THE CAPCO INSTITUTE

JOURNAL

OF FINANCIAL TRANSFORMATION

CYBER

A semantic framework for analyzing "silent cyber"

KELLY B. CASTRIOTTA

CLOUD

#55 MAY 2022

a **wipro** company

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

CLOUD

CRYPTO

CYBER

DEAR READER,

Welcome to edition 55 of the Capco Institute Journal of Financial Transformation. Our central theme is cloud computing, which has transformed from an efficiency initiative for our clients, to an indispensable growth driver for financial services.

The pandemic has changed consumer expectations, with consumers now demanding 24/7 access to their financial resources from anywhere, as well as hyper-personalized products that reflect their lifestyle choices.

In this edition of the Journal, we explore the power of cloud and its potential applications through the lens of a joint Capco and Wipro global study, and take a deeper look at the financial services data collected in Wipro FullStride Cloud Services' 2021 Global Survey. The survey was focused on perceptions of cloud and its importance to business strategy from over 1,300 C-level executives and key decision-makers across 11 industries.

The study indicates that cloud is becoming ever more intelligent, hyperconnected, and pervasive, and enables companies to offer their end users the personalized, user-centric experience that they have come to expect. It's clear that only the financial services firms that can successfully leverage cloud, will thrive.

In addition, this edition of the Journal examines important topics around digital assets and decentralized finance, including central bank digital currencies, and bitcoin's impact on the environment, and cybersecurity and resilience.

As ever, you can expect the highest calibre of research and practical guidance from our distinguished contributors, and I trust that this will prove useful in informing your own thinking and decision-making.

Thank you to all our contributors and thank you for reading. I look forward to sharing future editions of the Journal with you.

Lance Levy, **Capco CEO**

A SEMANTIC FRAMEWORK FOR ANALYZING "SILENT CYBER"

KELLY B. CASTRIOTTA | Global Cyber Underwriting Executive, at Markel Corporation[1]

ABSTRACT

Insurers developed property and casualty insurance policies prior to widespread computerization and the prolific use and transmission of electronic data. Many such insurance contracts did not expressly address cyber exposures at the time of their initial creation. In 2015, the Prudential Regulatory Authority (PRA) formally introduced a theoretical problem of "silent cyber" to the insurance industry, contemplating catastrophic cyber scenarios with not only a potentially powerful impact on dedicated Cyber insurance portfolios, but also on traditional insurance portfolios. The issue soon became a reality in the wake of the expansive losses associated with the NotPetya attacks of 2017.

In response to the requests made by the PRA to insurers to manage "silent cyber", Lloyd's of London introduced a mandate to eliminate "silent cyber" on all Lloyds policies, first charting a course for the transformation of insurers' contractual wording to more appropriately address cyber risk. This article discusses the general concerns around "silent cyber" as presented by the PRA, the challenges of defining cyber risk across the insurance industry, and steps taken to rectify the silent cyber issue. The article then explores the idea that the silent cyber problem is at its core a semantic one rather than one of risk perception. The article concludes by offering solutions as to a semantic framework under which to analyze and address "silent cyber".

1. INTRODUCTION

Historic buildings are worth preserving not only because of their cultural significance, but also because they can be a potential source of revenue.[2] It may occasionally make economic sense to rebuild certain architectural structures in the face of new environmental threats or newfound recognition of the ways that existing threats impact aging structures.[3] However, there are alternatives to a destroy and rebuild approach, one of which is retrofitting older buildings with new materials or design features.[4] Seismic retrofitting, for example, is the act of performing engineering treatments such as preservation, rehabilitation, restoration, and reconstruction, to improve a historic building's ability to withstand earthquakes.[5] With appropriate retrofitting, contemporary architects can maintain older buildings by implementing and layering emerging design technologies upon older ones, thereby maintaining the integrity of cultural structures.[6]

[1] The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of Markel Corporation or any of its subsidiaries or holdings. All content within is for general informational and academic research purposes only and not intended as legal advice. Article republished from original source, Castriotta, K. B., 2021, "A sematic framework for analyzing "silent cyber"," Connecticut Insurance Law Journal 27:2, 68-104.

[2] See Sigmund, Z., V. Ivanokovic, and A. Braun, 2011, "A challenge of retrofitting a historical building," 2nd WTA International PHD Symposium Building Materials and Building Technology to Preserve the Built Heritage, at 1.

[3] See Hutchinson, T., 2012, "Retrofitting is expensive – let's demolish and start again," The Guardian, April 3, https://bit.ly/3sYnnh9.

[4] See Sigmund, supra note 2 at 2.

[5] See id.

[6] See id.

We can look at the issue of "silent cyber"[7] in a similar light. The insurance industry[8] has developed and maintained a prolific body of contractual architecture (policies) that has created a legacy of meaningful risk transfer products for customers. Among those products is the relatively emergent Cyber insurance product, specifically designed to cover certain aspects of so-called "cyber risk". The insurance industry has historically paid losses associated with their insurance products and remained profitable.[9] Similar to the architectural community, the insurance industry also occasionally encounters emerging appreciation of the catastrophic[10] reach of specific threats. In recent years, one such concern is the wide reach of cyber risk[11] and with it, concerns as to whether the insurance industry will be able to withstand an event like a malware attack on the United States' power grid.[12] Compounding this fear is a recognition that perhaps "silent" cyber exposure will extend beyond the realm of monoline Cyber[13] insurance portfolios and threaten the sustainability of traditional[14] lines of insurance coverage. Specifically, the industry is concerned about risks that it failed to consider and to adequately price for cyber losses (attritional[15] or otherwise).

As such, the industry has, on the one hand, a vast set of traditional risk transfer products not specifically engineered to withstand such cyber risk, and on the other hand, an emerging set of risk transfer products (and in some cases, services) that have been intentionally created to address cyber risk. This article proposes that one solution to the concerns regarding "silent cyber" is to "retrofit" traditional insurance products with language and other normative concepts borrowed from standalone Cyber products.

> *"New ideas must use old buildings."*
>
> **Jane Jacobs** – *The life and death of great American cities*

A prerequisite to solving the problem of "silent cyber" is the adoption of a consistent semantic framework to be implemented across an insurance enterprise. This approach will ultimately lead to better evaluation and quantification of cyber exposure within any specific firm's insurance portfolio and across the industry. The framework should be flexible enough to adapt to the iterations of the Cyber insurance product sold today and in the future. In turn, this article will offer a definition of "silent cyber" that can be used to determine what should and should not be covered by non-Cyber policies. Such a semantic framework focuses on the "nesting"[16] of Cyber and non-Cyber policies, and emphasizes that losses that are covered by Cyber policies should not be covered by non-Cyber, and vice versa (unless done so intentionally). Just as auto and homeowner's policies "nest" together by covering mutually exclusive risks, the same should be true of Cyber and non-Cyber policies. To accomplish this, non-Cyber policies should continue to cover losses where a cyber-as-a-peril is involved in the causal chain of a loss and there is a physical alteration to the structure of tangible property. By contrast, traditional policies should not cover any losses that are in fact covered by current Cyber insurance policies.

[7] When used as a noun, the term "silent cyber" will appear in quotations, but when used as an adjective, the phrase will appear without quotations.
[8] The phrase "insurance industry", when used throughout this article, is to be construed broadly to include businesses that partake in the underwriting and procurement of insurance or reinsurance products.
[9] For a quick snapshot of 2020 profitability, see "Visualizing the 50 most profitable insurance companies in the U.S.," August 10, 2020, https://bit.ly/34Vf6lo. For a historic view, see Lynch, J., 2016, "The property/casualty landscape profitability, growth – disruption?" Insurance Information Institute, September 26, https://bit.ly/3uPBV55. For a forward-looking view, see Shaw, G., and N. Baumann, 2020, "2021 insurance outlook: accelerating recovery from the pandemic while pivoting to thrive, Deloitte, December 3, https://bit.ly/3sF3V8N.
[10] When this article refers to "catastrophic" losses, this is generally intended to mean the same as correlated losses, systemic losses, or accumulated losses – all losses other than attritional losses. See infra at 15.
[11] See Reinsurance News, 2017, "Swiss Re highlights role of re/insurance in cyber risk," March 6, https://bit.ly/3LyeR0M.
[12] See Trevor Maynard, et. al., "Lloyd's emerging risk report – 2015," Innovation series: The insurance implications of a cyber-attack on the U.S. power grid," Centre for Risk Studies, University of Cambridge Judge Business School, https://bit.ly/36dfKvs.
[13] References to cyber-specific insurance policies are denoted with capitalized version of the word "Cyber". References to cyber-as-a-peril (or hazard) are denoted with a lower-case version, "cyber".
[14] References to "traditional lines" or "traditional property and casualty" insurance policies include the broad array of products to cover bodily injury, property damage, liability, and professional risk developed prior to 1990.
[15] References to "attritional losses" are those losses other than losses associated with catastrophes. When I refer to expected losses, non-systemic losses, or non-catastrophic losses, I am referring to attritional loss.
[16] In this context, the "nesting" of sets of insurance policies refers to policies that, as a rule, complement each other, by covering specific aspects of a risk, but not the same aspects of a risk.

The article ends with prescriptive view of how to view cyber risk: by embracing the Cyber insurance product framework that the industry has developed. To reach this conclusion, this article will examine the current semantic frameworks offered (as set forth by the PRA and other regulatory bodies) and the problems with having disparate frameworks for such, and offer potential solutions to be implemented on a firm-by-firm basis.

2. CYBER AS A COVERAGE

Three conceptual coverage parts comprise a contemporary Cyber insurance product: (1) third-party liability coverages; (2) first-party coverages; and (3) business interruption coverages (which are technically first-party coverages, but of a specific "time element" nature). Each respond to a variety of cyber incidents, spanning from cyberattacks on one's own network, to system failures and other outages, to cyberattacks on a network provider's system (herein "cyber event"). Liability coverages are typically offered as follows: privacy and security liability, media liability, regulatory coverage, and payment card industry (or "PCI") coverage. The first-party coverage includes incident response (including call center costs, credit monitoring, and related mitigation costs), cyber extortion payments, and restoration costs. The business interruption part typically includes coverage for the costs of interruption of business due to a cyber event, whether the event is perpetrated upon the policyholder itself or a business upon which a policyholder depends. This often includes the reputational costs associated with a cyber event.

The coverages[17] are a good place to find a common understanding of what the industry considers to be covered or potentially covered cyber loss. For example, liability coverages naturally respond to the legal costs and the damages (judgments, fines and penalties, or settlements) that arise from a cyber event. First-party coverages tell us in detail what cyber losses a business may suffer. For instance, an incident response insuring agreement tells us about the costs incurred to engage a host of service providers that are needed to respond when there is a security or privacy incident. These include breach counsel, privacy counsel, credit monitoring services for customers, forensic providers, and public relations firms. The extortion and restoration agreements provide coverage for ransomware payments made to cyber criminals and the costs of a cybersecurity firm to restore one's data (and in some cases, hardware). And finally, the business interruption coverages tell us that companies may undergo loss of income and even loss of contractual or other business opportunities due to a cyber event.

3. FROM ABERRATION TO AGGREGATION

The next step is to elucidate industry concerns surrounding "silent cyber". The insurance industry has been formally discussing the issue of "silent cyber" since 2015, with most crediting the PRA as the initial regulatory catalyst for the movement towards eradicating "silent cyber" in insurance portfolios. In many ways, the silent cyber problem has existed well before 2015, following a history of professional advice as to where to find cyber coverage under traditional insurance policies.[18] For example, until around 2014,[19] commercial general liability policies rarely included concepts or language specific to cyber risk and even then, they were specifically focused on privacy exposures associated with computer hacking (as opposed to other security and business threats). Conflicts between insurers and policyholders developed over the applicability of coverage as they applied to emerging situations, such as whether coverage existed for damage to data and whether data was tangible property.[20] Other examples of such disputes include those where policyholders sought coverage under property policies because of power outage events (impacting computerized systems) under a theory of "loss of use or functionality", even where the outage did not

[17] Note that the insuring agreements of a Cyber policy provides a normative view of what constitutes cyber loss, even though Cyber policies typically only extend to financial loss (defined as pure economic loss that would be reflected as loss in a balance sheet only). To achieve a more nuanced picture of what constitutes cyber loss, we could also look to the common exclusionary language in Cyber policies. This article will not address common exclusions in Cyber policies.

[18] See Clarke R., 2013, "Cyber liability: where to find cyber coverage," Insurance Journal, January 28, https://bit.ly/3JueAd4.

[19] In 2014, ISO introduced endorsements "addressing the access or disclosure of confidential or personal information," https://bit.ly/3rOLKhV.

[20] See, e.g., West Bend Mutual Ins.Co. v. Krishna Schaumburg Tan, Inc., 2020 Ill. App. LEXIS 179, at 12 (Ill. Ct. App. Mar. 20, 2020) (holding that under a general liability policy, coverage part b, "publication" encompasses the act of providing plaintiffs fingerprint data to a third party, alleged to be in violation of the Biometric Information Privacy Act (Act) (740 ILCS 14/1 et seq. (West 2014)); Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 803 (8th Cir. 2010) (describing invasion of privacy and deceptive practices allegations from the installation of advertising tracking software on a non-consenting plaintiff, and finding "loss of use" of computer allegations fell within "tangible property" terms of general liability policy); Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185 TUC ACM, 2000 WL 726789, at *3 (D. Ariz. April 18, 2000) (describing how a power outage knocked out systems, causing loss of data and loss of software functionality, and the court found there was "property damage" per CGL terms). Compare, Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 97–99 (4th Cir. 2003) (finding that data, information, and instructions are not "tangible property," and that an "impaired property" exclusion precluded coverage for loss of use of tangible property that is not physically damaged), with Zurich Am. Ins. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141, at *67–72 (N.Y. Sup. Ct. February 24, 2014) (describing how an insured sought coverage under CGL terms for alleged transmission of private information by hackers and finding no coverage).

amount to actual physical damage.[21] Much of the focus of these disputes focused on underwriting and drafting intent. In other words, did the policy wording offer coverage for a cyber loss, even though the insurers did not price the policy to cover this type of risk? In this type of scenario, underwriters did not necessarily contemplate losses caused by cyber threats and, therefore, the definition of loss expanded beyond the intended scope of coverage.

The conversation about unexpected cyber losses began to morph after the PRA performed a cross-industry survey regarding cyber risk in 2015.[22] The initial PRA findings were grim, including the finding that the failure to account for cyber exposure in traditional insurance lines was material and likely to worsen with time.[23] The PRA also found that the industry was hamstrung from taking appropriate corrective action due to a lack of effective cyber exclusions, lack of clear strategy and risk appetite, and an insufficient grasp of aggregation and tail potential of affirmative cyber.[24] As the focus of the PRA findings revolved around potential catastrophic losses, the conversation circles about "silent cyber" broadened from the plaintiff's bar to the C-suite of insurance companies.[25]

A secondary catalyst for this broader conversation was the series of cyberattacks in 2017, known as NotPetya,[26] which amounted to more than U.S.$10 billion in losses.[27] As the loss picture of the NotPetya[28] attacks sharpened in 2019,[29] the concerns shifted from attritional losses (usually due to aberrations in coverage) to mountainous aggregation[30] issues. Aggregation concerns arise when multiple policies or multiple lines of coverage offered to an insured (either by design or inadvertently) are triggered from a single event, and as such, there is an accumulation of loss across product lines underwritten by any one insurer. "Silent cyber" poses a particular aggregation challenge to insurers because monoline Cyber policies are often the only policies underwritten to cyber risk. As aggregation concerns relate to "silent cyber", underwriters underestimate the accumulation risk within a product line or for a specific insured across multiple product lines due to the possibility that traditional policies may unexpectedly respond to cover such losses. A large scale, or geographically expansive cyberattack could impact multiple insureds and multiple policies, both traditional and Cyber-specific.

4. SEEKING NORMATIVITY

The PRA's definition of "silent cyber" evolved over the course of its surveys, findings, and publications. Some versions rely on normative concepts of "cyber risk", "cyber exposure", or "cyber-related losses", while others rely on terminology commonly used and defined in Cyber-specific insurance policies. By describing the issue of silent cyber both with normative cybersecurity concepts on the one hand and with Cyber policy concepts on the other, the PRA was touching upon the two main categories of silent cyber loss: ensuing loss and cyber product loss. Both categories are important. A definition of Cyber product loss allows insurers to effectively treat situations in which overlapping coverages are inadvertently provided. A definition of ensuing loss is equally important, given that non-Cyber policies will in fact respond to losses caused by cyber risk.

[21] See Am. Guarantee, 2000 WL 726789, at *2 (describing an electrical outage, where an insurer said there was no "physical damage" pursuant to "all risks" policy language, yet finding that "physical damage" is not restricted to physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality); see also, National Ink & Stitch, LLC v. State Auto Property & Casualty Insurance Company, 2020 U.S. Dist. LEXIS 11411 (U.S.Dist. Ct., Maryland) (holding that loss/corruption of electronic data and software and reduced efficiency of computer systems due to a ransomware event amounted to direct physical damage under BOP policy). But see Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co., 114 Cal. App. 4th 548, 554–55 (Cal. Ct. App. 2003) (finding no coverage for costs of recovery of data or business interruption because there was no loss of, or damage to, tangible property).

[22] See Letter from Chris Moulder, Director of General Insurance at Bank of England, PRA (Prudential Regulatory Authority), August 10, 2015, https://bit.ly/3gNE09v (including questionnaires as to cybersecurity and resilience, cyber insurance, and conduct).

[23] See Moulder, 2016 Letter, infra note 39 at 1.

[24] See id. at 1–2.

[25] See Consultation Paper CP39/16, "Cyber insurance underwriting risk", Bank of England: Prudential Regulation Authority (Nov. 2016) at 5, https://bit.ly/34YjeRC (noting that the responses to its investigation were made by the following roles within insurance firms: Chief Underwriting Officer, Chief Risk Officer, Chief Actuary, Lead Cyber Underwriter, and Head of Exposure Management).

[26] See Krebs on Security, 2017, 'Petya' ransomware outbreak goes global," June 27, https://bit.ly/3Jri1kZ.

[27] See generally Abraham, K., and D. Schwarcz, 2021, "Courting disaster: the underappreciated risk of a cyber-insurance catastrophe," Connecticut Insurance Law Journal (forthcoming) (discussing the prospect of cyber incidents having the potential to simultaneously cause very large losses to numerous firms across the globe, thus resulting in a cyber "catastrophe"); see Willis Towers Watson , 2020, "The problem of silent cyber risk accumulation," February 25, https://bit.ly/3rOt3ul. See also Mondelez v. Zurich, No. 2018L011008, 2018 WL 4941760 (Ill.Cir.Ct) (subject litigation filed by Mondelez).

[28] See Johansmeyer, T., 2019, "Could NotPetya's tail be growing?" Verisk, https://vrsk.co/34AudRN (referring to a PCS study that NotPetya's economic losses were estimated at U.S.$10 bln by 2017).

[29] See Ward, C., 2020, "Cyber turned inside-out: three years after NotPetya," Carrier Management, June 17, https://bit.ly/3HORfSZ (estimating U.S.$10 bln in losses associated with NotPetya, but with estimated U.S.$3 bln in insurable losses from policies other than cyber dedicated lines).

[30] The term "aggregation" is used synonymously with the term "accumulation" throughout this article.

Put in terms of cause and effect, the "ensuing loss" category of silent cyber loss addresses "cyber" as a peril[31] or as a hazard and refers to losses[32] that flow from such cyber perils or hazard. In other words, as humanity grows increasingly dependent upon computers and digitization, the mere use of a computer or computer-operated technology will result in losses from otherwise covered perils. Another way to put this is that a computer is somewhere involved in the causal chain of the loss, even if the computer was not the sole cause[33] or the proximate cause[34] of the loss. This type of "silent cyber" is where a loss is caused by or results from computer-related acts or events, but where such cause does not change the nature of the expected loss under any given policy (but may change the magnitude or frequency of such loss). The exposure is typically "silent" due to the structure of all-perils policies. An example of ensuing loss is where a hacker (cyber incident) exploits a vulnerability in a computerized device that ignites a fire (a traditionally covered peril), which causes property damage to a building (an ensuing loss).[35] Historically, this type of incident would be covered under a property policy that covers damage to a building caused by fire, a covered peril, regardless of the use or involvement of a computer. Accordingly, there is no apparent mismatch between the policy offering and the underwriting intention in terms of type of risk, even though the policy's language may fail to expressly discuss computer-related technologies.

The other category of "silent cyber" relates to Cyber as an insurance product. This version of "silent cyber" is where the losses covered by a non-Cyber policy stemming from a cyber event overlap with losses specifically covered by a Cyber insurance product, against the insurer's intention that traditional policy and Cyber policies "nest" together to cover mutually exclusive sets of losses. In these cases, the cyber-related acts or events result in loss that is a change to the nature or the characteristics of expected loss under a traditional insurance policy. The result is tantamount to the type of coverage one would normally find in the insuring agreements of a Cyber policy. Such losses often come as a surprise to the underwriter, are brought under a novel theory of loss (from the perspective of the insurer), and were not factored into the underwriting process when pricing and terms were quoted. Put another way, such losses are aberrations as to what is underwritten to and ultimately modeled by pricing or CAT actuaries for that specific product line. This type of silent cyber loss has to do with "cyber," not as a normative concept of cyber risk, but as a normative concept of a distinct type of insurance product line ("Cyber"). An example of this is where a retailer experiences a cyberattack whereby the personal data of many customers is exfiltrated, including correlated bank account information. The banks, who must now re-issue all affected credit cards to consumers, proceed to sue the retailer-insured to recover the costs of the cards (Cyber product loss). Consequently, the insured alleges that this is a form of damage to tangible property due to their limited usability (novel loss theory).[36]

Earlier iterations of the PRA's definition of "silent cyber" have combined the two views of the phrase: one, having to do with "cyber" as a cause of loss, and the other, having to do with "Cyber" as a type of insurance coverage. In a 2016 advisory, for example, the PRA explained that it was investigating the question of underwriting risks emanating from affirmative[37] Cyber insurance policies, but also "from implicit cyber exposure within 'all-risks'[38] and other liability insurance policies that do not explicitly exclude cyber risk. This latter type of cyber risk is referred to as 'silent' cyber risk…"[39] In this characterization, the PRA focuses on scenarios where

[31] Peril, Black's Law Dictionary at 524 (2nd pocket edition 2001). Black's defines "peril" as follows: 2. Insurance: The cause of a loss to a person or property. Compare with, Black's definition of hazard: "The risk or probability of loss or injury esp. a loss or injury covered an insurance policy." Id. at 316.

[32] Generally speaking, "ensuing losses" are losses that follow from an incident that causes direct physical loss or damage.

[33] Sole cause, Black's Law Dictionary at 89 (2nd pocket edition 2001). Black's defines "sole cause" as follows: The only cause that, from a legal viewpoint, produces an event or injury. If it comes between a defendant's action and the event or injury at issue, it is treated as a superseding cause.

[34] Proximate cause, Black's Law Dictionary at 88 (2nd pocket edition 2001). Black's defines "proximate cause" as follows: 1. A cause that is legally sufficient to result in liability. 2. A cause that directly produces an event and without which the event would not have occurred. Id.

[35] See Wagensiel, P., 2011, "Printers can be hacked to catch fire," Scientific American, November 29, https://bit.ly/34GFNdZ (relaying findings by Columbia University researchers that attackers may spread malware causing printers to overheat and catch fire).

[36] This is a novel theory of loss because it involves an allegation that cards are damaged based on "loss of use" versus actual physical damage to the card, particularly because the cards were physically useable after the attack. In other words, users could physically swipe their affected credit cards, albeit not without consequence. See Target Corp. v. ACE American Ins. Co., et al, 2021 WL 424468 at *7 (D. Minn. Feb. 8, 2021) (holding that Target could not obtain coverage from its CGL to replace credit cards after a data breach under a "loss of use" theory as the cards diminution in value did not amount to loss of use).

[37] Affirmative Cyber policies are insurance policies that specifically respond to a variety of so-called "cyber incidents," including ransomware attacks, viruses, ddos attacks, but also to computer system failures, supply chain interruptions, and exfiltration of private data (both digital and non-digital).

[38] All-risks policies refer to traditional property and casualty policies that respond to all perils unless specifically stated otherwise.

[39] See Letter from Chris Moulder, Director of General Insurance, Bank of England, PRA, to CEO's [of various insurers], at 1, November 14, 2016, https://bit.ly/3p9XaLt. See also, Consultation Paper 39/16, supra note 25 at 5.

cyber exposure is implicitly covered within all-perils insurance policies. The reason why this would be an area of "silent cyber" is because such all-perils policies would readily have been developed, standardized, and well-established prior to the computerization of society. As such, the policies did not contemplate that the use of a computer to cause harm could be a peril, simply because computers were not in commercial use at the time the language was initially developed.[40] More appropriately, the cyber aspect was not so much silent as it was absent. Notably, these traditional policies were also first developed prior to the invention of a standalone Cyber policy. So, underwriters could not have possibly considered whether the type of loss would be redundant with an affirmative Cyber insurance product.

Later, in a 2017 Supervisory Statement, the PRA defined cyber insurance underwriting risk as "the set of prudential risks emanating from underwriting insurance contracts that are exposed to cyber-related losses resulting from malicious acts (e.g. cyberattack [sic], infection of an IT system with malicious code) and non-malicious acts (e.g. loss of data, accidental acts or omissions) involving both tangible and intangible assets."[41] Here, the PRA introduced a dichotomy between malicious and non-malicious behaviors that recurs in Lloyd's wording[42] developed to address "silent cyber".[43] In other words, a prudential risk – or a non-silent risk, rather – is one that is intentionally underwritten to and priced for, whereas with silent cyber exposures, one of those two elements is absent: underwriting intent as to cyber risk or pricing as to cyber risk.[44] In the same 2017 Supervisory Statement, the PRA simplifies the definition of non-affirmative cyber as: "insurance policies that do not explicitly include or exclude coverage for cyber risk."[45] Given that here the PRA is referring to insurance policies, which are contractual arrangements commemorated in writing, it follows that one of the primary issues of "silent cyber" is an issue of language – specifically, the failure of the underwriter to clearly express whether 1) cyber perils are covered and 2) that coverage is the same kind of coverage found in an affirmative Cyber insurance product.

One of the major issues with the PRA's earlier definition of "silent cyber" is that it attempts to define cyber underwriting risk in relation to a normative concept of "cyber risk" – a concept that the PRA does not define.[46] As such, in evaluating its portfolio's cyber risk, the carrier is then left to determine whether "cyber risk" is the same as "cyber underwriting risk" and in turn, whether this equates to "cyber-related losses" or is something else altogether. A lack of construct in this regard leads to ambiguity in insurers trying to assess, measure, and course correct as to cyber exposure across product lines. If the PRA is going to characterize a type of risk as prudential, there also must be some foundational concept of what that risk is (and what it is not).

In the PRA's Policy Statement[47] referencing a concept of "cyber risk", the PRA also explained that the definition of "silent cyber" should be understood as the equivalent of a concept of "non-affirmative cyber".[48] Here, the PRA departs from a definition of "silent cyber" that is entirely dependent upon a concept of "cyber risk" per se. According to the PRA, "silent cyber" and "non-affirmative cyber" can be used interchangeably.[49] Four of the thirteen respondents to the PRA's Consultation Paper pointed out that the use of the term "silent" cyber risk is problematic and may create ambiguity in future arbitration or litigation cases.[50] Moreover, two respondents suggested that the term "non-affirmative" cyber risk should be used instead

[40] See generally Lloyd's Wording Repository, https://bit.ly/3JwxfFr.
[41] Supervisory Statement SS4/17, "Cyber insurance underwriting risk," Bank of England, PRA, at 5, July 2017, https://bit.ly/34T0tPF.
[42] See generally Lloyd's Wording Repository, https://bit.ly/3JwxfFr.
[43] See Supervisory Statement SS4/17, supra note 41. But see, Consultation Paper CP39/16, "Cyber insurance underwriting risk," Bank of England, PRA, November 2016) at 5, https://bit.ly/34Z1Dt7 (PRA defines cyber underwriting risk is as the set of prudential risks emanating from underwriting insurance contracts that are exposed to losses resulting from a cyberattack).
[44] See Supervisory Statement SS4/17, supra note 41.
[45] See id. at 5.
[46] There is no known standardized definition of the term "cyber risk". I have come across a variety of definitions of cyber risk. See, e.g., CRO Forum, 2014, "The cyber risk challenge and the role of insurance," paragraph 3, December 2014, https://bit.ly/33l1Bv9; Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, 2016, "Guidance on cyber resilience for financial market infrastructures," June, https://bit.ly/3sFpwhl.
[47] See Policy Statement PS15/17, "Cyber insurance underwriting risk," Bank of England, PRA, July 2017, https://bit.ly/3JrQGyZ. Policy Statement SS4/17 is responsive to Consultation Paper (CP) 39/16 "Cyber insurance underwriting risk," including Supervisory Statement (SS) 4/17 "Cyber insurance underwriting risk," which sets out the PRA's final expectations regarding the prudent management of cyber insurance underwriting risk. Id. at 1.
[48] Policy Statement PS15/17, supra note 47 at 5. See also, Supervisory Statement SS4/17, supra note 41 at 5-7.
[49] See Policy Statement PS15/17, supra note 47 at 5. See, Supervisory Statement SS4/17, supra note 41 at 5 (stating "non-affirmative cyber risk, i.e., insurance policies that do not explicitly include or exclude coverage for cyber risk. This latter type of cyber risk is sometimes referred to as 'silent' cyber risk by insurance professionals.") Other definitions of "silent cyber" exist. For an example, see Guidewire's definition in "Silent cyber scenario: opening the flood gates," October 2018), https://bit.ly/34BcXMe ("We define "silent cyber" exposure as the potential for cyber risk to trigger losses on policies where coverage is unintentional, unpriced, or both. "Unintentional" coverage means not explicitly excluded or affirmed (with any applicable sublimit)").
[50] Policy Statement PS15/17, supra note 47 at 5.

whereas one respondent suggested a distinction based on whether a cyberattack is a named peril or not.[51] Finally, one respondent suggested that the distinction between "silent" and "affirmative" should be completely removed and instead referred to "cyber risk exposures". As a result, the PRA agreed that the use of "non-affirmative" cyber risk would be less ambiguous and adopted the use of affirmative cyber risk (insurance policies that explicitly include coverage for cyber risk); and non-affirmative cyber risk (policies that do not explicitly include or exclude coverage for cyber risk).[52] This is important because it points to one of the PRA's major concerns: aggregation.[53] Specifically, PRA seeks to identify the potential for "clash" (wherein an insurer can experience excessive covered losses due to one insurable event).[54] In its equivocation of "silent cyber" as "non-affirmative cyber", the PRA's reference point is not only "cyber risk" per se, but affirmative Cyber coverage, meaning, an actual cyber-specific product offered by the insurance market.

Others who have attempted to define "silent cyber" also embrace the two distinct concepts: normative risks from cyber-as-a-peril and Cyber as an insurance product. For example, the European Insurance and Occupational Pensions Authority (EIOPA) utilizes a definition of "silent cyber" akin to the PRA's definitions: "Non-affirmative cyber risk refers to instances where cyber exposure is neither explicitly included nor excluded within an insurance policy. The latter type of cyber risk is also referred to as 'silent' cyber risk."[55] Like the PRA, the EIOPA's definition of "silent cyber" both references a concept of cyber risk and refers (albeit loosely) to a Cyber insurance offering. Unlike the PRA, the EIOPA attempts to define "cyber risk". The EIOPA's methodology for this exercise involved asking participants[56] for their enterprise's definition of cyber risk, while providing a cyber risk definition from the Financial Stability Board (FSB) Cyber Lexicon[57] as an initial reference.[58] The results of the EIOPA's survey varied widely with some groups relying on FSB definitions, some on the American Association of Insurance Services (AAIS) definitions, some relying on regulatory concepts, and others not having a working definition whatsoever.[59]

The EIOPA concluded[60] that having a clear and common set of definitions would foster a more productive dialogue regarding cybersecurity challenges, including quantification methods for "silent cyber". Its straightforward observation aligns with the PRA's findings regarding disparate opinions as to the amount and severity of cyber risk within traditional lines of coverage. As discussed, this divergence in view likely stems from a lack of a collective semantic framework. What the EIOPA, the PRA, and the FSB overlook, however, is the idea that an established semantic framework already exists and is fully accessible to insurers. The sector has already built a strong framework based upon a series of normative constructs and definitions that comes close to a fully formed concept of "cyber risk" vis-a-vis its current Cyber product offerings.

5. CYBER INSURANCE AS THE SEMANTIC SOLUTION

What if, instead of relying upon definitions derived from outside the insurance industry to address "silent cyber", the insurance industry drew upon its own resources as a normative guide for cyber risk? Even though a market-standard monoline Cyber policy will typically only provide coverage for financial loss (and does not typically extend to bodily injury and property damage), insurance carriers can still refer to the insuring agreements of such a standalone policy to formulate a comprehensive idea as to what "cyber risk" means, both to the insurance industry and to its policyholders.

[51] Id.
[52] Id. at 5–6.
[53] Clarification of wording alone will not stymie the impact of catastrophic cyber losses to any single insurance firm. However, clarifying the wording and "channeling" the coverages to the appropriate products may serve to gain better or more accurate outputs from cyber models.
[54] See Supervisory Statement SS4/17, supra note 41 at 7 (describing minimum standards for insurers to incorporate cyber insurance underwriting risk stress tests that explicitly consider the potential for loss aggregation (e.g., via the cloud or cross-product exposures) at extreme return periods (up to 1 in 200 years)).
[55] EIOPA, 2019, "Cyber risk for insurers: challenges and opportunities," European Insurance and Occupational Pensions Authority, at 18, https://bit.ly/3oMIFxK.
[56] See id. at 3. Participants included 41 large (re)insurance groups across 12 European countries representing a market coverage of around 75% of total consolidated assets.
[57] See generally Cyber Lexicon, Financial Stability Board, November 12, 2018, https://bit.ly/3Jq2JwF. The FSB developed a cyber lexicon in November 2018, in part, to assess and monitor financial stability risks of cyber risk scenarios.
[58] The Cyber Lexicon defines cyber risk as "the combination of the probability of cyber incidents occurring and their impact." Id. at 9 (adapted from Committee on Payments and Market Infrastructures-International Organization of Securities Commissions, International Association of Insurance Supervisors (CPMI-IOSCO, ISACA) Fundamentals and ISACA Full Glossary).
[59] See Cyber risk for insurers, supra note 55 at 7 (emphasis added).
[60] Id.

Since its earliest iterations, the Cyber policy offering has evolved to stay fit for purpose. The coverage will continue to evolve as offerings expand and contract in response to the threat environment, customer needs, and the performance of affirmative Cyber portfolios.[61] However, there are two main reasons to rely upon cyber concepts that are already formulated in a Cyber insurance coverage policy. One is that the Cyber insurance policy is developed from a set of norms that the industry already accepts, some of which was directly in reaction to the threat environment experienced by actual companies, so it is a good place from which to establish common dialogue.

A second reason is that the industry's preoccupation with "silent cyber" is due in large part to the potential "clash" risk involved with having accumulative and redundant cyber coverages available to the same client or subject to the same cyber event, unbeknownst to the underwriters. Namely, of the two theories of "silent cyber" loss, the Cyber product loss is the more pressing aspect of the silent cyber problem. By its very definition, ensuing loss from a cyber event is likely contemplated by the underwriter and priced for accordingly. And because the cyber event is one event among others on the causal chain, as opposed to being the single event on the causal chain, ensuing loss has an anchor to a time and place type peril (e.g., fire), which helps to anchor the loss in a predictable pricing manner. On the other hand, cyber risk as a form of product loss is where insurers can start to see the pronounced effects of accumulation across a portfolio. Because Cyber as a product loss refers specifically to covered losses under affirmative Cyber policies, where traditional policies respond to the cyber perils in the same type of way as Cyber policies, there is a real potential for an insurer to have significant limits exposed to a cyber event at significantly reduced pricing. Accordingly, if Cyber product loss accumulation is the more prominent concern of "silent cyber," correcting traditional policy language to eliminate (or at least price for) redundant Cyber coverage becomes the first priority[62] of the "silent cyber" solution. To accomplish this objective, an enterprise must be well-versed in the mechanics and semantics of a typical standalone Cyber offering.

[61] See Jones, J. H., 2021, "AIG introduces ransomware co-insurance and sub-limits at 1.1 cyber renewals," Insurance Insider, January 8, https://bit.ly/3HPPcOR.

[62] A secondary component of the "silent cyber" solution is the capability to accurately map and quantify the areas of Cyber product losses, regardless of the original intent of the underwriter at the time of binding. Quantifying this accumulation exposure can be done more meaningfully if insurers map cyber exposures to the general categories of insurable Cyber losses throughout their portfolios.

To some, the following analysis may seem to presuppose that affirmative Cyber coverage is an accurate reflection of the real cybersecurity landscape. Certainly, there is an overlap as to the realities of cyber, as a peril, and "Cyber," as an insurance product as demonstrated further in the history of the Cyber product section of this article. Regardless, while it may be the case that an insurance policy is a kind of representation of the threat or peril that it purports to cover, it uses abstractions to describe both the coverage triggers and the losses.[63] Accordingly, that policy language accurately reflects the actual threat environment or encompasses all that can be imagined as "cyber risk", is less important than it is for the insurance policy to accurately reflect the intentional and insurable (whether potential or actual) cyber risk. By "insurable" cyber risk, I am referring to the causes of loss and the types of loss to be covered, as contemplated by the underwriter.

As such, the appropriate definition of cyber risk for "silent cyber" is simply the type of risk that insurers of affirmative Cyber are generally willing to cover at a given point in time. Of course, there is no one single standard for a standalone Cyber coverage offering now or in the past, and there continue to be changes in policy offerings across various firms, along with nuances of certain offerings. However, there are coverage norms from which the insurance industry can gain a better understanding of the risk landscape as it seeks to correct the problem of "silent cyber". In other words, what we are looking to do with "silent cyber" is align portfolios within insurance companies and across the insurance industry. To realize this goal, a common language and framework for understanding must be accessed from within so that the industry can retrofit its aging architecture of insurance terminology to confront this emerging risk.

6. CONCLUSION

Many organizations and government bodies are widely concerned about the risks associated with computers. The media attention does not allow the public to ignore cyber threats, albeit much of the attention is dedicated to individual attacks against disparate companies, and less of it is focused on events that would lead to widespread, cumulative, and catastrophic loss. Since the PRA's work on "silent cyber" in 2015, however, there has been increased awareness of correlated cyber risk, especially silent cyber exposures, and fears of underpricing for it within an insurer's portfolio.[64] Most stakeholders seem to agree that cyber risk is a risk that should be measured, priced, underwritten, and otherwise treated appropriately. So, how do we then reconcile the acute variations in understanding cyber exposures simply as differences in perception of risk? Instead, insurers must admit that there is an emerging consensus around the perceived severity of cyber risk. They must also recognize that the central issue of "silent cyber" is first and foremost a problem of semantics. When insurers and governing agencies have looked for a common language regarding cyber, they have looked outward, instead of looking inward. This has led to confusion and discord, which in hindsight was largely avoidable had the industry and its regulators used the nomenclature at its disposal.

Carriers' first step to addressing "silent cyber" has been to review and potentially alter policy wording with regard to cyber risk. Curiously, most of the characterization has been dedicated to insurers making efforts as to "clarifying intent".[65] The suggestion is that the intent the insurance company seeks to clarify is "subjective" intent.[66] The characterization is a strange one considering insurance contracts: 1) consist of a series of logical syllogisms;[67] and 2) are (for the most

[63] Wollner, K. S., 1999, How to draft and interpret insurance policies, at 80, Casualty Risk Publications (explaining how abstractions are useful in succinctly drawing together a series of concrete ideas into a single concept and in anticipating unforeseen circumstances).
[64] O'Connor, A., 2018, "Insurers' worst fear: cyber hurricane or silent cyber?" Insurance Journal, March 21, https://bit.ly/3HThHv4. 65 See Marsh, 2020, "Silent cyber: what it is and how you can cover cyber perils," August, https://bit.ly/3BjsEUb.
[65] *See* Marsh, 2020, "Silent cyber: what it is and how you can cover cyber perils," August, https://bit.ly/3BjsEUb.
[66] Notably, the EIOPA promotes a mutuality in this undertaking: https://bit.ly/3LKDk35 ("A mutual understanding of contractual definitions, conditions and terms, for both, policyholders and insurance undertakings. Clear and transparent cyber coverages are crucial from a consumer protection perspective. It is the role of industry and consumers associations to provide this clarity and align expectations on cyber insurance coverages to avoid the potential for coverage disputes and costly litigation.").
[67] Wollner supra 63 at 140 ("normalized drafting represents an attempt to bring the certainty of symbolic logic to the drafting process.").

part) standardized. As such, legal interpretation of contracts (especially ones that fit this linguistic structure) depend almost entirely on the plain meaning of the text with the assumption that there is in fact an objective meaning to be communicated and understood. In such an interpretive undertaking, questions of intent on the part of the drafters or ratifiers of the document are rare and reserved for coverage litigation.

If insurers would recognize the futility in arguing over whether they should have seen the problem of "silent cyber" coming, and if they would cease their public posturing over the "original" intent of the policy language, perhaps they could then turn their attention to retrofitting the wording to the realities of the current threat environment, giving this problem some further thought as the PRA had suggested. I propose that insurers (and deciding courts) acquire a deeper understanding of the plain meaning of the wording contained in Cyber insurance forms, take those concepts, and apply them to traditional wording. The best frame of reference for analyzing whether there is Cyber coverage lurking in a traditional policy (and therefore more broadly within a product line) is the coverage afforded by a standalone Cyber policy. Not only will this reveal the plain meaning of critical definitions that govern both cyber as a peril and Cyber as a coverage, but this understanding will be derived from the collective expectation of coverage from the insurance consumer point of view. In other words, if one wants to know if a non-Cyber policy offers Cyber coverage, one must first read and understand what an affirmative Cyber policy offers. From this vantage point, insurers can begin to assess and measure the extent of "silent cyber" within their portfolios.

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company