PUBLISHED AUGUST 2021

Cyber Data
CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

Cyber Data

Published August 2021

Unlike most other property/casualty insurance lines of business where insurers typically have relied on vast amounts of premium, exposure, and claims data collected over many years to develop tools based on statistically significant results, cyber insurers have historically had a lack of in-house data for evaluating cyber risk. While the amount of data available to cyber insurers is growing, standard actuarial pricing models used for other property/casualty lines of business do not work as well with cyber because insurers have either just entered the market and therefore have limited data, or they have been writing cyber for years but the exposure continues to evolve. This same limitation applies to reserving for cyber as well.

Through the lens of cyber, incident data may be viewed as referring to events whether insured or uninsured, cyber insurance applications, threat intelligence,[1] outside-in vendor scoring,[2] an organization's internal risk assessment, and security vendor research papers, among others. The term "data" in the context of cyber can be difficult to define as each individual or organization may have a different perspective of what to include when it comes to cyber data. For the purpose of this general overview, details will be primarily discussed that are directly related to cyber data as collected via the cyber insurance placement process and claims activity received from insureds that have purchased cyber insurance. For future overviews and actuarial research, there are other areas of cyber data to explore such as security industry publications, threat intelligence feeds,[3] vulnerability scans, and professional services publications from law firms and forensics providers.

Availability

Historically and even today, there is limited data on the linkage between an entity's propensity to experience a cyber incident and its security risk and vulnerabilities. In addition to the continuously developing and changing cyber landscape, the high level of complexity of these risks and breaches can lead to a misattribution of signal versus noise when it comes to the leading indicators of a future cyber incident. However, the availability of cyber data from both a security and incident perspective are growing with the digitization of society and business. The digitization of organizations changes the cyber risk landscape but also allows for valuable information to be extracted and organized by technology in a way that helps inform cyber insurance decision making.

1 Cyber threat intelligence: information about threats and threat actors which helps mitigate harmful events. Example of sources: social media, intelligence from the dark web.
2 Risk/threat measures by scanning a company's network perimeter to identify security risks and weaknesses.
3 Real-time data providing information on potential cyber threats and risks.

Actuaries often look at historical events as being indicative of future risk. In the cyber risk environment, a continually improving internal security environment within organizations and continually evolving adversaries create additional complications that are not as pervasive with other insurance lines of business. Just because a certain vulnerability is patched within an organization does not mean that a threat actor will not pivot to a different vulnerability or access point to achieve their objectives and cause a loss to the organization. Additionally, reliance upon common software suites or technology vendors creates a systemic aggregation issue that is not as common with other types of risks.

In addition to the evolving changes, new laws surrounding cybersecurity and data privacy are being put in place around the globe. These new laws provide additional potential liability risks associated with noncompliance or a lack of appropriate internal controls. Understanding the potential liabilities associated with these laws is important, as a historical event may have a significantly higher cost to an organization had the incident occurred after the law went into effect. Where certain liability lines of business deal with social inflation and nuclear verdicts,[4] cyber events have a similar concern over inflation due to changing laws and class action settlement trends.

Challenges

Within any new insurance market, insurers are hesitant to underwrite risk they do not fully understand. To prevent unexpected losses, insurers have historically employed a conservative strategy by structuring coverage under narrow terms and conditions (e.g., low limits, high retentions, etc.). As a new line of business matures and more experience emerges, these initial restrictions might be loosened. A similar evolution has been observed in the cyber insurance marketplace in which sub-limits that were once common have now been removed, waiting or qualifying periods have decreased, and the amount of capital to support most limits requested by insureds has increased. However, the broadened coverage terms always have the potential to revert back toward more restrictive terms if significant losses materialize.

4 Awards that are considered to be out of proportion with the damages suffered.

Despite the maturation of cyber insurance, there is still a concern around how well organizations understand what cyber insurance will or will not cover. Due to restrictions in terms and conditions or a lack of understanding of the product, insurance buyers may feel the product does not adequately meet their needs. For example, an organization may choose *not* to purchase cyber business interruption coverage within its cyber insurance policy. If that organization has a cyber business interruption event, the insurer will appropriately deny covering the claim because business interruption coverage was not purchased. The organization may still sue for coverage either because they did not understand that they did not have coverage or they are hoping there is enough ambiguity in the insurance policy that coverage may still be provided. This conundrum over the lack of understanding of terms and conditions within cyber insurance policies could lead to a lower amount of cyber insurance purchased, which can in turn reduce the amount of data insurers can collect.

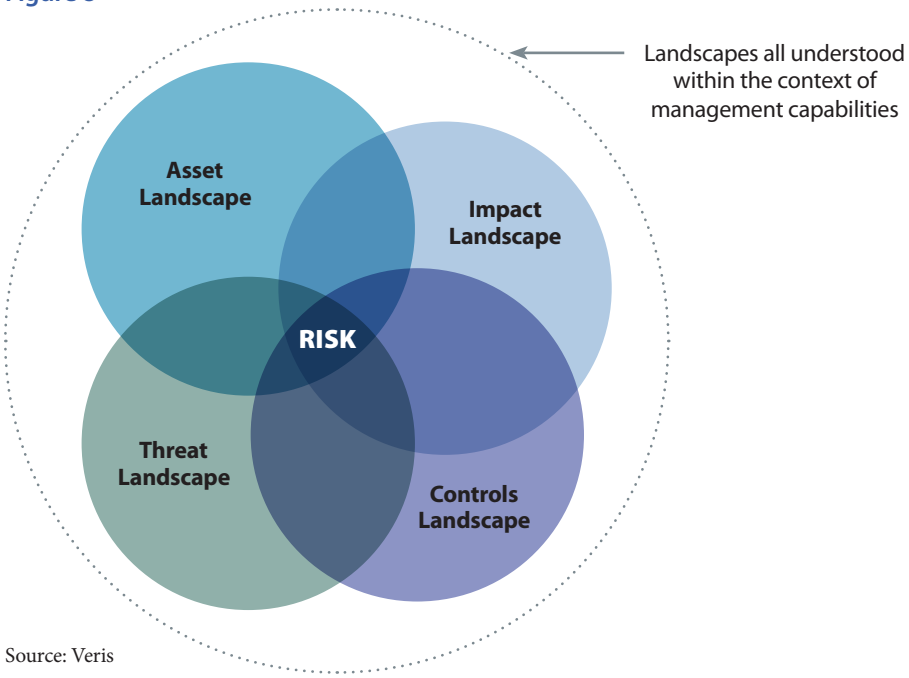
Regardless of the social environment and understanding of cyber insurance, cyber insurers may look to supplement the information obtained via the underwriting process and claims activity with third-party data. Armed with this additional data, insurers may simplify the process of providing cyber insurance, increase their confidence in selling adequate cover, and expand to segments of the market where they previously were unwilling or uncapable to enter using data of their own. Third-party data may include cyber catastrophe models, licensed incident data from risk aggregators, outside-in security scoring vendors, common technology vendor/software aggregation, and threat intelligence data, among others. The pivotal step to making this third-party data useful is gathering and reviewing all available information in a way that makes it easy for insurers to access and cross-reference with their internal data. The essential component is the matching algorithm work done to map the insurer's data to the various third-party data elements.

Insurers may face challenges in collecting data on their own as they are bound by policy and claim systems that may need significant amendments in order to respond to the evolving nature of cyber policies. These policies often require new policy and claims fields to be coded, such as new coverages, attack vectors, assets impacted, etc. Making these IT changes is difficult for companies due to legacy systems and associated high costs and therefore companies may not capture all of the important information that may be valuable for analysis and ratemaking.

Enhanced Data Collection

As insurers in the cyber insurance market look to evolve their understanding and use of data when evaluating cyber risks, third-party vendors and data providers have been working to bridge this gap. There are many vendors available with different products and capabilities. Each insurer can assess its needs, data availability, and the capabilities it requires in reviewing vendors. The following provides an illustration of the work being undertaken in the broader cyber security and cyber insurance industries.

Figure 8



Source: Veris

Which Data Elements Should Be Collected and Why

The management and analysis of cyber data collected is not consistent across the cyber insurance industry. This inconsistency can create issues while evaluating risk since there is no commonly adopted data classification and security rate scoring map. Additional time and energy must be spent standardizing the cyber data collected to analyze trends overtime. Not only are insurers capturing different data, the data they do collect may not be continuous and contextualized. It is crucial to have continuity of assessment of cyber risks.

Data limitations and availability results in significant challenges for cyber insurance underwriters. Examples of ways cyber insurers can overcome some of these challenges include:

- Expand sources and collection of data—ask companies about their endpoints, servers and encryptions; include questions about known previous security threats and breaches, which should be validated by a third party; listing of all the domains of the company as well as their subdomains, certificates, port scanning and all hostnames pointing to IP blocks the company owns. All these are of critical importance to getting a picture of the company's infrastructure. Finally, collecting the publicly available information about the company is important as that is the information that attackers are most likely to exploit first.
- Receive input from a variety of subject matter experts—it is important to engage the corporate information security officer (CISO), IT department, chief financial officer, risk managers, legal department, claims department, and the marketing team.
- Obtain an understanding of the industry and its exposure to cyber—work with companies closely related to the industry you are most familiar with so you can most accurately assess what kind of coverage is necessary.
- Leverage information from third-party cyber information providers—leverage companies providing cyber threat intelligence and aggregation risk data to help create a better-informed cyber risk profile.

Information to inform cyber underwriting and cyber risk is not as scarce as some believe. Technology firms are providing a diverse range of data, including:

- Firmographics—organizational characteristics, such as industry, revenue, and employee count, are extracted from public and private data sources.
- Outside-in scans—sensors on the public space of the internet scan a company's network perimeter to identify their virtual supply chains and monitor security outcomes.
- Inside-out scans—sensors installed in a company's network scan its internal architecture to identify assets, device configuration, access points, and other security aspects.
- Threat monitoring—machines read streams of data from the surface, deep, and dark webs to uncover intelligence on compromised organizations and new vulnerabilities.
- Process and policy—data exchanges, used by organizations to assess compliance with security process and controls, are mined for cyber information.
- Incident data—scraping algorithms compile cyber incident and loss data from governments and other public sources.
- Incident tracking—incident ID, source ID, incident confirmation, incident summary, related incidents, confidence rating, and incident notes.
- Victim demographics—victim ID, primary industry, country of operation, state, number of employees, annual revenue, locations affected, notes, and additional guidance.
- Incident description—actors (external, internal, and partner), actions (malware, hacking, social, misuse, physical, error, and environment), assets (variety, ownership, management, hosting, accessibility, cloud, and notes), and attributes (confidentiality/possession, integrity/authenticity, and availability/utility).
- Discovery & response (incident timeline, discovery method, root causes, corrective actions, targeted vs. opportunistic, and additional guidance).
- Impact assessment (loss categorization, loss estimation, estimation currency, impact rating, and notes).

Sample Cyber Data Websites

The list below includes sample websites that may be accessed to understand cyber incident data and trends in the cyber landscape.[5]:

https://breachlevelindex.com/

https://www.advisenltd.com/data/cyber-loss-data/

http://veriscommunity.net/vcdb.html

https://www.privacyrights.org/data-breaches

https://www.hackmageddon.com/

https://cyber.fsi.stanford.edu/

https://businesslawtoday.org/2018/03/whats-lurking-back-there-cybersecurity-risks-in-legacy-systems/

https://www.sitelock.com/blog/black-box-vs-white-box-part1-dast/

https://www.sitelock.com/blog/tag/white-box-testing/

https://securitytrails.com/blog/improve-cyber-insurance-underwriting

https://www.cyberriskanalytics.com/#features

5 These links are being provided as a convenience and for informational purposes only; they do not constitute an endorsement or an approval by the American Academy of Actuaries of any of the products, services, or opinions of the corporation or organization or individual. The Academy bears no responsibility for the accuracy, legality, or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**