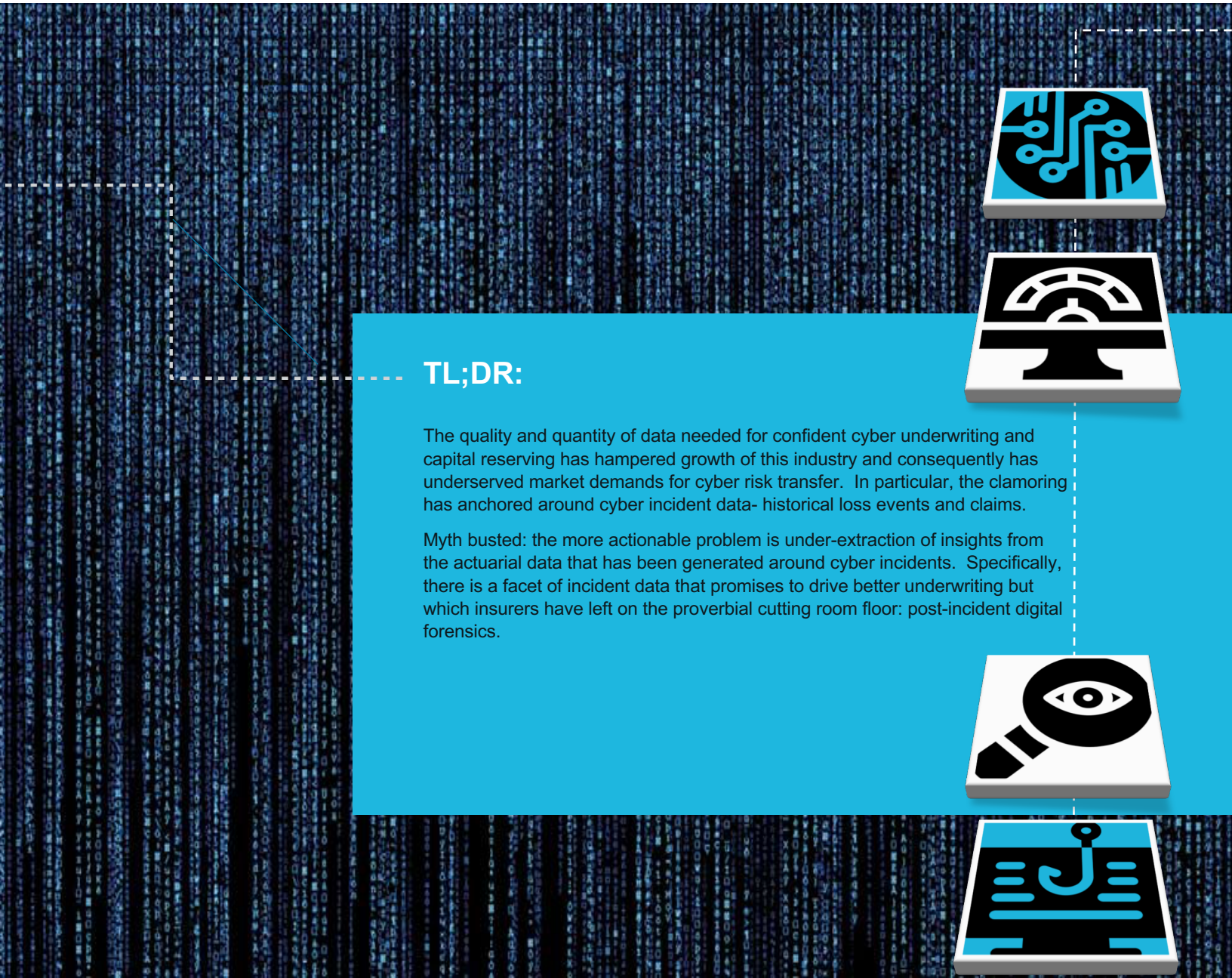
White Paper

GUIDEWIRE

Hiding in Plain Sight: Towards Now-Gen Cyber Risk Underwriting

Erin Kenneally, Director Cyber Risk Strategy
Guidewire Cyence Risk Analytics



TL;DR:

The quality and quantity of data needed for confident cyber underwriting and capital reserving has hampered growth of this industry and consequently has underserved market demands for cyber risk transfer. In particular, the clamoring has anchored around cyber incident data- historical loss events and claims.

Myth busted: the more actionable problem is under-extraction of insights from the actuarial data that has been generated around cyber incidents. Specifically, there is a facet of incident data that promises to drive better underwriting but which insurers have left on the proverbial cutting room floor: post-incident digital forensics.

Risk Underwriting Self Help - Closing the Data & Analytics Feedback Loop

Take a gander at any report, paper or article on the state of cyber insurance during its entire multi-decade existence and you'll find at least one universal bellyaching: there is a lack of actuarial data upon which to reliably assess insurance risks and calculate premiums. The quality and quantity of data needed for confident underwriting and capital reserving has hampered growth of this industry and consequently has underserved market demands for cyber risk transfer. In particular, the clamoring has anchored around cyber incident data- historical loss events and claims.

Myth busted: the problem is not lack of data, rather, it is under-extraction of insights from the actuarial data that has been generated around cyber incidents. Specifically, there is a facet of incident data that promises to drive better underwriting but which insurers have left on the proverbial cutting room floor: post-incident digital forensics.

Quantifying and qualifying the end-to-end relationships between cyber threats, vulnerabilities, security controls, assets, and incident outcomes is riddled with blindspots that create risky inference leaps. [Fig 9] This relational data linking signifies the holy grail for cyber underwriting enlightenment. Yet heretofore the industry has mined incident data monolithically and superficially for its firmographics (industry and revenue segmentations and distributions) and insurable impacts, which in turn have bounded risk selection and pricing.[1] An industry predicated on reducing the uncertainty around what exposures it's on the hook to indemnify has overlooked a key data and analytical feedback loop whose closure would move insurers beyond the self-perpetuated actuarial Groundhog Day. Digital forensics & incident response (DFIR) data about incident attack vectors and controls deficiencies collected at the backend of an incident (during the claims phase) will evolve the quality of risk correlation and causation and enrich the frontend underwriting of cyber risk.

Twenty years in and the promise of an intra-industry repository of claims data remains aspirational, to the dismay of governments and cyber-exposed companies yet agreeable to many cyber carriers who have (by strategic choice or necessity) turned this putative scarcity into a competitive asset. The focus herein is neither to weigh-in on that open secret, nor to reiterate the virtues of incident data sharing.[2] To be sure, juxtaposed to other perils and lines of business, cyber insurance has a systemic handicap with regard to authoritative incident data sources[3] and most incidents are not objectively observable. This has resulted in optics about risk and claims that are disconnected, compartmentalized, and variably skewed. Aside from reluctance to share data to protect competitive advantage, shared truths about cyber risk and incidents are further impeded by legal risk concerns, lack of generally accepted security standards, inadequate incident reporting requirements, policy and terminology inconsistency, and complexity of cyber risk in its own right.

Solutions to advance these prominent impediments are well-served and in fact necessary for industry maturity yet are all predicated on intra-carrier collective agreement and/or action. Immediate progress on the "data problem" need not depend on slow-moving, industry-level harmonization. Neither does progress depend on writing six figure checks for the latest blockchain-based, quantum AI Precog. If cyber insurers even just independently optimize the DFIR data that they currently control and have access to, significant progress toward lower insured and ground-up loss uncertainty is within near term reach.

[1] See, e.g., Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones, Content analysis of cyber insurance policies: how do carriers price cyber risk?, Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz002, doi.org/10.1093/cybsec/tyz002.
[2] See, e.g., Assessment of the Cyber Insurance Market, DHS CISA (Dec 2018), available at cisa.gov/sites/default/files/publications/20_0210_cisa_oce_cyber_insurance_market_assessment.pdf; DHS CISA Cybersecurity Insurance Industry Readout Reports, available at cisa.gov/publication/cybersecurity-insurance-reports; DHS S&T CyRiE, Cyber Risk Economics Capability Gaps Research Strategy, 2018, available at cisa.gov/publication/cybersecurity-insurance-reports.
[3] E.g., P&C insurance for natural catastrophes leverages authoritative sources, namely the U.S. Geological Service and the U.K. Met Office as well as various other public & quasi-government agencies across the world.

What's Inhibiting the Cyber Risk Feedback Loop?

There are two main dynamics that impede inclusion of DFIR data into the actuarial record and stifle improved underwriting: misaligned insurer-law firm data governance, and disjointed business process.

The Tail Wagging the Dog: Legal Privilege

Cyber carriers are positioned to collect DFIR data and utilize it to inform frontend risk underwriting yet remain largely abstracted from the data because of how they structure the incident response process. Insurers cover the cost of forensic incident response in the wake of breaches and govern the relationship between policyholders and response firms. They empanel DFIR providers in advance of loss events through a process of sourcing and negotiating rates, in an attempt to facilitate efficient IR for compromised policyholders.

Significantly, however, cyber insurers commonly appoint law firms to manage the incident response functions and workflow, which has been packaged to include digital forensics, public relations and notification, and credit monitoring (often referred to as "breach coaches"). There is more at play than just outsourcing logistics. Insurers afford law firms the authority to choose which DFIR firms to engage and more importantly, to oversee the composition of the forensics report and associated investigation.[4] [Fig 1] This practice strategically and deliberately leverages attorney-client privilege or work product doctrine to prevent third party liability and E&O exposure that may arise if causal details from the DFIR report were otherwise discoverable during litigation proceedings. The goldmine of who, what, when, where, why, and how that is extracted in the DFIR process is nevertheless often left entombed within the ore of firmographic and loss figures associated with the claim.

Common components of 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 the forensic details on the cutting room floor in claim reports, foregoing valuable lessons-learned and perpetuating a piecemeal and disconnected approach to underwriting.[5]

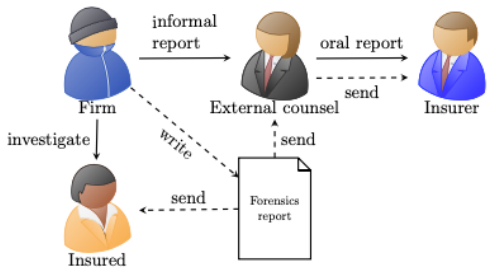


Figure 1. Workflow of insurer-legal counsel communication of incident data.
(Source: Woods & Bohme 2021)

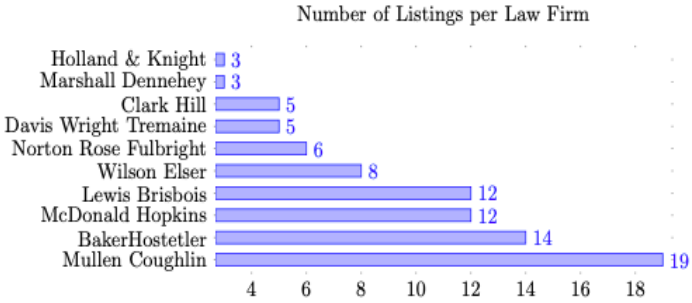


Figure 2. Law firms with multiple insurer engagements. E.g., Mullen Coughlin was listed by 80% of the insurers in the study.
(Source: Woods & Bohme 2021)

[4] DW Woods and R Bohme. How Cyber Insurance Shapes Incident Response: A Mixed Methods Study. The 20th Workshop on the Economics of Information Security (WEIS 2021).
[5] Kenneally, Erin E., Ransomware: A Darwinian Opportunity for Cyber Insurance (December 29, 2020). Forthcoming, CONNECTICUT INSURANCE LAW JOURNAL FALL SYMPOSIUM EDITION (VOLUME 28.1) Fall 2021, Available at SSRN: ssrn.com/abstract=3849120 or dx.doi.org/10.2139/ssrn.3849120.

Insurers across the board hail the promise of data analytics and modeling for operating (underwriting and ERM) effectiveness and innovation, and the market of insurtech analytic firms corroborate that demand.[6] If continuous-loop data analytics and modeling is a progressive solution to cyber risk uncertainty why then would law firms *not* marshal better DFIR data?

Relinquishing DFIR reporting to law firms, without formal direction and requirements to capture vital artifacts that can close the loop with underwriting insight demands strikes as self-defeating. The economic justification for deferring to avoidance of potential liability cost to the detriment of continuous-loop analytics and ex ante risk reduction has grown frail. Wielding attorney-client privilege to shield access to DFIR data is a vestige of an era when cyber policies were liability-centric and losses were driven by third party litigation following a data breach.

Present day losses and risk transfer needs of cyber compromised companies are skewing more heavily toward business income, interruption (BI) and recovery costs that flow from *technical* compromise, largely as a result of the ransomware epidemic.[7] [Fig 3] Even before the peak onslaught of RW incidents in 2020-21, a prominent claims study from 2019 revealed that the average incident cost for a BI claim was much higher than the average cost of other incidents. [Fig 4] Others have found that the top three coverages sought in 2020 were cyber-related business interruption, cyber extortion/ransom and funds transfer fraud/social engineering, respectively… with third party data breach liability not even making it into the top 12 concerns.[8]

Proponents of this insurer-law firm DFIR data governance arrangement may point to these low liability losses as proof that the obfuscation strategy is working. However, this overlooks socio-economic facts to the contrary: (a) at least as far as the costly breach class action cases are concerned, dampened liability losses likely have less to do with non-disclosure of DFIR data than the fact that courts have largely dismissed these cases for failure to establish standing or prove cognizable damage and actionable harm;[9] (b) ransomware cases accompanied by data breach (the double-extortion tactic) and the associated liability risk are a growing norm,[10] yet it's the BI losses that are decimating loss ratios; and, (c) smart insurers who are playing the long game realize that the delta between the economic cost of cyber crime and claim payouts[11] portends a grim future for the cyber market unless improvement is made in risk prevention and mitigation. Put simply, profitable survival in the cyber line of business demands that carriers ask and answer whether adherence to a convention that squanders an opportunity to connect the back and front-end data is working.[12] [Fig 2]

Notably, recent rulings in three breach cases may foretell a shift in this DFIR data governance convention. Within the past year, courts have dismissed attempts to legally shield DFIR data by ordering the production of internal forensics reports in

---

[6] See, e.g, globenewswire.com/news-release/2021/05/26/2236758/0/en/Global-Insurance-Analytics-Market-By-Component-By-Application-By-Deployment-Type-By-Application-By-End-User-By-Regional-Outlook-Industry-Analysis-Report-and-Forecast-2021-2027.html; https://www.the-digital-insurer.com/search-insurtech-directory/#.

[7] E.g., Ransomware attacks increased nearly 150% since Covid19-induced work-from-home commenced (carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/); ransomware claims and the cost of payments jumped approximately 230% between 2018-19 according to Beazley PLC (spglobal.com/marketintelligence/ en/news-insights/latest-news-headlines/cyber-insurers-tighten-underwriting-raise-prices-as-ransomware-wave-hits-60829821); 2020 recorded 73% direct loss ratios for standalone cyber primarily by ransomware losses according to Fitch Ratings.

[8] Advisen & Partner Re, Cyber Insurance — The Market View 2020.

[9] The U.S. Circuit Courts are split on this issue: some do not recognize risk of future harm as conferring standing, others recognize an allegation of future harm if, for example, there is "danger of sustaining some direct injury" that is "both real and immediate"—such as identity theft.

[10] For e.g., Coveware claims 50- 70% of ransomware attacks involve data exfiltration (Ransomware Marketplace Report Q3 2019 and Q4 2020, respectively)

[11] The White House Counsel of Economic Advisors estimated the economic cost of cybercrime to be $57-109B with $356M in claims paid, which was <1% of total cyber losses paid by insurers in 2016. Compare this to natural catastrophes, where 50% of losses between 2015-2018 were paid by insurers. whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[12] See, Woods & Boehm, "The community should not under-estimate how legal risk shapes and even prevents ex-ante mitigation. Insurers appoint law firms at the top of the IR hierarchy and considerations around client-attorney privilege prevent the documentation and sharing of forensics investigations. Quantifying the opportunity cost of squandered knowledge is impossible, but legal risk is no doubt limiting the ability of insurers to build knowledge over time."

discovery to presumably uncover details about the source, cause, and scope of incidents.[13] As well, questions about the use of attorney-client privilege arose in a hearing of the House Homeland Security Committee in relation to the Colonial Pipeline attack. In particular, the chairwoman sought information as to whether Colonial had retained its DFIR firm through counsel in order to trigger the protection.[14] If these developments signal a trend, it could take the privilege decision out of the hands of insurers and force disclosure of valuable DFIR data. Conversely it could disincentivize robust IR even more as a counter-move to compelled disclosure. In either case, insurers would do well to wield a sword rather than a shield when it comes to data insights.

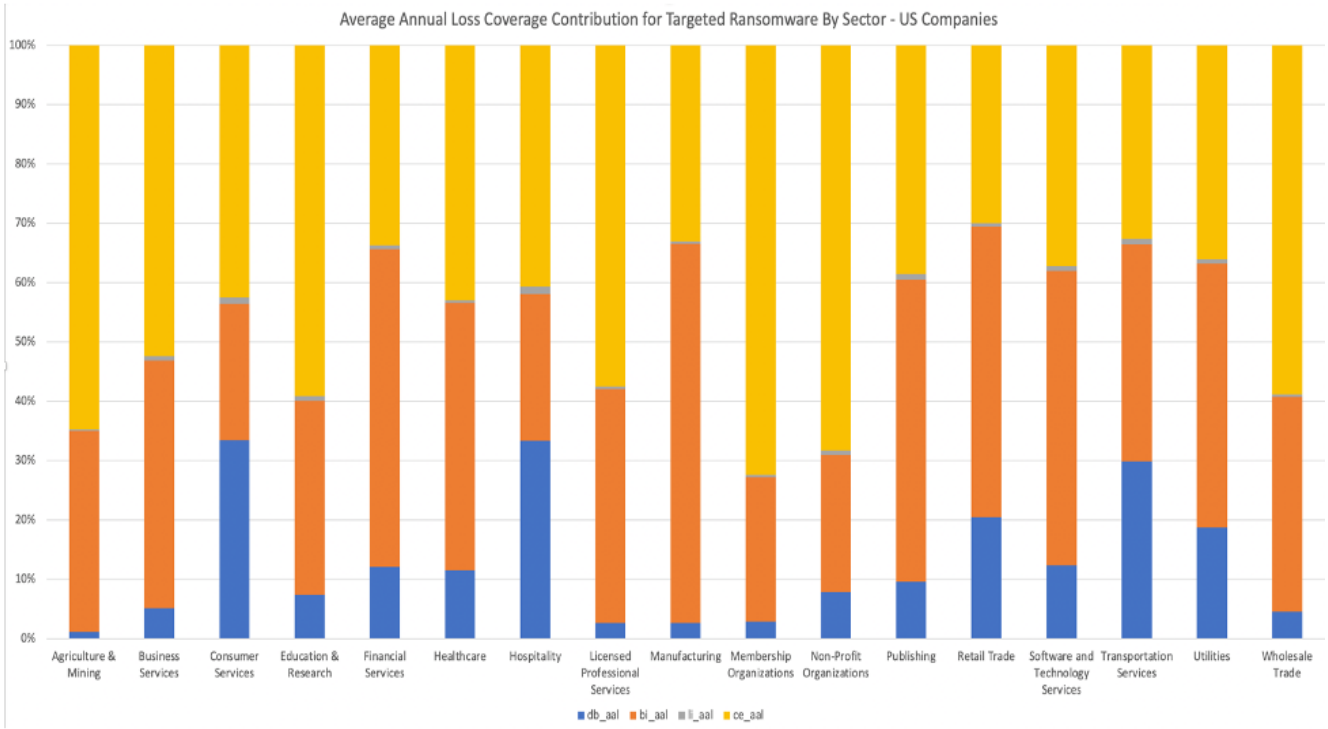


Figure 3. Relative distribution of predicted loss associated with ransomware from sample population. Note the difference between BI and DB, with the latter comprising third party liability loss projections. (Source: Guidewire- Cyence Cyber Risk Analytics, Model 5 Preview, July 2021)

[13] These rulings were issued: in July 2021 against Rutter's convenience store chain in a data breach class action suit that affected consumers' credit card data at nearly 70 stores (In re Rutter's Data Sec. Breach Litig., No. 1:20-CV-382, 2021 U.S. Dist. LEXIS 136220, at *2 (M.D. Pa. July 22, 2021); in May 2020 against Capital One for its exposure of 100M credit card applications the year prior (In re: Capital One Customer Data Security Breach Litigation, E.D. Va., No. 1:19-md-02915); and, in January 2021 against Clark Hill Law Firm in a case brought by an exiled Chinese businessman whose client information was hacked and published online (Guo Wengui v. Clark Hill, PLC, No. 19-3195, 2021 WL 106417 (D.D.C. January 12, 2021)).

[14] Homeland.house.gov/activities/hearings/cyber-threats-in-the-pipeline-using-lessons-from-the-colonial-ransomware-attack-to-defend-critical-infrastructure.

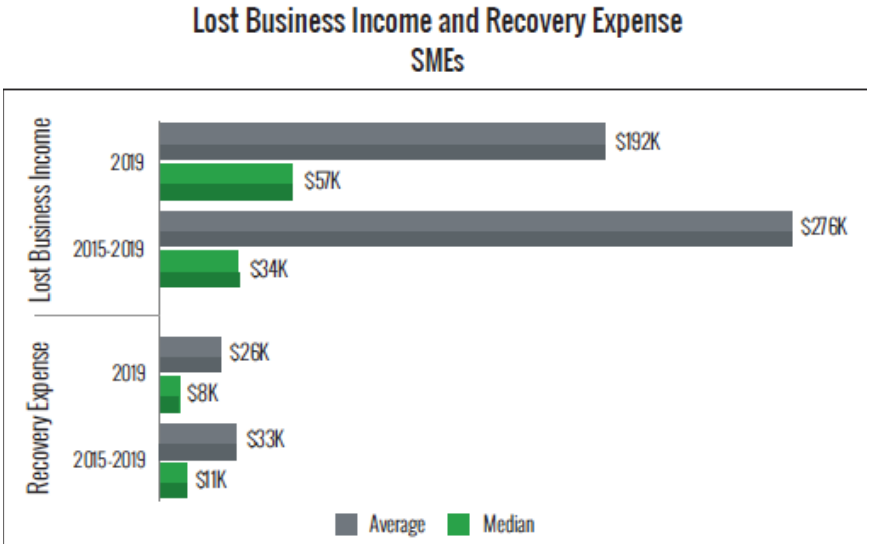


Figure 4. NetDilgence 2020 BI Expense Growth

Lastly, positioning the data privilege vs. disclosure as a zero-sum tradeoff is innovation-challenged. Advances in disclosure control technologies like multiparty computation (MPC), trusted execution environments, and federated learning afford technical solutions to the data sensitivity-underwriting utility tension. [15] Because these solutions have only recently begun transitioning to the marketplace it's an open question how laws dealing with evidentiary discovery will be applied. The takeaway for cyber underwriters is that there are opportunities to realize the hidden insights in data while safeguarding against other risks.

Disjointed Insurance Business Processes

In addition to the questionable economic and strategic underpinning that holds DFIR data hostage, another hidden force that's mooring this convention is disjointed insurance business processes.

First, there is a gap between the risk assessment data that's engaged prior to binding a policy and what's collected in the post-incident claim. Current underwriting methods are suboptimal in this regard, relying on combinations of questionnaires, outsourced third party risk assessments & threat intelligence, desk research, and client meetings.[16] Noticeably absent is IR data that can among other purposes offer empirical grounding to the efficacy of risk controls that underwriters aspire to know pre-binding and throughout the policy period. The business process issue for many cyber insurers is not a function of authority over IR data, but rather, structuring and processing more robust claims data to inform underwriting. This includes legacy claims platforms that are constrained by the types of data that can be ingested into insurers data management workflow, non-standard data formats, siloed technical systems, and/or fragmented paper-based data processing. So even if carriers were to exercise their governance authority to acquire better data from the IR process, the cyber incident details, metadata, and more granular forensics may not be integrated into legacy database schema and tables to close the loop with front-end risk analyses.

Alongside this technical and syntactic gap whose remedy is a matter of applied IT engineering, lays also semantic challenges. [Fig 5] Prerequisite for systems or platforms that capture, search, and analyze data is standardized fields.

[15] See, e.g., Royal Society, "Protecting privacy in practice: the current use, development and limits of Privacy Enhancing Technologies for data analysis" (March 2019).
[16] See, e.g., ENISA, "Commonality of risk assessment language in cyber insurance." (Nov 2017).

Role	Objectives	Functions	Data Types
Underwriter Risk Engineer	• Attritional loss prediction: What's the probability that Company X will be attacked this year causing payouts in excess of policy limits, attachment points, or retention? • How can the insured buy-down exposure with security controls?	• Prospect, Assess, Monitor, Select individual company risks • Advisement on security controls	• Firmographics • Technographics • Cyber incidents, risk scores/ratings, threat trends • Risk Factors • Example: Open ports, patching cadence, security policy training and enforcement, Network footprint
ERM	• Aggregate loss prediction: What's the probability that my portfolio losses will exceed a certain amount over the next N-years?	• Estimate Aggregate Losses • Determine Risk Appetite • Allocate Capital Reserves • Regulatory Reporting	• Portfolio Loss (Exceedance Probability (EP) & Probable Maximum Loss (PML) curves • Scenario Modelling • Example: realistic disaster scenarios
Claims **Risk Control**	• How can security controls prevent or mitigate exposures? • What people, processes, tech failed and need improvement	• Investigate, contain, recover from incidents	• Claims and Notice of Loss reports • Example: Threat source & vector, attack technique, root cause; impact, recovery & restoration costs

Figure 2. Cyber risk semantic stack.

Finally it's worth mentioning that market forces play a role in facilitating this feedback loop gap.

The prior soft market prioritized the need to write more policies ahead of optimizing underwriting analytics. The current hardening market makes it easier for carriers to institutionalize an analytics feedback loop that shifts priorities to higher quality continuous-loop analytics in lieu of a focus on high quantity, shallow underwriting.

Unhiding What's in Plain Sight

While there is variability across IR documentation, the lack of carrier-driven standards and the expanded role of insurers in proactive risk reduction argue that smart engineering of IR data for claims should take a cue from infosec industry data standards. As raised in the previous section, views of risk along the insurance stack and across ecosystem stakeholders are inconsistent because of disparate semantics and syntactics. The continuous analytics feedback loop between claims and underwriting uniquely offers both cross-functional and cross-domain learnings and insight.

Innovative infosec and DFIR firms are embracing the VERIS and Mitre ATT&CK frameworks, so it's logical that these should be the connective tissue for carriers who seek to effectuate that learning and insight. With VERIS both incidents and risks are represented using the same language. The canonical categories of data include Threat Actors, Assets, Impact, Controls, and Attributes.[17] [Figs 7 & 8]. While VERIS offers a strategy-level IR classification scheme, Mitre ATT&CK presents a tactical-level

[17] VERIS- The Vocabulary for Event Recording and Sharing, veriscommunity.net.

perspective on IR.[18] ATT&CK normalizes cyber adversary tactics, techniques, and practices [Fig 6] and is steeped in a behavioral economics logic that attackers leverage playbooks to enable efficient operations (minimize cost and maximize gain). In either case, these classification schemes offer a path to continuous-loop analytics and more sophisticated cyber underwriting insight.

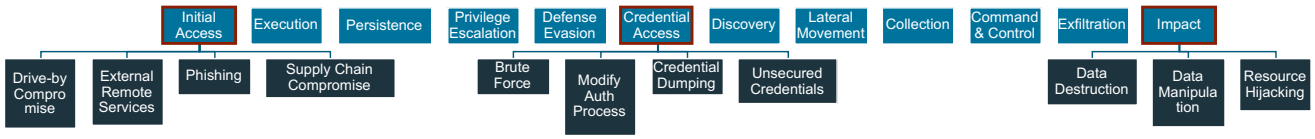


Figure 6. Mitre ATT&CK TTP Data Classification

If IR and claims are classified in this way an underwriter considering a cyber policy application can consult its corpus of VERIS/ATT&CK-informed claims to augment its assessment of likelihood and severity of the applicant's cyber losses. A notional example may look like the following: companies in the professional services sector with revenues between $20-50M revenue [FIRMOGRAPHICS] who are attacked by financially-motivated attackers [ACTOR] who misuse stolen credentials [ASSET], obtained as a result of deficient email authentication [CONTROLS], to execute ransomware [ACTION →Malware →Ransomware] which encrypts and exfiltrates [Attribute→ Confidentiality, Integrity] data [ASSET] have a 15% higher chance of exceeding prescribed policy limits. Infosec services and products are continually trying to uncover adversary behavioral patterns and controls failures … cyber insurers can play a very complementary role.

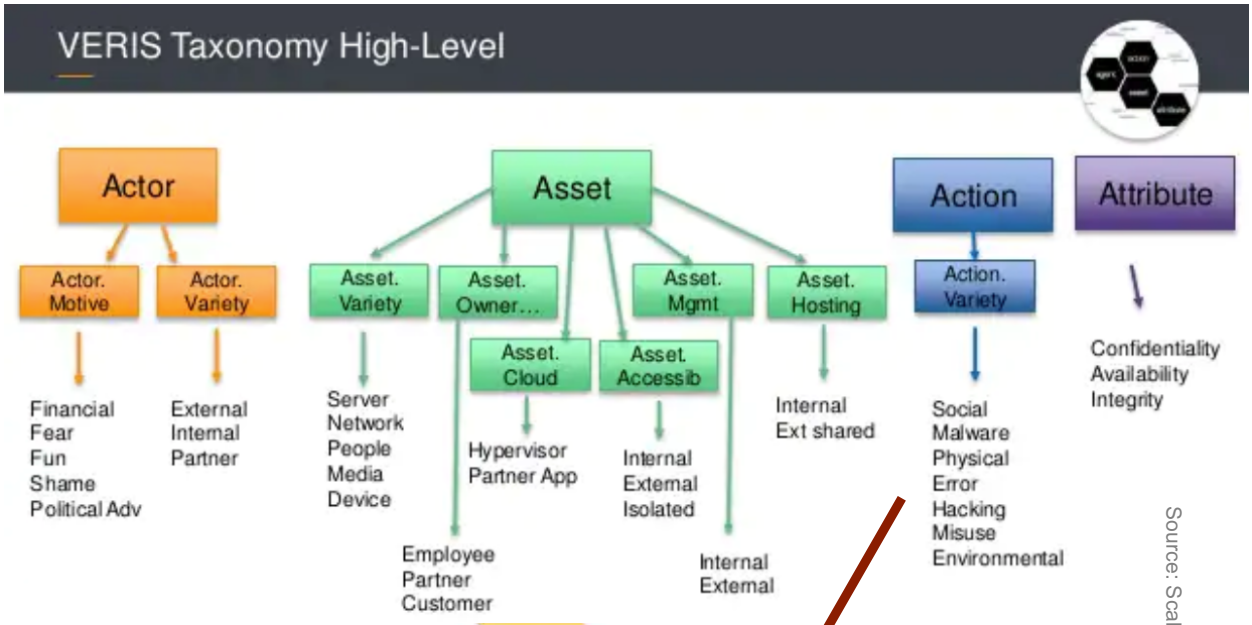
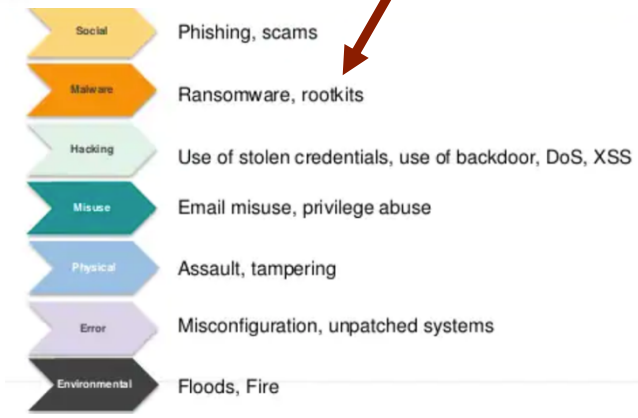


Figure 7. VERIS Incident Classification.



Source: Scalar, B-Sides 2016

Figure 8. VERIS ACTIONS Sub-classification.

[18] Mitre ATT&CK, attack.mitre.org.

Now-Gen Cyber Underwriting: Building a More Robust Cyber Risk Playbook

Tackling Visibility Bias. Now-generation cyber underwriting requires going beyond indemnifying, pooling, and diversifying risks at the policy level to proactively managing insureds' cyber risk at the technical and governance levels.[19] To do so, underwriters need a view of risk that is consistent across the insurance stack. Insurers cannot effectively paint this picture unless they build a continuous feedback loop and learning between post-incident response & recovery that informs pre-incident risk selection, and prevention & mitigation controls. Gathering and integrating data according to the "Cyber Risk Playbook" [Fig 9] will reduce blindspots and subjective inference risk. Ultimately this is the path toward next generation risk selection, pricing, control, & capital allocation.

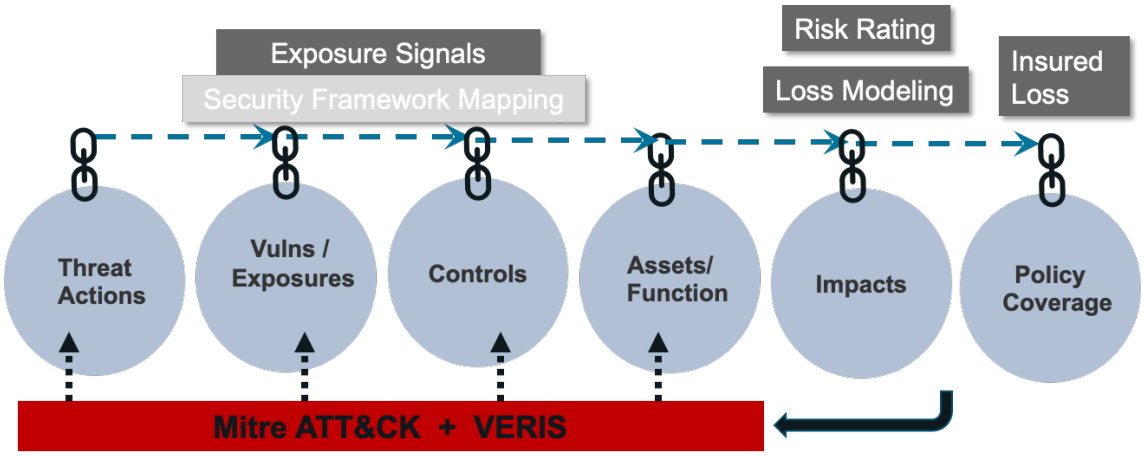


Figure 9. Cyber Risk Playbook

Pushing Standards. Another benefit that derives from this continuous feedback loop is private ordering of standards and the reduced uncertainty that follows . Rather than reactively wait for exogenous (legislation, regulation, or case law) enforcement of standards, cyber insurers can be a forcing function onto itself. By dovetailing risk assessment and incident response data and because of their cross-industry vantage point, insurers are uniquely situated to observe security controls efficacy and drive de facto standards through their policy incentives. While infosec firms can offer invaluable recommendations based on empirical dealings with compromised companies, insurers are highly leveraged to drive implementation of those standards.

Untapped Potential: A further advantage of continuously looping DFIR data for frontend underwriting is it provides a level of objectivity and firm-level specificity that can complement technical risk assessments and that outperforms other conventional approaches used by underwriters to proxy risk evaluation. [Figure 10] As well, DFIR-informed claims can accord insurers a competitive advantage in a cyber market where most other data is commoditized and can be easily purchased.

[19] Kenneally, Erin E., Ransomware: A Darwinian Opportunity for Cyber Insurance (December 29, 2020). Forthcoming, CONNECTICUT INSURANCE LAW JOURNAL FALL SYMPOSIUM EDITION (VOLUME 28.1) Fall 2021. Available at SSRN: ssrn.com/abstract=3849120 or dx.doi.org/10.2139/ssrn.3849120.

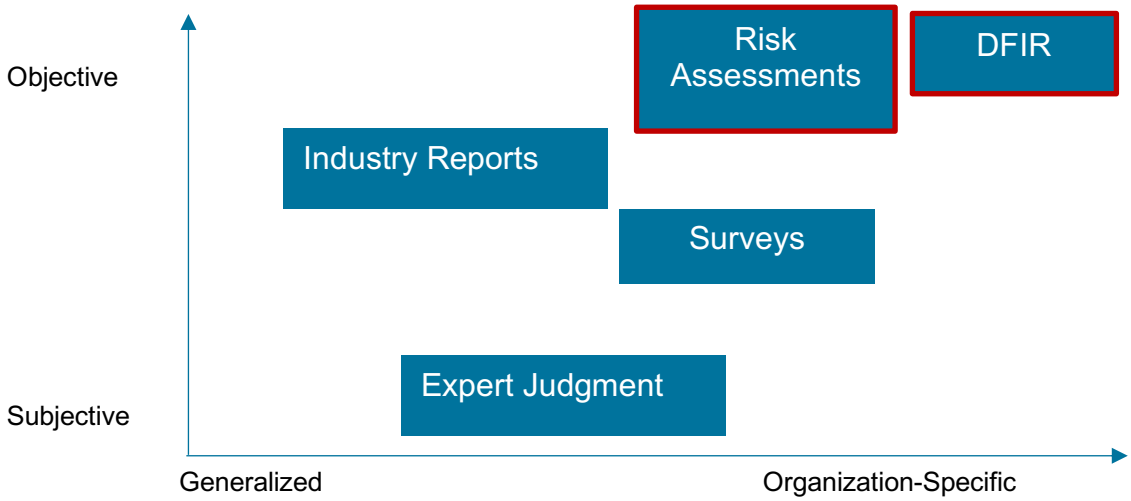


Figure 10. Cyber Underwriting Risk Assessment Sources

Price Reflecting Value. The disparity between cyber security spend and insurance premiums has been estimated to be $116B. [Fig. 11] Global cyber insurance expenditures and risk transfer are growing at slower rates than overall infosec spending and cyber crime losses.[20] These two trajectories signal the current incongruity between what should be a symbiotic relationship, as well as an underserved opportunity for cyber insurers. If this delta is to be narrowed, cyber insurance and infosec cannot afford to continue on disconnected trajectories. For risk transfer to be relegated to the residual risk that remains after implementing reasonable security controls, continuous looping of backend DFIR and frontend risk assessment plays a vital role.

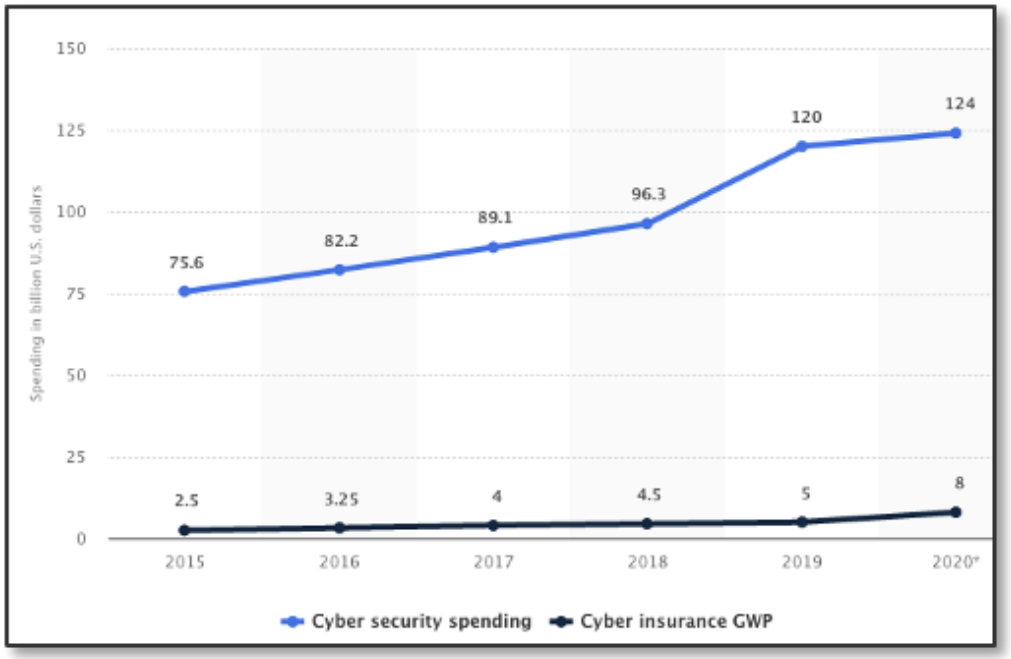


Figure 11. Annual Cyber Security and Cyber Insurance Spending Worldwide (Statista)

[20] Statista, 2020 Annual Cyber Security and Cyber Insurance Spending Worldwide.

History Rhymes and Repeats. While continuous loop analytics may be new to cyber insurance, the notion of extracting the value from incidents to prevent and mitigate risk is far from novel. A quarter of a century after the first known fatal collision, auto wrecks were the leading cause of accidental death in the U.S. Most of those deaths, however, were not attributed to the multi-ton hunks of steel on the road. In the past fifty years the car crash death rate has plummeted almost 80% in the U.S. This is owing in large part to the accident report forms filled out by police officers in response to crashes that record weather conditions and other variables relevant to causal analysis. Many of these reports are committed to the Fatality Analysis Reporting System, which provides auto manufacturers, consumer safety advocates, and regulators the ability to understand the root causes of auto deaths. As well it armed designers and engineers with the raw knowledge to build safer vehicles and roadways.[21] For example, seat belts and collapsible steering wheels have saved hundreds of thousands of lives.

The fact that cyber incidents involve malicious adversaries compared to cars and roads misses the teachable artifacts for cyber risk. The analogous critical question for cyber insurers is how capabilities that cause risk can be modified or augmented to prevent or reduce loss exposure. Similar to what occurred with vehicle standards, perhaps it will similarly take politics to move the needle. Regardless, now-gen cyber insurance risk strategy needs to consider the dangers associated with inter-connected organizations, reliance on homogenous technologies, and designing for efficiency at the expense of security. The path to these insights is lined with continuous loop analytics.

[21] 99percentinvisible.org/episode/nut-behind-wheel/.