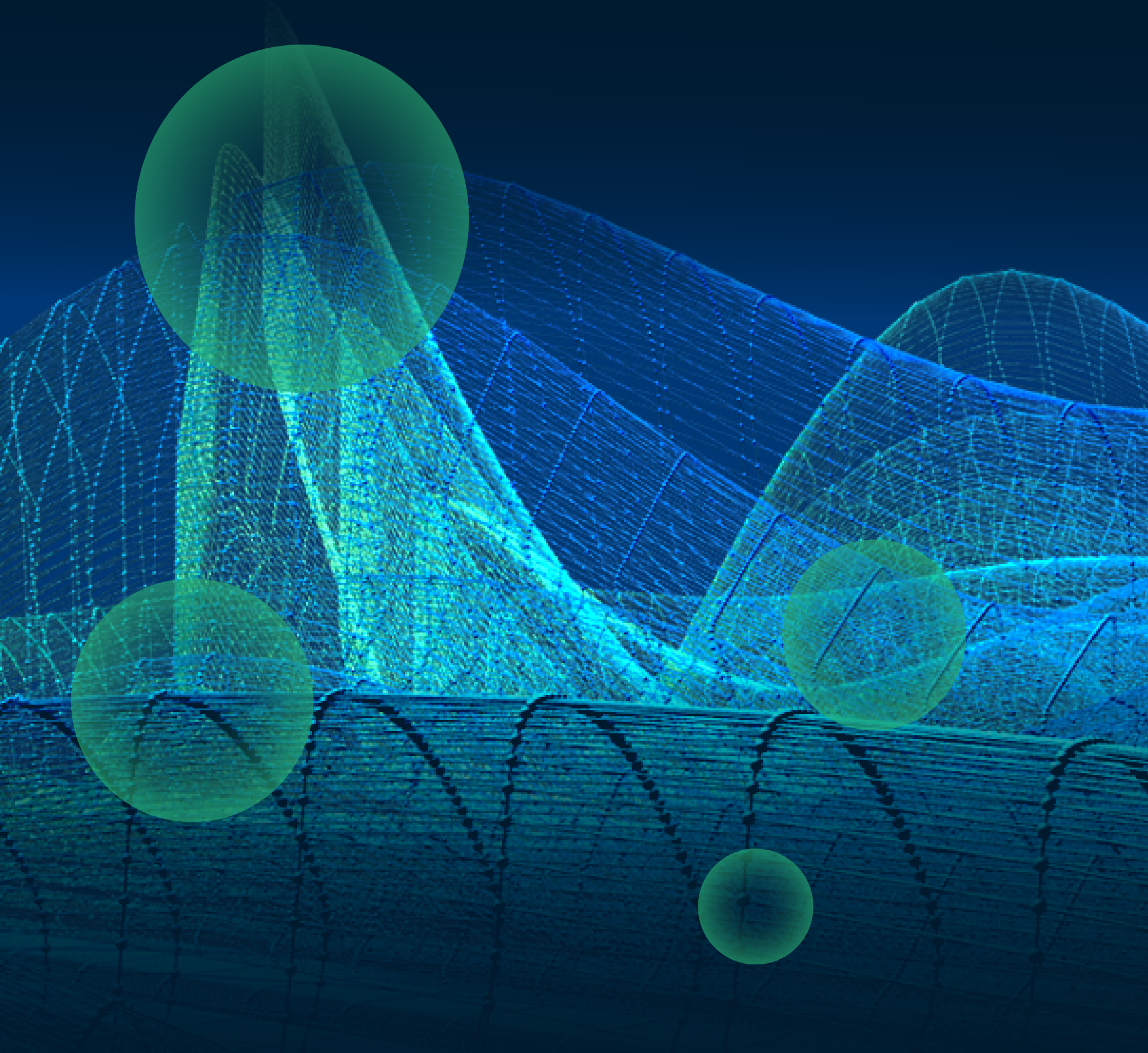
CyberCube

SPOTLIGHT ON ACTIVITY
SIX MONTHS LATER



UKRAINE CYBER WAR UPDATE

SEPTEMBER 2022

In the six months following Russia's invasion of Ukraine on February 24, 2022, cyber warfare has been an important tool for assisting physical activity on the ground.

As of 13 June, 2022, there were at least 76 cyber groups participating in the war in Ukraine. This number has doubled since the beginning of March. There has also been a constant barrage of Russian cyber attacks aimed at Ukrainian citizens, businesses, and critical infrastructure. At the same time, CyberCube has observed an unprecedented number of attacks aimed at Russian corporations and the government.

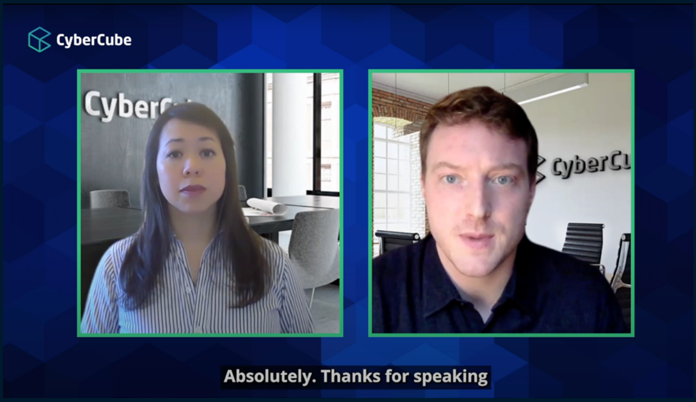
THIS REPORT SUMMARIZES KEY CYBER ACTIVITY AND NOTABLE TRENDS SINCE THE WAR BEGAN. IT NOTES:

- Russian ransomware gangs are focusing on large targets that fall just under the critical infrastructure threshold.
- Russia is using criminal ransomware gangs to undermine the US economy while also avoiding direct war with the US. European energy companies are also increasingly being targeted for their strategic value.
- Russia is targeting governments in Europe that are assisting in Ukraine's defense.
- There has been a dramatic rise in the normalization of wiper malware being used as a weapon in this war.
- The creation of a sovereign Russian internet could lead to greater confidence that attacks can be carried out without consequences.
- In response to this pattern of increased cyber activity, (re)insurers and brokers need to take proactive measures to manage their exposures.
- Lloyd's recently introduced a requirement that all standalone cyber attack policies must exclude liability for losses arising from state-backed attacks. CyberCube believes this mandate will help reduce uncertainty and enable more insurers to participate with confidence, based on a clearer understanding of what is covered, and what is excluded.

FURTHER RESEARCH

In March, CyberCube published a report titled "War in Ukraine creates a fundamental shift in the cyber threat landscape" analyzing the cyber events coinciding with Russia's invasion of Ukraine and their potential implications for the (re)insurance industry.

A video outlining the highlights of that report can be viewed here.



CyberCube's Global Threat Briefing Report H2 2022 published in July examined cyber activity following the Russian invasion of Ukraine, as well as other key trends such as new ransomware tactics and industries likely to be targeted by cyber criminals.

DOWNLOAD NOW

RANSOMWARE DECLINES OVERALL, SHIFTS FOCUS

Prior to the invasion, Russia was generally excluded from many ransomware target lists. There is evidence that this has now changed, with ransomware threat actors today focussing their efforts more on Russia than on other parts of the world. The reasons for this include the rise of ransomware hacktivists protesting Russia's war, and the general lack of international appetite for stopping cyber attacks aimed at Russia. For example, the group NB65 attacked Russian space agency Roscosmos, and state-owned Russian TV and radio, using this approach. At the same time, tighter international sanctions are making it harder for companies in the US and Europe to pay Russian-speaking ransomware gangs This has led to a slight downturn in the number of ransomware attacks in the US and Europe.

Although there have been some high-profile attacks, the overall volume of ransomware detections declined 4% between July 2021 and March 2022, according to ESET telemetry. Notable attacks include the Conti gang attacking Honduras, accounting for 53% of ESET's daily detections. Conti has since disbanded and the LockBit gang is quickly taking its place as one of the most feared ransomware gangs. Other attacks include an array of criminal and Russian state-sponsored attacks on Ukrainian organizations. There are large ransomware gangs that remain loyal to the Russian government and are targeting businesses and governments around the world.

TARGETED GEOGRAPHICAL REACH

There has been a noticeable increase in activity from Russian actors targeting governments outside of Ukraine, particularly in cyber espionage campaigns. This is likely intended to gather intelligence on Western allies assisting Ukraine's war effort. Since the start of the war, Microsoft has detected Russian network intrusion efforts on 128 different targets in 42 countries outside of Ukraine.

The past six months have seen a steady number of attacks from Russian-speaking ransomware gangs, with threat actors openly pledging allegiance to Russia. Those attacks have largely been against US and European businesses, with private enterprises as key targets. In the US, attacks have tended to center on large multi-billion dollar companies that are not considered critical infrastructure. This reflects the care taken by Russian attackers to disrupt high-value targets without eliciting a response that could lead to war.

At the same time, Russian threat actors are targeting energy companies in Europe to undermine those countries' ability to move away from Russian oil toward cleaner energy sources. European companies in the renewable and alternative energy industries are under attack.

Germany, the second largest importer of Russian oil just behind China, has become a particular target for Russian activity. For example, at the start of the war, Germany's Enercon saw approximately 5,800 of the wind turbines it operates via a SATCOM link in central Europe lose contact with their SCADA server. Over the last six months, there have been at least two more notable cyber attacks on German wind energy companies. There were also attacks on wind turbine manufacturer Nordex and wind farm maintenance company Deutsche Windtechnik.

There is a spectrum of state sponsorship at play for criminal cyber threat actors in countries other than Russia. This relationship ranges from tacit approval for criminal operations aimed at the state's enemies to outright state coordination and execution, utilizing criminals as cyber mercenaries for hire. CyberCube expects ransomware gangs loyal to Russia will continue hitting enterprise targets while state actors focus on government entities.

RUSSIA'S METHODS OF ATTACK

One notable trend has been a dramatic rise in the use of wiper malware by Russian threat actors. Unlike ransomware, this has no financial element to it but is specifically designed to destroy data and systems.

Russia has used wiper malware previously, most recently in the NotPetya attack of 2017. In December 2016, Ukrainians were the victims of the first-ever cyber attack utilizing malware specifically designed to attack electricity power grids. The malware was found to be linked to Russian APT group Sandworm, and named as Industroyer. Researchers noted that the malware was "second only to Stuxnet" in its sophistication.

Industroyer lay dormant for more than five years, until April 2022 when incident responders stopped an attack on the Kyiv North transmission substation and, in the process, discovered a new variant named Industroyer2. This attack type is now clearly seeing a resurgence, with Russia deploying a more targeted wiper malware approach over the last six months.

As well as utilizing wiper malware, Russia is separately focusing on deploying its "Sovereign" internet - a completely independent, isolated, totalitarian network. This has several potential implications for cyber activity:

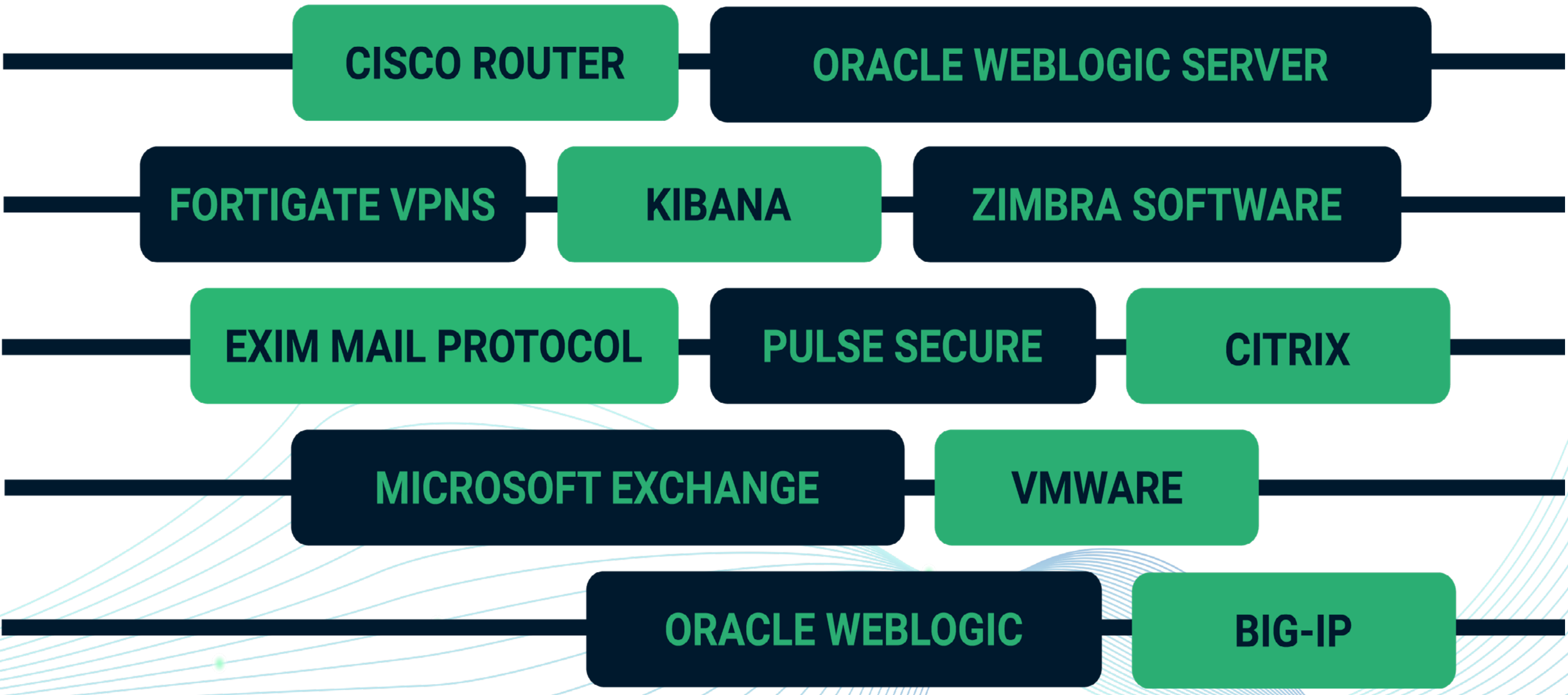
1 Rival nations will find it more difficult to acquire intelligence on Russia and might resort to more drastic measures to achieve this goal, potentially causing collateral damage.

2 Russian actors can cause more damage, feeling safer behind the wall provided by an isolated internet.

3 There is a potential for future "collaboration" between Russian, North Korean and Chinese internets, which would increase threat actors' ability to launch attacks. Nation states are increasingly aligning along ideological lines, devising new ways of isolating their internet space. This, in turn, defines clearer battle lines than have ever previously existed in cyber space.

A Single Point of Failure (SPoF) is a service provider whose failure or outage could disrupt large swaths of organizations that rely on it to carry on their operations. CyberCube believes a completely independent Russian technology infrastructure would enable even more destructive SPoF attacks. For (re)insurers, understanding the concentration of SPoFs across a portfolio is critical to managing SPoF risk accumulations.

CyberCube can help (re)insurers identify companies that rely on a heavily-targeted SPoF. For example, we have observed Russian advanced persistent threat actors (APTs) exploiting a preferred set of technologies as initial network entry vectors. According to the US Cybersecurity and Infrastructure Security Agency (CISA), there are at least 13 technologies that Russian APTs typically exploit to gain initial access *(see Exhibit 1)*:



CISCO ROUTER

ORACLE WEBLOGIC SERVER

FORTIGATE VPNS

KIBANA

ZIMBRA SOFTWARE

EXIM MAIL PROTOCOL

PULSE SECURE

CITRIX

MICROSOFT EXCHANGE

VMWARE

ORACLE WEBLOGIC

BIG-IP

EXHIBIT 1 Russian APT targeted technologies

Source: CISA

Cyber (re)insurers can use *CyberCube's SPoF Intelligence* tool to identify their potential exposure to companies using SPoF technologies known to be targeted by Russian APTs

Exhibit 2 depicts the count of companies in the Forbes 1000 group of companies using SPoF technologies that are known to be targeted by Russian APT actors. These companies are at higher risk of having vulnerabilities exploited in these SPoF. *Exhibit 2* shows the number of businesses using Russian APT targeted SPoF by country.

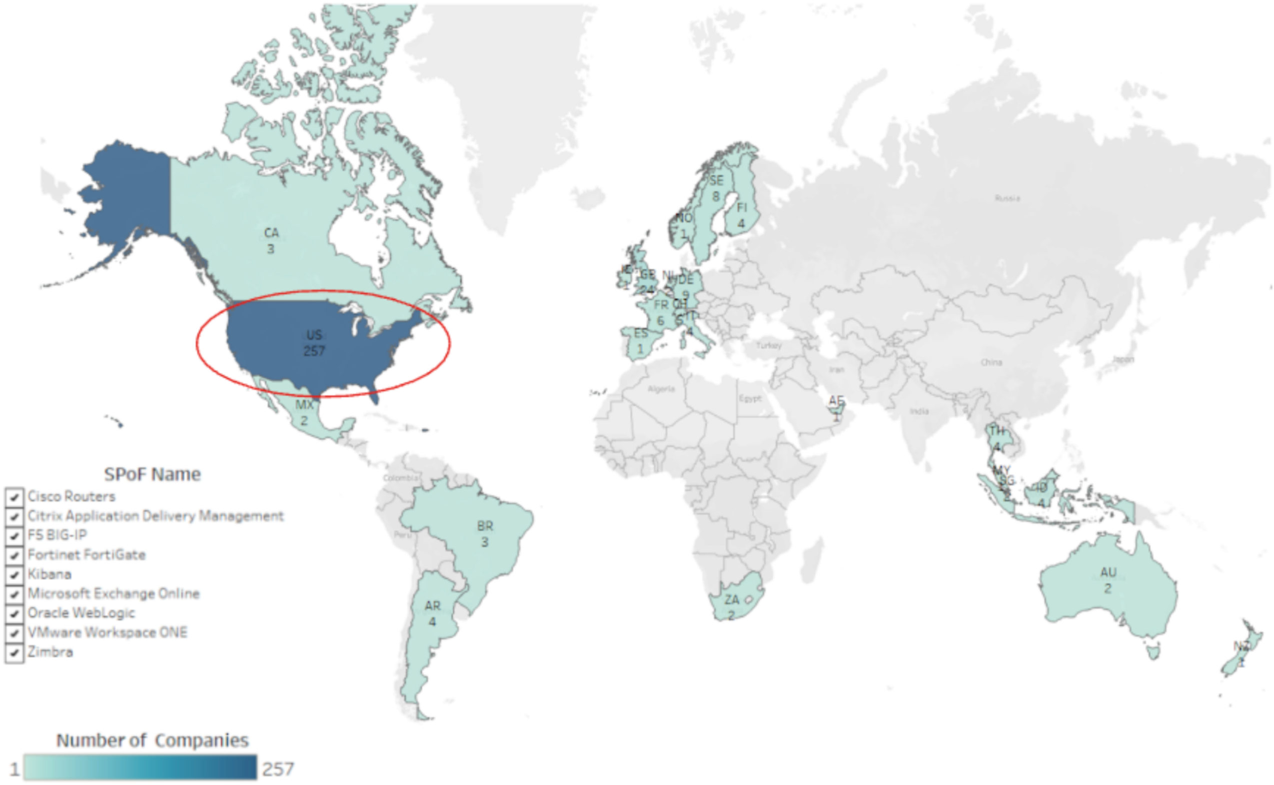


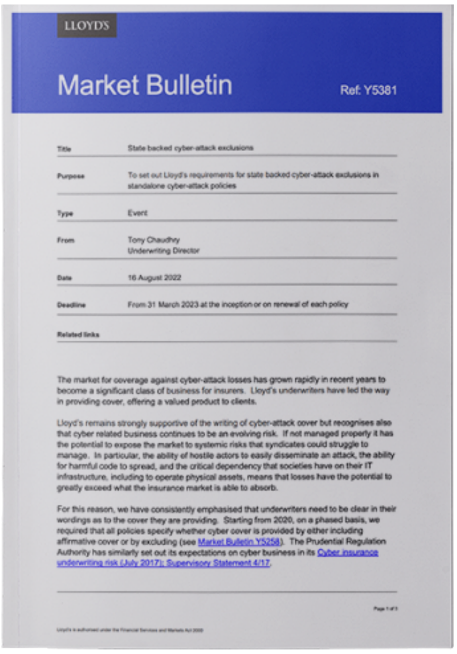
EXHIBIT 2 CyberCube SPoF Intelligence: Global Forbes 1000 List

Source: CyberCube Analytics

Forward-looking (re)insurers are starting to adopt a threat-modeling approach to portfolio risk management. Understanding the threat actors targeting your insureds, and devising risk strategies accordingly, is quickly becoming the standard for world-class cyber product lines.

INSURANCE INDUSTRY RESPONSE TO CYBER ACTIVITY

Lloyd's published a market bulletin on August 16, 2022 requiring all standalone cyber policies to include a suitable clause excluding liability for losses arising from any state-backed cyber attack. This clause must apply ***in addition*** to any war exclusion, and the requirement will take effect from 31 March 2023 on the inception or renewal of each policy.



LLOYD'S

Market Bulletin

Ref: Y5381

Title	State backed cyber-attack exclusions
Purpose	To set out Lloyd's requirements for state backed cyber-attack exclusions in standalone cyber-attack policies
Type	Event
From	Tony Chaudhry Underwriting Director
Date	16 August 2022
Deadline	From 31 March 2023 at the inception or on renewal of each policy
Related links	

The market for coverage against cyber-attack losses has grown rapidly in recent years to become a significant class of business for insurers. Lloyd's underwriters have led the way in providing cover, offering a valued product to clients.

Lloyd's remains strongly supportive of the writing of cyber-attack cover but recognises also that cyber related business continues to be an evolving risk. If not managed properly it has the potential to expose the market to systemic risks that syndicates could struggle to manage. In particular, the ability of hostile actors to easily disseminate an attack, the ability for harmful code to spread, and the critical dependency that societies have on their IT infrastructure, including to operate physical assets, means that losses have the potential to greatly exceed what the insurance market is able to absorb.

For this reason, we have consistently emphasised that underwriters need to be clear in their wordings as to the cover they are providing. Starting from 2020, on a phased basis, we required that all policies specify whether cyber cover is provided by either including affirmative cover or by excluding (see Market Bulletin Y5258). The Prudential Regulation Authority has similarly set out its expectations on cyber business in its Cyber insurance underwriting risk (July 2017): Supervisory Statement 4/17.

Page 1 of 3

Lloyd's is authorised under the Financial Services and Markets Act 2000

DOWNLOAD NOW

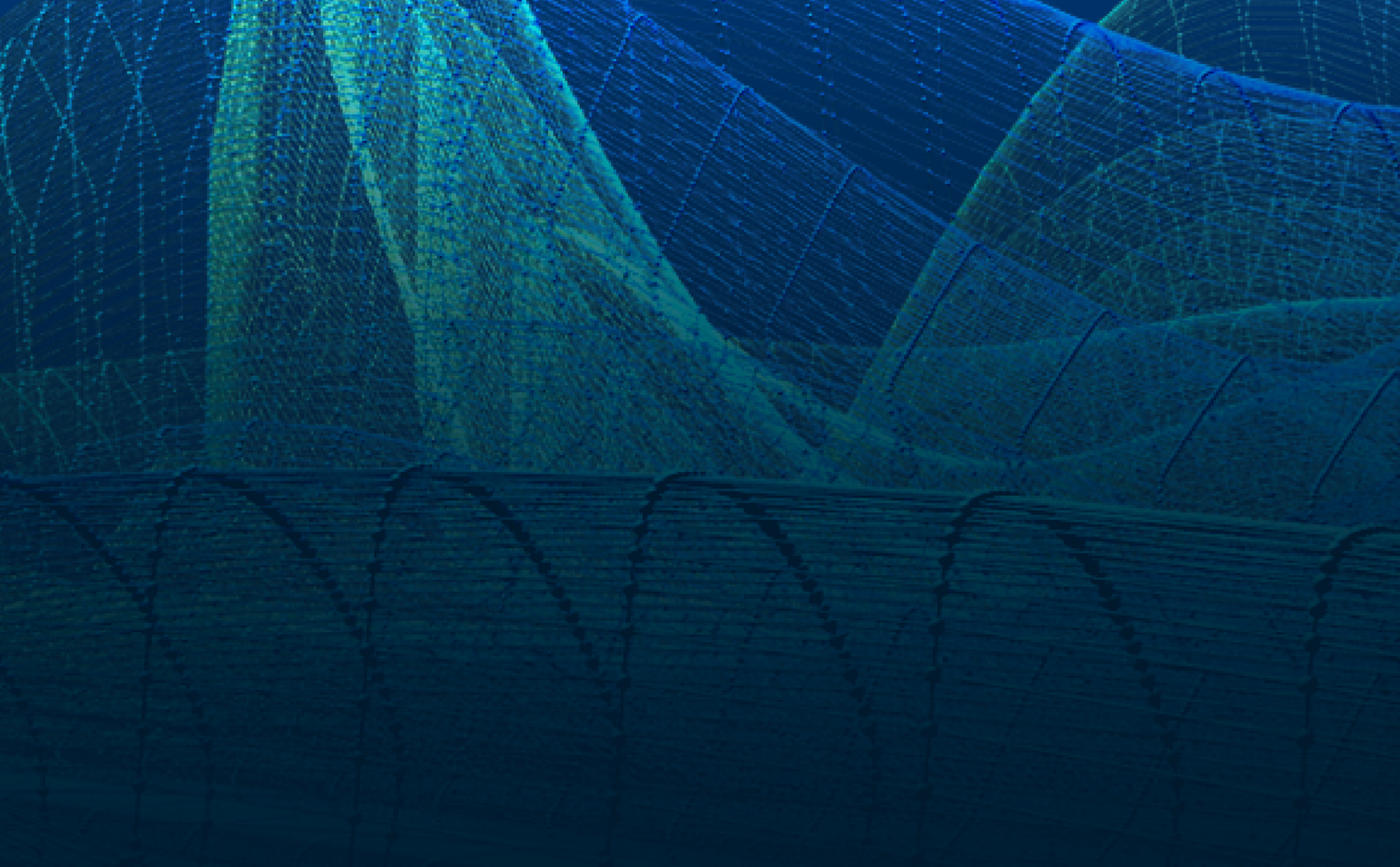
These (and similar) clauses have been discussed extensively in the market, and there is an emerging consensus that they are important for market consistency in what is a complex and rapidly changing area. The goal of such clauses is to create a shared set of expectations between underwriters, brokers, and insured clients, and to reduce ambiguity in interpretation. Implementing them across the market, reduces uncertainty around the potential systemic risk associated with war, and lies beyond the scope of the commercial insurance market.

In CyberCube's opinion, Lloyd's mandate should increase clarity and help buyers and insurers alike develop a common understanding of the limits of insurance. The potential challenge will be in applying such clauses to a specific set of facts. For example, attribution can be notoriously difficult. But Lloyd's taking a leadership position on the issues should have a positive impact, and other insurance markets will be looking to Lloyd's for guidance.

CyberCube is working with (re)insurance and broking clients to measure and mitigate risk in response to cyber activity. There are some positive signs that underwriters, reinsurers and brokers are adopting a proactive stance in addressing cyber risk emerging from the war in Ukraine. Insurers and brokers should be focusing on renewals three to six months in advance, helping their clients fix issues cyber threat actors are known to take advantage of. These include ensuring companies use multi-factor authentication and have secured their remote desktop protocol (RDP) and other remote support connections.

Reinsurers should look across their portfolios for indications that certain companies may be susceptible to different threat actors. For example, analysis of leading Russian-speaking ransomware gangs shows the use of particular tactics, techniques and procedures they currently favour. This can help build an understanding of the types of companies and characteristics that would make them attractive targets for specific threat actors.

The cyber threat landscape is certainly fast-paced and dynamic, but there are also some common tactics, techniques, and procedures in use among cyber threat actors. We can study the kill chains that are commonly executed in attacks to learn which types of pre-breach indicators are predictive of risk. This analysis has been done in cyber security for decades. Now insurers are catching up.



AUTHORS:

William Altman, Principal Cyber Security Consultant

Yvette Essen, Head of Content & Communications

DESIGN:

Alesia Auramenka, Graphic Designer

DISCLAIMER

For further information please contact:
CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108
Email: info@cybcube.com
Telephone: +1(415)6354157

This document is for general information purpose only and is correct as at the date of publication. The product described in this document is distributed under separate licences with CyberCube which restricts its use, reproduction, distribution, decompilation and reverse engineering. Whilst all reasonable care has been taken in the preparation of this document including in ensuring the accuracy of its content, this document is provided on an "as is" basis and no liability is accepted by CyberCube and its affiliates for any loss or damage suffered as a result of reliance on any statement or opinion, or for any error or omission, or deficiency contained in the document. This document is subject to change from time to time and it is your responsibility for ensuring that you use the most updated version. This document and the information contained herein are CyberCube's confidential and proprietary information and may not be reproduced without CyberCube's prior written consent. Nothing herein shall be construed as conferring on you by implication or otherwise any licence or right to use CyberCube's intellectual property.All CyberCube's rights are reserved.

CyberCube is on a mission to deliver the world's leading cyber risk analytics.

We help the cyber insurance market grow profitably using our world-leading cyber risk analytics and products. The combined power of our unique data, multi-disciplinary analytics and cloud-based technology helps with insurance placement, underwriting selection and portfolio management and optimization. Our deep bench strength of experts from data science, security, threat intelligence, actuarial science, software engineering, and insurance helps the global insurance industry by selecting the best sources of data and curating it into datasets to identify trustworthy early indicators of risks and to build forward-looking views of them.

Discover how you can leverage leading cyber risk analytics for your busines
by contacting us at: sales@cybcube.com