non-existent, or poorly handled.

Existing approaches range from purely statistical analysis of incidents in the firm itself (or in comparable firms) to a more systemic analysis of the physical network structure. Popular approaches tend to focus on event statistics and frequency-based models, models that are based on the fundamental assumptions that cyber crimes are regular and repeatable. However, we believe this view is inaccurate: cyber crime is irregular, unpredictable, and constantly changing; historical cyber crime events are not necessarily a good indicator of future ones.

What is more, when FIs quantify or evaluate risk they fail to take into account an organization's network characteristics, behavioral issues, and operational and commercial characteristics.

- **Network characteristics:** connections between nodes or groups of nodes, locations of mitigating factors in the network, and the general network architecture.
- **Behavioral issues and operational characteristics:** the culture at the FI, the experience/training of its staff, and its consideration of cyber risk when it defines its processes and best practices.
- **Commercial characteristics:** the company's insurance, liabilities, contractual arrangements, etc.

Valuation models are vulnerable for a number of reasons:

- They depend on high dimensional fitting models, which are based on complex mathematics involving large numbers of polynomials.
- They depend on low-frequency events.
- They use data from past events to predict future losses (cyber crime changes relatively quickly, however, so this kind of anlysis works best with recent data).
- They use one-dimensional event frameworks, which are not suitable for complex long-running and highly compounded risks, such as cyber risk (which combines IT, business, and information risk) or conduct risk.
- They have no mechanism to link specific behavior to low-frequency events.

Developers and users of valuation models could learn much from firms in other safety-critical industries, such as energy companies – many of which have specific techniques for managing their risk. And cyber risk teams often lack the communication standards that their counterparts in market and credit risk have taken for granted, with standard quantification strategies such as Value-at-Risk (VaR) and expected shortfall.

Our new methodology looks to rectify this. By identifying the physical, commercial, and behavioral aspects of networks, we can analyze complex network behavior, and model the impact not only on the FI in question but on every entity in its information network.

TOWARD A NEW METHODOLOGY: BOTTOM-UP VERSUS TOP-DOWN

The method we propose aims to:

- Simulate how likely cyber attacks are to propagate in the presence of standard mitigants (such as anti-virus software and network barriers).
- Compute the VaR from the simulated loss distribution.

This "bottom-up" approach captures and aggregates all relevant enterprise processes, giving risk professionals a comprehensive evaluation of a firm's cyber risk exposure. It contrasts with "top-down" techniques, which consider the whole organization, and which may incorrectly identify some risks, or incorrectly estimate correlations between individual risks.

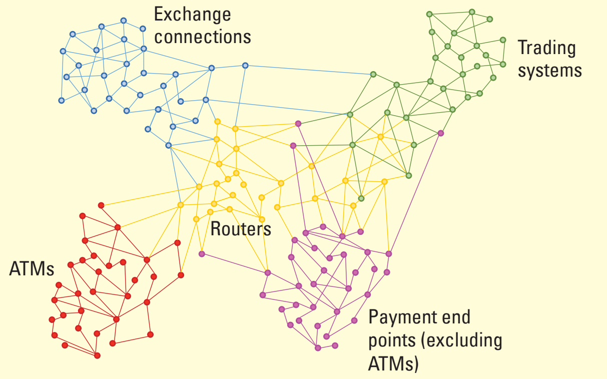
Our approach provides insight into the relative and absolute economic costs of cyber attacks, and it can operate on physical computer networks at any level of detail, and aggregate as many attack trees as required. It also allows regulators to specify benchmark or reference architectures for different lines of business (such as retail brokerage, exchange infrastructure, payment infrastructure, etc.).

EXPOSING RISK TO MANAGE RISK

Our methodology uses "exposure networks" to pinpoint and attribute risk in an FI. By combining attack trees, an exposure network identifies a network of connected nodes. Each connection between nodes has a set of properties that are distinct from the two nodes that create it, essentially breaking down overall cyber risk into smaller categories. A typical exposure network for a single FI is shown in Figure 2.

The methodology builds on the concept of exposure networks developed in a wide variety of financial markets.[2] To develop the concept, the probability of specific events is used to define the network edges and topology. Once created, exposure networks can be used to identify specific areas that are exposed to high levels of cyber risk and, through the connections to other nodes, identify whether the risk originates from other areas, or if it could spread to other connected nodes.

Exposure networks are powerful because they enable us to create more realistic networks by enhancing them with a variety of commercial, behavioral, and related characteristics. Hence, for example, we could enhance the basic sub-networks included in our methodology to include behavioral characteristics. These might include the decision to regularly run anti-virus software or modify exposure based on the availability of legal remedies. And, as we have effectively generated attack trees of unlimited depth, this allows us to model the true complexity and multidimensional nature of cyber risk.



Source: Chartis Research

Figure 2 – An example of an exposure network, in which each node represents an aggregation of multiple nodes

To test the idea that network structure affects cyber risk, we created a sample network, belonging to a universal bank with four equal divisions (retail banking, transactional banking, investment banking, and retail brokerage). The results of the analysis highlighted big differences in cyber risk VaR between the four divisions. Retail banking accounted for most of the cyber risk that our sample bank was exposed to: between 55% and 77% of the total, depending on the strength of the mitigation applied to the network.

If we assume that the universal bank held $250 bln in notional assets, the total cyber risk VaR was calculated at $234 mln, of which retail banking accounted for more than half, at $129 mln. The retail brokerage came next with $48 mln, followed by investment banking ($45 mln) and transactional banking ($12 mln).

Box 2 – Putting theory into practice

[2] Amini, H., R. Cont, and A. Minca, 2016, "Resilience to contagion in financial networks," Mathematical Finance 26:2, 329–365

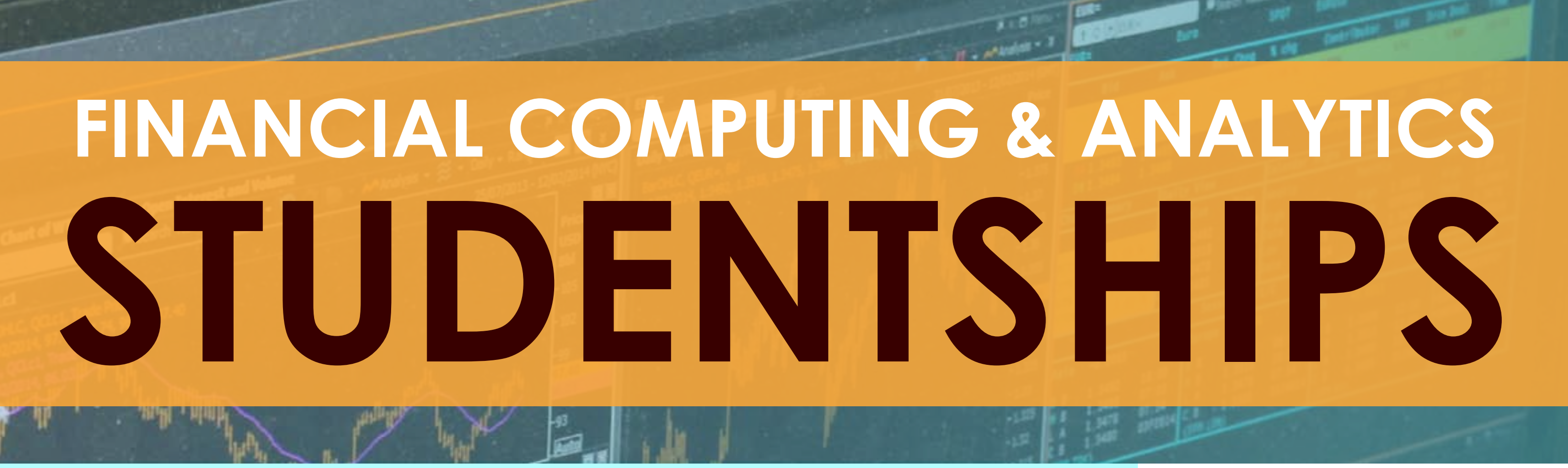
CONCLUSION

FIs already widely apply standards for cyber risk, but these are often a basic minimum, and provide only an initial structure for tackling the issue. Cyber risk is intricate and multidimensional: it depends on the physical, behavioral, and commercial characteristics of all the components of an organization, linked in a complex interconnected network. Current models for quantifying cyber risk can produce an overall value for it, but they struggle to identify the sources of risk. Ultimately, these gaps in functionality make cyber risk management solutions less effective.

In our new methodology for quantifying cyber risk, a firm's physical IT network is used as a base to create exposure networks with nodes that consist of IT infrastructure, threats, security, and assets. The various properties assigned to nodes allow the network to capture all aspects of cybersecurity more completely. Not only does the methodology give a holistic view of a firm's cyber risk, it also offers a customizable approach to assessing and quantifying cyber risk.

One key strength of our methodology is that it can be scaled – any number of attack trees can be used to generate exposure networks; only with very large networks will there be limits in the computational power available. Even at the bigger end of the scale, techniques to aggregate nodes (or remove insignificant ones) can reduce the computational burden, allowing us to use even larger exposure networks, and even allowing us to create exposure networks that span multiple firms, if necessary. Another key benefit of the methodology is that it can focus on network sections of any size or structure; by removing system sections that are not of interest, we can remove them from the analysis, so that it focuses only on the relevant areas.

A central focus of the methodology is attributing and allocating risk to specific processes and sectors, which allows the responsibility for risk to be assigned effectively – identifying who should be tasked with managing and reducing it. Allocation and attribution provide actionable, dynamic views of the cyber risks within combined physical and network structures, and are essential in ultimately modifying the behavior of firms and individuals.



FINANCIAL COMPUTING & ANALYTICS STUDENTSHIPS

Four-Year Masters & PhD for Final Year Undergraduates and Masters Students

As leading banks and funds become more scientific, the demand for excellent PhD students in **computer science, mathematics, statistics, economics, finance** and **physics** is soaring.

In the first major collaboration between the financial services industry and academia, **University College London, London School of Economics,** and **Imperial College London** have established a national PhD training centre in Financial Computing & Analytics with £8m backing from the UK Government and support from twenty leading financial institutions. The Centre covers financial IT, computational finance, financial engineering and business analytics.

The PhD programme is four years with each student following a masters programme in the first year. During years two to four students work on applied research, with support from industry advisors. Financial computing and analytics encompasses a wide range of research areas including mathematical modeling in finance, computational finance, financial IT, quantitative risk management and financial engineering. PhD research areas include stochastic processes, quantitative risk models, financial econometrics, software engineering for financial applications, computational statistics and machine learning, network, high performance computing and statistical signal processing.

The PhD Centre can provide full or fees-only scholarships for UK/EU students, and will endeavour to assist non-UK students in obtaining financial support.

UCL LSE Imperial College London

financialcomputing.org

INDUSTRY PARTNERS

Financial:

Barclays
Bank of America
Bank of England
BNP Paribas
Citi
Credit Suisse
Deutsche Bank
HSBC
LloydsTSB
Merrill Lynch
Morgan Stanley
Nomura
RBS
Thomson Reuters
UBS

Analytics:

BUPA
dunnhumby
SAS
Tesco

MORE INFORMATION

Prof. Philip Treleaven
Centre Director
p.treleaven@ucl.ac.uk

Yonita Carter
Centre Manager
y.carter@ucl.ac.uk

+44 20 7679 0359

Layout, production and coordination: Cypres – Daniel Brandt, Kris Van de Vijver and Pieter Vereertbrugghen

De Kleetlaan 6, B-1831 Machelen

Imperial College Business School | Centre for Global Finance and Technology

Centre for Global Finance and Technology

The Centre for Global Finance and Technology at Imperial College Business School will serve as a hub for multidisciplinary research, business education and global outreach, bringing together leading academics to investigate the impact of technology on finance, business and society.

This interdisciplinary, quantitative research will then feed into new courses and executive education programmes at the Business School and help foster a new generation of fintech experts as well as re-educate existing talent in new financial technologies.

The Centre will also work on providing intellectual guidance to key policymakers and regulators.

"I look forward to the ground-breaking research we will undertake at this new centre, and the challenges and opportunities posed by this new area of research."
– Andrei Kirilenko, Director of the Centre for Global Finance and Technology

Find out more here:
imperial.ac.uk/business-school/research/finance/centre-for-global-finance-and-technology/

CAPCO

BANGALORE
BRATISLAVA
BRUSSELS
CHICAGO
DALLAS
DÜSSELDORF
EDINBURGH
FRANKFURT
GENEVA
HONG KONG
HOUSTON
KUALA LUMPUR
LONDON
NEW YORK
ORLANDO
PARIS
SINGAPORE
TORONTO
VIENNA
ZÜRICH