CyberCube's Global Threat Outlook

A perspective on the threat landscape for Q4 2023

CyberCube

The cyber insurance market is stabilizing, with premium increases slowing. Sectors including professional services and healthcare face increased attacks, and nation-state cyber activities are expected to impact war exclusion language. Striving for consistency and clarity across cyber (re)insurance products is crucial to the industry's sustainability.

This Global Threat Briefing has been prepared as part of CyberCube's Concierge offering, our threat intelligence service tailored specifically for the broking and cyber (re)insurance market. It highlights some of CyberCube's perspectives on the nation-state cyber threat landscape and how we have incorporated different threat actors' activities into our model to enable world-class risk aggregation analytics.

Key findings of this report include:

- Cyber (re)insurers can look to moderate/low-risk sectors for underwriting opportunities in the fourth quarter of 2023. The combination of CyberCube's Exposure and Security Scores paints a clear picture of industry-level differentiated cyber risk opportunities, and sectors to scrutinize. The highest-risk sectors to keep an eye on in Q4 include *Professional Services* and *Healthcare*. These sectors are under-secured and make attractive targets, with high levels of sensitive data leaving companies vulnerable to ransomware and extortion tactics.

- Nation-state cyber hot zones offer a glimpse into the potential future of cyber war. CyberCube has conducted an analysis of state-nexus cyber threat actors including those in Russia, China, Iran, and North Korea. (Re)insurers can model realistic cyber disasters considering recent state-nexus cyber activities using CyberCube's Portfolio Manager.

- In Q4 2023, CyberCube expects to see nation-state cyber threat actors conduct themselves in ways that push the cyber (re)insurance industry to consider deeply the limitations and strengths of current war-exclusion language.

Expect continued cyber market stabilization in Q4

The cyber (re)insurance market has been showing signs of stabilization throughout the first half of 2023, with premiums beginning to settle. According to The Council of Insurance Agents & Brokers' Commercial Property/Casualty Market Report for Q1 2023 (January 1 – March 31), increases for cyber insurance premiums slowed in Q1 2023. The average premium increase was 8.4% in Q1 this year, compared with 15% in the previous quarter and more than 20% a year ago. CyberCube expects this to continue through the end of the year.

Carriers are expected to continue focusing on insureds' implementation of basic cyber risk management measures such as multi-factor authentication (MFA) and measuring good cyber hygiene over time. CyberCube expects insurers to continue refusing outright to underwrite or provide quotations for accounts deemed to have inadequate cybersecurity. At the same time, brokers will be building momentum this year, taking a more proactive approach, educating clients on cyber risk preparedness, and requesting more information earlier in the renewal process.

Certain sectors are under the spotlight. In Q1 2023, there was a 57% increase in attacks on professional services firms compared with the last quarter of 2022. This was driven by ransomware and extortion activity, particularly against legal firms. Incident response company Kroll, which partners with CyberCube to offer cyber threat intelligence, has identified an ongoing search engine optimization poisoning campaign against small and medium-sized law firms, with lawyers being convinced to download templates laden with malware. CyberCube expects threat actors to continue focusing on small and medium-sized targets in sectors with sensitive data, including law firms. (Re)insurers should also be on the lookout for similar-sized professional services firms that require extra diligence and care, due to the sensitive client information they hold.

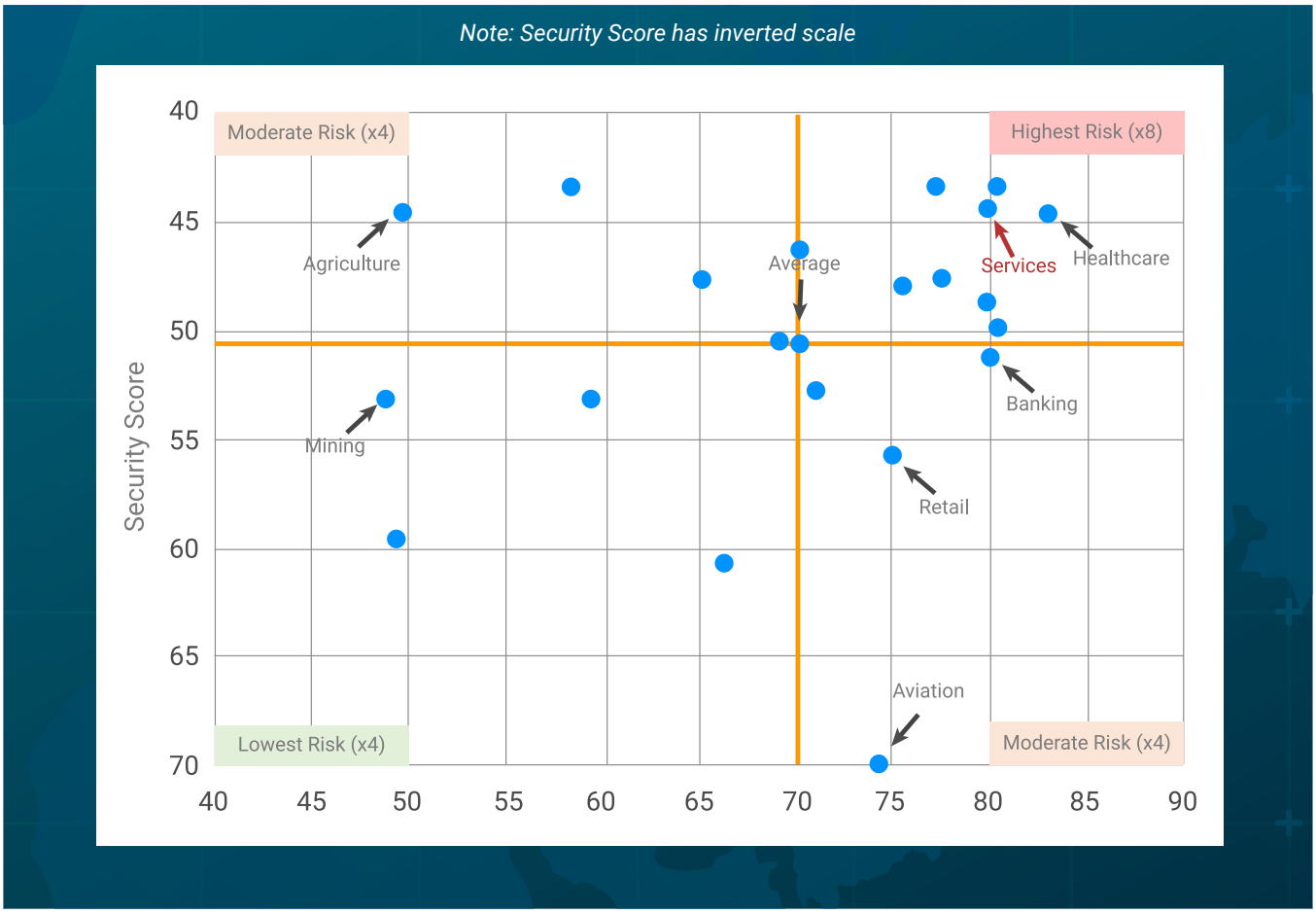
Ransomware and extortion gangs are expected to continue a relentless targeting of the manufacturing and technology/telecoms sectors. Retail/restaurants and financial services are also expected to be in the crosshairs at the end of 2023.

CyberCube's ***Security Score*** can help identify industry sectors with more cyber risk than others, as well as sectors that present opportunities for (re)insurers. The Security Score measures a single company's ability to satisfy the core elements of the National Institute of Standards and Technology (NIST) cyber security framework.

CyberCube can aggregate scores amongst companies in different industries and by sizes. **Exhibit 1** shows a representation of medium-sized companies in the U.S. ($250 million to $1 billion of revenue) that also have cyber insurance. Medium-sized professional services rank among industries with the lowest security scores. For that reason, they are also underprepared in the face of their inherent exposure and increased targeting by threat actors. CyberCube expects more attacks in this sector during the remainder of 2023.

Exhibit 1

Average Industry Exposure vs Security Score - Medium Compaines, United States (June 2023)



Source(s): CyberCube Account Manager (v4.7), Industry Exposure Database

CyberCube's ***Exposure Score*** measures companies' inherent exposure to cyber threats. The Exposure Score accounts for the value of sensitive data inherent to each industry that could make it an attractive target for cyber threat actors. It measures the extent to which some industries have more endpoints exposed to the internet, as well as other indicators. Businesses that are inherently highly exposed to cyber threats should have security in line with that exposure to protect themselves.

When both ***Security Scores*** and ***Exposure Scores*** are placed in the matrix highlighted in **Exhibit 1**, the highest-risk industries are highlighted in the upper right quadrant. These sectors are highly exposed, attractive targets for threat actors, but also under-secured relative to the threats they face.

The average industry Exposure Score for medium-sized companies in the U.S. in June 2023, shows 12 highly exposed industries. Five are medium, and three are low exposure. As highlighted in CyberCube's last Global Threat Report H1 2023, Healthcare remains the most exposed industry sector, followed by Professional Services.

Sectors such as Banking and Retail are still targeted and represent a more moderate risk, but exercise better cyber security, while Aviation is highly exposed, but also relatively secure. Aviation, Public, Oil and Gas, Marine, Energy, Utilities, and Banking all fall into the High Security category, but are highly-regulated industries. For example, in some cases, the FBI and CISA can enter the networks of critical infrastructure organizations and make changes to defend them more proactively. Mining and Agriculture can represent opportunities for cyber (re)insurers as they are inherently less exposed than other industry sectors.

CyberCube's U.S. Cyber Exposure Databases

These analyses are made possible by CyberCube's U.S. Cyber Exposure Databases - the first, industry-backed, U.S. cyber exposure data sets. The Economic Exposure Database (EED) comprises detailed exposure information on a representative sample of over 200,000 U.S. companies exposed to cyber threats. The Industry Exposure Database (IED) is a statistical representation of all companies across the U.S. market expected to have cyber insurance today. The databases are designed and calibrated to work seamlessly with CyberCube's catastrophe and attritional loss models to produce an Industry Loss Curve (ILC), which represents the potential range of losses that could result from cyber incidents. Configurable settings allow users to run custom analyses against the IED and/or EED, just as with any other portfolio.

Reinsurers can use these databases to understand cyber risk from different workflows, such as benchmarking company exposures against the industry, assessing real time losses as cyber incidents occur, validating models, creating industry loss curves, creating pro-forma portfolios and results. The databases also build support for cyber ILS transactions by broadening the structures available to the ILS market, including ILWs and allowing stakeholders to review and validate structures in a familiar way.

Nation-state cyber hot zones offer a view into the future of cyber war

CyberCube monitors selected nation-state cyber hot zones to gain insight into the potential cyber (re) insurance impacts of future cyber wars and whether there are indications that the boundaries of acceptable behavior in cyberspace have been pushed beyond historic precedent. The (re)insurance industry should note evidence of cyber attacks bridging the divide between digital and physical impacts. The nation-state cyber hot zones analyzed include Russia vs. Ukraine, China vs. Taiwan, Iran vs. Israel, and North Korea vs. South Korea.

Russia vs. Ukraine: persistent intelligence gathering and destruction expected in Q4 2023

CrowdStrike has identified Russian activities in the war, including intelligence gathering and information operations that influence public opinion, as well as destructive malware attacks. The start of the war (Q1'22) was marked by a high volume of attacks including unprecedented use of destructive malware. More destructive malware was used in Q1'22 than in the previous eight years combined. These destructive tactics made a comeback in Q'22 and are expected to continue in 2023, as Russia becomes more desperate. For that reason, reinsurers should model the potential impacts of widespread destructive wiper malware disasters.

CyberCube's point of view

(Re)Insurers and cyber risk modelers can use CyberCube's Portfolio Manager solution to assess the financial loss impact of catastrophic destructive malware events. This includes the targeted use of destructive malware against major cloud service providers causing widespread outages and impacting the cloud providers' customers. The destructive malware event family also includes attacks on endpoint and server operating systems globally, based on the infamous global NotPetya wiper malware attack of 2017. Today, CyberCube customers can model the impacts of widespread destructive malware attacks that could target both servers and endpoints simultaneously.

China vs. Taiwan: preparing to degrade critical internet and telecommunications assets

China remains a highly active threat actor on the global stage, consistently engaging in a range of cyber activities. Notably, China-nexus adversaries were observed targeting nearly all of the 39 global industry sectors and 20 geographic regions that CrowdStrike Intelligence tracks.

Throughout 2022 and into 2023, CrowdStrike identified instances where adversaries with ties to China directed their efforts at Taiwanese technology firms. This aligns with their probable objective of economic espionage, serving China's ambitions for technological self-reliance and supremacy. Moving forward, CyberCube anticipates a shift towards more forceful and destabilizing cyber campaigns by China-nexus threat actors, targeting both Taiwanese and U.S. entities.

In June 2023, Microsoft discovered targeted malicious activity by Volt Typhoon, a Chinese state-sponsored threat actor, aimed at U.S. critical infrastructure. The campaign focused on post-compromise credential access and network system discovery, with the potential to disrupt critical telecommunications infrastructure in future crises.

It is widely believed that Chinese threat actors are intending to disrupt critical internet and communications infrastructure in the event of an invasion of Taiwan and that the U.S. would offer assistance. CyberCube expects telecommunications and internet infrastructure (especially U.S. infrastructure) could be targeted in the event of a full-scale Chinese invasion of Taiwan.

CyberCube's point of view

(Re)insurers and cyber risk modelers can use CyberCube's Portfolio Manager to assess the impact on their portfolios of cyber attacks on critical communications and internet infrastructure Single Points of Failure (SPoFs). These include attacks on traditional communications infrastructure such as mobile network operators and internet service providers. The scenarios also include attacks on SPoFs that are core internet backbone infrastructure such as certificate authorities (CA). The compromise of CA SPoFs could result in widespread internet downtime and inaccessibility of online communications applications. The cascading impacts of one of those technologies going down could have a catastrophic impact.

Iran vs. Israel: attacks on operational technology with the potential for physical impact

Iranian threat actors are seeking to enhance their cyber capabilities to achieve proportional retaliation after attacks - and to achieve regional objectives in line with the regime's goals. Unsurprisingly, Iran is primarily targeting adversaries regionally, with a focus on Israel, but is also focusing on other countries, including the UAE and Saudi Arabia. Iranian threat actors have also been observed engaging in malicious cyber operations targeting a range of government and private-sector organizations across a range of sectors in Asia, Africa, Europe, and North America. The potential for destructive Iranian attacks remains a threat. Iranian threat groups are seeking

to attack operational technology - technology that specifically controls the physical operations of machinery, often in critical infrastructure, manufacturing and heavy industry environments.
In early April, Microsoft observed Iranian-linked threat actors targeting the water controllers of at least ten Israeli farms and replacing images on their programmable logic controllers with the message “Down with Israel”. This is considered an attack on critical infrastructure, potentially impacting water, farming, and the food supply chain. The attacks directly targeted the operational technology that enables farming machinery to function. These types of attacks are likely to increase and the potential for physical impact is escalating.

CyberCube’s point of view

(Re)Insurers and cyber risk modelers can use CyberCube’s Portfolio Manager to assess the impact on their portfolios of cyber attacks on operational technology SPoFs. These are all categorized in the physical damage impact family, and model disasters such as attacks on oil rigs, aircraft weaponization, and destructive malware against maritime vessels causing them to capsize. These SPoFs include technologies that are central to the operations of physical infrastructure such as critical energy, transportation, and logistics machinery uptime. For example, a supply chain attack on an oil refinery’s supervisory control and data acquisition systems (SCADA) could lead to downtime and energy supply disruptions, with myriad consequences for millions of downstream oil and gas consumers.

N. Korea vs. S. Korea: attacks on governments and theft from money systems

According to data from Recorded Future, North Korea’s cyber operations have a significant global reach. However, it is evident that the country’s primary focus remains on its longstanding adversaries, namely South Korea and the United States.

For years, North Korea has been known to engage in diverse illicit financial activities to generate funds for its regime. This conflict is primarily characterized by the North Koreans attacking government targets for espionage purposes and then targeting money systems to fund the regime in the face of sanctions.

The recent surge in the popularity and adoption of cryptocurrencies has created an opportune intersection with North Korea's aggressive and adaptable cyber capabilities. This is primarily taking the form of attacks on cryptocurrency exchanges. However, highly anticipated regulations focused on know-your-customer (KYC) and anti-money laundering could make it harder for threat actors to conceal their identities at exchanges and to launder the proceeds from these illicit activities. Should these regulations come into force, North Korea, in particular, is likely to reorient its cyber threat activity away from crypto and back toward the traditional money system.

CyberCube's point of view

(Re)Insurers and cyber risk modelers should look at different disasters that include money systems SPoFs. They can use CyberCube's Portfolio Manager to assess the impact of cyber attacks on critical money system SPoFs on their portfolios. These attacks include attacks on leading financial transaction providers such as the SWIFT banking system (a target the North Koreans have successfully breached in previous attacks), as well as attacks against leading outsourced payroll providers, online banking services, mobile point-of-sale systems and e-commerce platforms.

These attacks can result in cash theft, as well as data theft leading to fraud and identity theft losses. Large banks in a portfolio could see losses due to costs associated with issuing new credit cards, and identity protections.

Key nation-state takeaways

- **Russian state-nexus cyber threat actors are expected to engage in more destructive attacks in H2 2023.**
- **China state-nexus cyber threat actors will continue to target critical internet and telecommunications infrastructure.**
- **The cyber conflict between Iran and Israel offers a look into the future of attacks targeting operational technology with the potential for physical damages.**
- **Highly-anticipated cryptocurrency regulations could prompt North Korea to re-engage in targeting the traditional money system.**
- **CyberCube's Portfolio Manager can help (re)insurers model realistic cyber disasters considering recent state-nexus cyber activities.**

CyberCube's 2023 cyber threat outlook

CyberCube expects nation-state cyber threat activity will push the boundaries of war exclusion language. While there has been substantial progress and momentum achieved this year, including, in March, Lloyd's of London rolling out an exclusion for cyber war and severe state-backed attacks, the reinsurance market is yet to settle on a consistent approach that is acceptable to all stakeholders.

The approaches currently being adopted carry significant uncertainty, mainly due to the complexities surrounding the attribution of cyber incidents and the scarcity of historical parallels. By striving for consistency and clarity, we can bolster confidence in the cyber reinsurance sector, shielding it from the impact of outlier events, while reinforcing the overall value of cyber insurance products.

It is widely acknowledged that tackling systemic risks that could endanger the market is crucial. Considering the distinctive nature of systemic losses and geopolitical events, governmental bodies will have a substantial influence on the market's future trajectory.

Author

William Altman, Cyber Threat Intelligence Principal

Editorial Content

Yvette Essen, Head of Content, Communications & Creative

Designer

Muhammad Ahmad, Graphic Designer

www.cybcube.com