CyberCube's Global Threat Outlook

H1 2024

CyberCube

The cyber insurance market is witnessing a surge in capacity and competition, leading to a decrease in premium rate hikes. The Healthcare and Public sectors face escalating attacks, while nation-state cyber activities are anticipated to affect critical infrastructure.

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

Key findings of this report include:

- The ongoing decline in cyber premium pricing can be partly attributed to increased competition and additional capacity entering the market in 2023. Healthcare is the most Exposed industry tracked by CyberCube. The (re)insurance community should be aware of potential widespread cyberattacks that impact healthcare provider systems in 2024. The Public sector is under-secured relative to the advanced threats it faces in 2024. Attacks that impact state and local governments during the 2024 US presidential election are expected.

- Recent nation-state cyber threat activity offers a glimpse into the potential future of cyber catastrophes. CyberCube has conducted an analysis of state-nexus cyber threat actors, including those in Russia, Iran, and China. (Re)insurers can model realistic cyber disasters considering state-nexus cyber activities using CyberCube's *Portfolio Manager.*

- CyberCube foresees an escalation in the attacks perpetrated by state-nexus threat actors targeting critical infrastructure. Specifically, Iranian state-sponsored threat actors are likely to target critical infrastructure opportunistically. Russian and Chinese state actors are expected to strategically position themselves to disrupt infrastructure in sectors crucial to the national economy and security of the US and its allies.

Premium rate increases for cyber continue to decelerate

The average increase stood at 1.6%, a significant drop from the 3.6% rise observed in the previous quarter and the 20% plus uplift recorded a year ago. This ongoing decline in cyber premium price hikes can be attributed to (re)insurers gaining better insight into the favorable impacts of price adjustments and underwriting modifications made between 2020 and 2022, as well as heightened competition in the market.

As carriers compete for business, this intensified competition has resulted in a decrease in both premiums and retentions, along with an easing in required sub-limits. Moreover, the growing readiness of carriers to underwrite cyber insurance is bolstered by the findings on underwriting capacity in Q2 2023. According to a survey conducted by the Council of Insurance Agents & Brokers, 40% of respondents reported an increase in capacity, while only 18% noted a decrease.[1]

Certain sectors are under the spotlight, specifically for how inherently Exposed they are to cyber risk. 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, as well as the extent to which some industries have more endpoints that are exposed to the internet, and other indicators. The average industry Exposure Score for medium-sized companies in the United States, in December 2023, reveals 12 highly Exposed industries.

[1] *The Council of Insurance Agents & Brokers' Commercial Property/Casualty Market Reports*

Healthcare is Exposed, look out for industry wide SPoF attacks

Healthcare organizations have increasingly digitized, and internet-facing networks hold sensitive health data that is subject to encryption, theft, and extortion. Health entities have a low tolerance for unplanned downtime, leaving them susceptible to data encrypting ransomware attacks.

This high inherent Exposure reflects a persistent and growing threat to the Healthcare sector, especially as more threat actors declare healthcare as a viable target (in contrast to the restraint of previous years). **The impact of ransomware attacks on entire healthcare systems is particularly alarming,** causing simultaneous shutdowns of health providers and sometimes resulting in the diversion of patients from emergency rooms. This development underscores how vulnerable interlinked health institutions are to malicious cyber activities and highlights the far-reaching consequences, affecting not only data security but also patient care and public health on a broader scale.

CyberCube's Security Score measures companies' ability to protect themselves. Industries with an above average Security Score include companies that demonstrably invest in satisfying the core elements of the National Institute of Standards and Technology (NIST) cyber framework.

Potential attacks on the Public sector targeting government and election infrastructure

In the US, medium-sized state and local governments, as monitored by CyberCube, typically maintain an average Security Score. These entities face challenges in protecting themselves against heightened targeting for espionage and increasingly even disruption.

As the US settles into a presidential election year, the Public sector becomes an increasingly attractive target for malicious actors seeking to sow chaos and undermine faith in democracy. Consequently, government agencies and officials must bolster their cybersecurity measures, enhance election integrity safeguards, and collaborate with cybersecurity experts to mitigate these threats and uphold the integrity of democratic institutions. Given the potential for significant attacks, bolstering defenses in the Public sector is paramount in 2024 and beyond.

Moreover, around 64 countries plus the European Union will hold national elections this year, involving nearly half the world's population.[2] In some cases, the same cyber threat actors that are attempting to meddle in the US presidential election will be active in other countries too.

Of particular concern is the involvement of nation-state cyber threat actors, equipped with the capability to orchestrate systemic attacks against the Public sector. As geopolitical tensions escalate, H1 2024 is expected to witness increased activity from these sophisticated adversaries. The potential for systemic attacks emphasizes the need for the Public sector to enhance its cybersecurity, fortifying defenses to safeguard against the evolving cyber threats that pose risks to national security and public trust.

[2] https://www.ndi.org/elections-calendar

CyberCube highlights eight Highest Risk industry sectors

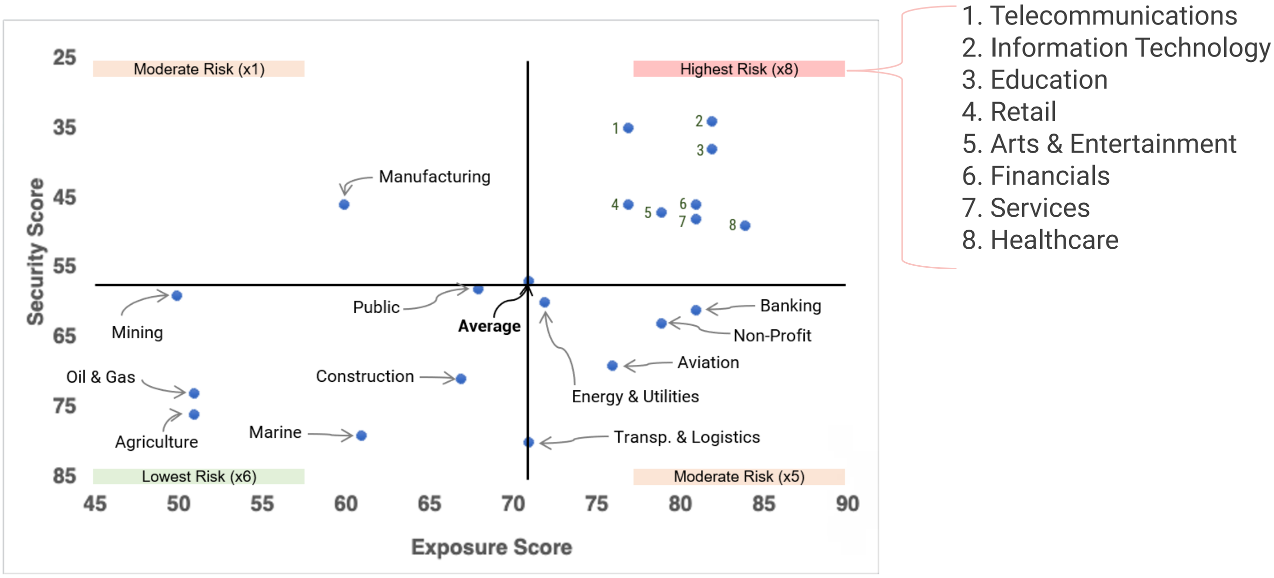
CyberCube data shows there are eight sectors which are under-secured and attractive targets, leaving companies vulnerable to criminal ransomware and extortion tactics as well as catastrophe events. Sectors such as Banking and Aviation are still Exposed and targeted but have better cybersecurity. These sectors tend to be more regulated and well-resourced to invest in security. Mining and Agriculture remain opportunity sectors for cyber (re)insurers as these sectors are less Exposed to cyber threats relative to other industries, yet they still maintain a high level of Security.

Exhibit 1 shows a representation of medium-sized companies in the US ($250 million to $1 billion of revenue) that also have cyber insurance. The combination of Exposure and Security paints a clear picture of industry-level differentiated cyber risk opportunities and sectors to scrutinize.

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

Exhibit 1: Average Industry Exposure vs Security Score – Medium Companies, United States (December 2023)

Note: Security Score has inverted scale



Source(s): CyberCube Account Manager (v5), Industry Exposure Database (IED) Medium Companies, N = 4334, Updated Security Score

CyberCube's US Cyber Exposure Databases

These analyses are made possible by CyberCube's US *Cyber Exposure Databases* — the first industry-backed, US cyber exposure data sets. The Economic Exposure Database (EED) comprises detailed exposure information on a representative sample of over 200,000 US companies exposed to cyber threats. The Industry Exposure Database (IED) is a statistical representation of all companies across the US 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.

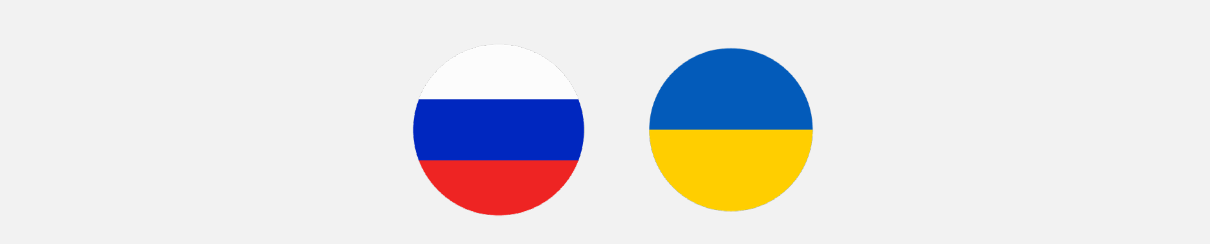
Reinsurers can use these databases to understand cyber risk from different workflows, such as benchmarking company exposures against the industry, assessing real time losses as cyber incidents occur, validating models, creating industry loss curves, and creating pro-forma portfolios and results. The 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 threat activity shines a light on cat event risk

Russian cyber threat actors took a Ukrainian mobile network operator offline in 2023.

After three days of outages that affected 24 million users, Ukraine's largest mobile network operator successfully resumed operations. This destructive attack was one of the most significant cyberattacks since Russia initiated its war on the country in February 2022. The assault on Kyivstar, which served over half of Ukraine's mobile subscribers, disrupted services, caused damage to IT infrastructure, and jeopardized millions of people by impeding alerts about potential Russian air assaults. Millions of Ukrainians rely on phone alerts to receive warnings about air attacks. Additionally, two Ukrainian financial institutions, PrivatBank and Oschadbank, experienced disruptions in ATMs and card terminals due to the outage.[3]

CyberCube Point of View: (Re)insurers and cyber risk modelers can use CyberCube's Portfolio Manager solution to assess the financial loss impact of a catastrophic attack on a Mobile Network Operator. In CyberCube's Scenario 23, a mobile network operator in the US is taken offline for several hours when threat actors infiltrate a primary data center and deploy wiper malware infecting critical servers. In affected regions, cellular data service is unavailable and no calls can be made. The main difference between the attack on Kyivstar and CyberCube's modeled scenario is the geographic footprint. We model a scenario in the US and the attack occurred in Ukraine. However, the threat actors' motivations, kill-chain, and the nature of the impact from the attack are aligned with CyberCube's scenario. In both cases, geopolitically motivated attackers have an intent to disrupt and cause long-lasting outages for a variety of organizations.



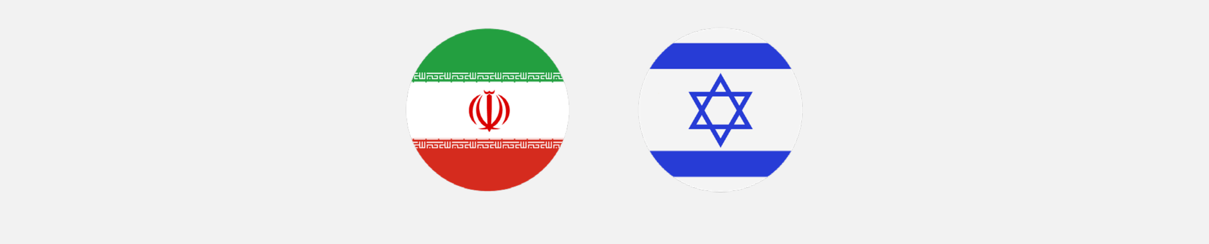
[3] https://radar.cloudflare.com/as15895?dateRange=7d

Iranian threat actors target Israeli-made software globally, impacting US water utilities.

On November 22, 2023, threat actors linked to the Islamic Revolutionary Guard Corps illicitly entered the networks of several US-based water utilities. One of the breaches made headlines after the Tehran-linked Cyber Av3ngers group claimed responsibility for hitting a water authority in Pennsylvania. These facilities use Israeli-made Unitronics Vision Series Programmable Logic Controllers (PLCs) with a Human-Machine Interface (HMI). Cyber threat actors compromised these PLCs since the PLCs were internet-facing and used Unitronics' default password. The impacted PLCs exhibited a message proclaiming "You have been hacked, down with Israel. Every equipment 'made in Israel' is Cyber Av3ngers legal target."[4]

CyberCube Point of View: CyberCube's Single Point of Failure solution, *SPoF Intelligence*, includes a variety of Israeli-made software that could be targeted in mass-exploitation campaigns by Iranian threat actors. (Re)insurers can use SPoF Intelligence to assess which companies in a portfolio are reliant on select Israeli-made software.

Data-wiping attacks are becoming more frequent on Israeli computers as researchers discovered variants of the BiBi malware family that destroy data on both Linux and Windows systems. The attacks are part of a larger cyber offensive that targets Israeli organizations, including in the education and technology sectors. An analysis of the attacks from researchers at Palo Alto Networks Unit42 attributes the data-wiping attacks to a threat actor that has "strong connections to an Iranian-backed APT group", tracked as Agonizing Serpens. The BiBi Wiper Malware was seen in late October by researchers at cybersecurity companies ESET and SecurityJoes, who noted that it was launched by pro-Hamas actors.[5]



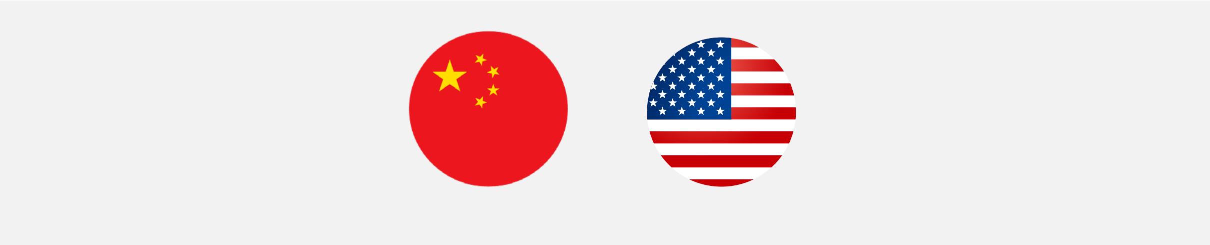
[4] https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems
[5] https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows

CyberCube 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 target both servers and endpoints simultaneously.

Chinese threat actors focus on the US and Asia, but their impact also reaches Europe.

China's cyber operations against the US have taken a strategic turn, emphasizing disruption in industries that could assist Taiwan in the event of a Chinese invasion. Data sourced from the European Repository of Cyber Incidents underscores China's role as a source of cyberattacks against Europe. While disruptive attacks from China on the US and Europe have not materialized so far, there is an active development of capabilities with the potential for future disruptions. This evolving landscape poses a substantial risk, not only to the US but also to targeted nations in Europe and Asia.[6]

CyberCube Point of View: CyberCube's Portfolio Manager assesses the impact on portfolios of cyberattacks on critical communications and internet infrastructure Single Points of Failure (SPoF). It also identifies losses for industries that are targeted by China, including: Telecommunications, Marine, Transportation & Logistics, Energy & Utilities, Oil & Gas, and Manufacturing.



[6] https://eurepoc.eu/

Key nation-state takeaways:

RUSSIA

- Russian cyber threat actors are targeting mobile network operators in Ukraine, signaling a potential warning sign for the US.
- CyberCube's Portfolio Manager Scenario 23 (Long Lasting Outage - Leading Mobile Network Operator) can be used to model losses.

CHINA

- Chinese threat actors concentrate on the United States and Asia, yet their influence extends to Europe.
- Look to Portfolio Manager to assess the share of catastrophe losses for attacks on industries targeted by China.

IRAN

- Iranian threat actors are targeting Israeli-made software, including programmable logic controllers (PLCs) inside critical infrastructure.
- SPoF can be used to uncover exposure to Israeli-made software such as Enterprise Applications, Productivity Solutions, and Security Tools.
- Iran is also targeting Israeli-based organizations with wiperware that destroys Windows and Linux operating systems (OS).
- CyberCube's Portfolio Manager Scenario Families 3CI and 4OS can be used to assess losses from wiperware attacks on OS SPoF.

CyberCube's H1 2024 cyber threat outlook

In light of the escalating cyber threats outlined by CyberCube, the imperative for (re) insurers to proactively model the potential impact of catastrophic cyberattacks on critical infrastructure has never been more urgent.

Our assessment accentuates the vulnerabilities faced by critical infrastructure owners in the US due to Iran's opportunistic cyberattack strategies, China's significant capabilities in disrupting crucial services, and Russia's ongoing efforts to target critical infrastructure globally. To address these pressing challenges, (re)insurers and cyber risk modelers can leverage CyberCube's Portfolio Manager to assess the ramifications of cyberattacks on SPoF in operational technology (OT). These efforts are essential for safeguarding the resilience of vital sectors such as energy, transportation, and logistics against emerging cyber threats and ensuring the continuity of essential services in an increasingly interconnected world.

What's next?

CyberCube remains committed to tracking and calibrating its models and data to accurately reflect emerging cyber threats. By staying abreast of the latest developments and trends in cyber, CyberCube ensures that its clients have access to the most up-to-date and comprehensive risk intelligence available.

Through CyberCube's data and analytics software and services, clients can leverage advanced predictive analytics and scenario modeling capabilities to anticipate rising threats and adapt their risk management strategies accordingly. By harnessing the power of CyberCube's insights, clients can proactively identify risk, strengthen resilience, and mitigate losses.

AUTHORS

William Altman, Cyber Threat Intelligence Principal
Richard DeKorte, Cyber Security Consultant

EDITORIAL CONTENT

Yvette Essen, Head of Content, Communications & Creative

CyberCube

www.cybcube.com