MOODY'S INVESTORS SERVICE

OUTLOOK

7 November 2022

Send Your Feedback

TABLE OF CONTENTS

Contacts

Leroy Terrelonge 1.212.553.2816
Vice President - Senior Analyst
leroy.terrelonge@moodys.com

Irina Dimitrova +49.69.86790.2106
Analyst
irina.dimitrova@moodys.com

Luigi Bucci +44.20.7772.1961
AVP-Analyst
luigi.bucci@moodys.com

Srikanth Vadlamani +65.6398.8336
VP-Sr Credit Officer
srikanth.vadlamani@moodys.com

Lesley Ritter +1.212.553.1607
VP-Sr Credit Officer
lesley.ritter@moodys.com

» *Contacts continued on last page*

Cyber Risk – Global

2023 Outlook - Governments and industries toughen cyber stance; credit effects mixed

Summary

In response to growing cyber risk, governments, regulators and insurers are taking actions to reduce financial exposure to cyberattacks. These measures will be credit positive insofar as they reduce the risks of near-term financial distress. But the same actions will produce negative credit effects for organizations if risk is shifted from one group to another, or if the measures result in unintended consequences.

» **Ransomware attacks will shift from the US, raising risks for issuers in other regions.** The US has increased its pursuit of cybercriminals with sanctions, arrests and cryptocurrency seizures. As a result, cybercriminals are pivoting to less resilient targets outside the US.

» **Scrutiny from governments and regulators will increase.** Cybersecurity requirements aimed at strengthening disclosure mandates are credit positive in that they help raise a baseline set of information about the scope of cyberattacks. But public reporting on attacks could arm hackers with details that allow them to strike more effectively.

» **Passwordless technology will provide a powerful cyber defense, but adoption will be slow.** Passwordless alternatives will allow organizations to almost eliminate successful phishing attacks. But slow adoption will give cybercriminals a foothold to exploit.

» **Hacktivism will intensify and deepfake-enabled fraud will rise.** Hacktivism largely disappeared for half a decade, but has returned with greater technical sophistication and state support, raising the level of threat. Deepfake attacks are also evolving, and fraudsters will use the technology to make their scams more convincing.

» **Demand for cyber insurance will outweigh supply.** Premiums are rising and coverage is narrowing, a credit positive for insurers as they look to reduce their exposure to losses. On the other side, issuers will have to invest in better cyber hygiene or find alternative risk transfer strategies, such as cloud adoption. Organizations can transfer some of their risk to the cloud, but will still need to ensure good security and monitor the IT practices of their cloud providers.

» **Quantifying an expected financial loss from a cyberattack will play a growing part in risk mitigation.** A more data-driven approach will foster improved decision-making by managers and enable better communication of risk mitigation strategies and exposure.

Ransomware attacks will shift away from the US, raising risks for regions that have largely been spared

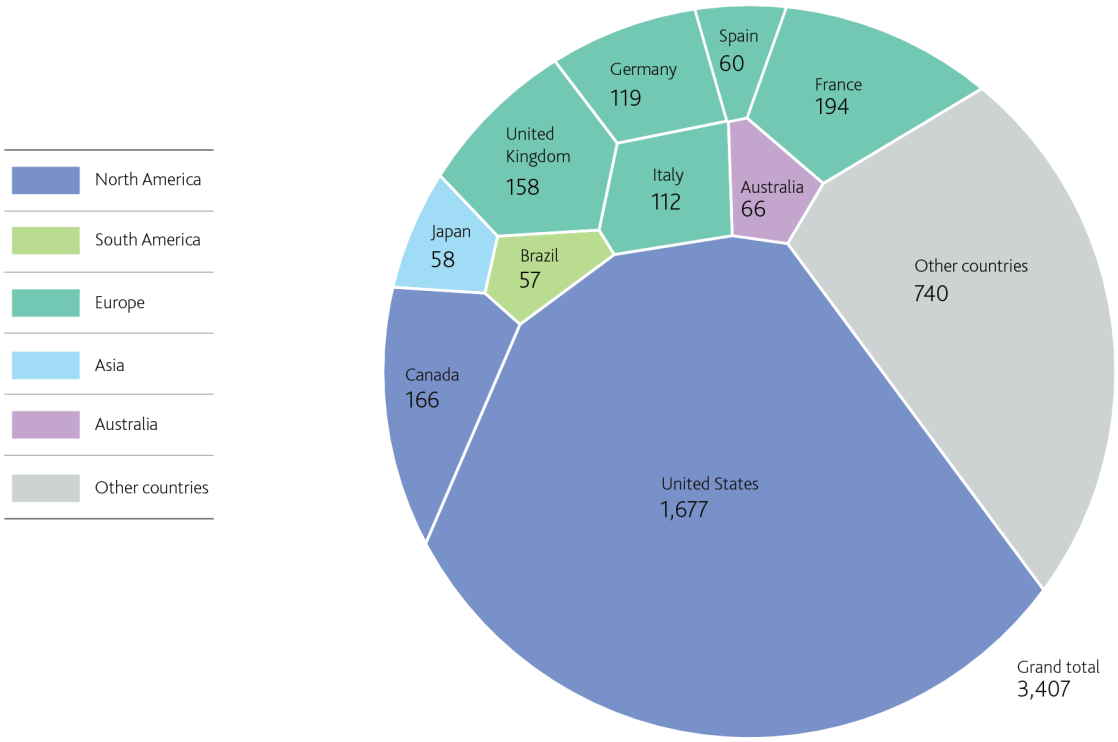
The US government has put ransomware gangs under increasing pressure in recent months through sanctions, arrests, and cryptocurrency seizures. In response, cybercriminals will broaden their attacks to target organizations in other countries. This shift will be credit positive for US issuers experiencing a relative reprieve from attacks but negative for issuers in regions with an uptick in ransomware incidents. Ransomware attacks are credit negative when they disrupt business operations, require costly remediation, result in loss of intellectual property, or damage issuers' reputations.

Historically, the US has by some distance been the biggest target for ransomware. As shown in Exhibit 1, ransomware attacks against entities in the US accounted for approximately 49% of such attacks worldwide in 2021, according to data from cyber risk modelers at RMS.[1]

Exhibit 1

The US is by far the country with the most ransomware attacks

Ransomware cases by country in 2021



Source: RMS

Ransomware gangs, however, are starting to diversify their geographic attack patterns, and while the US remains the country with the most attacks, its prominence is waning. Data from RMS (see Exhibit 2) show that the global share of ransomware attacks in North America fell from 65% to 46% from 2020 to 2022. The share of attacks in other regions, meanwhile, is rising.

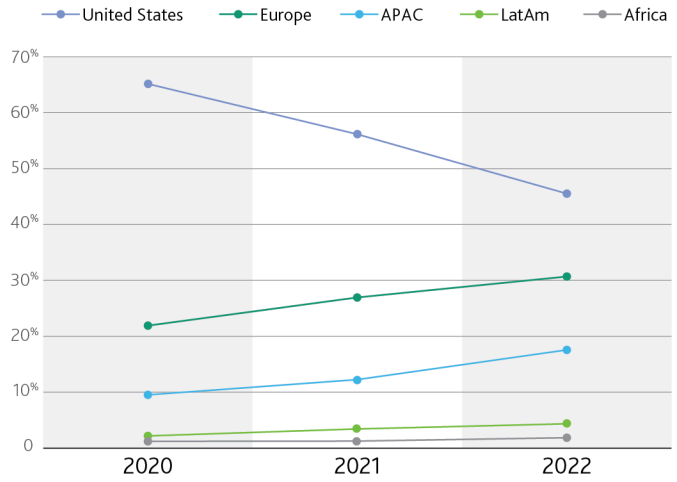
The shift follows increased US government pressure on ransomware gangs and the infrastructure that facilitates their criminal activity. US sanctions have deterred payments to certain ransomware gangs operating from Russia, North Korea and Iran, and led to the shuttering of cryptocurrency platforms that facilitate illicit transactions.

In response, ransomware gangs are targeting other regions, such as Europe. Cybersecurity firm SonicWall notes that attacks there shot up 63% in the first half of 2022.[2] Recent ransomware incidents in Europe include an August attack against 10 national government institutions in Montenegro (B1 stable) that threatened to disrupt the country's critical infrastructure.

Exhibit 2

US share of global ransomware attacks is decreasing

Ransomware cases by regional share from 2020 to 2022

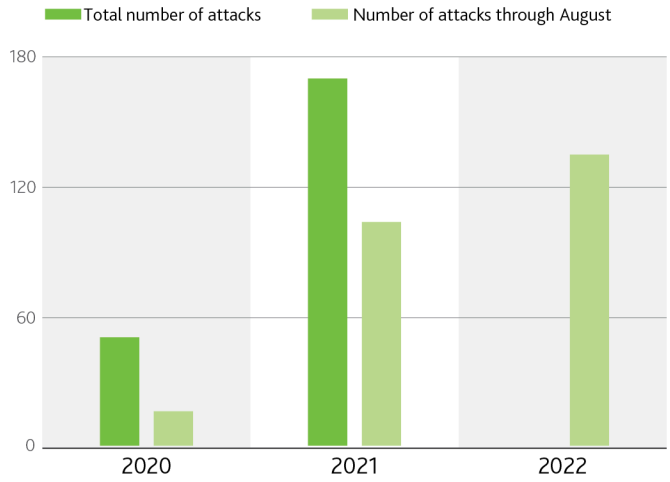


Source: RMS

Exhibit 3

Ransomware attacks have risen sharply in Latin America

Ransomware cases in Latin America from 2020 to 2022



Source: LeMagIT[3]

In addition to Europe, cybersecurity researchers regard countries in the global south as a new hot spot for ransomware attacks, with Latin America in particular experiencing a large increase. Exhibit 3 shows attacks in the region grew by 30%, from 104 between January and August 2021 to 135 in the same period of 2022, which includes a cyberattack against the government of Costa Rica (B2 stable) that temporarily prevented the national government from collecting taxes and distributing social security. The attack was credit negative for the sovereign, which will likely need to increase spending this year to resolve the situation and increase its cybersecurity.

Governments and regulators will tighten cybersecurity requirements for companies and strengthen incident disclosure mandates

A trend of tougher requirements on cyber risk management and incident reporting is likely to continue, a credit positive since more standardized frameworks for disclosure will provide increased transparency into an opaque but growing risk. Increased disclosure is also likely to spur companies to sharpen their focus on cybersecurity, with more robust reporting requirements helping to establish benchmarks that organizations can use to improve their cyber preparedness. Industry lobbyists, however, warn that measures with tight reporting deadlines and public disclosure will increase risk for their members. The compliance burden of additional cybersecurity requirements will also impose costs.

Disclosure requirements have been increasing over the past year, prompted by an enhanced focus on systemic resilience to cyberattacks, particularly in light of Russia's invasion of Ukraine (Caa3 negative) and high-profile ransomware attacks such as the one against Colonial Pipeline Company (A3 stable) in May 2021. In the US, the Securities and Exchange Commission (SEC) in March proposed rules to enhance disclosures on cyber risk management and incident reporting by registered companies – a significant strengthening of mandatory public disclosures. Governments and regulators in the EU, Canada and India have also introduced measures that will tighten cybersecurity and disclosure requirements.

Disclosure mandates are credit positive for several reasons. First, they provide more transparency to market participants. The SEC's proposed rules would allow participants to differentiate between companies according to the strength of their cyber risk governance. Disclosures also benefit governments, which require data to understand the extent of cyber risks and develop appropriate policies for curbing the effects of attacks.

Disclosure mandates help establish defense benchmarks that organizations can use to improve their cybersecurity. They also reduce systemic risk because information about attack campaigns is shared with organizations, which can use it to block attacks or identify malicious behavior on their networks. In the US, for example, the Cybersecurity and Infrastructure Security Agency (CISA) collects cyber incident reports from targeted organizations, analyzes trends, and shares anonymized information that helps entities manage risk.

Some provisions of disclosure mandates, however, may prove challenging for issuers. Short timelines for disclosure are one such challenge, because public reporting on an attack still in progress could arm hackers with real-time feedback allowing them to make the attack more effective. A disclosure that takes place too soon could hamper an ongoing investigation into an attack. Disclosure mandates add operational burdens, too, especially for entities that report to more than one regulator. The resources required for complying with these measures can be considerable.

Passwordless technology will provide a powerful defense against cyberattacks, but adoption will be slow

An authentication standard that is being rolled out on a large scale – the "Fast Identity Online" (FIDO) protocol – will reduce reliance on passwords. Since most cyberattacks involve guessing or stealing passwords, FIDO has the potential to significantly reduce issuers' exposure to these attacks. Widespread adoption will take time, however, and researchers have identified a workaround that attackers can exploit in the meantime.

Passwords, though ubiquitous, are problematic

Despite their important role in securing access to resources, passwords present numerous challenges for cybersecurity. Perhaps most challenging is the fact that users consistently choose weak passwords, such as "password," "123456" and "qwerty". Many widely available hacking tools allow attackers to rapidly guess weak passwords by trying every possible combination of characters (brute forcing). Exhibit 4 shows how long it takes to crack passwords with varying levels of complexity. Many passwords can be brute-forced instantly.

Exhibit 4

Weak passwords can be cracked instantly

Length of time to crack password as a function of number of characters and password complexity

VERY WEAK WEAK MODERATE STRONG

Number of characters	Numbers only	Lowercase letters	Upper and lowercase letters	Numbers, upper and lowercase letters	Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Source: Hive Systems[4] and Moody's Investors Service

Instead of passwords, the FIDO protocol will allow users to log in to online services through public key cryptography tied to users' devices. Eliminating passwords in this way would likely prevent most current types of cyberattack. According to CISA, over 90% of all attacks begin with phishing.[5] And according to Verizon's annual Data Breach Investigations Report, stolen credentials/passwords (45-50% of breaches) and phishing (15-20%) are the most common pathways to stealing victims' data.[6]

Adoption of FIDO faces hurdles, however. Apps and websites will require time to be updated to accept FIDO passkeys. Users will then need to be trained how to log in using the new process. It will also take time for newer devices and operating system versions that support FIDO passkeys to filter through to a large portion of users. As a result, many services will have to continue offering password-based logins.

The persistence of a password option would be welcomed by cybercriminals. In a 2020 study, researchers found they could trick users into downgrading from FIDO to an alternative authentication method that is more vulnerable to phishing.[7] Cybercriminals could adopt this technique to continue successful phishing attacks, though likely at a much reduced volume.

Hacktivism will intensify and deepfake-enabled fraud will rise

At the end of the last decade, hacktivism waned as a risk for issuers, with five to six years of relative quiet. But it has returned, with greater technical sophistication and state support, raising the level of threat from nuisance attacks to attacks that are disruptive and even destructive. At the same time, deepfakes are becoming more and more convincing, and fraudsters are using them to steal large sums of money from organizations. As the technology evolves, it will subvert conventional systems of trust, causing financial loss and forcing organizations to spend more on developing new business practices to combat fraud.

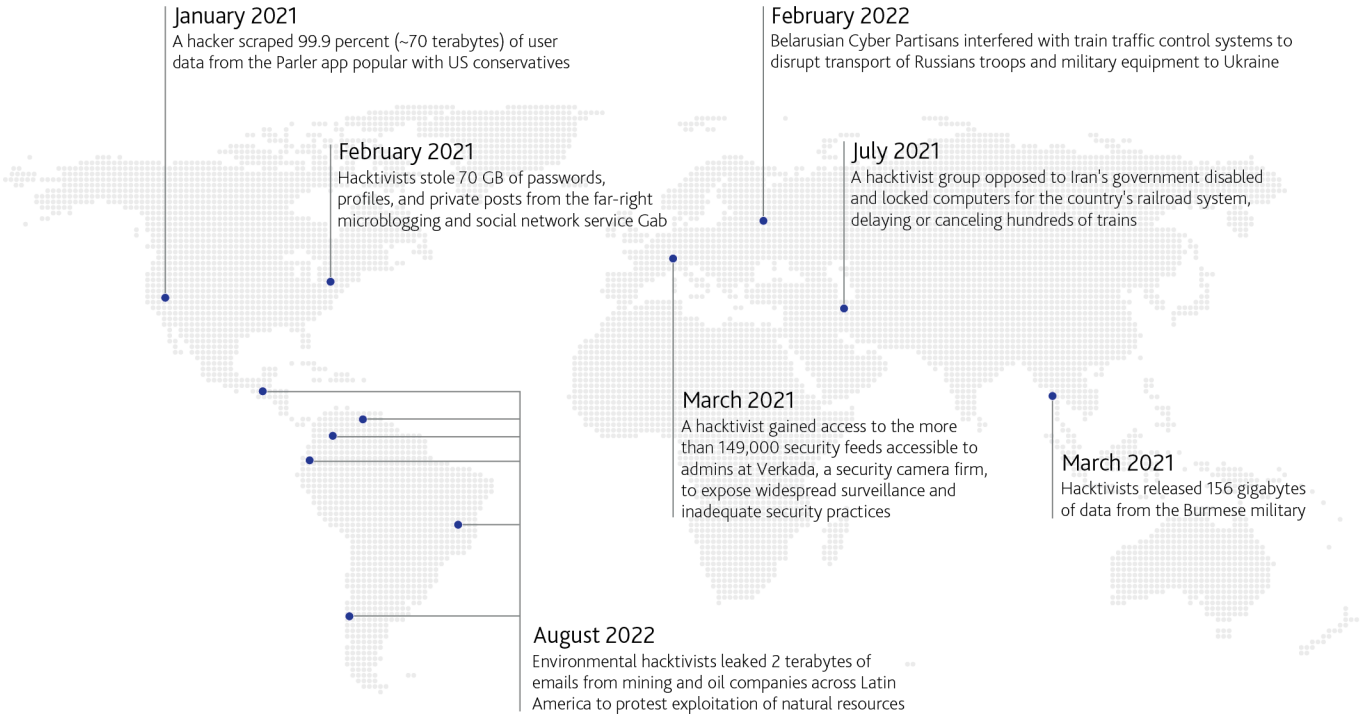
Hacktivism, a portmanteau of "hack" and "activism," refers to cyberattacks conducted in support of an ideology, political belief or social movement. Since 2020, such attacks have surged, driven by increased political polarization.[8] Russia's invasion of Ukraine has kept hacktivism levels elevated throughout 2022 and will challenge issuers into 2023. Attacks were frequent in the late 2000s and early 2010s when groups such as the Anonymous collective used low-grade distributed denial-of-service (DDoS) attacks to disrupt access to the websites of prominent organizations. Following arrests of some of the perpetrators, however, hacktivism declined sharply in the second half of the 2010s, with IBM (A3 stable) saying in 2019 that attacks had fallen by 95% since 2015.[9]

As hacktivism has returned, initial attacks have centered on race in the US. In May 2020, hacktivists launched a DDoS attack against the Minneapolis Police Department during protests in the city following the murder of George Floyd. In the past year, attacks have ramped up further with the introduction of state-mobilized hacktivist crews. According to cybersecurity company Check Point, hacktivism has become better organized, more highly structured and more sophisticated over the past year, resulting in attacks against governments and major corporations that in some cases have caused a significant impact (see Exhibit 5).[10]

Exhibit 5

Hacktivism's resurgence is a global phenomenon

Recent examples of hacktivist activity



Sources: Washington Post, CyberScoop, The Guardian, The New York Times, Tech Monitor

As a result, the baseline of attacks has increased significantly. Issuers are facing much more powerful DDoS and disruptive attacks that can directly impair their operations. In one attack, a group known as Predatory Sparrow got access to the industrial controls of one of Iran's largest steel producers, the Khuzestan Steel Company, and caused the plant's machines to spew molten steel and fire, damaging the company's equipment.

Use of deepfakes is increasing

Deepfake attacks are also evolving to become more damaging. Deepfakes are so called because they employ deep learning artificial intelligence to create fake images, audio, or video. In 2020, we highlighted the potential use of deepfakes in disinformation campaigns against companies to damage their reputations. Since then, cybersecurity researchers have discovered that deepfakes are being widely used to improve on business email compromise (BEC) scams.

BEC fraud (also known as Funds Transfer Fraud) occurs when a scammer tricks an organization into sending money to an account the scammer controls. The scammers often target employees that handle accounts payable, socially engineering them to change payment details such as bank account information for the organization's suppliers and vendors. BEC is the leading cause of cyber-related financial loss. The FBI said in 2021 that BEC fraud was the top cybercrime by victim loss, with incidents reported to the agency amounting to an aggregate loss of $2.4 billion.

Deepfakes have emerged as a significant upgrade to the traditional BEC scheme. In 2020, scammers used an audio deepfake to trick a Hong Kong bank manager into transferring $35 million out of the bank. Symantec, a cybersecurity company, said as early as 2019 that it had observed at least three cases of audio deepfakes being used to commit BEC fraud, resulting in losses up to millions of dollars. And though audio deepfakes have tended to be more effective, fraudsters are trying their hand at video deepfakes as well. In August 2022, fraudsters used deepfakes of the Binance cryptocurrency exchange's chief communications officer (CCO) to fool multiple individuals into thinking they were speaking with him in video meetings.

The technology that undergirds deepfakes is evolving rapidly. Whereas deepfakes in the past relied on many hours of source material, tools available free today allow anyone to clone another human's voice using as little as 3 seconds of that person's voice.

While premium increases will moderate, cyber insurance demand continues to outweigh supply

As the frequency, magnitude and sophistication of cyberattacks worldwide increase, insurance companies remain cautious about their exposure to systemic cyber risk. Measures taken by insurers to limit the financial impact on the industry include increasing prices, narrowing cyber coverage and making underwriting standards stricter. These steps are credit positive for insurers because they help improve the profitability of the product and lower the potential for large losses. At the same time, as coverage narrows and becomes more expensive, organizations will need to invest more in improving their cyber preparedness so they can access cyber insurance, or find alternative strategies for transferring cyber risks.

Cyber insurance prices will continue to rise, although at a slower pace

Prices for cyber insurance have risen sharply in the last couple of years as insurers globally have sought to compensate for rising losses on ransomware claims. And while the pace of rate increases has slowed this year, it is likely to remain significant.

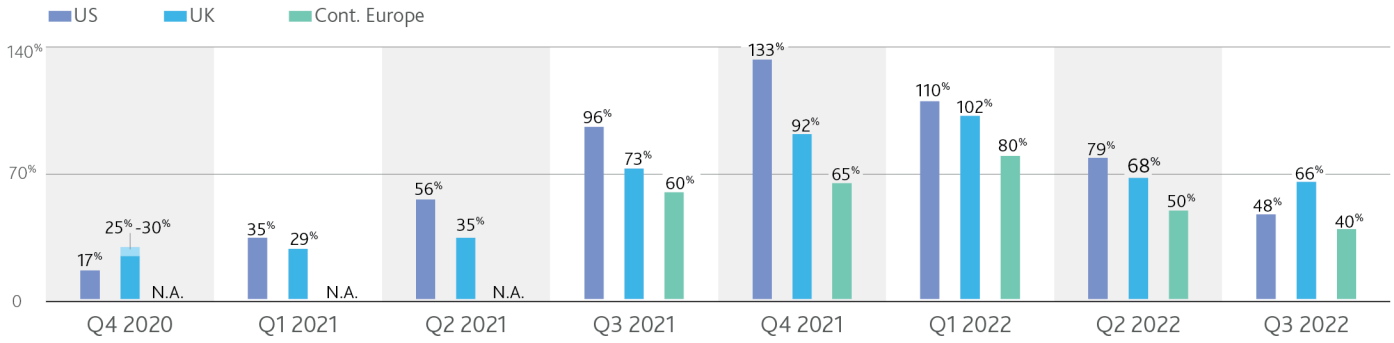
The surge in ransomware claims following the onset of the pandemic pushed down profitability of the cyber insurance business. In the US, the average loss ratio for standalone cyber insurance (including direct costs for defense and cost containment) deteriorated to 73% at the end of 2020 from 47% a year earlier, prompting the industry to respond with double- and triple-digit price increases in 2021. Organizations with significant losses and those with poor cyber defense practices generally experienced rate increases that were well above the average.

In the first half of 2022, ransomware attacks and associated claims payments declined. Price increases for cyber insurance have slowed correspondingly, but are still significant. After a 133% increase in the 2021 fourth quarter (see Exhibit 6), price growth in the US was still a robust 48% in the third quarter of 2022, according to insurance broker Marsh (Marsh & McLennan Companies, Inc., Baa1 positive). Pricing dynamics in the UK and continental Europe are similar.

Exhibit 6

Growth in cyber insurance prices has slowed but remains significant

Cyber insurance pricing change (quarterly data), 2020 – 2022



Data for continental Europe unavailable Q4 2020 to Q2 2021. UK data for Q4 2020 provided as a range between 25% and 30%.
Sources: Marsh, Moody's Investors Service

Thanks to the increased prices and heightened underwriting scrutiny, the US standalone cyber loss ratio among insurers declined to 65% at year-end 2021. For the first six months of 2022, Beazley, one of the largest cyber insurers, reported a cyber loss ratio of 49%, down from 69% at the end of 2021, likely reflecting improved profitability for the rest of the market. Barring a large systemic event, we expect insurers' profitability will improve in the year ahead. As profitability returns, more competition will enter the market, which will ease cyber capacity constraints and help stabilize prices. Nevertheless, insurers will likely remain highly cautious on pricing given the constantly evolving cyber threats.

Cyber insurance demand will continue to outweigh supply

Despite the hardening of the cyber insurance market, demand for coverage is growing, fueled by the rapidly changing threat landscape and increasing risk awareness among businesses and governments. The market is likely to grow to $22 billion by 2025 from around $9.2 billion at the beginning of 2022, according to Munich Reinsurance Company (Aa3 stable).

Nevertheless, we expect available cyber insurance capacity will continue to fall short of demand. The surge in ransomware claims in 2020 and 2021 prompted underwriters to significantly narrow the scope of their cyber coverage and tighten policy terms and conditions. Many insurers have been cutting cyber policy limits, while others have been introducing coinsurance, requiring policyholders to share the costs of a claim. Some carriers have introduced restrictions for certain highly exposed industries or for ransomware attacks.

At the same time, the underwriting process has become much stricter, making access to cyber coverage increasingly difficult. To buy insurance, companies need to meet more stringent cybersecurity requirements. While tightened standards incentivize insureds to enhance their cyber hygiene, some businesses with poor protection and limited resources to invest in security are at risk of becoming uninsurable and will need to find other ways to transfer cyber risk. Larger corporations that are most vulnerable to cyber risk are also increasingly likely to look for alternative solutions in response to limited coverage availability and costly premiums.

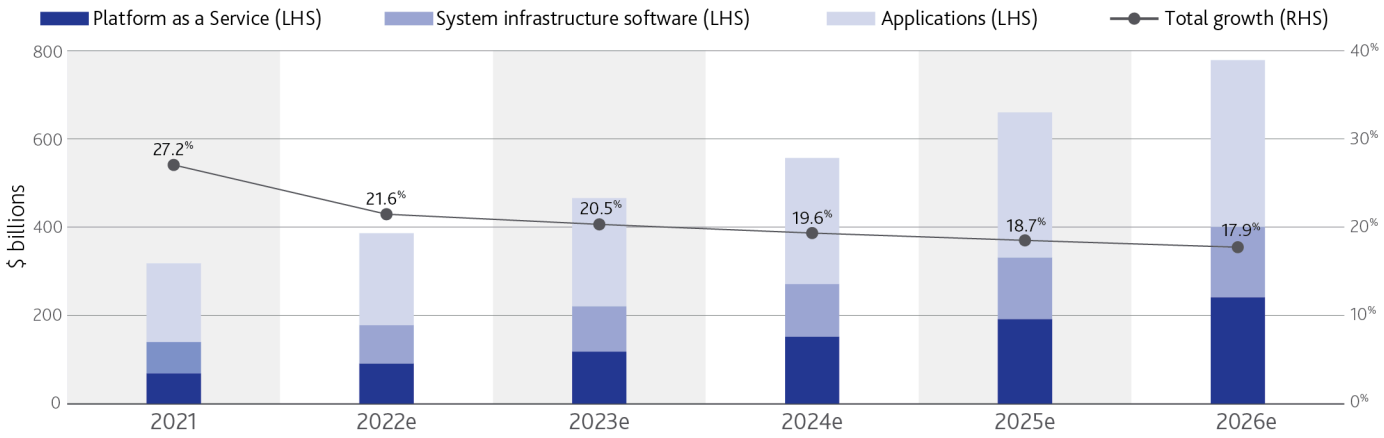
Cloud adoption will grow, but transfers only some of organizations' cyber risk

Growth in the adoption of one such cyber risk transfer alternative, public cloud services, will remain strong in 2023 (see Exhibit 7), supporting organizations' cyber resilience by leveraging the security expertise of sophisticated technology companies. Migration to the cloud will not, however, fully transfer customers' cyber risk responsibilities. Companies and governments will still need to ensure good security practices while monitoring the IT practices of their cloud providers.

Exhibit 7

Cloud growth will remain strong in 2023 and beyond

Revenue (LHS) and growth (RHS) for public cloud services, 2021-2026



Source: International Data Corporation

Failure to appropriately implement cloud security measures can result in cyber breaches. In some instances, intrusions occur because customers do not adequately protect their points of access to public cloud vendors. In others, compromised credentials or improperly configured security protocols enable attackers to gain access to organizations' networks and cloud accounts. In addition, application programming interfaces, which are used to exchange data or to access applications in the cloud, can be exploited for cyberattacks if not configured properly.

Business continuity is also a key consideration in cloud adoption. Large organizations mitigate exposure to cloud outages by deploying their IT infrastructure across a mix of on-premise facilities and cloud providers. Walmart Inc. (Aa2 stable), for example, is developing a system that will enable the company to switch seamlessly between Google's and Microsoft's cloud services and its own servers in real time, reducing the likelihood of a cloud outage causing material operational disruption.[11]

Quantifying financial impacts of cyber bolsters risk management decisions

Material cyber incidents can affect an issuer's credit profile, but proactively identifying which incidents will cause a sustained, negative financial impact can be challenging. Across the private and public sectors, boards and trustees will increasingly seek to financially quantify cyber risk, because a more rigorous, data-driven approach can identify material cyber incident scenarios and lead to better risk prioritization.

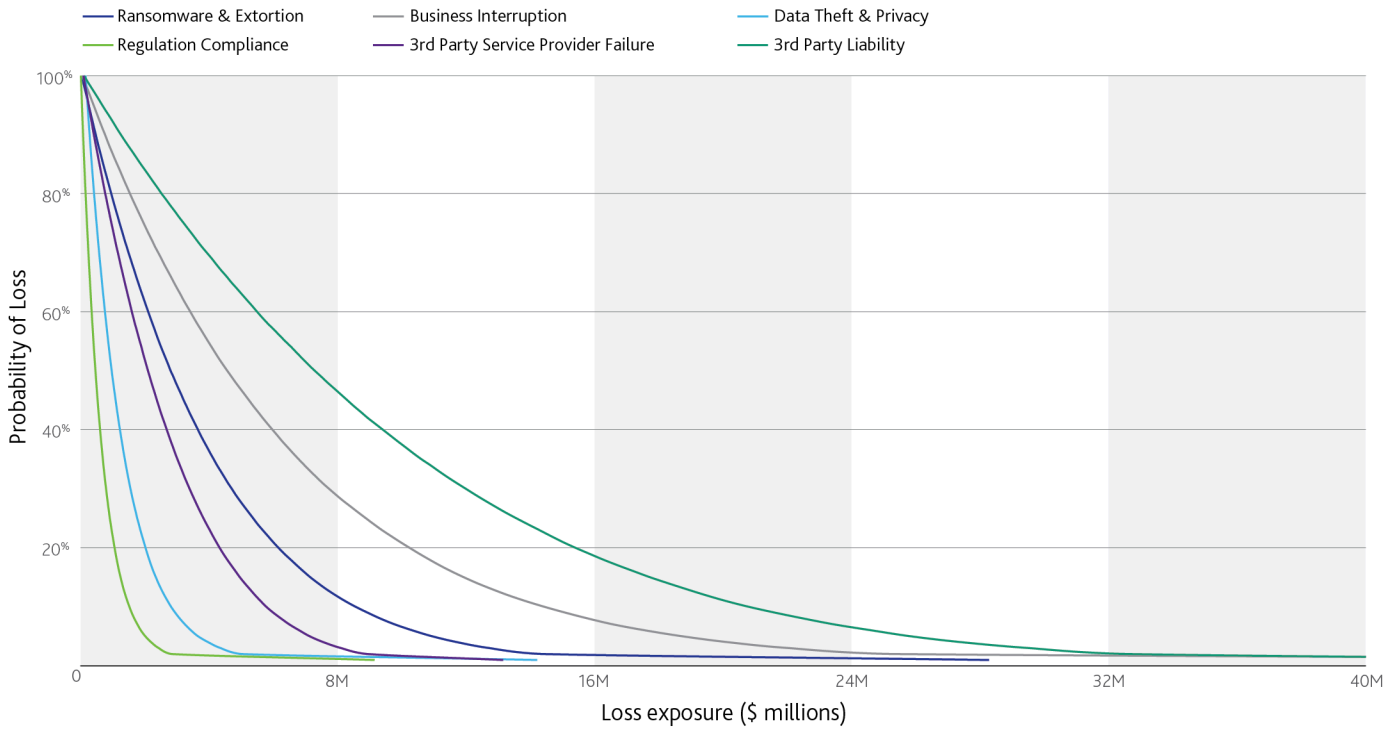
A consistent approach to quantifying the financial losses associated with cyber risk also enables better communication of risk mitigation strategies and exposure – to regulators, investors and other stakeholders. As a result, issuers' efforts to integrate these tools into their broader enterprise risk management (ERM) models is usually credit positive, though we recognize the complexity of quantifying scenarios as issuers digitize their operations.

Cyber risk quantification can provide insight into credit by identifying an amount of loss relative to an organization's revenues, assets, margins or reserves. Exhibit 8 shows how expected financial losses are calculated across different cyber scenarios. In this illustration, the risks around third party liability, defined as liability from a cyber incident targeting a vendor or supplier, clearly represents an area that warrants further evaluation. This insight would be of interest to an issuer's board and risk managers, who could prioritize resources accordingly.

Exhibit 8

Technical, threat and financial data can be combined to produce probabilistic loss curves based on different cyber scenarios

Single loss cyber exposure by impact scenario



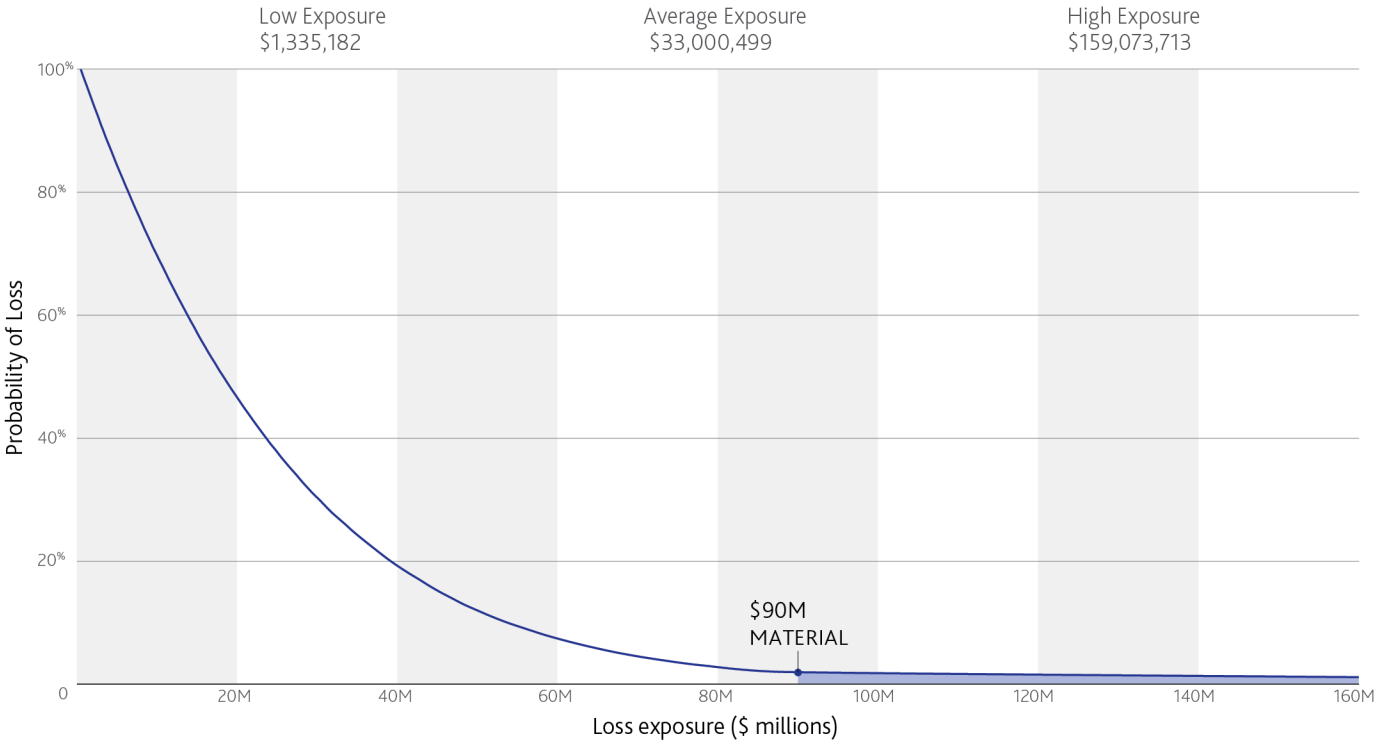
Source: BitSight

A quantitative approach to assessing cyber risk is also important in light of tougher disclosure requirements, in particular the SEC's proposed rules that base disclosure on materiality. Today, determining the materiality of a cyber incident is mostly a qualitative exercise, resulting in inconsistent disclosures. A more structured approach to losses, such as the loss curve illustrated in Exhibit 9, allows an issuer to weigh its expected financial loss exposure against its overall financial position, and drives more consistency across disclosure policies.

Exhibit 9

Weighing loss exposure against a company's financial position will make determinations of a cyber incident's materiality more consistent

Single loss cyber exposure



Source: BitSight

Moody's related publications

Outlook

» Cyber Risk: 2022 Outlook – Workplace shifts open new attack channels, while insurance costs rise and coverage narrows, November 2021

» Cyber Risk: 2021 Outlook – Cyber vulnerabilities in software supply chains, rising cost of ransomware will be key risks, January 2021

Heat map

» Cyber Risk – Global: Cyber heat map: Risks are rising, but many sectors are boosting defensive capabilities, September 2022

» Cross-Sector - Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019

Sector research

» Public Finance – US: Issuers face additional exposure to cyber risk through third-party software vendors, October 2022

» Cyber Risk – Europe: European cyber risk is rising; EU directive to foster resilience but take time, raise costs, October 2022

» Cyber Risk – US: Midterm election cyber threats expose federal, local governments to credit risks, October 2022

» Consumer Credit Services – US: Strong business profiles, balanced financial policies mitigate high social risks, September 2022

» Infographic: Healthcare is rich in cyber targets, poor in cyber defense, August 2022

» Government of Costa Rica: FAQ on the sovereign credit implications of recent cyberattacks, June 2022

» Clarion Housing Group Limited (UK): Recent cyberattack on Clarion highlights growing risks to the housing association sector, June 2022

» P&C Insurance – Global: Cyber insurers raise rates, narrow coverage as military conflict in Ukraine heightens risk, June 2022

» Cyber Risk – Global: Cloud adoption transfers some but not all of organizations' cyber risk, June 2022

» Cyber – Europe: New EU cybersecurity legislation is credit positive, June 2022

» Infographic: Retail and Hospitality industries attract a higher level of cyber incidents, but strong preparation has kept data breach costs low relative to other sectors, June 2022

» Infographic: Sub-Sovereign UK HAs cyber risk survey, May 2022

» Local Government – US: Legislation to ban ransom payments shows states' support in fighting cyber crime, May 2022

» Cyber Risk – US: SEC disclosure rules would improve transparency of cyber risk management, April 2022

» Banks – US: SEC's proposed cybersecurity disclosure rules would highlight banks' mature cyber risk management, March 2022

» Cyber Risk – Global: Broad sanctions against Russia raise risks of financially motivated cyberattacks, March 2022

» Insurance – Global: Russian invasion of Ukraine will drive investment volatility, more claims inflation, March 2022

» Infrastructure & Project Finance – United States of America: Passage of cyber legislation including reporting requirements is credit positive for the critical infrastructure sector, March 2022

» Global – Cyber Risk: Russia-Ukraine tensions increase cyber risks across regions, asset classes, February 2022

» Sovereigns – Europe: Energy ties raise risks, but credit impact from limited Russia-Ukraine conflict is low, February 2022

- Funds & Asset Management – North America: SEC's proposed cybersecurity rules would strengthen investment industry's cyber resiliency, February 2022
- Banking – Cross Region: Heightened focus on rising cybersecurity threats bolsters banking industry's preparedness, February 2022
- Cyber Risk – Global: Free and open-source software security flaws are a recurring source of cyber risk, February 2022
- P&C Insurance and Reinsurance – Global: Court ruling highlights risks of hidden cyber coverage in P&C policies, January 2022
- Banks – US: New rule requiring timely notification of cybersecurity incidents is credit positive, November 2021
- Cyber Risk – Global: New cyberattack targets technology supply chain, posing risks to affected entities, October 2021
- State and Local Government – US: Bipartisan infrastructure bill set to strengthen cybersecurity, a credit positive, August 2021
- Cyber Risk – Global: digitization, improving attacker capabilities leave critical infrastructure vulnerable, June 2021
- Hospitals - US: Healthcare cyber risk remains elevated given increasing reliance on technology, May 2021
- Cyber Risk – US : Cybersecurity executive order is credit positive, but disruptive for small software vendors, May 2021
- Midstream – North America: Colonial's suspension of pipeline operations shows sector's vulnerability to cyber risk, May 2021
- Higher Education – US: FBI warning for universities underscores vulnerability to cyberattacks, May 2021
- Cyber Risk – Global : Sunburst attack on public and private entities raises credit risks as extent of breach unfolds, February 2021

MIS cyber survey reports

- Cyber Risk – Global: Cyber risk survey of issuers finds growing investments, but gaps in preparedness, March 2022
- Healthcare – Global: Amid growing cyberattacks, healthcare survey shows moderate cyber strength, January 2022
- Services – N. America, EMEA: Cyber survey shows uneven cyber practices, despite risks, January 2022
- Cyber risk survey: regional and local government, December 2021
- Cyber Risk - Global: Banks of all sizes and credit strengths are increasing cybersecurity investment, November 2021
- Higher Education - Global : Cyber defenses improve across sector but stronger at larger and US-based universities, October 2021
- Technology, Media and Telecommunications – Global: Survey points to cyber strength across TMT, particularly in tech and telecom, July 2021
- Sovereigns – Global: Cyber risk survey indicates sovereigns define and rank risks differently, but preparedness is common priority, June 2021
- State and Local Government – US: Cybersecurity stronger among larger organizations, including states and transits, May 2021
- Insurers, Insurance Brokers and Asset Managers — Global: Survey signals cybersecurity strength, with some differences across sectors, regions, March 2021
- Banks – North America: Cybersecurity strength rests on governance and prevention, March 2021
- Electric Utilities – Global: Cybersecurity readiness depends on scale, business model and generation ownership, November 2020

Podcasts

- Moody's Talks - Emerging Markets Decoded - Costa Rica cyberattacks highlight key risk area as emerging markets move toward digitization, August 2022

» Moody's Talks - Inside Economics - The macroeconomics of cyberattacks, May 2022

» Moody's Talks - The Big Picture - Cyber risk's growing intersection with credit risk, May 2022

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.

Endnotes

1 RMS is a Moody's Analytics company

2 2022 SonicWall Cyber Threat Report (Mid-year Update), SonicWall, July 2022

3 Ransomware: Has Moscow given free rein to its cybercriminals in Latin America?, Valéry Rieß-Marchive, LeMagIT, May 12, 2022

4 Are Your Passwords in the Green?, Corey Neskey, Hive Systems, March 2, 2022

5 CISA kicks off cybersecurity awareness month, CISA, Oct. 1, 2021

6 Data Breach Investigations Report, Verizon, May 2022

7 Is Real-time Phishing Eliminated with FIDO?: Social Engineering Downgrade Attacks against FIDO Protocols, Ulqinaku et al, ETH Zurich and Carleton University, 2020

8 Why hacktivism came roaring back in 2021, Mikael Thalen, The Daily Dot, Dec. 16, 2021

9 The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015, Camille Singleton, IBM Security Intelligence, May 16, 2019

10 The New Era of Hacktivism – State-Mobilized Hacktivism Proliferates to the West and Beyond, Check Point, Sept. 29, 2022

11 Walmart amps up cloud capabilities, reducing reliance on tech giants, Aaron Tilley, The Wall Street Journal, June 23, 2022

REPORT NUMBER 1339484

Contacts

Nicky Vogt
AVP-Communications
nicky.vogt@moodys.com

Gerald Granovsky +1.212.553.4198
Senior Vice President
gerald.granovsky@moodys.com

Matthias Hellstern +49.69.70730.745
MD-Corporate Finance
matthias.hellstern@moodys.com

Steven Libretti +1.212.553.1826
Analyst
steven.libretti@moodys.com

Sarah Hibler +1.212.553.4912
Associate Managing Director
sarah.hibler@moodys.com

Jim Hempstead +1.212.553.4318
MD - Global Infrastructure & Cyber Risk
james.hempstead@moodys.com

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

MOODY'S
INVESTORS SERVICE