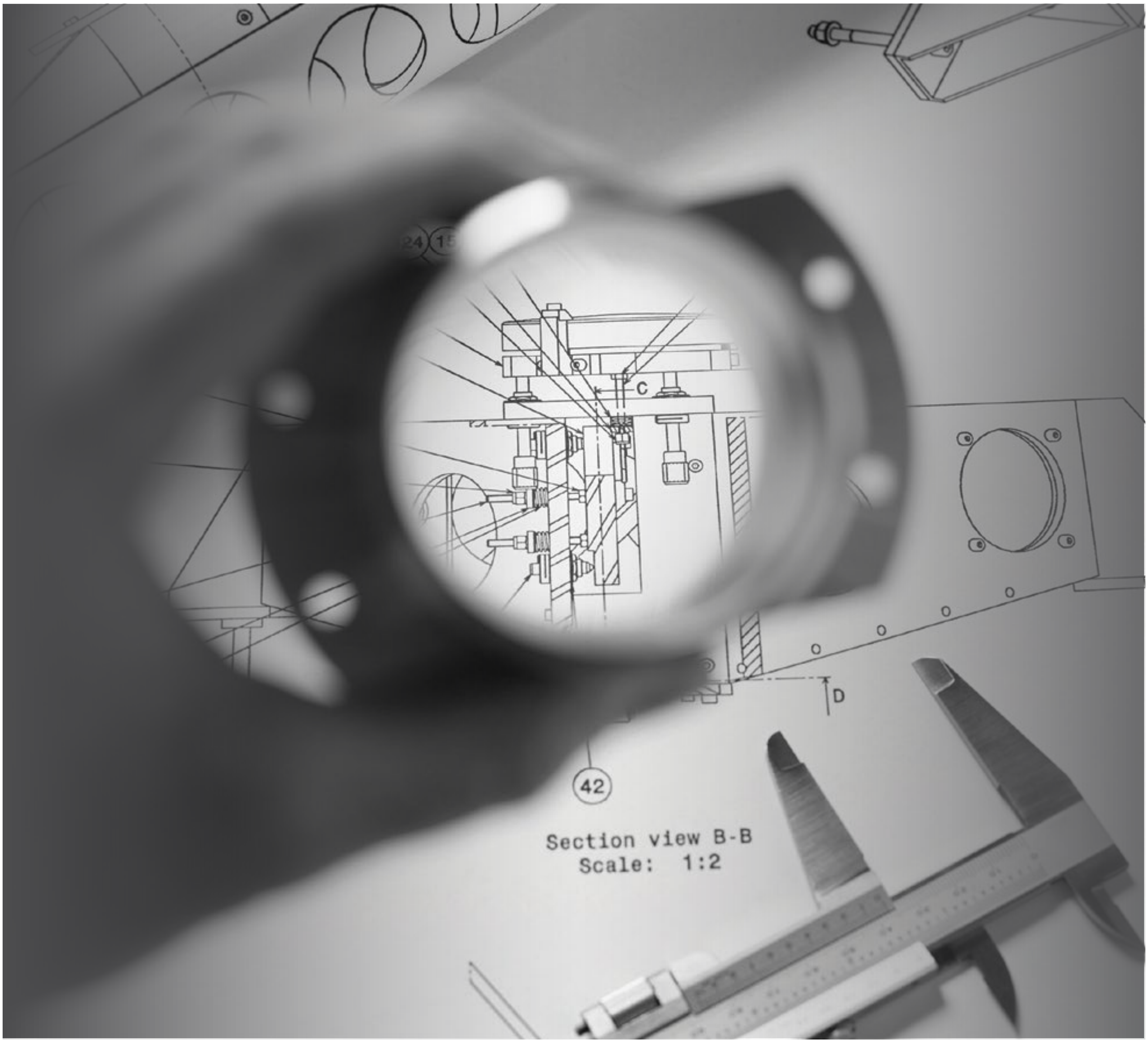


# MEASURING CYBER AGGREGATION RISK

Ashwin Kashyap and Julia Chu

Cyber risk is now an embedded feature of the global risk landscape, and preventative risk management and post-event remediation are gaining importance as shareholders, customers, supply chain partners, and regulators are increasingly focused on how companies are managing for cyber risks. Insurance is becoming an important piece of the strategy for helping businesses address these risks.

Cyber insurance is one of the fastest growing lines for insurers and reinsurers. While insurers are developing pricing tools for underwriting cyber risks, the focus on aggregation has increased – how to understand and control their potential exposure. Unlike traditional property insurance where aggregation is monitored by physical locations, cyber insurance aggregation can span connected systems that extend beyond physical geographies. While a large systemic risk has not yet materialized, it does not mean the risk is not present. Moreover, there is limited history and lack of data for this emerging exposure, which makes it difficult for insurers to measure cyber risk and calculate capital needs. In other words: how to grow a portfolio of cyber risks profitably, without exceeding risk tolerances.

For decades, insurers have considered aggregation from natural perils, and developed catastrophe models. These models go beyond the insured loss experience by blending the historical evidence and expert understanding of the nature of the peril, and provide a more robust understanding of future exposure. Modeling for cyber risk introduces new challenges, including:

- **Changing perils:** The types of cyber attacks, as well as the nature/motivation of the attackers, are in constant flux.
- **Extended duration:** Related attacks against different defenders may take place simultaneously, or may repeat over a period of months.
- **Definition of damage:** Cyber damage is harder to quantify, due to the gap between the technical and business impact.
- **Reporting lag:** It may take days/years to discover the cyber attack

Much of the cyber aggregation research to date in the insurance industry and academia has concentrated on finding a handful of potential attack scenarios and assessing the likely impact. But there is a gap in understanding who is likely to launch these attacks, what their primary motivations are, and ultimately how they accomplish these attacks without getting compromised. All of these dimensions play a critical role in the quantitative assessment of risk posed by these scenarios.

Symantec, in collaboration with Guy Carpenter, has developed a series of frameworks to systematically break down this complex problem into tractable components. Many of these components are impossible to observe directly from insured exposure or historical loss (much as wind or tides could not be inferred purely from insured hurricane loss.) But as a cybersecurity expert, Symantec has spent decades tracking the emergence of new cyber threats and attack vectors, and has unparalleled proprietary telemetry database, providing a unique capability to identify and quantify the nature of each phase of cyber attacks.

First and foremost, it is important to distinguish between the technical and business impacts of a cyber attack. The technical impact provides a mechanism to understand how an attack was carried out, but rarely provides a handle on the far greater consequences on a collection of businesses. To resolve this, Symantec has invented the CUBE framework that clearly articulates every facet that is relevant to a business user.

## CYBER INSURANCE IS ONE OF THE FASTEST GROWING LINES FOR INSURERS AND REINSURERS

The framework consists of six complementary dimensions to break down the technical complexity of a cyber attack into a meaningful and complete narrative. The dimensions are:

- Attackers
- Targets
- Objectives
- Vulnerabilities
- Impact
- Consequences

We will take a specific aggregation scenario to illustrate how this framework plays a useful role in describing these events. A cloud service provider disruption scenario has been widely regarded as one of the manifestations of aggregation on cyber portfolios. In the narrative below, the business impact on a leading cloud platform lasts for 24 hours and causes cascaded impacts on other businesses dependent upon its services. The attack is caused by a state-sponsored threat actor whose primary motivation is to showcase their sophisticated technical capabilities to the rest of the world. This scenario can play out in many different ways, and we can use the CUBE framework to showcase one such realization of this scenario.

The multi-dimensional view of risk provided by the CUBE framework not only helps insurers understand the key aspects of a scenario but also helps them control risk aggregation by avoiding higher degrees of exposure in their portfolios to the "footprints" of each of the attacks. The framework also minimizes the possibility of a misrepresentation of the description of a scenario and, consequently, the quantification of its frequency and severity. In essence, the CUBE framework provides a foundation to create an event set that can be understood easily by business users in the context of managing cyber aggregation risk.

It may be essential to think beyond the CUBE framework for building sophisticated risk models where

## ATTACKER(S)

**NAME** Iranian Cyber Army

**TYPE OF THREAT ACTOR** Nation State

**SUB-TYPE** Nation State-sponsored

**OUTSIDER/INSIDER NATURE** Outsiders

**GEOGRAPHY** Iran

**DEMOGRAPHICS** Unknown

**TRACK RECORD** Operation Abadil (2012)/ Operation Cleaver (2014)

**MODUS OPERANDI** APT

**COMMUNICATION CHANNEL(S)** Unknown

## TARGET(S)

**NAME** Leading cloud platform provider

**VERTICALS** Cloud Services

**LOCATION** Global

**PRIMARY ASSETS** All types – GovCloud-focused

**EMPLOYEE COUNT** Est. 15,000 - 20,000

**CUSTOMERS** 1 million (30%+ market share)

**RECORDS HELD** -

**ANNUAL REVENUES** $8 billion (2015)

**HISTORY WITH CYBER ATTACKS** Mostly at individual customer level

**PEERS** Amazon Web Services, Microsoft Azure, IBM Cloud Services, Google Cloud Platform, Salesforce Service Cloud, Rackspace Cloud, etc.

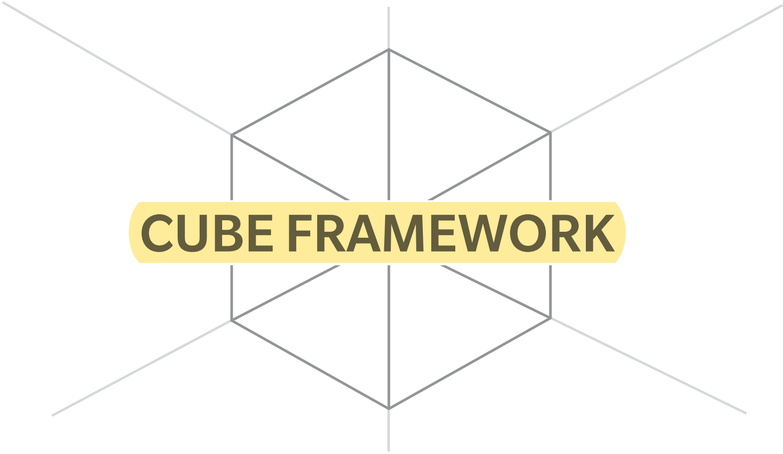
## OBJECTIVE(S)

**PRIMARY MOTIVE** Compromise targeted system availability as long as possible

**SECONDARY MOTIVES** None

**INTENDED IMPACT** (1) triggering relatively small short-term economic losses (business interruptions), (2) shattering corporate and public confidence in cloud solutions, and (3) showcasing Iranian Cyber Army capability as payback for recent wave of intrusion (payback)

**LIKELIHOOD OF SCALING ATTACKS** Low-Medium



# CUBE FRAMEWORK

## VULNERABILITIES

**VULNERABILITIES MOST LIKELY TO BE EXPLOITED** Human targets (large employee count/very large user base), software vulnerabilities (host servers use variants of Red Hat Linux and Xen hypervisor), reliance on critical infrastructure (electricity, network, etc.), etc.

**HORIZONTAL** Outage

**DEFENSE POSTURE OF TARGET** Advanced – secure overall architecture – playbook for standard DDoS attacks

**RELATIVE PREPAREDNESS OF TARGET COMPARED TO PEERS** Highest

**LIKELIHOOD OF SUCCESSFUL ATTACK GIVEN DEFENSE POSTURE** Low-Medium

**Source:** Symantec

## IMPACT

**LOSS QUANTIFICATION ASSUMPTION** Bottom-up economic model

**ACTUAL ECONOMIC LOSSES** $75 million

**ACTUAL REPUTATION LOSSES** 2% - 5% market share

**INSURABLE COMPONENT OF LOSSES** $10 million

**DURATION AND INTENSITY OF ATTACK** Cloud services unavailable for 24 hours

**REALIZED IMPACT** Shattered confidence in the the cloud services industry creates concern among companies

## CONSEQUENCE(S)

**TIMING OF INSURANCE CLAIM FILING** Six plus months after the event

**AFTERMATH FOR TARGET** Forensics investigation/computing job day credits offered to affected customers/additional expenses incurred to beef up security

**LEGAL REPERCUSSIONS FOR TARGET** Most likely none

**RESTORATION DURATION** Two to three days for full service/performance recovery

**AFTERMATH FOR THIRD-PARTY** Cyber insurance business interruption claims made by companies/some customers challenge the vendor

**LEGAL REPERCUSSIONS FOR ATTACKER** None

EXHIBIT 1: EXAMPLE KILL CHAIN

**RECON**

**Reconnaissance means:** open source research and automated network and machine scans
**Resulting target entity:** cloud provider with largest market share (31 percent), large customer base (1 million), but very advanced security maturity
**Underlying human targets:** 50 system admin members of staff (subset of the entire 15,000-20,000-person workforce)

**WEAPONIZATION**

**Deliverable used:** JavaScript file for advertising/banner
**"Weaponizer":** basic 8-bit encryption of the malware within the deliverable

**DELIVERY**

**Delivery method:** browser/web application
**Malvertising campaign sophistication:** a unique piece of cyber security research on cloud services capability is published on a reputable web blog with malware in advertising and linking back to a bogus cybersecurity firm with the same malware in website banners

**EXPLOITATION**

**Vulnerability used:** Zero Day Vulnerability on Xen Hypervisor (virtual machine environment of host servers)
**Vulnerability status:** unknown and applicable to most machines
**Vulnerable machines:** all machines

**INSTALLATION**

**Malware installed:** Advanced Remote Access Trojan (RAT) not relying on known signatures
**Malware actions:** (1) Escape the virtual machine, (2) privilege escalation to administrator/super user, (3) spread malware to other machines in other "Availability Zones", (4) lock out other system admin stealthily, and (5) take down the cloud platform for as long as possible

**COMMAND AND CONTROL**

**Communication channel:** command-and-control (C2) communication channel established with the threat actor
**Extra pieces of malware download:** none

**ACTIONS ON OBJECTIVES**

**Compromise system availability:** take cloud platform down for as long as possible

**Source:** Symantec

uncertainty quantification becomes the primary goal. For this purpose, Symantec recommends using the "kill chain" methodology below for a technical persona to capture the different phases of a cyber attack. For example, an insider attack on a confidential database in a large data aggregator will have a very different likelihood when compared to a financially motivated threat actor carrying out the same attack through a phishing campaign. A sequential model can capture this differentiation, specifically in the area of frequency quantification. More importantly, the quantification can be driven by security telemetry that Symantec has access to.

Here is a description of the same scenario from above using the kill chain to illustrate the concept. The kill chain provides an end-to-end temporal sequence of different states in the overall scenario.

The kill chain tends to fall closer to the technical end of the spectrum in cybersecurity and is not as business-friendly as the CUBE framework. It is, however, extremely useful in understanding the diminishing probabilities of success as you move down the kill chain, where each subsequent step in the attack process poses a challenge to the attackers that not only depends on the motivation and capability of attackers but also the security controls that exist within the target(s).

## CONCLUSION

The relative importance of each of these frameworks is context dependent. If you are trying to model the frequency and severity of scenarios as an actuary or a data scientist, you will find the kill chain much more similar to your toolkit of techniques, but if you are a portfolio manager or a business stakeholder within an insurer, you are likely better served by the CUBE framework which transforms layers of complex cybersecurity concepts into simplified "snackable" content. ♦

**Ashwin Kashyap** is a San Francisco-based Director, Product Management at Symantec Corporation. **Julia Chu** is a New York-based Managing Director at Guy Carpenter, where she focuses on Global Strategic Advisory.