Vantage Risk

The Cyber Event Set: An Evolving Catalogue

Introduction

Cyber insurance is a line of coverage that requires a thoughtful approach and flawless execution. From hiring the right team, to building a sound underwriting strategy and risk management approach, cyber risk necessitates a holistic view that enables insureds to *see their risk differently*. The ubiquitous and dynamic nature of cyber risk requires a feedback loop of risk awareness, mitigation, and resilience. This must be an active process for both insurers and insureds throughout the policy lifecycle. Both incumbent and new entrant cyber insurers (and MGAs) are making strides in the right direction. Now that the rubber has met the road with the actualization of cyber risk in recent years, underwriting standards are driving more deliberate risk management by both insurers and insureds alike. This will hopefully lead to a sustainable marketplace over the long term.

The cyber risk landscape is fast moving and full of unknowns, with the potential to cause large societal disruption and significant financial loss. This is evident in the progression of ransomware events which are occurring with increasing frequency and severity. Some ransom demands are now approaching unprecedented amounts near $50 million[1]. Ransomware has been around for quite some time, but initially manifested as less targeted, more opportunistic attacks. Early ransoms were in the neighborhood of $500 dollars per infected machine and caused far fewer notable losses for insurers than we see today. It was not until the WannaCry event in 2017 that a ransomware attack had the ability to spread broadly using a network worm-style propagation. While the overall insured loss resulting from WannaCry was limited, it highlighted the catastrophic potential of cyber risk. Ransomware events are currently one of the primary exposures driving the cyber conversation today due to the marked uptick in frequency and severity; this was not always the case.

Some of the most challenging attributes of cyber risk for insurers include its accumulation potential, the shifting risk landscape, and uncertainty around what the event set truly consists of. Attacker tactics and procedures are shifting to evade security defenses, and business reliance on technology is evolving rapidly. We have seen a swift acceleration of digital transformation efforts and increased reliance upon corporate network infrastructure for nearly all businesses and sectors due to the COVID-19 pandemic. Microsoft's CEO, Satya Nadella noted that "we've seen two years' worth of digital transformation in two months"[2] in the early days of the pandemic and that trend has persisted with no sign of slowing down. Corporate attack surfaces have vastly expanded and evolved due to this activity. Operational reliance on this enhanced connectivity is only growing.

Uncertainty around the potential set of events can create blind spots and leave organizations at a loss for who and what to protect themselves from. And while a number of sizable cyber events have occurred in the market over the last decade, the ones with the most systemic potential have had relatively limited realized insured losses. To date, the losses that cyber insurance has paid are mostly attritional in nature.

[1] https://www.infosecurity-magazine.com/news/accenture-tied-up-in-50m-ransom/
[2] https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

Vantage Risk

The Cyber Event Set: An Evolving Catalogue

Last year, the NAIC reported that the top 20 groups in the cyber insurance market had 2020 direct loss ratios ranging from 24% to 114.1% with an average of 66.9% (up from 44.6% in 2019)[3]. These figures beg the question of whether catastrophe losses are being adequately accounted for in carrier pricing strategies given this loss year did not include a major cyber catastrophe.

So, what does the cyber event set look like? When considering this, insurers and insureds alike are probably asking themselves, *"Where's the cat? And what's in the tail?"*

The Cyber Event Set

The below is meant to serve as a primer highlighting some types of cyber events that organizations and their insurers should be thinking about. This list is in no way comprehensive but meant to outline some of the broad categories and provide real-world examples that have been observed.

Data Breach

Cyber insurance's initial uptake was largely driven by data breach notification laws. These laws place strict obligations on corporations to notify individuals if their private information has been exposed. The first of these laws was inked in California in 2002; now nearly every US state has a similar law, and Europe has the General Data Protection Regulation (GDPR). Data breaches come with immediate first-party costs for advisors and providers to isolate, identify, and remediate the affected systems. In addition to notifying individuals, it has become customary to offer credit monitoring to affected individuals as well. Depending upon the circumstances, corporations can face liability, fines, and penalties for a data breach as well. Finally, the business interruption, reputational blow, and loss of customer trust often leads to reduced sales for some amount of time.

Some notable data breaches include:

- Target Corporation's 2013 breach of 40 million customer credit cards via BlackPOS which siphoned unencrypted credit-card transactions in transit and exfiltrated the data without detection. A notable early loss that cost the company approximately $290 million of which only $90 million was insured[4].
- US Office of Personnel Management's 2015 breach which exposed over 4 million individuals background investigation records[5].
- Yahoo's 2017 data breach of 3 billion accounts which negatively impacted acquisition negotiations with Verizon to the tune of $350 million[6].
- First American Financial's 2019 breach of 885 million customers' financial information including bank account information, social security numbers, wire transactions and mortgage details[7].

[3] https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf

[4] https://www.reuters.com/article/us-target-breach-settlement/target-in-39-4-million-settlement-with-banks-over-data-breach-idUSKBN0TL20Y20151203

[5] https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[6] https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

[7] https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=24cce637567f

Ransomware

If data breaches drove the first wave of cyber insurance, then the second wave has certainly been dominated by the dramatic shift in the ransomware landscape. Ransomware deploys malicious code onto a system, encrypts the machine's contents so they cannot be accessed by the user, and demands a ransom payment, typically in cryptocurrency, to decrypt the data. Surprisingly, there is honor among thieves; though there is no guarantee, cyber criminals typically make good on decryption when the ransom is paid. Some groups are even known to have decent customer service helping victims through the process.

Ransomware is a much more direct monetization scheme for bad actors than stealing data. In the data breach era, cybercriminals would monetize their efforts by selling the stolen data on the dark web where other criminals leverage the information to commit fraud and steal identities. In contrast, ransomware simplifies the process and tightens the connection between delivering the payload and monetization, and has become the attack du jour. In addition to the direct loss due to the ransom, organizations will typically suffer first-party losses for remediation, business interruption, and potential data breach related costs as well.

Some recent individual company ransomware events include:

- CNA's 2021 ransomware which led to a $40 million ransom payment and exposed 75,000 personal records including social security numbers[8].
- Colonial Pipeline's 2021 ransomware attack, which caused the operators to shut down an entire pipeline which normally transports 2.5 million barrels of oil per day. This was the first full scale shut-down in its 57-year history. The company paid $4.4 million ransom and lost nearly 100 gigabytes of data. Additionally, gas shortages due to the outage caused price increases[9].

Targeted data breaches and ransomware payloads are often delivered via phishing and spear-phishing attacks rather than complex brute force hacking of a network. Manipulative emails and social media activity are used to dupe well intentioned employees into clicking on malicious files and links thus creating an entry point for attackers.

Widespread Events

Many of the events noted thus far are targeted and impact one company at a time. However, the interconnectivity of the internet and commonality of software, hardware, and service provider usage creates the potential for risk correlations which can lead to cyber catastrophe events with accumulation losses.

Zero Day Vulnerabilities

Zero-day vulnerabilities are security flaws that a software vendor has not yet created a patch for due to either not knowing of the vulnerability yet or because it has only recently been discovered. Upon discovery, attackers will scour the internet for vulnerable systems to exploit, resulting in the potential for aggregated losses in the period before a patch is released and broadly adopted.

[8] https://www.chicagotribune.com/business/ct-biz-cna-cyberattack-exposed-personal-information-20211102-2jle5opb65hczlpz6tifik6n2a-story.html

[9] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Some notable zero-day vulnerabilities include:

- The ‘ShadowBrokers’ hacker group disclosed the EternalBlue zero-day vulnerability for Windows in 2017 which was leveraged by both the Wannacry and NotPetya ransomware attacks. These attacks enlisted a worm propagation method to infect large numbers of corporate machines across the world. Claims emanating from these events have tested the policy language on cyber and non-cyber policies, sparking industry debate about intent and coverage litigation. The US White House estimated the total economic damages from NotPetya to be approximately $10 billion, an unprecedented single-event ransomware loss[10].
- Solarwinds Orion software is used to help manage network infrastructure for public and private sector entities. In 2020, Hackers inserted malicious code into legitimate software updates, leveraging a backdoor to infect Solarwinds Orion customers and providing broad access to their networks. In an SEC filing, Solarwinds stated that fewer than 18,000 of 33,000 Orion customers were affected[11]. A Russian advanced persistent threat group named Cozy Bear was reported to be behind these attacks, impacting notable targets including The US Treasury, The US Department of Homeland Security, and cybersecurity firm FireEye (now Trellix)[12].
- In early 2021, four zero-day vulnerabilities were discovered which, when used together, enabled remote code execution in Microsoft Exchange servers. Microsoft exchange servers are widely used for business email and calendars across the globe, so the scope of vulnerable machines was quite broad. Attacks leveraging the vulnerabilities have been linked to several state-sponsored advanced persistent threat groups. According to CNN, approximately 30,000 US companies and 250,000 companies globally were impacted[13].
- Kaseya offers IT software that enables remote monitoring and management of network endpoints. Customers include Managed Service Providers (MSPs) who offer security and IT services as a provider to many companies. In 2021, a supply chain attack was launched impacting MSPs using the Kaseya software and their customers resulting in between 800-1500 successful ransomware attacks[14].
- Log4J is a zero-day vulnerability discovered in late 2021 which enables remote code execution in the Java logging framework that is widely used across the internet. Although potentially broad in scope, thus far the known impact has been limited with some insurers citing the difficulty in exploiting the vulnerability as the saving grace which has limited ultimate impact for their insureds[15].

These examples highlight how differences in exploitability, severity, and usage can have widely varying outcomes. There are many other notable zero-day vulnerabilities that have occurred, but this provides a good set of examples to draw from.

[10] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[11] https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

[12] https://arstechnica.com/information-technology/2020/12/18000-organizations-downloaded-backdoor-planted-by-cozy-bear-hackers/

[13] https://www.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html

[14] https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

[15] https://www.at-bay.com/articles/log4j-practical-exposure/

Service Provider Attacks

The proliferation of cloud computing has intentionally aggregated companies to shared computing and storage resources, bringing many benefits and efficiencies to business users. However, service provider aggregations like this create circumstances that drive correlated risk across companies. To date, most outages have been regional and relatively short, but looking at the limited outages which have been realized through a counter-factual lens shows that circumstances can certainly escalate to higher severities than we have seen to date, at least in the tail. Cloud service providers like Amazon AWS are, by-and-large very reliable, but outages affecting even a subset of a cloud provider's network can impact the many companies who rely on that portion of shared infrastructure. US East 1 is Amazon AWS's largest set of data centers. It is currently comprised of 6 availability zones (us-east-1a through 1f). When contracting with a cloud provider, companies can specify which availability zones the infrastructure they are leveraging is located in and can purchase access to additional availability zones for redundancy in case of an outage. Other leading providers such as Google Cloud Platform and Microsoft Azure offer similar redundancy configuration options.

- In 2016, domain name service (DNS) provider, Dyn, suffered a significant distributed denial-of-service attack (DDoS), bringing down major internet platforms including Amazon, Netflix, The New York Times, Reddit, Slack, Twitter, among others[16]. DDoS attacks flood servers with requests in an attempt to degrade performance and cause a failure of the servers due to the overload of requests. This attack was achieved by flooding Dyn's DNS servers with requests from tens of millions of IP addresses. DNS servers typically provide the IP addresses associated to a website, serving as a phonebook for users of web browsers looking up a URL and routing them to the associated IP address. This attack was achieved via a botnet of zombie printers, camera, cable boxes, and other personal connected devices which had been infected by and controlled via the Mirai malware and botnet servers. Botnets are networks of infected machines that are controlled as a group by the botnet's operator unbeknownst to the actual owners of the infected machines. The Mirai botnet was first seen a month prior when it delivered a DDoS attack of unprecedented intensity reaching 620 Gbit/s and bringing down investigative journalist Brian Krebs' website[17].
- Amazon AWS has had an incredible record of reliability and overall uptime, but has suffered a number of notable outages over the years. To their credit, Amazon is incredibly transparent and thorough in their reporting of the details of each of their outage events. In 2017 the S3 service suffered a four-hour outage affecting the US East 1 region due to a human error during a system update[18]. In 2020 Amazon's Kinesis service was disrupted for over twelve hours in the US East 1 region[19] impacting several companies using the service including Ring, Roku, Adobe, Target, and the NYC MTA[20]. Most recently, AWS suffered a seven-hour outage in 2021 in US East 1 region[21] which impacted Amazon's delivery operations and Whole Foods orders along with impacting third party services including Disney+, Netflix, Slack, Ticketmaster, Coinbase, and a number of universities[22].

[16] https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/
[17] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[18] https://aws.amazon.com/message/41926/
[19] https://aws.amazon.com/message/11201/

While zero-day vulnerabilities have very broad potential impact, there is a high likelihood that a given vulnerable company is not impacted just by chance. However, outages at a service provider will definitively impact any users reliant upon the affected shared infrastructure, unless they have built redundancy into their technology stack that can be switched over when needed.

Physical Cyber Events

The above examples have all been purely digital in nature. While the Colonial Pipeline ransomware example resulted in the pipeline being shut down, this was done voluntarily out of caution given the potential risk and uncertainty around the attacker's identity and motivations. But cyber events can also directly impact the physical world. Several attacks have impacted industrial control systems resulting in direct physical consequences.

A few notable examples include:

- In 2010, the Stuxnet malware was discovered in the wild with a disproportionate number of infections located in Iran. The worm spreads indiscriminately causing no affect to most infected systems. The malware also carries a payload that targets Siemens SCADA systems which control uranium enrichment processes in Iran. Stuxnet leveraged multiple zero-day vulnerabilities and is said to be the most sophisticated malware ever seen[23]. This attack highlighted that even air-gapped systems, which are not connected to the internet in any direct or indirect manner, are not imperviable; the virus was spread via USB sticks and successfully disrupted nuclear enrichment equipment and processes[24].
- In 2015, a cyber-attack on the Ukrainian power grid resulted in power outages affecting approximately 225,000 citizens. The attack was the first publicly acknowledged successful cyberattack on a power grid and was attributed to a Russian state-sponsored advanced persistent threat group called Sandworm[25]. While the severity of this event was relatively mild, it serves as a proof of concept of what is possible of a cyberattack targeted at critical infrastructure.
- In 2019, Norsk Hydro, an aluminum and renewable energy company, fell victim to an extensive cyber-attack involving the LockerGoga ransomware which cost approximately $70 Million. Norsk Hydro decided not to pay the ransom demands and remediated their network themselves. Unlike Colonial Pipeline's voluntary decision to shut down the pipeline's operations out of caution, Norsk Hydro's disruption in production was not by choice as the impacted systems were directly involved in the company's automated manufacturing processes[26,27].

[20] https://www.cnbc.com/2020/11/25/amazon-web-services-outage-takes-some-services-offline.html
[21] https://aws.amazon.com/message/12721/
[22] https://www.cnbc.com/2021/12/07/amazon-web-services-outage-causes-issues-at-disney-netflix-coinbase.html
[23] https://www.computerworld.com/article/2516028/iran-confirms-massive-stuxnet-infection-of-industrial-systems.html
[24] https://www.cnet.com/culture/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/
[25] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf
[26] https://time.com/6080293/norsk-hydro-ransomware-attack/
[27] https://www.darkreading.com/attacks-breaches/6-things-to-know-about-the-ransomware-that-hit-norsk-hydro

As the geopolitical landscape becomes more precarious, physical cyber-attacks become a more likely tool to be utilized independently or as part of a multi-pronged act of hostility. Warring nations could leverage a cyber-attack on critical infrastructure to further destabilize their adversary in tandem with more traditional warlike activities. The underwriting community has been striving for greater clarity on their coverage intent around cyber risks for a number of years; many traditional P&C policies were written at a time when cyber exposures were not top of mind and the contractual language remained silent, not clearly addressing whether there was or wasn't coverage afforded under the policy. The Lloyds Market Association and several large international carriers have made public commitments to either affirmatively cover or exclude cyber exposures on their policies[28]; this contract certainty and transparency is beneficial to (re)insurers, brokers, and insureds.

Conclusion

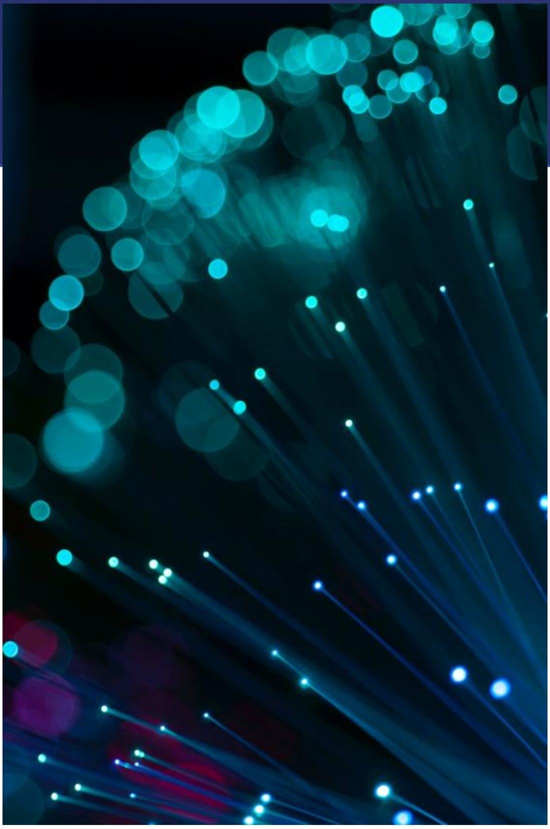
This paper is meant to serve as a primer for cyber risk, establishing a foundation by identifying the primary exposures in the event set. The risk landscape will continue to evolve and (re)insurance carriers will play an increasingly critical role in the cyber risk ecosystem. Insurers are in a unique position to help their insureds better understand their exposures, adapt their processes and technology, and drive resilient behaviors which mitigate loss potential. Ultimately, these interactions promote a more sustainable cyber insurance market that functions to efficiently reduce and transfer risk.

[28] https://assets.lloyds.com/assets/y5277-update-providing-clarity-for-lloyds-customers-on-coverage-for-cyber-exposures/1/Y5277%20Update%20%20Providing%20clarity%20for%20Lloyds%20customers%20on%20coverage%20for%20cyber%20exposures.pdf

About the Author

Phil Rosace is VP, Data Asset Lead at Vantage Risk.

Phil has spent the last 12 years working in the insurance and insurtech industry. He has held product and market facing cyber underwriting, and analytics roles at leading carriers. Phil has also served technology product management, solution architect, and sales and marketing roles at leading early stage and mature insurtech companies including Cyence (6th employee), Guidewire, and Two Sigma IQ. He is an inventor on a cyber risk quantification patent. Phil holds a master’s degree and bachelor’s degree, both in economics from Boston University.



This material is provided for informational purposes only. It is not intended as, nor does it constitute, legal, technical or other professional advice. While reasonable attempts have been made to ensure that this information is accurate and current as of its publication date, Vantage is not responsible for any errors or omissions and makes no guarantees, representations or warranties, either express or implied, as to the accuracy, completeness or adequacy of any information contained herein. Additionally, this material does not address all potential risks and may contain time-sensitive information. Vantage is under no obligation, and expressly disclaims any obligation, to update or revise this material. This material may not be reproduced or distributed without the express, written permission of Vantage Group Holdings Ltd.