RANSOMWARE: A DARWINIAN OPPORTUNITY FOR CYBER INSURANCE

ERIN KENNEALLY*

TABLE OF CONTENTS

I. TAKING A CUE FROM NATURE

Charles Darwin's survival of the fittest theory maintains that an organism's ability to adapt to changes in its environment and adjust

* Erin Kenneally is the Global Director of Cyber Insurance at SentinelOne, where she provides cyber risk strategic thought leadership and domain expertise, and leads cyber security and data-driven innovation for cyber insurance solutions. Kenneally was previously Director of Cyber Risk Strategy at Guidewire-Cyence; and served as Portfolio Manager in the Cyber Security Division for the U.S. Department of Homeland Security, Science & Technology Directorate. At the U.S. Department of Homeland Security, Kenneally directed nearly twenty projects across programs in cybersecurity research data infrastructure, privacy, cyber risk economics, and technology ethics. Kenneally also previously served as Technology-Law Specialist at the International Computer Science Institute (ICSI) and the Center for Internet Data Analysis (CAIDA) and Center for Evidence-based Security Research (CESR) at the U.C. San Diego. Kenneally also founded and is CEO of Elchemy, Inc. Kenneally is a licensed attorney specializing in information technology law, including privacy technology, cyber security, AI & autonomous systems ethics and legal risk, trusted data sharing & governance, technology policy, and emergent IT legal risks. She holds Juris Doctorate and Masters of Forensic Sciences degrees and is a graduate of Syracuse University and the George Washington University.

accordingly over time determines its survival success.[1] This process of adaptation at the heart of Darwinism is apropos for the cyber insurance industry amidst the selective pressures introduced by ransomware incidents and claims. This case study proffers adaptations to the changes wrought by ransomware in order to increase cyber insurance resiliency against this peril and prevent coverage extinction. These adaptations exist on a spectrum of controllability and speed of impact. This includes risk management guidance; mandatory ransomware incident disclosure regulation; security controls failure reporting; information security ("InfoSec") prevention and mitigation controls incentives; data-driven risk models; and cyber extortion policy reform.

Borrowing from adaptation theory, there are three potential outcomes for the cyber insurance industry from the "habitat changes" caused by ransomware incidents: (1) extinction; (2) habitat tracking, whereby an organism moves away from the newly dangerous habitat to one more familiar; or (3) genetic change.[2] Respectively, these translate to: (1) insolvency—meaning the forced retreat from the entire cyber line of business as a result of attempting to support demand growth at unreasonable costs—or a rating event;[3] (2) reversion to an environment similar to pre-ransomware pressures, which means either jettisoning ransomware coverage, or pricing premiums or limits in-line with carriers' ransomware risk uncertainty that may result in underserving the quality and quantity of market demands; or (3) evolving capabilities that enable cyber insurers to maintain profitability and/or achieve reasonable loss ratios (based on risk-model-informed capital reserves and risk selection and pricing) for indemnifying ransomware victims.

Cyber insurers are scrambling to wrap their arms around ransomware risk and domesticate this peril. The industry has seen

---

[1] CHARLES DARWIN, THE ORIGIN OF SPECIES BY MEANS OF NATURAL SELECTION (John Murray ed., 6th ed. 1882).

[2] Susan King, *What is Adaptation Theory?*, SCIENCING (Mar. 13, 2018), https://sciencing.com/adaptation-theory-5105998.html.

[3] To date, and based on the author's knowledge, ratings institutions have not lowered any cyber insurance company ratings due solely to cyber peril. A rating event could conceivably derive from losses that would materially affect capital reserves/liquidity, which is a key credit consideration, such as the case with Moody's downgrade of Equifax following its 2017 data breach. *See* Kevin Townsend, *Moody's Downgrades Equifax Outlook to Negative Over 2017 Data Breach*, SECURITYWEEK (May 23, 2019), https://www.securityweek.com/moodys-downgrades-equifax-outlook-negative-over-2017-data-breach.

appreciable jumps in frequency and cost of reported incidents and claims, payouts, and demands in the last several years. Notable statistics include:

- Ransomware attacks increased nearly 150% after remote work increased due to the Covid-19 pandemic;[4]
- Ransomware claims and the cost of payments jumped approximately 230% from 2018 to 2019;[5]
- Cyber extortion demands paid in 2019 were four times higher than the previous year;[6]
- Average ransomware payouts for U.S. businesses went through the roof between third quarter 2018 and second quarter 2020—from under $10,000 in the latter half of 2018 to more than $178,000 per event by the middle of 2020, with large enterprises averaging over $1 million;[7] and

---

[4] *Amid Covid-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted*, VMWARE: SEC. BLOG (Apr. 15, 2020), https://blogs.vmware.com/security/2020/04/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted.html.

[5] Ben Dyson, *Cyber Insurers Tighten Underwriting, Raise Prices as Ransomware Wave Hits*, S&P GLOB. MKT. INTEL. (Oct. 22, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-tighten-underwriting-raise-prices-as-ransomware-wave-hits-60829821; Barnaby Page, *Ransomware: A Perilous Price to Pay*, SENTINELONE: BLOG (Dec. 7, 2020), https://www.sentinelone.com/blog/ransomware-and-the-perils-of-paying/.

[6] Page, *supra* note 5.

[7] *See Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase,* COVEWARE (Aug. 3, 2020), https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report*;* PALO ALTO NETWORKS, RANSOMWARE THREAT REPORT 3 (2021), https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf ("The average ransom paid by organizations in the US, Canada, and Europe increased from US$115,123 in 2019 to $312,493 in 2020—a 171% year-over-year increase.").

- Ransomware claims have comprised up to 40% of some insurers' cyber books,[8] along with a putative 10% loss ratio increase due to ransomware in 2019.[9]

As a result, premiums have risen[10] and insurers have become more selective,[11] undoubtedly underserving the quality and quantity of coverage demands. Taking a cue from Darwin, the path forward lies in recognizing ransomware as the functional equivalent of a natural selection event, admitting the possible outcomes, and taking responsibility for the trajectory that assures adaptation. Simply put, ransomware is a clarion call for cyber insurance industry adaptation.

II. PACE LAYERING

The starting point in crafting the cyber insurance industry's path forward is understanding the changed cyber insurance habitat ushered in by ransomware. The flag markers that the habitat has changed include:

- Insufficient actuarial data (loss history) for pricing premiums and coverage loss limits;
- Lack of risk control efficacy and attack vector lessons-learned;
- Expanding delta between cybercrime loss and claims paid;

---

[8] COALITION, CYBER INSURANCE CLAIMS REPORT 9–10 (2021), https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2021-07-Coalition-Cyber-Insurance-Claims-Report-2021-h1.pdf (noting that the claims frequency in the first half of 2020 was 41%).

[9] JON LAUX, CRAIG KERMAN & SAMMIE COAKLEY, US CYBER MARKET UPDATE: 2019 US CYBER INSURANCE PROFITS AND PERFORMANCE 4–5 (2020), https://aon.io/2020-us-cyber-market-update.

[10] *See, e.g.*, *id.* at 3; Page, *supra* note 5 (quoting Chris Keegan of Beecher Carlson, "[i]nsurance carrier [premium] increases of zero to five percent rate in the second quarter 2020, gave way to five to fifteen percent increases in the third quarter which were raised again to ten to thirty percent in the fourth quarter. Not all increases are in this range, but cyber insurance buyers should be prepared for requests at these levels. Some adjustments to the structure of programs, such as raising retentions, can be made to limit the increased costs and carriers are amenable to these discussions.").

[11] Page, *supra* note 5 (quoting Chris Keegan of Beecher Carlson, "[i]n addition, insurers are focusing on more careful selection of their policyholders.").

- A gap in spending between cyber security and risk transfer;
- Uncomfortable ransomware loss ratio distributions;
- Premiums that are more sensitive to market competition rather than organizations' security posture and perceived ransomware threat; and
- Incongruency between threat capabilities and modeled risk profiles, including loss accumulation potential.[12]

The next step in the process of crafting a path forward is assessing and identifying the adaptations—change agents—that will put cyber insurers on the path to survival regarding ransomware coverage. Enter "pace layering," a framework for diagnosing and prescribing how adaptable an entity[13] is to change.[14] Pace layering proposes that every entity is the product of adaptation to the demands of six-time scales that move and change at different paces.[15] Ordered from slow to fast, these are nature, culture, governance, infrastructure, commerce, and aesthetics (e.g., art and fashion).[16] The slower layers are thought of as lower, more foundational and methodical, but provide stability.[17] The fast layers are more innovative and less encumbered, but also less stable.[18] For example, in a healthy, strong society our legal systems change slower than the rate of commerce, throttling the rate of change in a society to enable social normative grounding. As pace layering's framer, Stewart Brand, notes, "[f]ast gets all our attention, but slow has all the power."[19]

---

[12] *See generally* Ben Dyson, *Cyberrisk Models Advance Quickly, but Still Lag Natural Catastrophe Reliability*, S&P GLOB. (Dec. 30, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyberrisk-models-advance-quickly-but-still-lag-natural-catastrophe-reliability-61766574.

[13] An umbrella term used here to represent a system, organism, or organization.

[14] Stewart Brand, *Pace Layering: How Complex Systems Learn and Keep Learning*, J. DESIGN & SCI. (Feb. 4, 2018, 2:45 PM), https://jods.mitpress.mit.edu/pub/issue3-brand/release/2.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

Each layer interplays with the others to adapt to change in different ways, with the continuity of all the layers determining survival.[20] When faster layers move too slowly, the entity may become stagnant as it seeks to recover from its fast growth, or have cultural level misalignment.[21] Conversely, faster layers (e.g., commerce) can move too quickly for what infrastructure and culture can support, causing a system breakdown.[22] Similarly, when slower layers move too quickly, they can cause turmoil, whereas, if they move too slowly, they impede progress at higher layers.[23]

The 1906 San Francisco earthquake is relevant and illustrative of how pace layering can explain the mid- and higher-layer adaptations required to recover from abrupt changes at the lowest layer. The earthquake led to "a rapid change in nature [which] sent a shockwave all the way up to the commerce layer, destroying the city infrastructure, bankrupting businesses and households, and requiring governance to step in and subsidize the recovery."[24] The financial infrastructure could not absorb the shocks that were unbuffered by an insurance industry that was unable to underwrite damage on such a large scale, and the market panicked a year later.[25]

Autonomous vehicles are a more current example where change introduced at the fast layers exposes tensions at slower layers. At the commerce layer, auto manufacturers have mobilized quickly, moored by a relatively mature infrastructure.[26] But legal (e.g., governance) and ethical (e.g., culture) layers flounder when comes to assigning responsibility for the inevitable "trolley dilemma", where car driven by artificial intelligence is put in a position to make a choice to save the driver and plunge into a crowd or sacrifice the driver for the sake of bystanders.[27]

---

[20] *Id.*

[21] Jonathan Maricle, *Pace Layering: An Application Strategy for Resilient Products*, PURPLE, ROCK, SCISSORS: BLOG (Oct. 11, 2018), https://purplerockscissors.com/blog/pace-layering-application-strategy.

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *The San Francisco Earthquake of 1906: An Insurance Perspective,* INS. INFO. INST., https://www.iii.org/article/san-francisco-earthquake-1906-insurance-perspective (last visited Dec. 30, 2021) ("Of the $235 million in insured losses, only about $180 million was paid out in claims as many financially-strapped insurers could pay only a share of the actual losses.").

[26] Maricle, *supra* note 21.

[27] *Id.*

III. RANSOMEWARE ADAPTATIONS

We can apply the pace layering framework to diagnose and recommend adaptations to the current ransomware insurance challenges by answering the following three key questions.

1. In which layer(s) are ransomware impacts most felt?

Ransomware impacts have been felt most immediately through selective pressures at the commerce layer. Following the title of Jim Carrey's cult 1994 movie, *Dumb & Dumber,*[28] insurance companies have been throwing dumb capacity at the fast-growing commerce layer and dumber risk management at the infrastructure layer.[29] This emergence has been accelerated by the digital revolution of cryptocurrency technology, which has enabled a less risky and faster pay-out for attackers.[30] The industry is now struggling to absorb the commodification of ransomware coverage in response to dynamic ransomware threat trends and concomitant commoditization of attacks.[31] In short, there has been a disconnect between the actual risk and how it was priced in premiums. While this peril is not novel, carriers in the previous, longstanding soft cyber market with healthy reserves and capacity continued to write ransomware policies (albeit more selectively or with higher premiums) without the necessary supporting

---

[28] DUMB & DUMBER (New Line Cinema 1994).

[29] *See* Ryan Smith, *Cyber Insurance Market Continues to Accelerate*, INS. BUS. MAG.: AM. (May 11, 2018), https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurance-market-continues-to-accelerate-100346.aspx ("'As cyber underwriting exposure grows, more cyber incidents will be covered, generating claims that lead to weaker underwriting results,' said Gerry Glombicki, director at Finch. 'From an individual underwriter perspective, the risk of naïve capacity entering the market, growing rapidly without sufficient expertise and ultimately suffering outsized losses in cyber is an expanding possibility.'").

[30] *See* GUIDEWIRE-CYENCE, TAMING THE UNCERTAINTY OF RANSOMWARE RISK 4–5 (2020), https://success.guidewire.com/rs/140-LHX-683/images/WP_RansomwareInsights_June2020.pdf.

[31] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 19 (2021), https://www.gao.gov/assets/gao-21-477.pdf ("[E]ven as insurers collect more data and hone predictive models based on prior cyber threats, the underlying exposure keeps changing. This makes it difficult to create a reliable predictive model when it is not clear what new objective, strategy, or technique cyber threat actors may deploy.").

infrastructure needed to inform pricing and selection adjustments to the risk.[32]

2. Out of which layer(s) did the ransomware challenge emerge?

While the ransomware selective pressure has been felt most immediately at the commerce layer, it stemmed from inadequate growth at the governance and infrastructure layers. This tension has built up over the past five-plus years of expanded underwriting for this peril, without commensurate progress at the infrastructure and governance layers of cyber insurance that are needed to mitigate the balance sheet/loss ratio shocks that are now felt at the commerce layer.[33] These infrastructure deficiencies include the lack of policies and processes to bring about sufficient security risk management coordination or implementation incentives, learned knowledge of the efficacy of security controls in the face of specific incidents, and risk models that are informed by critical data and expert knowledge.[34]

3. From which layer(s) is a solution most likely to emerge?

The answer here includes multiple entities responding at multiple layers.[35] Ransomware challenges are best addressed by introducing adaptations[36] at the cyber insurance's cultural and governance layers,[37] and ultimately effectuated at the infrastructure and commerce layers. The

---

[32] *See id.* at 13–14 (noting that limited historical data on cyber losses makes pricing and quantifying risk difficult).

[33] *See id.* at 8–13; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., ASSESSMENT OF THE CYBER INSURANCE MARKET 9–10 (2019), https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf.

[34] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 31, at 17–26; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 33, at 2–17.

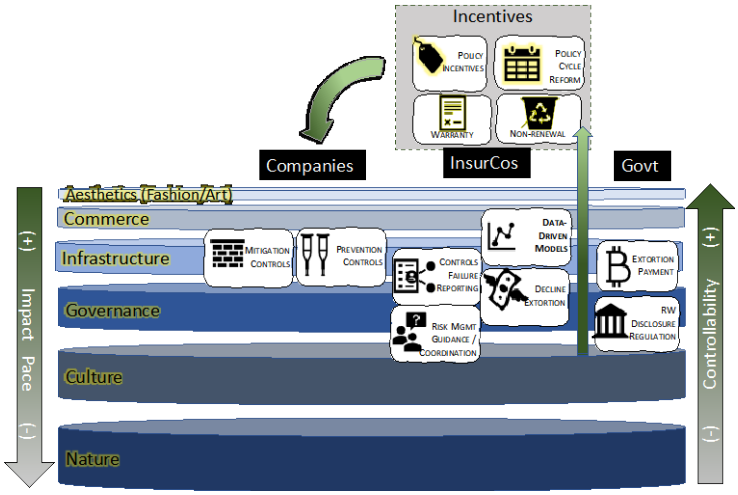
[35] *See infra* Figure 1.

[36] *See* adaptations discussion *infra* Section IV.

[37] In order to effectuate the adaptation, carriers need to embrace their role as stewards of risk management (see Figure 1) and thereby require/incentivize implementation of cyber security controls to prevent and mitigate loss. This is juxtaposed to what they've historically done which is look to another institution (i.e., government and case law) to be that forcing function for selection and implementation of security controls.

adaptations introduced at the infrastructure, governance, and culture layers are the core of the Darwinian path forward for cyber insurance and ransomware.

Figure 1: Layers of Ransomware Insurance Adaptations



IV. ADAPTATIONS–THE PATH FORWARD

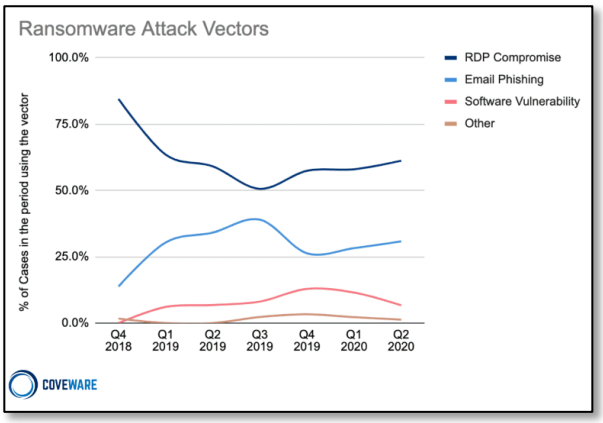
The rest of this paper explores in more detail the specific adaptions and necessary incentives to create a stable response to the ransomware risk.

A. INFOSEC LOSS PREVENTION AND MITIGATION CONTROLS

While the progress on gaining the necessary ransomware actuarial data leaves much to be desired, InfoSec statistics around the threat and vulnerability dimensions of risk have improved and show remarkable consistency in the case of ransomware. Reports from leading vendors assert that the most popular attack vectors and sources of ransomware incidents are

Remote Desktop Protocol ("RDP"),[38] email phishing ("SPAM"), and unpatched vulnerabilities.[39]

Figure 2: Common Ransomware Attack Vectors[40]



Knowing where to spend limited cyber security budgets can be challenging—especially in what some would refer to as a market for lemons, where product and service efficacy benchmarks are lacking, and successful attacks often exploit the human-technology interface gaps.[41] There are nonetheless "known-knowns," which involve basic blocking and tackling that can significantly decrease risk exposures. These known-knowns include: ensuring that RDP ports and services are not openly exposed to the internet; maintaining updated software patches for virtual private networks (VPN) and appliances that provide entryways to corporate networks; implementing

---

[38] For a description of RDP see Jareth, *How to Secure RDP From Ransomware Attacks*, EMSISOFT: BLOG (July 20, 2020), https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/.

[39] *See* RECORDED FUTURE, PULSE REPORT: ANALYZING THE THREAT OF RANSOMWARE ATTACKS AGAINST US ELECTIONS 7–9 (Allan Liska ed., 2020), https://go.recordedfuture.com/hubfs/reports/cta-2020-0820.pdf; Jareth, *supra* note 38; *Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, supra* note 7. *See also infra* Figure 2.

[40] *Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, supra* note 7.

[41] *See* Daniel W. Woods & Tyler Moore, *Cyber Warranties: Market Fix or Marketing Trick?,* 63 COMMC'NS ASS'N FOR COMPUTING MACH. 104 (2020).

endpoint detection, protection, and response (EDR); applying email fraud/social engineering controls; and enforcing multifactor authentication (MFA) and privilege access management (PAM) to harden IdAM (identity and access management).[42] These risk prevention controls are the direct responsibility of corporate policyholders, yet cyber carriers on the whole have done little to incentivize their adoption.[43]

In addition to prevention controls, arguably the closest thing to an InfoSec silver bullet for ransomware mitigation is backup recovery technology. Since locking systems and extorting payments in exchange for decryption keys is the trademark of ransomware, effective backups are its strongest antibody.[44] Indeed, implementation complexity, costs, and associated business continuity implications are not monolithic and can be complicated.[45] Yet, the difference between quick and local backups[46] and ransomware-resistant backups[47] is that the former may involve weeks of

---

[42] *See, e.g.*, Marisa Midler, *3 Ransomware Defense Strategies*, SOFTWARE ENG'G INST.: BLOG (Nov. 9, 2020), https://insights.sei.cmu.edu/blog/3-ransomware-defense-strategies/; *Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase*, *supra* note 7; Perry Carpenter, *5 Defenses for 5 Ransomware Root Causes*, CPO MAG. (Dec. 6, 2021), https://www.cpomagazine.com/cyber-security/5-defenses-for-5-ransomware-root-causes/.

[43] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 31, at 17 ("NAIC representatives told us the industry may offer additional cyber services to help policyholders manage their cyber risk. But they added that some small and mid-size businesses have limited technical resources or staff with cybersecurity expertise and are not taking full advantage of these services."); Shauhin A. Talesh & Bryan Cunningham, *The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy*, 5 UTAH L. REV. 967, 1003–04 (2021) (discussing pre- and post-breach services insurers provide their insureds but do not require them to use in order to get premium discounts or to qualify for coverage).

[44] *See* Emily Heaslip, *What Small Businesses Need to Know About Ransomware*, U.S. CHAMBER OF COM. (June 9, 2021), https://www.uschamber.com/co/run/technology/small-businesses-ransomware.

[45] *See Data Backup and Disaster Recovery*, ONTECH SYS., INC., https://ontech.com/data-backup-disaster-recovery/ (last visited Jan. 2, 2022).

[46] For example, simply keeping an archived copy of data.

[47] Best practices include the 3-2-1 Rule: keeping three backups on two different types of media with one of which being offsite; securing data using industry standard encryption, and regularly testing to ensure data accuracy and recoverability. *See*

downtime due to failed and insufficient recoverability and six to seven figure business interruption, whereas the latter may involve days of downtime and lower upfront cost.[48] Some statistics reveal that sixty percent of company backups are incomplete and fifty percent of restores fail.[49] This has resulted in insurers opting to pay ransoms as a result of cost-benefit analyses that find the business interruption costs associated with recovery and restoration from backups to be more painful than coughing up the extortion fees and hoping that attackers will honor their word.[50] The pink elephant question is, why then are insurers not insisting on provably robust disaster recovery technologies and processes as a precondition to coverage?

Ransomware is exposing cracks in the cyber resilience of both cyber insurers and victim organizations. More significantly, it lays bare the gap between the two, the closure of which is key to improving resilience for sets of stakeholders. Organizations targeted by ransomware are ultimately the ones in control of implementing prevention and mitigation controls, yet economic, talent, and governance deficiencies leave them unattended in many companies.[51] As transferors of financial risk from victim companies,

---

PETER KROGH, THE DAM BOOK: DIGITAL ASSET MANAGEMENT FOR PHOTOGRAPHERS 88 (Colleen Wheeler ed., 2nd ed. 2006).

[48] *See 4 Data Recovery Solutions for Small Businesses*, ONTECH SYS. INC., https://ontech.com/data-recovery-solutions/ (last visited Jan. 2, 2022).

[49] *5 Shocking Statistics About Data Backup and Recovery*, ONTECH SYS. INC., https://ontech.com/data-backup-statistics/ (last visited Jan. 2, 2022).

[50] *See* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019, 5:00AM), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

[51] *See* Ariel E. Levite, Scott Kannry & Wyatt Hoffman, *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance* 24 (Carnegie Endowment for Int'l Peace, Working Paper Oct. 2018), https://carnegieendowment.org/files/Cyber_Insurance_Formatted_FINAL_WEB.PDF (discussing the "perverse incentive structure[s] for many industries" and how it leads to the problems currently faced in cyber security); *The Role of Cyber Insurance in Risk Management: Hearing Before the S. Comm. on Cybersecurity, Infrastructure Prot., & Sec. Techs. of the Comm. on Homeland Sec.*, 114th Cong. (2016), https://www.govinfo.gov/content/pkg/CHRG-114hhrg22625/html/CHRG-114hhrg22625.htm [hereinafter *The Role of Cyber Insurance in Risk Management*]. *See generally* OECD, ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT 14, 74–77 (2017), https://www.oecd.org/daf/fin/insurance/

insurers are in a position to indirectly bring about these infrastructural changes by wielding various incentives to improve the cyber hygiene that can significantly impact ransomware loss.[52] Properly structured, the following incentives can be a behavioral-forcing function to reduce ransomware risk:

- Refuse to bind/renew companies who cannot attest to having these controls in place;[53]
- Institute premium reductions for those that have a clean exposure signal (e.g., open RDP) bill of health;[54]
- Change policy cycles to be more agile and responsive to cyber exposures;[55]
- Issue cyber warranty[56] for security vendors to enhance trust in efficacy claims;[57]

Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf (discussing that while companies are in control of their security procedures, insurance companies can help in various ways due to their expertise).

[52] *See* Levite, Kannry & Hoffman, *supra* note 51, at 20–21; *The Role of Cyber Insurance in Risk Management*, *supra* note 51; OECD, *supra* note 51, at 74–77; Letter from Linda A. Lacewell, Superintendent, N.Y. State: Dep't Fin. Servs., to All Authorized Prop./Cas. Insurers (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02; DANIEL M. HOFMANN, ADVANCING ACCUMULATION RISK MANAGEMENT IN CYBER INSURANCE: PREREQUISITES FOR THE DEVELOPMENT OF SUSTAINABLE CYBER RISK INSURANCE MARKET (2019), https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/research_brief_advancing_accumulation_risk_management_in_cyber_insurance.pdf.

[53] *See* Levite, Kannry & Hoffman, *supra* note 51, at 18 ("Third-party expert assessments of a policyholder's assets would give insurers greater insight and understanding of risk exposure. More important, these practices would directly raise the baseline level of security by identifying flaws and motivating efforts to mitigate them by making coverage conditional upon their being addressed."); *The Role of Cyber Insurance in Risk Management*, *supra* note 51; OECD, *supra* note 51, at 74.

[54] OECD, *supra* note 51, at 14–15 (noting premiums may also be reduced if policyholder seeks to reduce its risks by investing in better cyber security).

[55] *See generally The Role of Cyber Insurance in Risk Management*, *supra* note 51; OECD, *supra* note 51.

[56] Cyber warranty covers the cost to remediate and update a vendor's client system in the event its product and/or services are the cause of a cyber peril. *See* Woods & Moore, *supra* note 41, at 105–06.

[57] Arguably warranties may not incentivize controls investment, rather they prevent vendors from overexaggerating the functionality of products. *See id.* at 106.

- Policy cancellation or amendment of terms and conditions mid-policy if an insured neglects recommended security improvements.[58]

B. RISK MANAGEMENT COORDINATION

Incentivizing ransomware risk controls is a necessary but insufficient adaptation at the commerce layer if insurers want to withstand the dynamic, evolving risk that is ransomware. Unless incentives are intertwined with infrastructure layer security metrics, the prescribed controls will invariably lag behind threats and vulnerabilities. As well there will also be continued conceptual misalignment between the ransomware coverage (insured risk) and ground-up risk, which is a recipe for coverage blind spots and market mistrust when claims are denied.[59] Rather than relying primarily on exogenous factors like compliance or glacially-paced case law[60] to define risk, embracing a risk management coordination role enables cyber insurers to proactively address losses closer to where they are felt and take the fight to ransomware.[61] Security risk metrics coordination "between underwriters, brokers, and [I]nfo[S]ec professionals can better align risk optics, lower information asymmetries, and scale victimology beyond the current ad hoc

---

[58] *See* Levite, Kannry & Hoffman, *supra* note 51, at 20–21; *The Role of Cyber Insurance in Risk Management*, *supra* note 51; OECD, *supra* note 51, at 74.

[59] *See* OECD, *supra* note 51, at 8–9 (discussing insured's level of uncertainty over cyber insurance coverage); Levite, Kannry & Hoffman, *supra* note 51, at 18–19 (arguing for "[c]ontract simplicity and understanding.").

[60] *See* ANDREW GRANATO & ANDY POLACEK, FED. RSRV. BANK OF CHI., CHI. FED LETTER NO. 426, THE GROWTH AND CHALLENGES OF CYBER INSURANCE 4 (2019) ("This [legal] uncertainty standing in data breach litigation . . . directly affects the probability that an insurer will have to pay claims in the event of a data breach and this, in turn, affects how they should price their insurance policies."); U.S. DEP'T OF HOMELAND SEC., CYBER RISK ECONOMICS CAPABILITY GAPS RESEARCH STRATEGY 13, 16–17, 20 (2018), https://www.dhs.gov/sites/default/files/publications/3950_CYRIE_Report_FINAL508.pdf [hereinafter CYRIE REPORT].

[61] *See, e.g.*, Richard S. Betterley, *Cyber/Privacy Insurance Market Survey*, BETTERLEY REP., June 2015, at 13–14. Robust underwriting of cyber insurance coverage can contribute to reducing cyber risk at an aggregate level by disseminating and ensuring compliance with good security practices–similar to the market for large commercial property coverage where insurance companies play a valuable risk consulting role. *See id.* at 7; OECD, *supra* note 51, at 73–75.

dynamics."[62] Insurance companies have thus far formed partnerships with InfoSec organizations for post-event response and consulting.[63] What is needed now is synchronization with the InfoSec consortium and other organizations for prevention and mitigation measures and advisement.

Several notable statistics shed light on this coordination gap.[64] First, is the ratio between the economic cost of cybercrime and claim payouts, which was estimated to be less than one percent in 2016.[65] The difference between cybercrime costs and insurance premiums, estimated to be $695 billion, can serve as a similar proxy.[66] Similarly, the disparity between cybersecurity spending and insurance premiums is estimated to be $116 billion.[67] Global cyber insurance expenditures and risk transfers are growing at slower rates than overall InfoSec spending and cybercrime losses.[68] These

---

[62] Erin Kenneally, *Ways Insurers Can Reduce the Threat of Cyber Risks*, NU PROP. & CAS. (Feb. 4, 2022, 5:00 AM), https://www.propertycasualty360.com/2022/02/04/ways-insurers-can-reduce-the-threat-of-cyber-risks/. *See also* OECD, *supra* note 51, at 14.

[63] THE COUNCIL OF INSURANCE AGENTS & BROKERS, CYBER INSURANCE MARKET WATCH SURVEY: EXECUTIVE SUMMARY 7 (6th 2018), https://www.ciab.com/download/15077/.

[64] *See infra* Figures 3 and 4.

[65] The White House Counsel of Economic Advisors estimated the economic cost of cybercrime to be between $57 billion to $109 billion in 2016. COUNCIL OF ECONOMIC ADVISERS, EXECUTIVE OFFICE OF THE PRESIDENT, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 36 (2018), https://www.hsdl.org/?view&did=808776. "During that same period, U.S. insurance companies incurred $356 million in claims from policyholders, equivalent to less than 1% of estimated losses. Compare this to natural catastrophes, where 50% of losses between 2015 and 2018 were paid by insurers." GRANATO & POLACEK, *supra* note 60, at 5 (footnotes omitted). This information was "[b]ased on insurance statutory filings from S&P Global Market Intelligence. Data include both standalone and packaged policies, but not claims paid by surplus line insurers that are not required to report financials to the NAIC." *Id.* at 5 n.13.

[66] Manuel Adam & Simon Ashworth, *Cyber Risk in a New Era: Insurers Can be Part of the Solution*, S&P GLOB. RATINGS (Sept. 2, 2020, 11:43 AM), https://www.spglobal.com/ratings/en/research/articles/200902-cyber-risk-in-a-new-era-insurers-can-be-part-of-the-solution-11590046 (comparing the estimated $5 billion in commercial and private cyber insurance premiums to the estimated $700 billion for yearly economic costs of cybercrime). *See also infra* Figure 3.

[67] *See infra* Figure 4.

[68] *See* Adam & Ashworth, *supra* note 66; Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARV. BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem.

two trajectories signal the current incongruity between what should be a symbiotic relationship, as well as an underserved opportunity for cyber insurers.

Figure 3: Annual Cyber Security and Cyber Insurance Spending Worldwide[69]

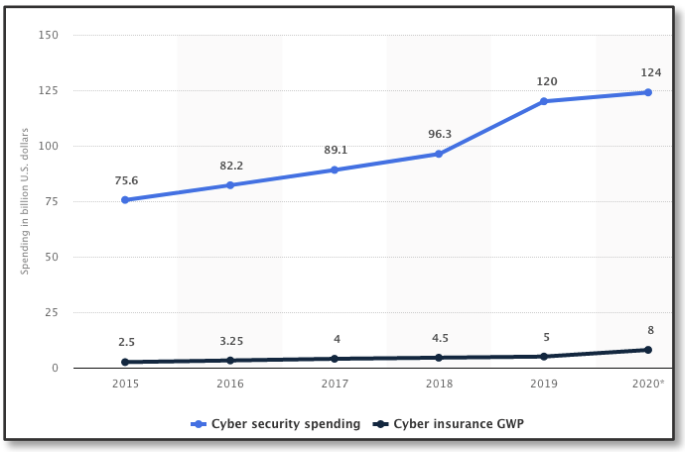
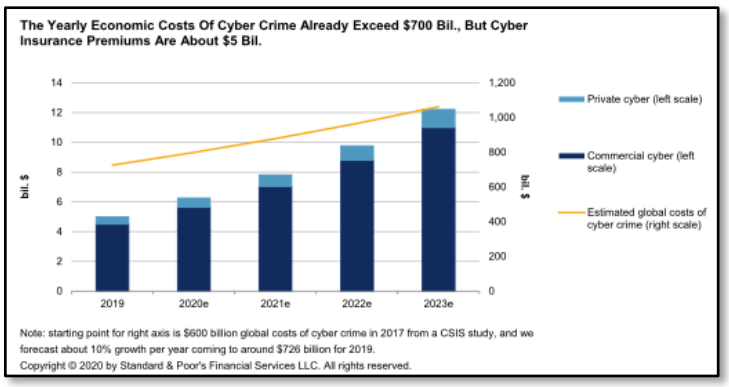


Figure 4: Cost Trend of Cyber Crime v. Cyber Insurance Premiums[70]



[69] Joseph Johnson, *Global Cyber Security & Cyber Insurance Spending 2015-2020,* STATISTICA (Jan. 25, 2021), https://www.statista.com/statistics/387868/it-cyber-securiy-budget/.

[70] Adam & Ashworth, *supra* note 66.

How the risk management coordination mantle can be taken up by cyber insurers lies on a spectrum. At a basic level, simply requiring policyholders/applicants to provide or verify fundamental firmographics and technographics (e.g., company domain name, subdomain ownership) for accurate cyber risk assessment is a trivial lift. On the other end of the spectrum, incentivizing insureds to share internal security telematics is a known missing link in cyber risk understanding.[71] While contribution of inside-the-firewall security data would require some technical, procedural, and policy changes on the part of the insured and insurer, incorporating this telemetry it would be a game changer for cyber risk insurance.

C. RANSOMWARE DISCLOSURE REGULATION

Since, arguably, industry-specific federal regulation, litigation, and state laws requiring reporting and disclosure of data breaches[72] drove the actuarial foundation upon which data breach coverage is anchored, it begs asking do we need a similar forcing function in order to adapt to ransomware risk? Regulatory fines, reporting requirements, liability and legal costs made data privacy and insecurity losses tangible and manifest, thereby capturing the attention of the industry.[73] This regulatory impetus fed the rational expectation that improved cybersecurity would result in reduced premiums and/or higher liability limits.[74]

As more ransomware attacks hybridize to exfiltrate and hold data hostage to pressure extortion payments, many of the existing public

---

[71] *See* OECD, *supra* note 51, at 96; JAMIE MACCOLL, JASON R C NURSE & JAMES SULLIVAN, CYBER INSURANCE AND THE CYBER SECURITY CHALLENGE 29–30 (2021), https://static.rusi.org/247-op-cyber-insurance-fwv.pdf.

[72] *See* CYRIE REPORT, *supra* note 60, at 20.

[73] *Special Report: Cyber Insurance Market: Stress Testing the Future*, BEST'S REV. (Oct. 2018), https://news.ambest.com/articlecontent.aspx?pc=1009&refnum=278309 ("The U.S. cyber insurance market took off as data breach notice and other privacy laws were implemented which highlights the tangible costs associated with data breaches.").

[74] *See* THE COUNCIL OF INS. AGENTS & BROKERS, CYBER INSURANCE MARKET WATCH SURVEY EXECUTIVE SUMMARY 7 (3rd ed. 2016), https://www.ciab.com/wp-content/uploads/2017/04/102016CyberSurvey_Final.pdf; THE COUNCIL OF INS. AGENTS & BROKERS, CYBER INSURANCE MARKET WATCH SURVEY EXECUTIVE SUMMARY 3 (2nd ed. 2016), https://www.ciab.com/wp-content/uploads/2017/04/2ndCyberMarketWatch_ExecutiveSummary_FINAL.pdf; THE COUNCIL OF INS. AGENTS & BROKERS, *supra* note 63, at 7–8.

disclosure requirements (and privacy claims) will be triggered.[75] Yet it is very much an open question as to whether that will be sufficient for robust underwriting of ransomware risk. At present, the industry has an inadequate understanding of ransomware risk distributions to select risks and underwrite policies proportional to reserves and risk appetite, while still being responsive to the needs of the market.[76] In any case, the government is uniquely situated to control for this adaptation.

D. CONTROL FAILURE REPORTING

The adage, "to not know history is to be doomed to repeat it"[77] is sage advice for ransomware adaptation. Standard components of cyber incident digital forensics and incident response ("DFIR") reporting include information about attack vectors and control failures, which is to say, how attackers were able to access company networks and what technical or administrative safeguards were deficient.[78] While the certainty of these attributions varies, insurers have by and large left these ransomware claims artifacts on the cutting room floor, foregoing valuable lessons-learned and

---

[75] For example, entities covered by Health Insurance Portability and Accountability Act ("HIPAA") that are infected with ransomware are presumed to have a reportable data breach unless it can be shown that there was a low probability that the protected health information ("PHI") has been compromised. Off. for Civ. Rts., *Breach Notification Rule*, HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. S*ee also* Yotam Gutman, *The Stopwatch Is Ticking | How Ransomware Can Set a Breach Notification in Motion*, SENTINELONE: BLOG (June 1, 2020), https://www.sentinelone.com/blog/the-stopwatch-is-ticking-how-ransomware-can-set-a-breach-notification-in-motion/.

[76] MACCOLL, NURSE & SULLIVAN, *supra* note 71, at vii.

[77] *See History Repeating*, VA. TECH COLL. OF LIBERAL ARTS & HUM. SCIS., https://liberalarts.vt.edu/magazine/2017/history-repeating.html (last visited Mar. 1, 2022) ("Spanish philosopher George Santayana is credited with the aphorism, "[t]hose who cannot remember the past are condemned to repeat it . . . .").

[78] *See Digital Forensics and Incident Response (DFIR)*, CROWDSTRIKE (July 1, 2021), https://www.crowdstrike.com/cybersecurity-101/digital-forensics-and-incident-response-dfir/; Stephen Watts, *Digital Forensics and Incidental Response (DFIR): An Introduction*, BMC (Feb. 13, 2020), https://blogs.bmc.com/dfir-digital-forensics-incident-response/?print-posts=pdf.

helping perpetuate underwriting whack-a-mole.[79] Imagine if, over the course of the last decade of claims, individual insurers, or better yet, the collective industry, had documented these DFIR or security audit data points as part of the claims process. While there is no guarantee that the past is prologue when it comes to cyber risk, attacker tactics, techniques, and practices ("TTPs") follow patterns and paths of least resistance, and knowing their playbooks goes a long way towards reducing exposures.[80]

Concerningly, there is a trend with insurers—mostly in the small and medium-sized enterprises ("SME") market—cutting costs by collecting less information during the underwriting process and eliminating data fields in the notification of loss.[81] This trend works counter to the below-suggested adaptation aimed at developing more mature and validated cyber loss models to align the underwritten risk with price premiums.[82]

Adaptation within a dynamic cyber risk landscape and a market of proliferating security widgets and services whose efficacy is hard to differentiate, requires committing this data to the actuarial record. Collecting and sharing controls failure data would mark a significant step toward being

---

[79] *See generally* ERIN KENNEALLY, HIDING IN PLAIN SIGHT: TOWARDS NOW-GEN CYBER RISK UNDERWRITING (2021), https://success.guidewire.com/Whitepaper-HidinginPlainSightTowardsNow-GenCyberRiskUnderwriting_Registration.html; Daniel W. Woods & Rainer Böhme, *How Cyber Insurance Shapes Incident Response: A Mixed Methods Study,* 20 WORKSHOP ON ECONS. INFO. SEC. (2021), https://informationsecurity.uibk.ac.at/pdfs/DW2021_HowInsuranceShapes_WEIS.pdf.

[80] Ken Dunham & Christopher Lucas, *TTPs Within Cyber Threat Intelligence,* OPTIV (Jan. 19, 2017), https://www.optiv.com/explore-optiv-insights/blog/tactics-techniques-and-procedures-ttps-within-cyber-threat-intelligence.

[81] *See* PWC, TOP ISSUES: SHIFTING COST CURVES TO STAY IN THE COMMERCIAL INSURANCE RACE 4–5 (2018), https://www.pwc.se/sv/pdf-reports/forsakring/insurance-top-issues-2018-commercial-cost-curve.pdf (noting seventy-five percent of insurers have implemented costs cutting programs, which may include reducing information gathering in the underwriting process). PWC, ARE INSURERS ADEQUATELY BALANCING RISK & OPPORTUNITY? FINDINGS FROM PWC'S GLOBAL CYBER INSURANCE SURVEY (2018), https://cyber-liability.org/reports/pwc-cyber-insurance-survey.pdf.

[82] *See, e.g.*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., ASSESSMENT OF THE CYBER INSURANCE MARKET 13 (2018), https://www.cisa.gov/sites/default/files/publications/20_0210_cisa_oce_cyber_insurance_market_assessment.pdf [hereinafter CISA REPORT].

able to qualify and quantify the end-to-end relationships between threats, security compliance, and incident outcomes.[83]

E. DATA-DRIVEN MODELS

Because ransomware is a dynamic threat whose prevalence is unknown, and because it operates within interconnected target landscapes, knowledge of yesterday's attacks is insufficient to inform us about tomorrow's outcomes.[84] Cyber foresight is, therefore, a prerequisite for effective ransomware risk segmentation, assessment, pricing, and defense. Foresight comes by way of predictive models that include both historical data and expert knowledge.[85] Simply fitting historical event frequency and severity distributions around ransomware event variables and parameters that appear to conform with what the market thinks is accurate, will not anticipate the future changes that are endemic to this risk.[86] The adaptation needed is empirical data-driven ransomware models which incorporate expert knowledge and that validate over time against actual results.[87] The end game is validated; predictive models that drive more robust and reliable pricing models and inform underwriting guidelines.

Models can be validated by measuring the difference between the predicted and observed outcomes.[88] This is typically done using historical data only, with ongoing monitoring of the actual results being a secondary consideration that is too often ignored.[89] But in an actively changing environment, historical results often lack necessary information for predicting the future, meaning that a model whose output agrees with

---

[83] *See id.* at 14; CYRIE REPORT, supra note 60, at 29–31.

[84] *See* MACCOL, NURSE & SULLIVAN, *supra* note 71, at 31.

[85] *See* Venkatesh Jaganathan, Priyesh Cherurveettil & Premapriya Muthu Sivashanmugan, *Using a Prediction Model to Manage Cyber Security Threats*, 2015 SCI. WORLD J. (SECURITY OF INFORMATION AND NETWORKS SPECIAL ISSUE) 1, 4 (2015), https://downloads.hindawi.com/journals/tswj/2015/703713.pdf.

[86] *See* MACCOL, NURSE & SULLIVAN, *supra* note 71, at 31.

[87] *See* Jaganathan, Cheruvreettil & Sivashanmugan, *supra* note 85, at 4.

[88] *See* Chris Cooksey, *Guidewire's Approach to Predictive Analytics, Part Five: Monitoring*, GUIDEWIRE (Oct. 23, 2020), https://www.guidewire.com/blog/technology/guidewires-approach-predictive-analytics-part-five-monitoring/.

[89] Correspondence with Chris Cooksey, Head Actuary, Guidewire Analytics (Jan. 2021). *See id.* ("Any predictive model on which a business process depends must be monitored for effectiveness.").

observed historical behavior (a validated model) may be inaccurate in the future.[90] At the same time, if the predictive model is created as a blend of data-driven historical patterns and expert knowledge, it can only truly be validated against the future that will manifest over time.[91] So, optimal validation of the accuracy of a predictive model consists of comparing which proportion of companies identified as high risk by the model go on to experience an actual ransomware event.[92] An example would be a model that predicts companies that are in the top twenty percent worst risks for experiencing ransomware account for over ninety percent of actual ransomware events.

One challenge with optimal validation is a confluence of lack of incident data, the need to update models in line with changing cyber risk, and the lag time in incorporating reported incidents into the model.[93] As such, other approaches can be assistive. For example, ransomware risks that are segmented based on a risk score/rating can be validated by backtesting—observing whether or not they had such an incident in the twelve months following the rating date—would inspire confidence that the model is performing in line with insurance objectives.[94] Another variation is to use area under the curve ("AUC") to measure how the predictive model performs compared to a baseline model built on revenue and industry, where the higher the positive result indicates the quantitative strength of the lift provided by the predictive model.[95] Even when the model prediction differs greatly from observed outcomes, there is value in identifying any weaknesses and limitations that account for the difference, and iterating the model to learn from the data. Comparing expectations and results for

---

[90] *See* Cooksey*, supra* note 88 ("[E]ven good predictive models can begin to deteriorate over time as the data on which it is based gets older and older. A need exists to track this to know when to update a model.").

[91] *See id.* ("The best way to verify the functioning of a good model and to know when it needs to be refreshed is to monitor that model's business performance.").

[92] Correspondence with Chris Cooksey, Head Actuary, Guidewire Analytics (Jan. 2021).

[93] *See* Roosevelt C. Mosley Jr. & Emily Stoll, PowerPoint Presentation: Process of Developing Predictive Models 10 (NAIC Insurance Summit 2017), https://www.actuary.org/sites/default/files/files/predictive-modeling/NAIC_PM_Section2.pdf.

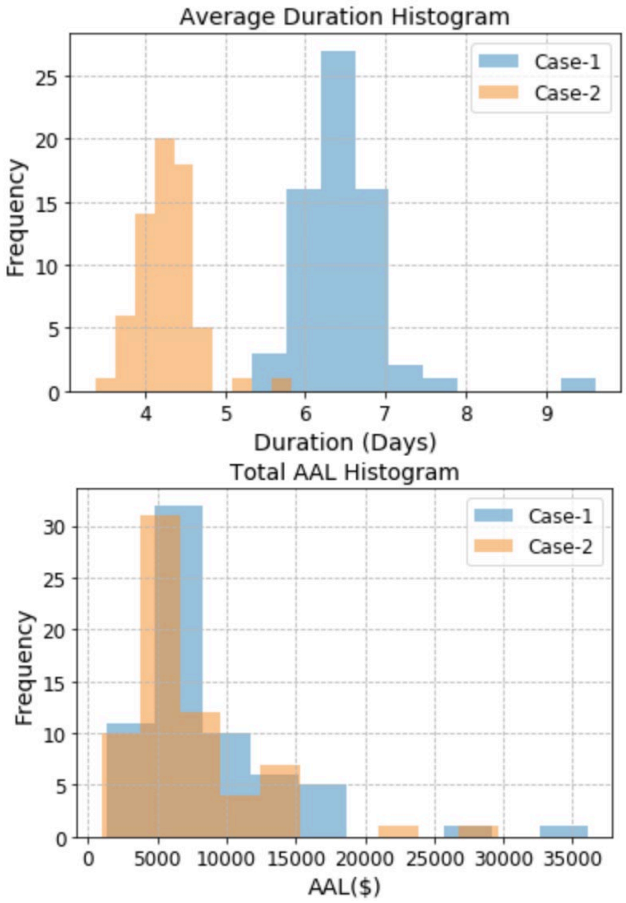
[94] Correspondence with Chris Cooksey, Head Actuary, Guidewire Analytics (Jan. 2021).

[95] *See* Dan Lans, *Illustrating Predictive Models with the ROC Curve*, TOWARDS DATA SCI. (June 30, 2019), https://towardsdatascience.com/illustrating-predictive-models-with-the-roc-curve-67e7b3aa8914.

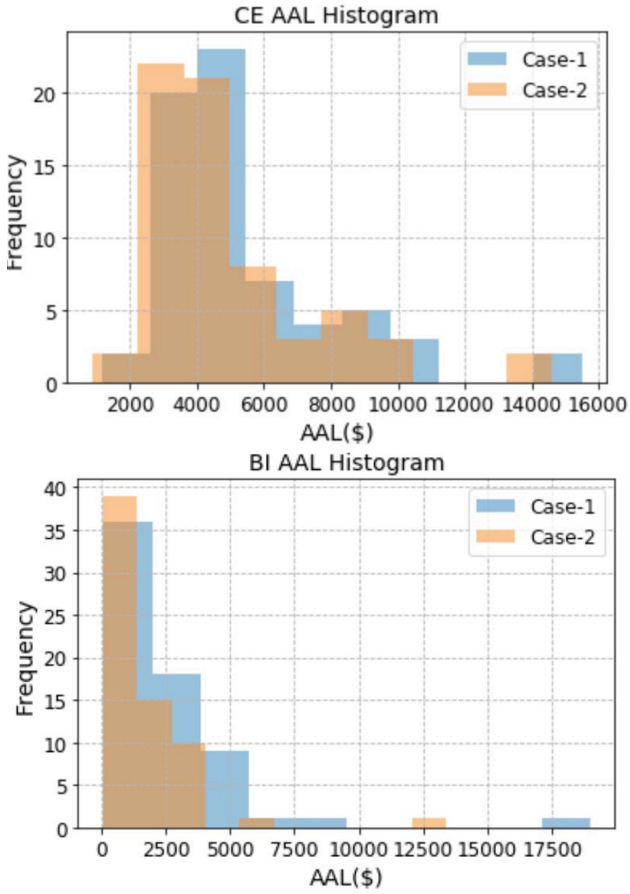
predictive models based on both event data and expert judgment offers myriad adaptation benefits such as: identifying gaps in our understanding of ransomware risk; making assumptions explicit; creating institutional memory; providing a grounded decision support tool; and generating insights.

The difference in model outputs that are informed by ground truth versus generalized or conjectured inputs can be significant. For instance, consider a ransomware loss model that accounts for the probability that ransomware victims have *backup* technology compared to a more nuanced model that has parameters for the probability of *successful restoration* from backup controls. The results illustrated in Figure 5 show the differing outputs of these two models. Specifically, the first incorporates the ground truth that roughly half of companies have backup controls and assumes full restoration (referenced in Figure 5 as Case 2) and the second considers that an average of fifty percent of those restorations will fail (referenced in Figure 5 as Case 1). When assessing predicted severity for this sample portfolio, we see longer business interruption ("BI") duration and larger BI and cyber extortion ("CE") average annual losses ("AALs")—all significant details for cyber underwriting.

Figure 5: Difference in Theoretical v. Empirical Data Informed Model Output[96]



[96] Guidewire Cyence, Cyber Risk Analytics Data (on file with Guidewire Software Inc.).



F. EXTORTION PAYMENT POLICY REFORM

But for cryptocurrency, the selective pressure introduced by ransomware incidents and claims would be unremarkable. Ransomware payments are typically demanded in cryptocurrency in exchange for a digital key to decrypt files and restore victims' access to systems or data.[97]

---

[97] *Insurance Watch: Ransomware*, CIFFA (Dec. 9, 2021), https://ciffa.com/ffo/insurance-watch-ransomware/.

Cryptocurrency has proven to be the *killer app* for ransomware attackers.[98] It optimizes payout efficiency by allowing direct extortion payment from victims rather than having to launder stolen data through the black market, and it lowers attribution risk by providing another layer of pseudonymity[99] to evade law enforcement's track and trace.[100]

Given the pivotal role that cryptocurrency plays in the ransomware ecosystem, governance layer adaptation interventions around extortion payment stands to reason. Options range from targeting supply side by outright prohibition of ransomware pay-outs, to aiming at the demand side by trying to improve attribution and enforcement against bad actors. An open question is if current regulations and policy appropriately guard against facilitating ransomware, or if more robust prohibitions are needed. These efforts include the Office of Foreign Assets Control's ("OFAC") Advisory on the sanction risks of paying ransoms[101] and the Financial Crimes Enforcement Network ("FINCEN") Advisory on reporting ransomware red flag indicators.[102] Softer law signals also emanate from law enforcement guidance that businesses generally should not pay ransoms to decrypt

---

[98] *See* Greg Myre, *How Bitcoin Has Fueled Ransomware Attacks*, NPR (June 10, 2021, 5:06 AM), https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks; DAVID W. PERKINS, CONG. RSCH. SERV., R45427, CRYPTOCURRENCY: THE ECONOMICS OF MONEY AND SELECTED POLICY ISSUES 7–8 (2020).

[99] "Cryptocurrency users typically use a pseudonymous address to identify each other and a passcode or *private key* to make changes to a public ledger in order to transfer value between accounts." PERKINS, *supra* note 98, at i.

[100] *See* Myre, *supra* note 98.

[101] On October 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an advisory to companies providing services to victims of ransomware attacks, informing them of the potential sanctions risks for facilitating ransomware payments to designated persons (individuals or an entity) who conduct certain cyberattacks. U.S. DEP'T OF THE TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [hereinafter TREASURY DEP'T ADVISORY].

[102] U.S. TREASURY FIN. CRIMES ENF'T NETWORK, FIN-2020-A006, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS 5–6 (2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

files.[103] In addition, the U.S. Department of Justice ("DOJ") has promulgated a new enforcement framework aimed at individuals that facilitate illicit trade using cryptocurrencies.[104]

The impact of these light touch governance interventions on cyber insurer adaptation to ransomware appears to be inadequate, but it may be too early to tell. The two advisories do not carry the force of law.[105] In fact, the OFAC advisory is not even a new policy or regulation, but a reminder of the existing regulatory framework in effect when paying funds to entities on the Specially Designated Nationals and Blocked Persons ("SDN") list.[106] Up until September 21, 2021, there had been no civil penalties levied against victim companies, insurers, or response firms for paying or facilitating the payment of cyber extortion.[107] There is a fair amount of enforcement discretion, and sanctions nexus decisions turn on attribution, which is rife with uncertainty in most cyberattacks, let alone when trying to identify if crypto wallet owners, or the source of malware are affiliated with an SDN.[108] "In a nutshell, since the ransom is often lower than the cost of recovery, business interruption and lost business – the convergence of which can spell

---

[103] *See* FBI, This Week*, Advocating Against Ransomware Payment Demands*, FED. BUREAU OF INVESTIGATION (Aug. 22, 2019), https://www.fbi.gov/audio-repository/ftw-podcast-ransomware-082219.mp3/view.

[104] Operators of mixers and tumblers "can be criminally liable for money laundering because these mixers and tumblers are designed specifically to 'conceal or disguise the nature, the location, the source, the ownership, or the control' of a financial transaction." U.S DEP'T OF JUST., OFF. OF THE DEPUTY ATT'Y GEN.'S CYBER-DIGITAL TASK FORCE, CRYPTOCURRENCY ENFORCEMENT FRAMEWORK 41–44 (2020), https://www.justice.gov/ag/page/file/1326061/download.

[105] TREASURY DEP'T ADVISORY, *supra* note 101, at 1 n.1; U.S. TREASURY FIN. CRIMES ENF'T NETWORK, *supra* note 102.

[106] *See* TREASURY DEP'T ADVISORY, *supra* note 101, at 3. *See also* Andrew G. Simpson, *Weighing Effects of Treasury's Ransomware Pay Warnings on Cyber Victims and Insurers*, INS. J. (Oct. 15, 2020), https://www.insurancejournal.com/news/national/2020/10/15/586564.htm.

[107] *See* Michael T. Borgia & Dsu-Wei Yuen, *OFAC Makes Waves in Fight Against Ransomware, but Practical Effects Unclear*, DAVIS WRIGHT TREMAINE LLP (Oct. 1, 2021), https://www.dwt.com/blogs/privacy--security-law-blog/2021/10/ofac-updated-ransomware-advisory#print.

[108] *See id.* ("Most payments to ransomware attackers do not have an apparent nexus to OFAC-sanctioned persons, so whether the Updated Advisory will defer many payments is hard to say.").

financial death – many victims and insurers simply pay the ransom and risk sanctions."[109]

As expected, insurers have taken a rational economics approach to ransomware, leading to a growing sentiment that the industry is worsening the problem by paying extortions.[110] While causality has yet to be proven, indicators suggest that ransomware is responsible for increasing Bitcoin prices.[111]

Figure 6: Correlation between the rise in Bitcoin price and ransomware attacks from May 1, 2019, to September 2, 2019[112]

---

[109] Alex Scroxton, *Is it Time to Ban Ransomware Insurance Payments?*, COMPUTERWEEKLY.COM (Feb. 11, 2021), https://www.computerweekly.com/feature/Is-it-time-to-ban-ransomware-insurance-payments (quoting author). *See also* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019, 5:00 AM), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks (quoting Fabian Wosar, chief technology officer for anti-virus provider Emsisoft, "[insurance companies] will pay anything, as long as it is cheaper than the loss of revenue they have to cover otherwise.").

[110] *See* Dudley, *supra* note 109.

[111] *See* Jareth, *Is Ransomware Driving Up the Price of Bitcoin?*, EMSISOFT: BLOG (Sept. 3, 2019), https://blog.emsisoft.com/en/33977/is-ransomware-driving-up-the-price-of-bitcoin/. *See also infra* Figure 6.

[112] *Id.*

Insurance adaptation in this context must consider interventions that are appropriate for what needs to be acknowledged as a collective action problem. While on an individual policy level it may be rational to pay extortionists. However, this approach when viewed in the cumulative and long-term, likely encourages ransomers (and arguably other bad actors whose profits stem from crypto market price increases).[113] Combined with the loose legal framework that can discourage payment transparency by victims, we have the high reward/low risk environment that likely predicates terrorist and state-sponsored actor affairs.

Insurers can double-down on DFIR to try and bolster post hoc attribution and enforcement, including trying to clawback payments,[114] or seek a license from OFAC to pay the ransom.[115] These approaches, however, are point solutions to a systemic problem, and thus fall short of what is needed to adapt. Invariably none of these approaches will alter the dynamics that inform the economics of ransomware payment strategy. Investigation and legal process can be protracted relative to business interruption costs, not to mention when life and safety of individuals are at stake in cases involving attacks on hospitals, and attackers can countermove to anonymity enhancing forms of payment.[116]

The other defining aspect of the ransomware risk ecosystem is the simple fact that "weak cybersecurity in affected organisations is the main reason why cybercriminals have been so successful in extorting money from them."[117] By removing incentives for attackers, the knock-on effect will

---

[113] *See* Dudley, *supra* note 109.

[114] *See, e.g.*, AA v. Persons Unknown [2019] EWHC (Comm) 3556, [26]–[27] (explaining how a UK insurer was able to recover ransom payments by tracing a wallet address at an exchange and obtaining an asset preservation order to disclose information on the individuals holding the accounts to which the payment had been transferred).

[115] TREASURY DEP'T ADVISORY, *supra* note 101, at 4.

[116] For examples of anonymity enhancing forms of payment see MONERO, https://www.getmonero.org/resources/about/ (last visited Mar. 2, 2022); ZCASH, https://z.cash/support/faq/ (last visited Mar. 2, 2022); DASH, https://www.dash.org/faq/ (last visited Mar. 2, 2022).

[117] Lena Connolly & David S. Wall, *Hackers are Making Personalised Ransomware to Target the Most Profitable and Vulnerable,* CONVERSATION (Mar. 15, 2019, 10:54 AM), https://theconversation.com/hackers-are-making-personalised-ransomware-to-target-the-most-profitable-and-vulnerable-113583.

serve as a further incentive for companies to address the fundamental blocking and tackling discussed prior and thus diminish the very preconditions for ransomware to succeed. The adaptation is a "whole-of-insurance, self-regulatory approach that establishes a ransom non-payment policy."[118] This is already being embraced on the victim-payer side[119] and certainly is not without precedent on the carrier end.[120] And it may be possible "by leveraging traditional compliance clause provisions, such as excluding payments that are subject to existing regulatory restrictions or freezing policy benefits subject to government oversight of sanctions violations compliance."[121] Alternatively, "the industry can act on its own and take a policy stance to refuse payment, barring defined, exceptional circumstances that threaten life and safety."[122]

V. SOLUTIONS HIDING IN PLAIN SIGHT

Hackers have the upper hand, in large part because they have adapted, forming partnerships and Ransomware as a Service ("RaaS") business models, constantly improving their malware, and operationalizing their motive, means, and opportunity more effectively.[123] "[T]he underground ransomware economy is now an industry that resemble commercial software – complete with development, support, distribution,

---

See also ALLIANZ GLOBAL CORPORATE & SPECIALTY, RANSOMWARE TRENDS: RISK AND RESILIENCE 17 (2021), https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/agcs-ransomware-trends-risks-and-resilience.pdf ("Hackers will typically hit those businesses with the weakest defenses first . . . .").

[118] Scroxton, *supra* note 109 (quoting author).

[119] United States Conference of Mayors, Opposing Payment to Ransomware Attack Perpetrators, 87th Annual Meeting, Resolution Adopted 2019, https://www.usmayors.org/the-conference/resolutions/?category=a0D4N00000FCb3LUAT&meeting=87th%20Annual%20Meeting (highlighting that more than 225 US mayors signed on to a resolution not to pay ransoms to hackers).

[120] *See, e.g.*, Matt Sheehan, *New Lloyd's Mandate to Require Clarity on Silent Cyber Coverage*, REINSURANCE NEWS (July 4, 2019), https://www.reinsurancene.ws/new-lloyds-mandate-to-require-clarity-on-silent-cyber-coverage/.

[121] Scroxton, *supra* note 109 (quoting author).

[122] Scroxton, *supra* note 109 (quoting author).

[123] *See* ALLIANZ GLOBAL CORPORATE & SPECIALTY, *supra* note 117, at 4; *The Ransomware Business Model That You're Probably Not Prepared for*, CYBERTALK.ORG (Aug. 14, 2020), https://www.cybertalk.org/2020/08/14/the-ransomware-business-model-that-youre-probably-not-prepared-for/.

quality assurance and even help desks."[124] The same cannot be said about the cyber insurance industry when it comes to ransomware peril coverage.

Critics contend that the cyber risk underwriting challenges lack foundational support to reduce cyber exposure.[125] While these arguments are well-founded, the proposed adaptation framework herein is aimed at addressing those capability gaps. To be sure, there are clear signals that these adaptations are taking root. There is more scrutiny of organizations' InfoSec controls for ransomware in the underwriting process pre-incidents.[126] Some insurers are also committing to proactive risk management coordination, security training, and network security vulnerability testing.[127] The notion of going beyond indemnifying, pooling, and diversifying risks to actively managing the cyber risk is not novel—it is what insurers of data breach instituted in the wake of breach notification regulation and privacy law compliance.[128] So the groundwork has been laid for embracing security best practices, cyber risk assessments and health checks, third party digital forensics and incident response vendors, evolving policy language, and risk management services. The difference with ransomware is there is no legal compliance driver upon which to rely, so simply transplanting a breach

---

[124] CARBON BLACK, THE RANSOMWARE ECONOMY 7 (2017).

[125] *See* CISA REPORT, *supra* note 82, at 15–16.

[126] *See* MARSH, MARKETS: PRICING INCREASES MODERATE IN SECOND QUARTER 6, 10 (2021), https://www.marsh.com/us/services/international-placement-services/insights/global-insurance-market-index-q2-2021.html; ALLIANZ GLOBAL CORPORATE & SPECIALTY, *supra* note 117, at 15; Michael Hill, *Buying Cyber Insurance in 2021? Expect Greater Scrutiny, Higher Premiums*, CSO (Apr. 27, 2021, 2:00 AM), https://www.csoonline.com/article/3616595/buying-cyber-insurance-in-2021-expect-greater-scrutiny-higher-premiums-thanks-to-ransomware-supply.html.

[127] *See, e.g.*, *Loss Mitigation for Cyber Policyholders*, CHUBB: CYBER SERVICES, https://www.chubb.com/us-en/business-insurance/loss-mitigation-for-cyber-policyholders.html (last visited Mar. 6, 2022); AM. INT'L GRP., INC., CYBER LOSS CONTROL SERVICES (2021), https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-loss-control-services-all.pdf; *Risk Management Tools & Resources*, BEAZLEY GRP., https://www.beazley.com/united_kingdom/cyber_and_tech/beazley_breach_response/cyber_services/risk_management_tools_and_resources.html (last visited Mar. 6, 2022).

[128] *See, e.g.*, Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 LAW & SOC. INQUIRY 417 (2018).

compliance strategy will not work. The industry must be a forcing function onto itself.

Is the cyber insurance industry at an inflection point due to ransomware? That answer is always hard to know while steeped in the middle of it. Just like the human appendix, some characteristics of the insurance culture, governance and infrastructure may be outdated adaptations, still hanging on past the point of their usefulness. The culture, governance and infrastructure layers require a change in both disposition and focus; along with an expanded notion of what opportunity means. Opportunity comprises more than just altering premiums and limits to meet acceptable loss ratios for the industry while underserving risk transfer needs in the market. Too narrow an understanding of opportunity has led to policies and practices that have rendered cyber insurance impotent to addressing on the ground ransomware cyber risk. The innovation that will ensure resiliency and impact ransomware risk itself is the opportunity that a Darwinian approach promises to deliver.