Corporates Up Their Cyber Preparedness As Cyber Attacks Become More Widespread

October 25, 2023

Keys Takeaways

- Threat actors predominantly target sectors with extensive and sensitive customer data or sectors that provide critical services, such as information technology (IT), telecommunications, media and entertainment, and retail. Yet, no sector is immune to cyber attacks.
- Our analysis indicates that data breaches and ransomware attacks are the most common types of cyber incidents.
- While a large proportion of cyber attacks are driven by phishing or employee errors, we noted that many cyber breaches arose from attacks on, or security lapses at, third-party vendors. This highlights the need for organizations to prepare more extensively for cyber risk that emanates from third parties.
- Given the scale and extent of business disruption arising from some recent cyber events, the financial impact is becoming more meaningful and leads to lower financial headroom under the credit metrics.
- While cyber incidents have not weakened business or financial risk profiles or directly resulted in negative rating actions, they increasingly have the potential to erode credit quality, accentuate other credit risks, and put downward pressure on credit ratings over a period of time.

PRIMARY CREDIT ANALYST

Raam Ratnam, CFA, CPA
London
+ 44 20 7176 7462
raam.ratnam
@spglobal.com

RESEARCH CONTRIBUTOR

Akshay Aggarwal
CRISIL Global Analytical Center, an S&P Global Ratings affiliate, Mumbai

LEAD CYBER EXPERT

Paul Alvarez
Washington D.C.
+1 2023832104
paul.alvarez
@spglobal.com

METHODOLOGY CONTACT

Nik Khakee
New York
+ 1 (212) 438 2473
nik.khakee
@spglobal.com

To identify common themes arising from cyber incidents, including the nature and type of cyber attacks, management teams' response and communication, and the impact of cyber attacks on credit quality, we analyzed certain cyber attacks that occurred since January 2022 on 75 of our rated non-financial corporates across the world. The data we used for our survey and analysis was based on publicly available information, management disclosures, our research, and press reports.

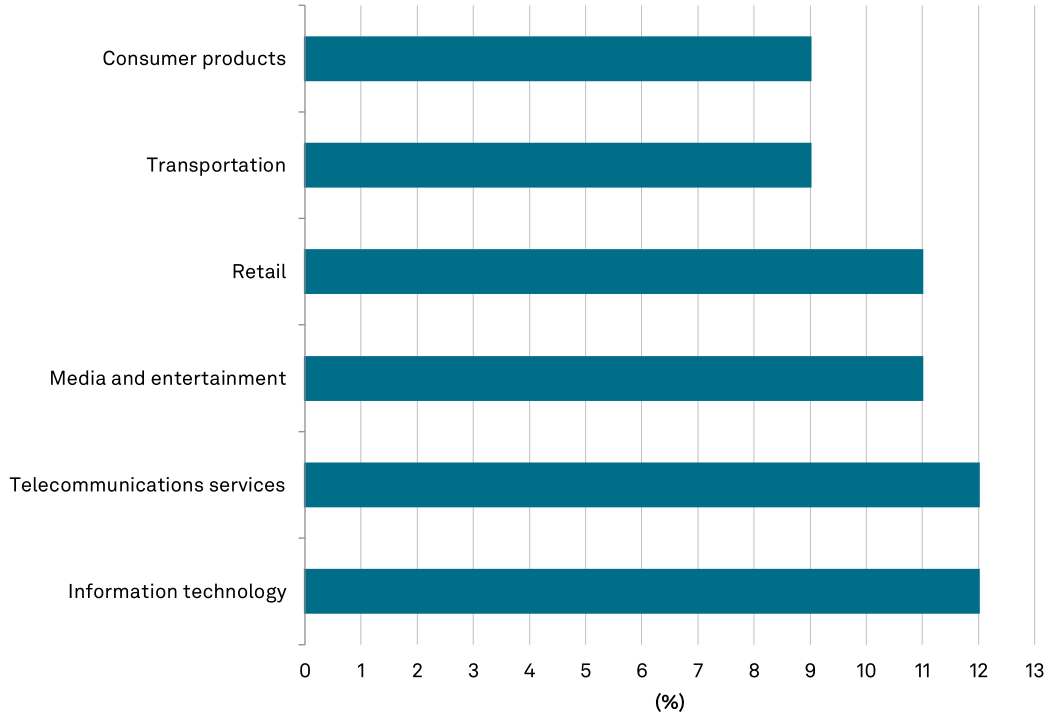
Cyber Risk Varies Across Sectors...

Sectors that process large amounts of data or provide critical services face heightened cyber risk. Yet, no sector is completely immune to cyber attacks. Our analysis of these 75 incidents revealed that the IT and telecommunications service sectors each accounted for 12% of cyber attacks, followed by media and entertainment (11%), retail (11%), consumer products (9%), and transportation (9%) (see chart 1).

Our survey results are similar to the findings of third-party reports, for example from Guidewire, which also showed that sectors such as technology, media and entertainment, retail, and restaurants are often more exposed to cyber risk than others. According to IBM Security's 2023 X-Force Threat Intelligence Index, the third-highest industry sector affected was what they refer to as the professional, business, and consumer services sector, which includes IT and media and entertainment. The report goes on to state that 18% of incidents involved backdoors (malicious software that provides a way for attackers to bypass security and access a compromised system) and ransomware attacks.

Chart 1

Sectors most impacted by cyber attacks



Source: S&P Global Ratings.
Analysis of certain cyber attacks that occurred since January 2022 on 75 of our rated non-financial corporates.

...And Regions

We currently witness a rise in cyber attacks across the globe. In the data we analyzed, the U.S. accounted for the highest proportion of cyber attacks, followed by Australia, and the U.K.

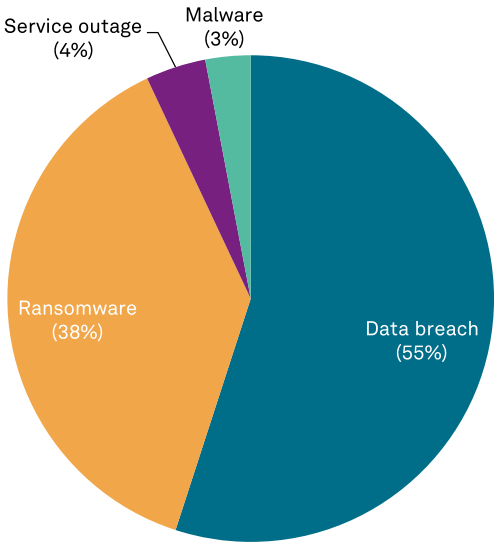
Cyber-related disclosure requirements are increasing worldwide, which will result in more companies having to report cyber events they previously would not have disclosed publicly. The introduction and enforcement of cyber security reporting will also enable financial market participants to better assess the impact of cyber attacks with more granularity. Reporting standards have evolved to improve the timeliness of market communication. For example, from Dec. 18, 2023, the U.S. Securities and Exchange Commission (SEC) will require public companies' to report material cyber security incidents on a Form 8-K (or Form 6-K for foreign private issuers) within four business days of materiality determination. Public companies will be required to describe the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact. Disclosures for risk management, strategy, and governance will be effective for all registrants for fiscal years ending on or after Dec. 15, 2023 (for more details, see "Cyber Risk Insights: New Regulations Will Increase Resilience, At A Cost," Aug. 3, 2023).

Data Breaches And Ransomware Are The Most Common Types Of Cyber Incidents

Our analysis showed that data breaches account for more than half of cyber incidents, followed by ransomware attacks (see chart 2). This aligns broadly with data from other sources, for example Verizon's 2023 Data Breach Investigations Report, which states that system intrusion represents the second most common type of security incident, just after ransomware attacks. We note that most of this activity occurred in the U.S., which aligns with corporate disclosures and news coverage. A recent report by cybersecurity company Malwarebytes stated that, with 43%, the U.S. accounted for the highest proportion of ransomware attacks globally between July 2022 and June 2023.

Chart 2

Cyber incident types



Source: S&P Global Ratings.
Analysis of certain cyber attacks that occurred since January 2022 on 75 of our rated non-financial corporates.

Monetary losses from data breaches have increased over the past few years. According to IBM Security's Cost of a Data Breach Report 2023, the global average cost of a data breaches reached $4.45 million in 2023--an all-time high and a 15% increase, compared with 2020. The report is based on data breaches experienced by 553 organizations globally between March 2022 and March 2023.

A high number of attacks happened through third- party vendors

While a large proportion of cyber attacks is typically driven by phishing or employee error, we have noted that many attacks were conducted through third-party vendors. Many cyber breaches arose from attacks on, or security lapses at, third-party vendors or service providers. Within our sample, about 15% of cyber attacks resulted from security vulnerabilities at third-party vendors, such as payroll and recruitment service providers. This highlights the importance of surveilling third-party vendors' cyber hygiene policies and practices. When dealing with third-party vendors, organizations must have end-to-end cyber policies, including onboarding, monitoring, and detection policies.

Our Take On Cyber Incidents From A Credit Perspective

We leverage our interactions with the management of our rated companies to identify their cyber security preparedness, including their commitment and prioritization of cyber security in their overall risk management efforts. When we become aware of cyber incidents at our rated issuers, we engage with management teams to identify and analyze how they respond to the incident. Within the context of ratings, we focus on elements of cyber security that are relevant and material for the assessment of credit risk for the rated company.

We aim to understand the various structural and operational steps companies take to contain the risks from the cyber incident, solidify their defenses, and prevent future attacks. Based on our assessment of recent cyber incidents and our interactions with various management teams, we identified four common themes and key areas that are important from a credit perspective (see chart 3).

Chart 3

Key takeaways from recent cyber incidents

Business impact

- Operations disrupted
- Containment measures
- Manual workarounds or partial service levels
- Reputational risk and brand damage

Communication

- Extensive investigations
- Comply with external reporting rules
- Inform and update diverse stakeholders
- Employee business process updates

M&G

- Reduce management bandwidth
- Multiple external and internal parties involved
- Enhance cyber security framework
- Expand employee training and awareness to cover new risk areas

Financial impact

- Increase in opex and capex spend to implement remediation program
- Cyber insurance–loss recovery and exclusions
- Financial position and liquidity
- Regulatory fines or litigation risk

M&G--Management and governance. Opex--Operational expenditure. Capex--Capital expenditure.
Source: S&P Global Ratings.

Business impact: Operational disruption is becoming more prevalent

We have observed an increase in the number of attacks against companies' core business processes and operations. This has a negative effect on business operations, either because threat actors directly target critical systems or because companies often shut down their systems to contain or limit the impact of the attack. In such cases, companies resort to manual workarounds or processes to continue servicing customers and to prevent longer-term reputational or brand damage. Well laid-out business continuity and thoroughly tested disaster recovery plans can help management teams significantly to continue servicing consumers using alternative workarounds or manual business processes.

Recent Case Study Examples Of Operational Disruptions From

Cyber Incidents

- Following the data breach in September this year, casino giant MGM Resorts International (MGM) took steps to protect its systems and customer data, including shutting down certain systems. The company believes these steps prevented the criminal actors from accessing any customer bank account numbers or payment card information. Yet, they led to disruptions at some of MGM's properties. For example, the company's website was down and customers had to call to make hotel and dining reservations at MGM's casino resorts across the U.S. It took nearly two weeks to restore the online reservation system.
- In the case of the cyber attack against cleaning products maker Clorox, also in September, the management team took certain systems offline and processed work manually. As a result, less orders were processed and some retailers ran out of Clorox products.
- The Aspen Group also experienced revenue losses from the temporary shutdown of its Aspen Dental operating systems after a cyber incident in April 2023.

Communication: A tricky balancing act

Keeping all stakeholders up to date in the aftermath of a cyber attack is a key aspect for senior management teams. In many cases, it takes them several weeks or even months to complete their investigations. During this time, they need to communicate timely and openly, as regulations in the U.S. and Europe demand that management ensure timely disclosure to market participants. At the same time, management needs to minimize the risk of unintentionally compromising ongoing investigations. If personal details of employees or customers are compromised, management teams have to communicate in a more detailed and timely manner to minimize longer-term impacts and limit the extent of fines or legal actions.

Management and governance: Cyber events test contingent risk management

Management teams' ability to deal with cyber events reflects their proficiency in contingent risk management. Those teams that lack dedicated resources, attention, or preparedness often find themselves ill-equipped in the face of cyber attacks, not least since cyber incidents can be exceedingly time-consuming. The complexity of dealing with cyber events eats into management's bandwidth and takes time away from operational priorities. Stricter regulations mean that an increasing number of management teams seek assistance from external cyber security experts, IT consultants, and law firms. We believe the level of cyber risk preparedness is uneven across corporate issuers and sectors and will become increasingly important in our analysis of issuers' management and governance. For companies with weak or limited focus on cyber preparedness, a cyber breach is an unwelcome wake-up call. After experiencing a cyber incident, it is not surprising that many management teams increase their cyber security budgets. We also observe that companies focus on reengineering their business processes, strengthening firewalls, and augmenting their cyber defenses. As many cyber incidents arise from employee error and oversight, quite often system defenses have to be supplemented by employee technical training to increase cyber risk awareness and implement practical steps to improve cyber hygiene.

Management and employee appreciation of the importance of cyber preparedness increases during and when assessing lessons learned from simulation and scenario-based games, which replicate the potential impact of cyber disruptions, serve to train employees, and test the resilience of disaster recovery plans.

Financial impact: Increase in visibility and extent

Given the extent of business disruption arising from some recent cyber events, the visibility and extent of cyber events' financial impact is increasing. Very few companies fully quantify the impact of cyber events in detailed monetary terms. Manufacturing companies could typically recoup production losses or lost orders over a few months or quarters, but the potential financial damage from the hit to brand reputation, which results from weaker service levels, is difficult to quantify and is only likely to become apparent over the long term. Compensation from cyber insurance claims is typically not extensive enough to fully offset the financial impact of business disruption and subsequent remedial spend. Protracted investigation times, remedial actions, regulatory fines, legal appeals, and potential litigation claims can make the financial quantification of cyber attacks even more complex and time-consuming.

Recent Case Study Examples Of The Financial Impact From Cyber Incidents

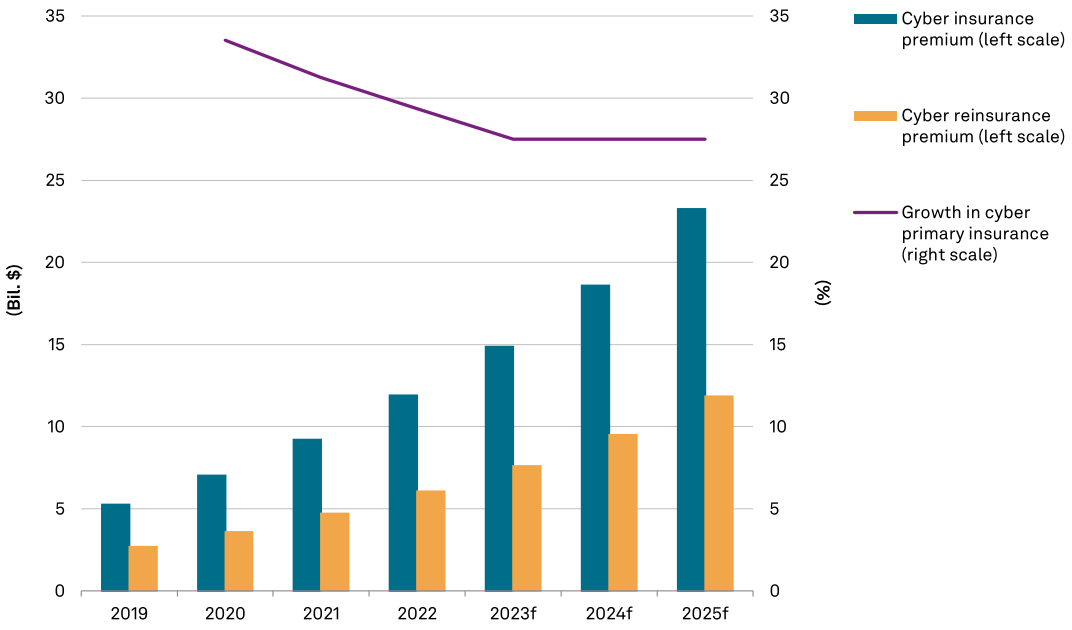
- MGM estimates the operational disruptions it experienced at its properties in September will constrain third-quarter 2023 domestic property EBITDAR by $100 million, predominantly in its Las Vegas operations. This reflects approximately 10% of the company's third quarter 2022 EBITDAR.
- Clorox expects a material negative impact on earnings and cash flow in at least the first fiscal quarter ending Sept. 30, 2023. However, we believe the event has now been contained and assume Clorox will successfully restart operations without a permanent adverse impact to its reputation and earnings strength. We expect replenishment orders from retailers will effectively shift a portion of the lost sales in the first quarter to later periods. Nevertheless, the company is still evaluating the business and financial impact from the attack.
- The Aspen Group: We now anticipate the incident will lower the company's revenue and EBITDA by about $120 million and $110 million, respectively, compared with previous estimates of about $90 million and $60 million, respectively.
- MKS Instruments Inc.: The ransomware incident in February 2023 had a total revenue impact of $160 million, of which $120 million has been recovered, with the remaining amount expected to be recovered in the third quarter.
- Even though Germany-based Metro AG, which is Europe's largest food wholesale and delivery operator, experienced a cyber attack in October 2022, it expects to incur up to an additional €50 million in cyber security costs in fiscal year 2024.

Corporates Increasingly Use Cyber Insurance

We see a trend that companies increasingly opt for cyber insurance to manage their exposure to cyber risks and offset costs from cyber incidents. Global cyber insurance premiums reached about $12 billion in 2022 and, in our view, will likely increase by an average of 25%-30% per year to about $23 billion by 2025 (see chart 4 and "Global Cyber Insurance: Reinsurance Remains Key To Growth," Aug. 29, 2023).

Chart 4

Cyber remains on a fast track
Global cyber (re)insurance premium



f--Forecast. Sources: Munich Re, S&P Global Ratings.

Cyber insurance providers can play a vital role in improving companies' cyber resilience. It is not uncommon that insurance companies demand minimum cyber hygiene standards as prerequisite for insurance coverage. This could help improve corporates' cyber security in the long term. Increasing complexity means companies need to be cognizant of exclusions in their cyber security coverage. Many insurance providers change terms to restrict coverage for systematic risks--such as compromised software infrastructure or cyberattacks that are deemed as acts of war--increase retention levels for corporates, or introduce coinsurance requirements for ransom payments, which could make it more challenging for companies to get full compensation. Additionally, more insurers raise their minimum cyber hygiene standards for policyholders, which further increases cyber-related costs for issuers.

Cyber Attacks Did Not Lead To Immediate Rating Actions

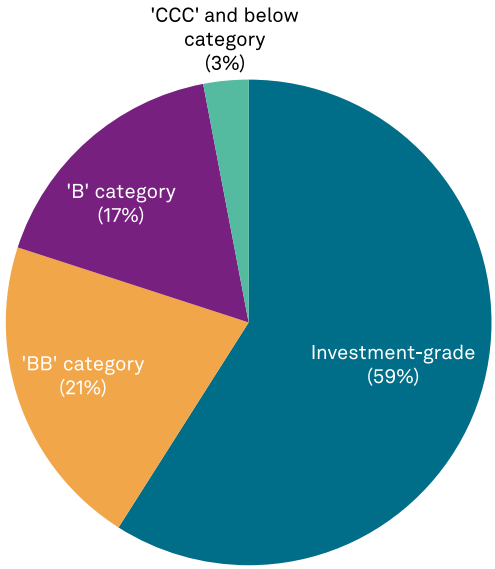
In our analysis of cyber events, we noted that cyber attacks didn't have a direct impact on ratings or outlooks in our rated corporate universe between January 2022 and now.

Yet, they can put downward pressure on companies' credit quality over a period of time. While not a material driver of credit rating actions to date, we note the rising nature of the threat, both in terms of frequency and monetary impact.

About 59% of the cyber attacks we recorded in our analysis focused on investment-grade companies and the remaining 41% on speculative-grade issuers (see chart 5). Additionally, we believe the potential for rating impact from cyber risks is accentuated for lower-rated speculative-grade companies since they typically have limited financial resources to absorb the fallout of a high-impact cyber attack.

Chart 5

Distribution of cyber attacks on rated companies



Source: S&P Global Ratings.

All the issuers who experienced cyber incidents to date in the sample that we analyzed had sufficient financial buffers to deal with the attack. This is mainly because monetary losses, such as ransomware or litigation payments, have been relatively modest so far, compared with issuers' financial resources. Expenses that arose in the aftermath of cyber attacks--including costs to remediate the incident, provide additional customer support, and hire cyber security experts--were so far manageable and did not have an material effect on organizations' liquidity or

earnings. In our analysis of these events, no cyber attack against any company we rate induced us to lower our assessment of these companies' financial risk profiles or liquidity modifiers.

Nevertheless, cyber attacks that target key operations or business processes are starting to result in revenue loss and increasing costs to resume full operability. In some cases, these are becoming quite meaningful or diminish financial headroom under the credit metrics, together with other operating pressures.

In addition to financial outflows for ransomware payments and regulatory fines, organizations are increasingly exposed to the potential longer-term impacts of cyber attacks. These include business interruption or reputational damage, which could have more severe and longer-lasting consequences on revenue, customer trust and attrition, business relationships, and companies' competitive positions. These are harder to quantify and often only materialize over a longer period. With the rising number, increasing sophistication, and frequency of cyber attacks, we believe cyber risk represents a growing threat and will likely pose greater downside risks to credit ratings in the coming years.

Related Research

- Stay Vigilant: Highlights From The Cyber Risk Seminar 2023, Oct. 20, 2023
- Global Cyber Insurance: Reinsurance Remains Key To Growth, Aug. 29, 2023
- Cyber Risk Insights: New Regulations Will Increase Resilience, At A Cost, Aug. 3, 2023
- Perspectives On Cyber Risk Across Corporates: The Potential Impact Of Cyber Threats Is Growing, Nov. 7, 2022
- How Cyber Risk Affects Credit Analysis For Global Corporate Issuers, March 30, 2022

Appendix

Recent cyber incidents we covered in our publications

Name	Sector	Country	Rating	Outlook	Extracts from our publications
Johnson Controls International PLC	Building Materials	Ireland	BBB+	Stable	"The timing of the attack, near JCI's fiscal year end, could affect the timing of its financial disclosures, although a delayed filing itself may not affect our view of its credit quality."
Clorox Co.	Consumer Products	U.S.	BBB+	Stable	"Clorox reported widescale disruption to its operations and expects a material negative impact on earnings and cash flow in at least the first fiscal quarter ending Sept. 30, 2023."
Caesars Entertainment Inc.	Hotels & Gaming	U.S.	B+	Stable	"While we don't expect Caesars' financial position to be materially affected by the breach, it is more difficult to quantify the potential reputational risk. The scope of the breach is massive and Caesars relies upon its loyalty program to sustain its substantial ability to attract loyal guests to its properties."
MGM Resorts International	Hotels & Gaming	U.S.	B+	Stable	"We will monitor the potential credit impact of the cybersecurity breach as events evolve over the next several weeks."

Recent cyber incidents we covered in our publications (cont.)

Name	Sector	Country	Rating	Outlook	Extracts from our publications
ADMI Corp.	Health Care	U.S.	B-	Negative	"..we do still attribute some risk that additional cyber event-related losses or incremental costs to bolster its defenses may further impede operating performance over the near term."
Barracuda Networks Inc.	Information Technology	U.S.	B-	Stable	"...and released containment and remediation patches and recommended all impacted customers isolate and replace compromised appliances."
Zellis Holdings Ltd.	Information Technology	U.K.	B-	Stable	"We do not foresee ransomware group Clop's cyber-attack materially affecting Zellis' fiscal 2024 financials. "
MKS Instruments Inc.	Information Technology	U.S.	BB	Stable	" We note that the ransomware incident in February had a total revenue impact of $160 million, of which $120 million has been recovered with the remaining expected to be recovered in the third quarter."
Maximus Inc.	Business & Consumer Services	U.S.	BB+	Stable	"The company believes that sensitive personal information of 14.5 to 17.5 million individuals has been compromised, and it currently estimates a total cost of about $22 million associated with the incident. Class action lawsuits have already been filed against the company in relation to this incident. "
ION Trading Technologies Ltd.	Information Technology	Ireland	B-	Stable	"The recent cyber attack had a limited financial impact, but ION Trading could be exposed to reputational damage in the longer term."
Dish Network Corp.	Media & Entertainment	U.S.	CCC+	Negative	"The recent cyber attack furthers cash flow uncertainty."
Coca-Cola Femsa S.A.B. de C.V.	Consumer Products	Mexico	A-	Stable	"The cyberattack did not fully breach its security systems, but breached some of its safeguard layers."

This report does not constitute a rating action.