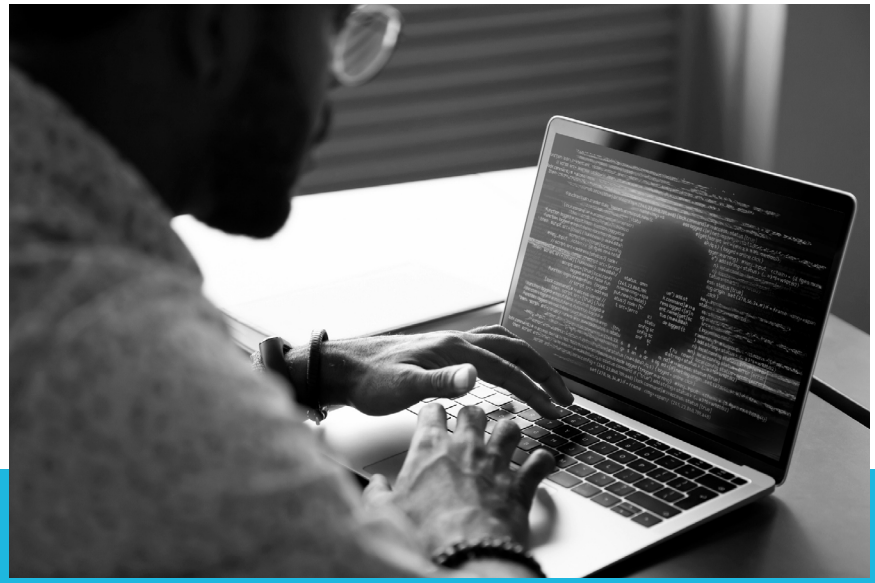
GUIDEWIRE

WHITE PAPER

Ransomware: A Darwinian Challenge for Cyber Insurance



Introduction

Darwin's scientific theory of evolution, outlined in *On the Origin of Species*, maintains that an organism's ability to adapt to changes in its environment and adjust accordingly over time determines its survival success.

This process of adaptation is a fitting model for the cyber insurance industry amid the pressures presented by ransomware incidents and claims. The ability to adapt to the challenges presented by ransomware will determine whether individual companies-and the industry-can evolve to prevent cyber insurance coverage extinction.

Adaptation theory provides three primary potential outcomes: (1) extinction, (2) habitat tracking, whereby an organism moves away from a newly dangerous habitat to one more familiar, and (3) genetic change or evolution.[1]

When applied to the cyber insurance industry, these translate into:

1. **Extinction** of cyber insurance coverage by way of insolvency, retreat from the entire cyber line of business, or a rating event.
2. **Reversion** to a more habitable environment, which translates into pricing premiums or limits in line with ransomware risk uncertainty, but which may not meet market demand.
3. **Evolution** of policies and capabilities to enable cyber insurers to maintain profitability or achieve reasonable loss ratios while also satisfying coverage demands; likely involves redefining the value proposition and advanced risk-models informing capital reserves, risk selection, and pricing.

Cyber insurers are scrambling to wrap their arms around ransomware risk. In the last several years, they've seen appreciable jumps in the frequency and cost of reported incidents and claims, including:

- **Attacks:** Ransomware attacks have increased nearly 150% since the start of Covid19-induced work from home.[2]
- **Claims:** Ransomware claims and costs of payments have jumped approximately 230% between 2018 and 19.[3]
  - Claims have comprised up to 40% of some insurers' cyber books.[4]
- **Extortions:** Cyber extortion demands paid in 2019?20 were three to four times greater than in the previous year.
- **Payouts:** Ransomware payouts for U.S. businesses have exploded in the last two years:
  - From under $10K to more than $178K per event at the end of Q2 2020
  - Average payouts of more than $1M for large enterprises[5]
- **Loss ratios:** Loss ratios increased 10% due to ransomware for the last documented year.[6]

As a result, premiums have risen and insurers have become more selective, undoubtedly underserving the quality and quantity of coverage demands.

If we take a cue from Darwin, the path forward lies in recognizing ransomware as the functional equivalent of a natural selection event-and taking action to ensure adaptation.

Pace Layering and the San Francisco Earthquake of 1906

The 1906 San Francisco earthquake is illustrative of how pace layering can explain the mid- and higher-layer adaptations required to recover from abrupt changes at the lowest layers in the model. In this case, the earthquake sent ripple effects to the commerce layer, demolishing city infrastructure, bankrupting businesses and households, and compelling governments to subsidize the recovery. The financial infrastructure couldn't absorb the shocks that were unbuffered by an insurance industry unable to underwrite damage on such a large scale. This insurance industry instability and readjustment set the stage for markets to react months later in the Panic of 1907.

Environmental Conditions

The starting point in determining how cyber insurance can evolve to meet the demands of the market-in balance with the threat of ransomware-is to understand the environment. The hallmarks of the current environment, in addition to those referenced above, include:

- Insufficient actuarial data (loss history) for pricing premiums and coverage loss limits
- Lack of risk control efficacy and lessons learned from attack vectors
- Expanding delta between cyber-crime loss and claims paid
- Spend gap between cybersecurity and risk transfer
- Uncomfortable ransomware loss-ratio distributions
- Premiums that are more sensitive to market competition rather than organizations' security posture
- Incongruency between threat capabilities and modeled risk profiles

Applying the Pace Layering Model to Cyber Insurance

Following the environmental analysis, we must assess and identify the adaptations (changes) that will put cyber insurance on the path to survival in the face of ransomware risk. Pace layering is an ideal model for such an exercise; it is a proven framework for diagnosing and prescribing adaptability to change.[7]

Pace layering enables us to take a more sophisticated look at the environment and potential adaptations. It proposes that every entity is the product of adaptation to the demands of 'time scales' or layers that change at different paces. According to the model, these time scales are ordered from slow to fast: nature, culture, governance, infrastructure, commerce, and aesthetics. For the purposes of the insurance industry with regards to ransomware, these layers translate to the market (nature), government (governance), technologies, the industry (commerce), and individual insurance companies.

In pace layering, the slower layers are considered to be more foundational and methodical, providing stability. The fast layers are more innovative and less encumbered, but also less stable. In a healthy society, for example, the legal systems change slower than the rate of commerce (businesses). As the framework's developer notes, "Fast gets all our attention, but slow has all the power."

Each layer interplays with the others to adapt to change, but each adapts in different ways and at different paces.

When faster layers move too slowly, the entity may be stagnant. Conversely, faster layers like commerce can move too quickly for what the infrastructure can support, causing a system breakdown. Moreover, when slower layers move too quickly, they can cause turmoil, whereas if they move too slowly, they impede progress.

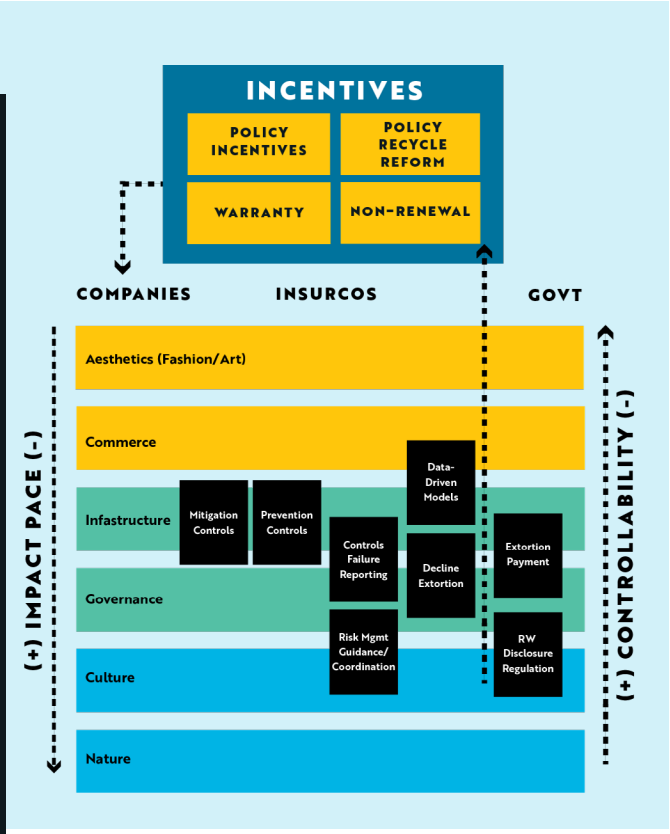


Figure 1. Layers of Ransomware Insurance Adaptations

Adaptations to Ransomware: The Path Forward for Insurers and the Insurance Industry

We can apply this layering framework to diagnose and recommend adaptations to the current ransomware insurance challenges—and describe the specific adaptions and incentives needed to create a stable response to ransomware risk.

We propose that adaptation must take place across the risk environment, including via the actions of individual insurers, the insurance industry, and government via enforcement or adoption of possible new regulations or laws.

These adaptations can be envisioned on a spectrum based on the degree of controllability and speed of impact, including: risk management guidance, mandatory ransomware incident disclosure regulation, security controls failure reporting, infosec prevention and mitigation controls incentives, data-driven risk models, and cyber extortion policy reform.

1. Infosec Loss Prevention and Mitigation

While progress on incident actuarial data leaves much to be desired, infosec statistics around threat and vulnerability dimensions have improved. In fact, they show remarkable consistency in the case of ransomware. Reports from leading vendors[8] agree that the most popular attack vectors and sources of ransomware incidents are remote desktop protocol (RDP), email phishing and spam, and unpatched vulnerabilities (Figure 1).

Knowing where to spend limited cybersecurity budgets can be challenging, but the vulnerabilities are nonetheless known. Basic "blocking and tackling" can significantly decrease risk exposures, including:

- Ensuring that RDP ports and services are not openly exposed to the internet
- Maintaining updated software patches for VPNs and appliances that provide entryways to corporate networks
- Implementing email and social controls
- Using multifactor authentication to harden identity and access management

These risk prevention controls are the direct responsibility of corporate policyholders, yet cyber insurance insurers on the whole have done little to incentivize their adoption.

In addition to prevention controls, arguably the closest thing to an infosec silver bullet for ransomware mitigation is backup recovery technology. Because locking systems and extorting payments in exchange for decryption keys are the trademarks of ransomware, effective backups are its strongest antibody.

The difference between quick backups and ransomware-resistant backups is weeks of downtime due to failed or insufficient recoverability and costly business interruption. Data reveals that more than half of all companies do not have backups at all; of those that do, 60% have incomplete backups.[9] This has resulted in insurers opting to pay ransoms as a result of cost-benefit analysis. Such analysis finds that business interruption costs associated with recovery and restoration are more painful than paying the extortion fees.

The obvious question is, "Why then aren't insurers insisting on robust disaster-recovery technologies and processes as a precondition to coverage?"

Insurers are in a position to bring about needed infrastructure changes by using various incentives to improve cyber hygiene in a way that significantly impacts ransomware loss. Properly structured, the following actions are behavioral incentives to reduce ransomware risk:

- Institute premium reductions for those that have a clean bill of health.
- Refuse to bind or renew companies that cannot attest to having controls in place.
- Change policy cycles to be more agile and responsive to cyber exposures.
- Issue cyber warranties for security vendors to enhance trust in efficacy claims.
- Cancel and/or amend terms and conditions mid-policy if an insured neglects recommended security improvements.

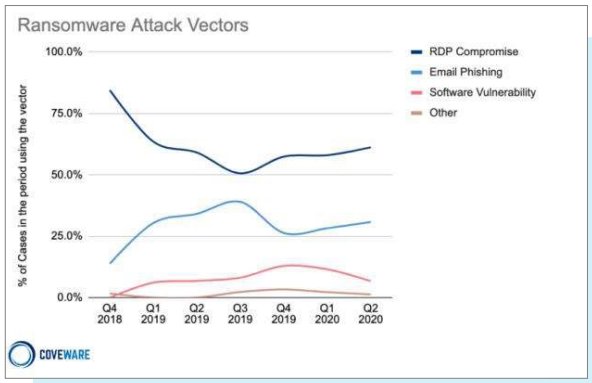


Figure 2. Common Ransomware Attack Vectors

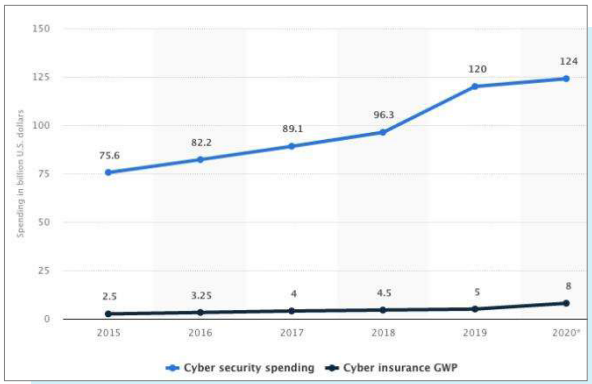


Figure 3. Annual Cybersecurity and Cyber Insurance Spending Worldwide (Statista)

2. Risk Management Coordination

Incentivizing ransomware risk controls is a necessary but likely insufficient adaptation if insurers want to withstand the evolving risk that ransomware presents. Unless incentives are intertwined with infrastructure layer risk mitigation coordination, the prescribed controls will invariably lag behind threats and vulnerabilities.

Rather than rely solely on factors like compliance or case law developing over time, embracing a risk management coordination role can enable insurers to take the fight to ransomware. A start would be to have underwriters, brokers, and infosec professionals coordinate closely on security risk metrics. Such coordination can better align risk optics, lower information asymmetries, and scale victimology beyond the current ad hoc dynamics.

Insurance companies have already formed partnerships with infosec organizations for post-event response and consulting. What's needed now is further synchronization with infosec consortiums and other organizations for prevention and mitigation measures.

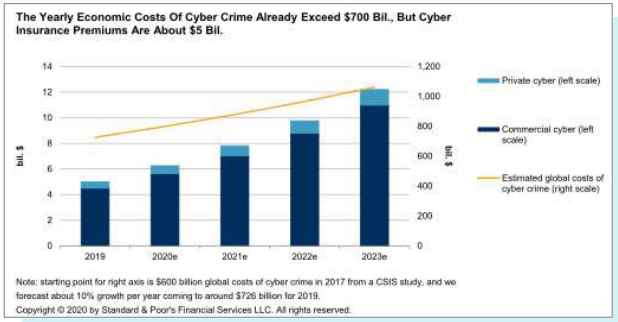


Figure 4. Cost Trend of Cyber Crime v. Cyber Insurance Premiums

Several notable statistics shed light on this coordination gap (Figures 2 and 3). First is the ratio between the economic cost of cyber-crime and claim payouts. These two trajectories shown in the graphs signal an incongruity where there should be a collaborative relationship. They display an underserved opportunity for cyber insurers.[10]

How risk management coordination can be taken up by insurers can be thought of as a spectrum. At a basic level, simply requiring policyholders to assist in providing or verifying fundamentals and technographics would bring about more accurate cyber risk assessment. On the other end of the spectrum, incentivizing insureds to share internal security telematics could add the missing link in cyber risk assessment and measurement. While contribution of inside-the-firewall security data would require technical, procedural, and policy changes on the part of the insured and insurers, instituting it would be a game changer.

3. Ransomware Disclosure Regulation

The foundations for data breach underwriting and coverage were based on federal regulations, litigation, and state laws that require the reporting and disclosure of data breaches. So we need to ask, "Do we need a similar enforcing function to adapt to ransomware risk?"

Regulatory fines, reporting requirements, and liability and legal costs have made data breach losses tangible, thereby capturing the attention of the industry.[11] This regulatory impetus has fed rational expectation that improved cybersecurity would result in reduced premiums and/or higher liability limits.[12]

As an increasing number of ransomware attacks hold data hostage to pressure extortion payments, many of the existing public disclosure requirements and privacy claims will trigger.[13] However, it's very much an open question as to whether that is sufficient for robust underwriting of ransomware risk. The industry currently has inadequate understanding of ransomware risk distributions to underwrite policies proportional to reserves and risk appetite, while still being responsive to the needs of the market. In any case, government (via legislation, regulation, or judicial rulings) is uniquely situated to play a role in reducing risk and enforcing compliance.

4. Controls Failure Reporting

The adage "Those who don't know history are doomed to repeat it" is sage advice that is highly applicable to ransomware adaptation. Standard components of digital forensics and incident response (DFIR) reporting include information about attack vectors and control failures: how attackers were able to access company networks and what technical or administrative safeguards were deficient.

While the certainty of these attributions varies, insurers have by and large left these ransomware claims details on the cutting room floor, foregoing valuable lessons learned and perpetuating a piecemeal approach to underwriting.

Imagine if, over the course of the last decade of claims, individual insurers (or the industry collectively) had documented these digital forensics and incident responses as part of the claims process. While there is no guarantee that the past is prologue to the future when it comes to cyber risk, attacker tactics, techniques, and practices (TTPs) definitely follow patterns of least resistance. Knowing their playbooks can go a long way to reducing exposures.

Concerningly, there is a trend with insurers (mostly in the SME market) of cutting costs by collecting less information during the underwriting process and eliminating data fields in the notification of loss.[14] This trend works counter to the suggested adaptation aimed at developing more mature cyber loss models to align risk with price premiums.[15]

Adaptation in the cyber risk landscape requires committing as much available data to the actuarial record as possible. Collecting and sharing controls failure data would mark a significant step toward being able to qualify and quantify the end-to-end relationships between threats, security compliance, and incident outcomes

5. Data-Driven Predictive Models

Because ransomware is a dynamic threat whose prevalence is unknown, and because it operates within interconnected landscapes, knowledge of yesterday's attacks is insufficient to inform us about tomorrow's outcomes. Any foresight is therefore highly valuable for effective ransomware risk segmentation, assessment, pricing, and defense.

Foresight in cyber insurance can come by way of predictive models that include both historical data and expert knowledge. Simply fitting historical event frequency and severity around ransomware event variables will not anticipate the future changes that underlie risk. The adaptations needed are empirical data-driven models that also incorporate expert knowledge. Such predictive models can drive more robust and reliable pricing models and inform underwriting guidelines.

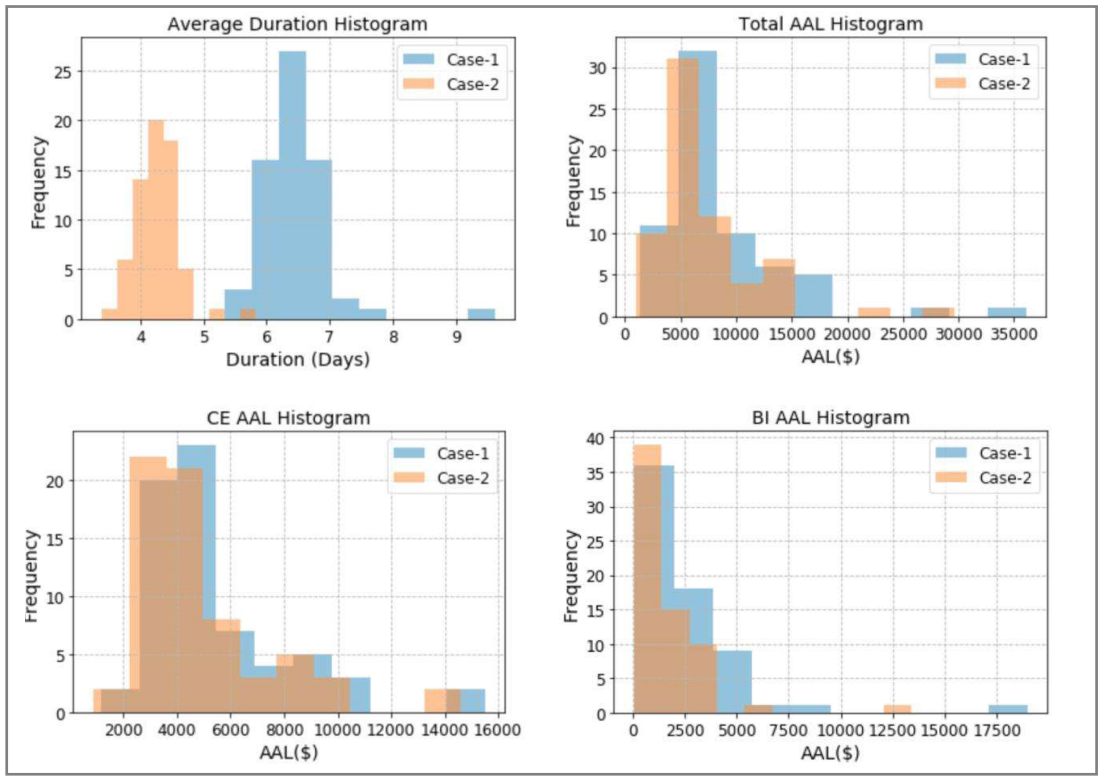
Models can be further validated by measuring the difference between the predicted and observed outcomes. This is typically done using historical data only, with ongoing monitoring of the actual results being a secondary consideration. However, in an actively changing environment, historical results often lack necessary information for predicting the future. A model which validates well on properly held out, but still historical, data may be inaccurate in the future.

If the predictive model is created as a blend of data-driven historical patterns and expert knowledge, it can only truly be validated against future results. 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. An example would be a model that predicts companies that are in the top 20% risk for experiencing ransomware account for over 90% of actual ransomware events.

Differences in Model Outputs

The difference in model outputs that are informed by grounded 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 below results show the outputs of two models: one that incorporates the ground truth that roughly half of companies have backup controls and assumes full restoration (Case 2), versus one that also considers that an average of 50% of those restorations will fail (Case 1). When assessing predicted severity for this sample portfolio, we see longer business interruption (BI) duration, and larger BI and cyber extortion (CE), all significant details for cyber underwriting.



Challenges with optimal validation include factors such as 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. To address these, other approaches can be applied to offer support. For example, ransomware risks that are segmented based on a risk score/rating can be validated by back testing: observing whether or not they had such an incident in the past year following the rating date. This would inspire confidence that the model is performing in accordance with insurance objectives.

Another variation or support mechanism 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 a higher positive result indicates the strength provided by the predictive model.

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 then iterating the model.

Comparing expectations and results for predictive models based on both event data and expert judgment offers myriad benefits, including:

- Identifying gaps in the understanding of ransomware risk
- Making assumptions explicit
- Creating institutional memory
- Providing a grounded decision support tool
- Generating deeper insights

6. Extortion Payment Policy Reform

Cryptocurrency is the fuel that drives the growth of ransomware. if it were not for cryptocurrency, the pressure introduced by ransomware incidents and claims would be unremarkable.

Ransomware payments are typically demanded in cryptocurrency in exchange for a key to decrypt files and restore access to systems or data. Cryptocurrency optimizes payout efficiency by enabling direct extortion payment from victims rather than having to launder money or stolen data through the black market. It lowers attribution risk by providing another layer of anonymity to evade law enforcement's tracking and tracing.

Given the pivotal role that cryptocurrency plays in the ransomware ecosystem, government interventions around extortion payments seems likely in the long term (assuming the problem persists). Government options range from an outright prohibition of ransomware payouts to aiming to improve attribution and enforcement against bad actors. What is not yet clear is if current regulations and policy appropriately guard against facilitating ransomware, or if more robust prohibitions are needed.

Figure 6. Correlation between the rise in Bitcoin price and ransomware attacks. Sources: CoinMarketCap and Emsisoft.

Current efforts include the U.S. Treasury's Office of Foreign Assets Control (OFAC) Advisory on the sanction risks of paying ransoms and its Financial Crimes Enforcement Network (FINCEN) Advisory on reporting ransomware red flag indicators. Softer signals also emanate from law enforcement guidance that businesses generally should not pay ransoms to decrypt files. In addition, the U.S. Department of Justice (DOJ) has promulgated a new enforcement framework aimed at individuals that facilitate illicit trade using cryptocurrencies. In the U.K., the former head of the National Cyber Security Council (NCSC), Ciaran Martin, has called for "urgent" action that includes a change in law to prevent businesses from paying ransoms and to make ransomware risks a board-level problem.

Although it may be too early to assess, the impact of these governance interventions appears to be inadequate.

Notably, the two U.S. Treasury advisories do not carry the force of law. In fact, the OFAC advisory is not even a new policy or regulation; rather, it is a reminder of the existing regulatory framework that is in effect when paying funds to entities on the Specially Designated Nationals and Blocked Persons (SDN) list. To date, there have been no civil penalties levied against victim companies or insurers. There is a fair amount of enforcement discretion, and sanctions decisions depend on attribution, which is rife with uncertainty in most cyberattacks.

In addition, since the ransom payments are often lower than the cost of recovery or business interruption, many victims and insurers simply pay the ransom and thereby risk sanctions.

While causality has yet to be proven, indicators suggest that ransomware is responsible for increasing Bitcoin prices (Figure 5).[16] Insurance adaptation in this context must consider interventions that are appropriate for what needs to be acknowledged as a collective problem. On an individual policy level, it may be rational to pay extortionists. However, when viewed in the cumulative and long-term, the current approach likely encourages cyber criminals. Combine that with the loose legal framework that can discourage payment transparency, and we have the high-reward/low-risk environment that can predicate terrorist and state-sponsored actor affairs.

Insurers can double-down on DFIR to try to bolster enforcement, including trying to claw back payments, or seek a license from the U.S. Treasury to pay the ransom. These approaches, however, are point solutions to a systemic problem, and therefore fall short of what's needed to adapt.

A defining aspect of the ransomware risk ecosystem is the fact that insufficient cybersecurity exists in targeted organizations. It is the main reason why cybercriminals have been so successful in extorting money. As a result, insurers must incentivize companies to address the fundamental blocking and tackling needed to prevent and discourage ransomware activity.

Ideally, the adaptation is an industry-wide, self-regulatory approach that establishes a ransom nonpayment policy. This is already being embraced on the victim-payer side and certainly is not without precedent on the insurer end.

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. 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.

Summary: Cooperative and Individual Adaption Required to Address the Ransomware Challenge

As it stands, cybercriminals 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 and means more effectively.

The underground ransomware economy has evolved to almost resemble the commercial software market complete with development, distribution, quality assurance, and help desks. The same cannot be said about the cyber insurance industry when it comes to ransomware peril coverage.

Critics contend that cyber risk underwriting lacks the fo undational support needed to reduce ransomware and cyber risk exposure.[17] While these arguments are well-founded, the measures above could clearly address these capability gaps.

There are clear signals that some insurance industry adaptations are taking root. There is more scrutiny of organizations' infosec controls for ransomware in the underwriting process pre-incident. Some insurers are also committing to proactive risk management coordination, security training, and network security vulnerability testing. 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 breaches have instituted in the wake of breach notification regulation and privacy law compliance.

So the groundwork has been laid for embracing security best practices, cyber risk assessments, and health checks, as well as third-party digital forensics, policy language, and risk management services. The difference with ransomware is there is no legal compliance driver on which to rely, so simply transplanting a breach compliance strategy will likely not succeed. Thus, the insurance industry must perform an enforcing function on itself.

The insurance industry must do more than simply alter premiums and limits to meet acceptable loss ratios while underserving risk transfer needs in the market. Too narrow an understanding of the environment has led to policies and practices that have rendered cyber insurance nearly impotent to address ransomware risk. Only innovation and evolution at the individual company, industry, and governmental levels will ensure the resiliency of the cyber insurance market—and ultimately impact ransomware risk itself.

Erin Kenneally is the *Director of Cyber Risk Analytics* at Guidewire. She provides cyber risk strategic thought leadership and domain expertise, and leads data-driven research innovation for novel risk analytics and modeling technology solutions.

Navigate what's next.

NOTES

1. Sciencing, The Three Types of Environmental Adaptation
2. Carbon Black, Global Orgs See a Spike in Ransomware Attacks, April 2020
3. S&P Global Market Intelligence, Cyber insurers tighten underwriting, October 2020
4. Carbon Black, Global Orgs See a Spike in Ransomware Attacks, April 2020
5. Coveware Quarterly Ransomware Report, August 2020
6. Aon, US Cyber Market Update, June 2020
7. Journal of Design and Science, Pace Layering: How Complex Systems Learn and Keep Learning
8. Reports from Coveware, Emsisoft, and Recorded Future
9. Ontech Systems, 5 Startling Statistics About Data Backup and Recovery
10. Council of Insurance Agents & Brokers (CIAB), Cyber Market Watch Survey
11. A.M. Best, Best's Review, Cyber Insurance Special Report, US cyber insurance market took off as data breach notice and other privacy laws implemented
12. Council of Insurance Agents & Brokers (CIAB), Cyber Market Watch Survey
13. SentinelOne, The Stopwatch is Ticking, How Ransomware Can Set Breach Notification in Motion, June 2020
14. PWC, Is your organization taking the right approach to cybersecurity?
15. US Department of Homeland Security, CISA, Assessment of the Cyber Insurance Market
16. Emsisoft, Is ransomware driving up the price of Bitcoin?
17. US Department of Homeland Security, CISA, Assessment of the Cyber Insurance Market