Defining and Pricing Systemic Cyber Events

By Jeff Sergio

Abstract

The cyber insurance market has a unique problem. Compared to other lines of insurance, cyber lacks the historical claims data that underscores the modeling and pricing of policies. As a result, cyber faces a challenge in defining systemic events. The significance of this issue is heightened in the context of the Russia-Ukraine conflict and the rise of first-party cyberattacks. This white paper examines the perspectives presented by primary insurers Beazley and Zurich about the feasibility of covering systemic cyber events. By comparing these viewpoints, this paper aims to identify strategies for accurately classifying and pricing such incidents. Additionally, this paper analyzes the intersection between cyber warfare and systemic cyber in the context of the Russia-Ukraine conflict, while also examining the role of reinsurers in shaping the future of systemic cyber.

Recent History of Cyber

Cyber is a relatively new line of business that only recently came to the attention of insurers. Risks were rarely ever explicitly insured before the 2010s. Instead, cyber risks were implicitly covered via “silent” cyber coverage. If an insured suffered losses due to a cyber event - whether through an intentional cyberattack or by accident - they could justify filing claims under their property or casualty policies. These P&C policies typically did not factor cyber risks into their pricing, leading to unexpected claims for the insurer and conflicts over unclear wording. This non-affirmative or “silent” cyber came into the spotlight following a spate of costly cyberattacks in the late 2010s, including WannaCry, NotPetya, and the Equifax data breach. In the aftermath of the NotPetya ransomware attack in 2017, the American pharmaceutical giant Merck claimed cyber

losses on its traditional property insurance policies. Unclear wording meant that Merck, alongside other NotPetya victims such as Mondelez International, could reasonably claim insurance as "damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of machine code or instruction" had occurred in the form of computers rendered unusable by the virus.[1] NotPetya sparked discussion about the changes necessary to cyber coverage in traditional insurance policies.

Throughout the 2010s, growing cyber risks prompted insurers to change how they covered cyber risks. The shift forced insurers to either factor cyber into traditional policy pricing or to price standalone cyber policies entirely. In July 2019, Lloyd's mandated that all insurance and reinsurance underwriters in the London market explicitly include or exclude cyber coverage in their property and casualty policies. Other global insurance regulating bodies followed suit.[2] These rulings signaled a departure from silent cyber and a shift towards expressly written cyber. According to A.M. Best, standalone cyber policies accounted for 70% of cyber premiums as of 2022.[3] The rest consists of insurers that chose to fold cyber coverage into their traditional policies with revised wording to minimize the risk of silent cyber. By explicitly including cyber coverage in traditional P&C policies or writing exclusive cyber policies entirely, the silent cyber mandates placed a new emphasis on accurately modeling and pricing cyber risks.

The COVID-19 pandemic combined with the Russia-Ukraine conflict sparked a rise in data breaches and ransomware, hardening and expanding the market for cyber insurance. The pandemic

---

[1] Burgess, Christopher. "Mondelez and Zurich's Notpetya Cyber-Attack Insurance Settlement Leaves behind No Legal Precedent." *CSO Online*, 3 Nov. 2022, www.csoonline.com/article/574013/mondelez-and-zurich-s-notpetya-cyber-attack-insurance-settlement-leaves-behind-no-legal-precedent.html.

[2] Gallin, Luke. "Lloyd's Details Phased Implementation of Silent Cyber Mandate - Reinsurance News." *Reinsurance News*, 30 Jan. 2020, www.reinsurancene.ws/lloyds-details-phased-implementation-of-silent-cyber-mandate/.

[3] Graham, Christopher, et al. "Best's Market Segment Report: First Hard Market Cycle in US Cyber Insurance Segment Brings Return to Profitability." *AM Best*, 13 June 2023, news.ambest.com/PR/PressContent.aspx?refnum=33449&altsrc=2.

shifted the workforce into a remote environment with few improvements to cybersecurity, giving cybercriminals the potential to conduct more impactful cyberattacks. Likewise, as will be discussed further in this paper, the Russia-Ukraine war saw the use of cyber warfare against Ukrainian businesses and government entities, which spread globally and caused further financial losses. These two incidents exploded demand for standalone cyber insurance policies, and insurers such as Chubb, Munich Re, Beazley, AXA, and AIG jumped on the opportunity. Direct written premiums from standalone cyber policies in the US market grew from $1.26 billion in 2019 to $5.07 billion in 2022. Existing cyber policies saw retention hikes and limit cuts to coincide with the hardening market. Rates skyrocketed, averaging a 26% quarterly increase in 2021.[4] The late 2010s and early 2020s hardened the cyber market dramatically, growing the business at an unprecedented rate.

Today, the cyber market has cooled slightly due to improvements in cybersecurity and a slower pace of rate increases. The hard market has pushed insurers to demand better cyber hygiene and greater commitments to cyber resilience from their clients.[5] As a result, clients have become more insurable, and prices have stabilized. Premiums only grew by 3.6% in the second quarter of 2023, and 40% of insurers reported an increase in capacity.[6] The slowdown has allowed actors in the cyber market to analyze growing pains and future challenges faced by the market. Of these many issues is systemic cyber, and how it may threaten or drive changes to the cyber insurance strategy.

---

[4] Auden, James B., et al. "US Cyber Insurers See Favorable Premium Growth, Results in 2023." *Fitch Ratings: Credit Ratings & Analysis for Financial Markets*, 13 Apr. 2023, www.fitchratings.com/research/insurance/us-cyber-insurers-see-favorable-premium-growth-results-in-2023-13-04-2023.

[5] Ibid.

[6] The Council of Insurance Agents & Brokers. "Commercial Property/Casualty Market Index Q2/2023." *CIAB,* 2023*, https://www.ciab.com/resources/q2-2023-p-c-market-survey/*

Systemic Events

Cyber insurers and reinsurers have sought to clarify the difference between systemic and non-systemic cyber events. Although a unilateral definition is currently lacking, systemic cyber risk is generally understood to have cascading effects that cause damage beyond that of the intended target. While a traditional cyberattack might only target one company or government entity, a systemic cyber event would have global consequences, potentially impairing the supply chain, state essential services, or the global internet infrastructure.[7] Nevertheless, the market has not reached a consensus definition, and many actors are navigating the issue of systemic cyber with the philosophy of "you'll know it when you see it."

Systemic cyber is perhaps best understood as a parallel to catastrophe events in the property insurance line. In property, catastrophe events are classified as comparably rare events that cause significantly more damage than a non-catastrophe event. Catastrophe events are modeled separately from attritional losses, and coverage is segregated into expressly designed catastrophe policies. When conceptualizing the difference between attritional and systemic cyber risk, this model is appealing for its familiarity and track record. However, the unique and limited history of cyber insurance complicates the previously understood model. Handling these complications is essential to the profitability of the cyber insurance market.

Firstly, cyber lacks historical claims data, which complicates the pricing and definition of policies. For comparison, property insurance is a line of business with decades of historical catastrophe data. Property underwriters and actuaries have tools to harness this data and regress models, painting a more accurate picture of how to price catastrophe coverage. This is a noticeable

[7] Forscey, David, et al. "Systemic Cyber Risk: A Primer - Carnegie Endowment for International Peace." *Carnegie Endowment for International Peace*, 7 Mar. 2022, carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531.

departure from the reality of cyber insurance, which has a shorter, less reliable history of catastrophes. Cyber insurers often use a host of indirect factors to price their products, such as market estimates of the costs of cyberattacks and questionnaires on the riskiness of the client.[8] This methodology creates a vicious cycle, where insurers and reinsurers feel uncomfortable pricing cyber risks, which creates no new reference points for historical cyber risks, which causes insurers to shy away even more. The lack of historical claims data for systemic cyber events underlies every possible attempt to get a handle on the industry.

Second, the lack of a consensus definition of systemic cyber risk complicates attempts to write insurance and reinsurance contracts. Catastrophe insurance contracts in property have agreed-upon and indisputable triggers. For example, a property CAT Bond might trigger if an earthquake has a certain magnitude, or a hurricane reaches a certain wind speed. Property insurers can use these measures to determine what counts as a catastrophe and what does not. Cyber insurers do not have the luxury of quantifiable, indisputible catastrophe triggers. Should a cyber catastrophe be defined by the number of organizations impacted? Or should the trigger be insured losses, regardless of how many systems the incident impacts? Where does cyber as a weapon of war fit in? Cyber insurers, reinsurers, and insured companies have competing ideas of what counts as a cyber catastrophe, and if private insurers alone can handle the issue.

Insufficient historical data combined with nonstandardized wording has molded different perspectives on the future of catastrophe cyber. This paper will examine two primary insurers, Beazley and Zurich, who have demonstrated different outlooks on the potential of systemic cyber insurance.

---

[8] Granato, Andrew, and Andy Polacek. "The Growth and Challenges of Cyber Insurance." *Chicago Fed Letter*, no. 426, Mar. 2019, https://doi.org/10.21033/cfl-2019-426.

Case Study 1: Beazley

In January 2023, Lloyd's insurer Beazley made headlines for introducing an unprecedented cyber CAT bond. The bond triggers when total claims from cyberattacks on its clients exceed $300 million, in which case the $45 million bond will pay out to Beazley. That July, Beazley added another $20 million to the bond's payout, effectively providing the insurer with $65 million in reinsurance against systemic cyber events. The bond, expressly designed to cover "remote probability catastrophic and systemic events", demonstrates the growing divide between an attritional component and a catastrophe component of cyber insurance.[9] Moreover, it represents the increasing comfort level cyber insurers claim to possess in dealing with systemic cyber events.

The attachment point of the Beazley CAT bond is $300 million, which is a level of catastrophic damage that only a few individual firms have reached from a cyber event. Merck, which suffered among the most from the 2017 NotPetya attack, lost an estimated $870 million. The Danish shipping giant Maersk lost between $200 and $300 million.[10] Given the rising frequency and severity of cyberattacks, future catastrophic events might reach this attachment point more easily.

Beazley defines a catastrophic cyber event as having one of two characteristics, or both. According to the firm, the two scenarios that define a catastrophic cyber event are:

1) An outage of a major cloud service provider that exceeds 72 hours

2) A contagion malware in a Computer Operating System causing major detrimental impact to a state's essential services[11]

---

[9] Beazley Group. "Leaders Need to Lead on Catastrophic Cyber." *Beazley*, 13 Jan. 2023, www.beazley.com/en-us/articles/leaders-need-lead-catastrophic-cyber.

[10] Greenberg, Andy. "The Untold Story of Notpetya, the Most Devastating Cyberattack in History." *Wired*, Conde Nast, 22 Aug. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[11] Beazley Group. "Leaders Need to Lead on Catastrophic Cyber."

The wording of these characteristics is noticeably vague, which may open the insurer up to future disputes in the event of claims. Terms like “major cloud service provider” and “major detrimental impact” have unclear thresholds that are left open to interpretation. At their worst, these ambiguities open insurers up to litigation, as was the case with Merck and Mondelez. However, attempting more specificity is difficult due to the aforementioned lack of historical data in the cyber insurance market.

Nevertheless, Beazley’s second criterion for a catastrophic cyber event is relevant in the context of cyber war. This paper will further analyze the relationship between systemic cyber and war, as the current understanding of systemic cyber risk is very much born from cyberattacks in the Russia-Ukraine conflict. Cyber as a weapon of war is responsible for detrimental losses to governments and private businesses in combatant and non-combatant countries, accounting for some of the largest financila losses in cyber history. As such, no definition of catastrophic cyber is complete without a thorough understanding of cyber war.

Beazley remains steadfast that systemic cyber is a problem the insurance industry can overcome with proper underwriting guidelines. This viewpoint is not shared by all firms in the industry, and others believe that cyber risks will grow to the point where profitability is unattainable.

Case Study 2: Zurich

In the wake of the 2017 NotPetya attacks, the food and beverage giant Mondelez International filed a claim worth over $100 million on its policy with Zurich Insurance Group. Mondelez suffered business interruption losses, stolen credentials, and over 24,000 computers permanently locked by the ransomware. Although Mondelez did not have a standalone cyber policy, the company invoked silent cyber and claimed that its property policy with Zurich should

cover cyberattacks. Zurich denied this claim citing a war exclusion, leading to a lawsuit that lasted five years before settling privately.[12]

While the decision of the Zurich-Mondelez suit remains undisclosed, similar cases have possibly established a precedent for cyber catastrophes that does not favor insurers. Merck also filed a $1.4 billion lawsuit against its insurers for a disputed war exclusion clause with NotPetya. Unlike the Zurich case, however, the courts publicly sided with Merck, leaving insurers on the hook.[13] The Merck case further pushed the catastrophic cyber issue away from being insurer-friendly and could be a precedent-setting decision for how litigation will handle systemic cyber incidents.

In the wake of this decision, the CEO of Zurich, Mario Greco, warned that systemic cyber events will become "uninsurable" as the frequency of cyberattacks rise. According to Greco, interconnectedness would create cyber risks too massive to quantify, let alone insure comfortably by the private insurance industry alone. Those that agree with this perspective have an array of foreboding evidence to draw upon. The ongoing MOVEit breach, currently the largest cyberattack of 2023, has already topped the cost of NotPetya according to estimates.[14] The cyber insurance market is expected to harden again, demanding more capacity from insurers, increasing reliance on reinsurers, and introducing more alternative sources of capital into the market to meet demand. The cooldown of the cyber market is only temporary, and as catastrophic events become more frequent and costly, insurers might find themselves with unbearable loss ratios year after year.

---

[12] Adriano, Lyle. "Zurich, Mondelez Settle Longstanding Lawsuit over $100 Million Claim." *Insurance Business America*, Insurance Business, 8 Nov. 2022, www.insurancebusinessmag.com/us/news/cyber/zurich-mondelez-settle-longstanding-lawsuit-over-100-million-claim-426741.aspx.

[13] Vanderford, Richard. "Merck's Insurers on the Hook in $1.4 Billion Notpetya Attack, Court Says." *The Wall Street Journal*, Dow Jones & Company, 2 May 2023, www.wsj.com/articles/mercks-insurers-on-the-hook-in-1-4-billion-notpetya-attack-court-says-528aeb01.

[14] Page, Carly. "Moveit, the Biggest Hack of the Year, by the Numbers." *TechCrunch*, 25 Aug. 2023, techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/.

If Beazley represents the aggressive and optimistic vision of insuring cyber catastrophes, then the perspective of Zurich and its CEO represents a more cautious, even pessimistic take. The divide between these two example firms is indicative of the larger debate sparked by systemic cyber risk. Insurers like Beazley see systemic cyber as a problem that insurers can overcome with disciplined underwriting and scrutinized contract wording. Others have concerns for the long-term longevity of the cyber insurance business fueled by the threat of systemic cyber.

Cyber War and Systemic Cyber

The Russia-Ukraine conflict has catalyzed a new wave of first-party cyberattacks. Russian-speaking hacker groups have executed malicious attacks on Ukrainian businesses and state services, some with disastrous consequences. The most notable example is the 2017 NotPetya attack, of which 80% of the victims were Ukrainian. Among the affected entities were the Chornobyl nuclear power plant, Ukraine's largest international airport, the national postal service, and the state telecom provider.[15] Further disruption occurred after NotPetya spread beyond Ukraine's borders, to companies like Merck, Mondelez, Maersk, and FedEx.

The intersection between cyber warfare and systemic cyber comes into focus in the context of NotPetya and the Russia-Ukraine war. Cyber warfare intends to damage critical infrastructure, inflicting cascading damage that compromises the target government. In other words, cyber warfare causes a major detrimental impact to a state's essential services - the very definition of a catastrophic cyber event as worded by Beazley. Systemic cyber can be a result or intention of cyber warfare when the disabling of businesses or essential state services aligns with strategic war objectives.

---

[15] Dearden, Lizzie. "Ukraine Cyber Attack: Chaos as National Bank, State Power Provider and Airport Hit by Hackers." *The Independent*, Independent Digital News and Media, 27 June 2017, www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html.

A question that arises in the relationship between cyber warfare and systemic cyber is where to draw the line between them. For example, Ukrtelecom, the state telecom provider impacted in the NotPetya attack, was targeted by DDoS hacks on February 10 and March 28, 2022, collapsing data connectivity to 13% of pre-war levels.[16] Given that this attack caused a protracted outage of an essential service, should the Ukrtelecom attack be considered a catastrophic cyber incident on its own? Or, should this hack be agglomerated with other attacks and considered as one under the umbrella of the Russia-Ukraine war? Questions such as these have aroused conversation of cyber war exclusions, in an explicit attempt to decouple cyber warfare from insurer liability.

The fear of a cyber war attack spiraling into a systemic cyber incident has given rise to cyber war exclusions. Regulating agencies have proposed frameworks to exclude warlike actions from cyber policies. In December 2021, Lloyd's published a set of exclusions for war, cyber war, and cyber operations expressly intended for standalone cyber policies. Lloyd's followed this with a bulletin in August 2022 that required all standalone cyberattack policies to "exclude coverage for specific losses related to state-backed cyberattacks, and include new exclusions that address cyberattack losses outside the traditional 'acts of war' exclusions".[17] Such rulings have proved controversial, with critics pointing out the occasionally ambiguous terms used in the definition and an unsatisfactory decision on what counts as a warlike act. CyberAcuView, a collaborative entity established between leading cyber insurers, has even put forward an alternate wording that claims to add standardization and clarity to the LMA wording. The challenge of wording cyber

[16] Condon, Stephanie. "'Massive Cyberattack' against Ukrainian ISP Has Been Neutralized, Ukraine Says." *ZDNET*, 28 Mar. 2022, www.zdnet.com/article/massive-cyberattack-against-ukrainian-isp-has-been-neutralized-ukraine-says/.

[17] He, Philip, and Eric M Gold. "Lloyd's of London Requires Insurers to Add Exclusions to Limit Coverage for State-Backed Cyberattacks." *Policyholder Pulse*, 9 May 2023, www.policyholderpulse.com/lloyds-london-state-backed-cyberattacks/.

exclusions is worth an entire study of its own. But in the context of systemic cyber, the threat of a systemic cyber attack is the source of urgency in creating clear cyber war exclusions.

Reinsurance and Systemic Cyber

Reinsurers have already played a critical role in the cyber market, and their relevance will only grow as the threat of systemic cyber continues. Reinsurance is necessary to help the primary industry grow and wrangle increasing exposures, but traditional reinsurers have exercised caution in underwriting standalone cyber policy. Direct loss ratios for standalone cyber policies reached 72.5 in 2020, and while the industrywide ratio has since fallen to 42.9 in 2022, reinsurers are still wary of primary underwriters' ability to price cyber risk.[18] At the same time, demand for reinsurance has grown, driven by the increase in ransomware attacks and forecasts of a future hard market. The supply for reinsurance no longer meets the increasing demand, and the onus is on insurers to further improve the hygiene of their cyber books to bring back traditional reinsurers.

Systemic cyber risk opened a hole in the market that collateralized reinsurance has attempted to fill. Due to the massive capacity that cyber catastrophes demand, reinsurers may need to tap into non-traditional markets to increase capacity. The insurance-linked securities market, or ILS, has presented itself as an option. The Beazley cyber CAT bond was backed by a panel of ILS investors, and in January 2023, Hannover Re announced a cyber retrocession deal worth $100 million with a capital market investor.[19] Non-traditional investors can help optimistic firms obtain vital reinsurance or retrocession cover when traditional reinsurance is hesitant or lacking capacity. However, capital markets investment may carry a higher risk than traditional risk transfers. An unprecedented systemic cyberattack could scare away ILS investors and dry up the capital needed

[18] Auden, "US Cyber Insurers See Favorable Premium Growth, Results in 2023."
[19] Gallin, Luke. "Hannover Re and Stone Ridge in $100m Retrocession Cyber Quota Share." *Reinsurance News*, 19 Jan. 2023, www.reinsurancene.ws/hannover-re-and-stone-ridge-in-100m-retrocession-cyber-quota-share/.

to fund cyber catastrophe coverage.[20] Monitoring the role of non-traditional investors in the systemic cyber strategy is therefore essential for reinsurers moving forward.

Reinsurance has been considerably responsible for the growth of the cyber insurance market in the last five years. The share of business ceded to reinsurers has jumped from 45% to 55% in a matter of years, and insurers will only require more protection as cyber books and risks grow. However, the looming threat of systemic cyber means that more reinsurance doesn't always create a safer market. In places where traditional reinsurers are hesitant or lack more coverage to give, the capital markets have offered an alternative that more insurers are picking up. The success of these ventures depends on if catastrophic cyber materializes and pushes investment away.

Conclusions

How do we define and price systemic cyber risk? Optimists may suggest that the exposure history of catastrophic cyber events has grown large enough for insurers to tackle the issue and turn a profit. The market is beginning to see this with the Beazley CAT bond and the uptick of ILS investors into reinsurance and retrocession contracts. More cautious actors suggest that further investment into cybersecurity is necessary to create insurable clients, after which the market will mature. Others may suggest that we haven't experienced a cyber catastrophe at all, or at least not one at its full potential. Despite all the attention awarded to systemic cyber, uncertainty lingers regarding the extent of its potential impact and the capability of insurers to handle it. However, the insurance and reinsurance markets can take away insights on how to navigate systemic cyber risk.

Firstly, the surge of litigation following major cyber events highlights the importance of unambiguous contract wording. Insurers and reinsurers must consider what elements of the cyber market can and cannot be modeled and covered, and make those decisions exceedingly clear in

[20] Evans, Steve. "Cyber Catastrophe Could Deter ILS Investors: Conning." *Artemis*, 14 July 2023, www.artemis.bm/news/cyber-catastrophe-could-deter-ils-investors-conning/.

their contract wording. Insurers must also avoid writing silent cyber into their traditional policies by analyzing their existing contracts to account for unintended cyber exposure. Silent cyber cases such as the Merck and Mondelez lawsuits should serve as warning signs for the industry to manage contract wording with greater scrutiny.

Second, traditional reinsurers should be patient in taking on catastrophe cyber until primary insurers and the insured improve their cyber resilience. Until more historical data enters risk models, more time is needed to determine the best loss ratios, tail lengths, and pricing to offer to reinsurers. As well, insured firms must take further steps to invest in cybersecurity and understand cyber risks. While alternative sources of reinsurance capital have entered the market, traditional reinsurers will remain a vital piece of the systemic cyber puzzle. Therefore, reinsurers should not overextend themselves, and instead observe how the cyber market develops in the coming years.

Lastly, the insurance market should prioritize collaboration to improve the shared understanding of systemic cyber risk. The lack of consensus at every level of the market poses challenges that no business can overcome alone. Cooperation between insurers, reinsurers, clients, and cybersecurity experts can remedy these issues and mature the market. The success of CyberAcuView in creating cyber war exclusions shows the benefits of cooperation, where experts from competing primary insurers come together to promote unity in approaching cyber risks. Collaboration, where appropriate, can help unify the cyber market under a common strategy to approach systemic cyber, providing resilience for the future.

Works Cited

Adriano, Lyle. "Zurich, Mondelez Settle Longstanding Lawsuit over $100 Million Claim." *Insurance Business America*, Insurance Business, 8 Nov. 2022, www.insurancebusinessmag.com/us/news/cyber/zurich-mondelez-settle-longstanding-lawsuit-over-100-million-claim-426741.aspx.

Auden, James B., et al. "US Cyber Insurers See Favorable Premium Growth, Results in 2023." *Fitch Ratings: Credit Ratings & Analysis for Financial Markets*, 13 Apr. 2023,

www.fitchratings.com/research/insurance/us-cyber-insurers-see-favorable-premium-growth-results-in-2023-13-04-2023.

Beazley Group. "Leaders Need to Lead on Catastrophic Cyber." *Beazley*, 13 Jan. 2023, www.beazley.com/en-us/articles/leaders-need-lead-catastrophic-cyber.

Burgess, Christopher. "Mondelez and Zurich's Notpetya Cyber-Attack Insurance Settlement Leaves behind No Legal Precedent." *CSO Online*, Foundry, 3 Nov. 2022, www.csoonline.com/article/574013/mondelez-and-zurich-s-notpetya-cyber-attack-insurance-settlement-leaves-behind-no-legal-precedent.html.

Condon, Stephanie. "'Massive Cyberattack' against Ukrainian ISP Has Been Neutralized, Ukraine Says." *ZDNET*, 28 Mar. 2022, www.zdnet.com/article/massive-cyberattack-against-ukrainian-isp-has-been-neutralized-ukraine-says/.

Dearden, Lizzie. "Ukraine Cyber Attack: Chaos as National Bank, State Power Provider and Airport Hit by Hackers." *The Independent*, Independent Digital News and Media, 27 June 2017, www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html.

Evans, Steve. "Cyber Catastrophe Could Deter ILS Investors: Conning." *Artemis*, 14 July 2023, www.artemis.bm/news/cyber-catastrophe-could-deter-ils-investors-conning/.

Forscey, David, et al. "Systemic Cyber Risk: A Primer - Carnegie Endowment for International Peace." *Carnegie Endowment for International Peace*, 7 Mar. 2022, carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531.

Gallin, Luke. "Hannover Re and Stone Ridge in $100m Retrocession Cyber Quota Share." *Reinsurance News*, 19 Jan. 2023, www.reinsurancene.ws/hannover-re-and-stone-ridge-in-100m-retrocession-cyber-quota-share/.

Gallin, Luke. "Lloyd's Details Phased Implementation of Silent Cyber Mandate - Reinsurance News." *Reinsurance News*, 30 Jan. 2020, www.reinsurancene.ws/lloyds-details-phased-implementation-of-silent-cyber-mandate/.

Graham, Christopher, et al. "Best's Market Segment Report: First Hard Market Cycle in US Cyber Insurance Segment Brings Return to Profitability." *AM Best*, 13 June 2023, news.ambest.com/PR/PressContent.aspx?refnum=33449&altsrc=2.

Granato, Andrew, and Andy Polacek. "The Growth and Challenges of Cyber Insurance." *Chicago Fed Letter*, no. 426, Mar. 2019, https://doi.org/10.21033/cfl-2019-426.

Greenberg, Andy. "The Untold Story of Notpetya, the Most Devastating Cyberattack in History." *Wired*, Conde Nast, 22 Aug. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

He, Philip, and Eric M Gold. "Lloyd's of London Requires Insurers to Add Exclusions to Limit Coverage for State-Backed Cyberattacks." *Policyholder Pulse*, 9 May 2023, www.policyholderpulse.com/lloyds-london-state-backed-cyberattacks/.

Johansmeyer, Tim. "The Cyber Insurance Market Needs More Money." *Harvard Business Review*, 10 Mar. 2022, hbr.org/2022/03/the-cyber-insurance-market-needs-more-money.

Page, Carly. “Moveit, the Biggest Hack of the Year, by the Numbers.” *TechCrunch*, 25 Aug. 2023, techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/.

The Council of Insurance Agents & Brokers. “Commercial Property/Casualty Market Index Q2/2023.” *CIAB,* 2023*, https://www.ciab.com/resources/q2-2023-p-c-market-survey/*

Vanderford, Richard. “Merck’s Insurers on the Hook in $1.4 Billion Notpetya Attack, Court Says.” *The Wall Street Journal*, Dow Jones & Company, 2 May 2023, www.wsj.com/articles/mercks-insurers-on-the-hook-in-1-4-billion-notpetya-attack-court-says-528aeb01.