Moody's Analytics

Cyber Risk and Creditworthiness: **A New Era of Risk Assessment**

Understanding the New Norm: **Why Cyber Threats are Central to Today's Risk**

Authors:
Eefje van Craen
Bill Weiss
Frank Hommersen

Many companies we've worked with in the past didn't prioritize credit checks on potential customers until they suffered their first significant bad debt loss.

Despite hearing about financial distress and insolvency in other companies, their own extended history without such incidents made them resistant to change. This pattern may also apply to trade credit managers dealing with cyber risk. High-profile cyber-attacks, are widely reported, but most remain unpublicized. Consequently, many might only begin to take cyber threats seriously after a direct experience with a customer or supplier falling victim to such an attack.

Cyber risk poses a multifaceted challenge for businesses worldwide. Beyond the immediate concerns of data breaches and system failures, cyber incidents can have long-term repercussions on a company's creditworthiness.

As recent events and research indicate, companies, both big and small, need to recognize the profound impact of cyber threats on their financial stability and reputation. Bad actors are getting smarter and new technology such as Generative Artificial Intelligence (Gen AI) is making ransomware attacks and phishing schemes easier to deploy. These advanced, evolving schemes are expected to lead to an increase in cybercrime.

Key effects of cyberattacks that can influence the cash flow of a company:

1. Financial Losses
2. Operational Disruption
3. Regulatory Penalties
4. Recovery Costs
5. Reputation Damage
6. Litigation
7. Insurance Premiums
8. Supplier and Customer Relationships

Financial **Losses**

Understanding the expenses associated with data breaches sheds light on the consequences of data breaches, which can result in direct financial repercussions in various ways.

One significant avenue through which companies may incur financial losses during a cyber-attack is through ransom payments. In ransomware attacks, cybercriminals encrypt a company's data and demand ransom for the decryption key. The cost of these ransoms can vary widely, from thousands to millions of dollars. Paying the ransom is a complex decision, and companies may weigh the cost of the ransom against the potential cost of not regaining access to critical data, considering factors like data value, legal obligations, and reputational damage. Paying the ransom, however, does not guarantee data recovery, and companies may still incur further costs in recovery efforts. If attackers steal funds or sensitive financial information, it can result in immediate monetary losses, affecting the company's cash flow.

As reported by Wall Street Journal[1], Clorox has reportedly spent $25 million in costs directly related to its recent cyberattack with more to come.

[1] *Clorox Warns of a Sales Mess After Cyberattack*

Operational **Disruption**

Cyberattacks often disrupt a company's operations. If critical systems or data are compromised, the business may not be able to function properly, resorting to manual processes. Downtime can result in lost sales, production delays, and increased operational costs, all of which can impact working capital. As reported by Reuters[2], MGM expects to lose $100 million, as a result of their recent ransomware attack.

[2] *Casino giant MGM expects $100 million hit from hack that led to data breach*

Regulatory **Penalties**

Breaches of data protection laws and regulations during some cyber-attack offensives can lead to substantial fines and penalties for the company. These financial penalties can strain cash flow resources. For example, as part of a settlement with Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories, related to their 2017 data breach, Equifax agreed to pay up to $700 million, according to the FTC[3].

[3] *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*

Recovery **Costs**

After an incident, a company must invest in cybersecurity measures, incident response, and recovery efforts all at once. These costs can be substantial, and they can quickly deplete available cash reserves. For example, according to its Securities & Exchange Commission (SEC) Form 8-K filing[4], T-Mobile committed to an aggregate incremental spend of $150 million for data security and related technology in 2022 and 2023, following their 2021 cybersecurity incident.

Reputation **Damage**

Leading to a loss of customers or reduced sales, a data breach can tarnish a company's reputation. Restoring trust and rebuilding the customer base takes time and requires significant marketing and public relations efforts, which in turn can strain cash flow. For example, the Buzz Score (an indication of how negative or positive people feel about a brand) for a company dropped points in the initial days after a data breach was publicized.

[4] *SEC Form 8-K Filing*

Litigation

In some cases, affected parties may take legal action against a company following a cyberattack, seeking compensation for damages. Legal fees and settlements can have a significant financial impact.

Insurance **Premiums**

If a company has cybersecurity insurance, filing a claim after the incident can lead to increased insurance premiums in the future. These higher premiums can add to ongoing operational costs and affect working capital.

Supplier and Customer **Relationships**

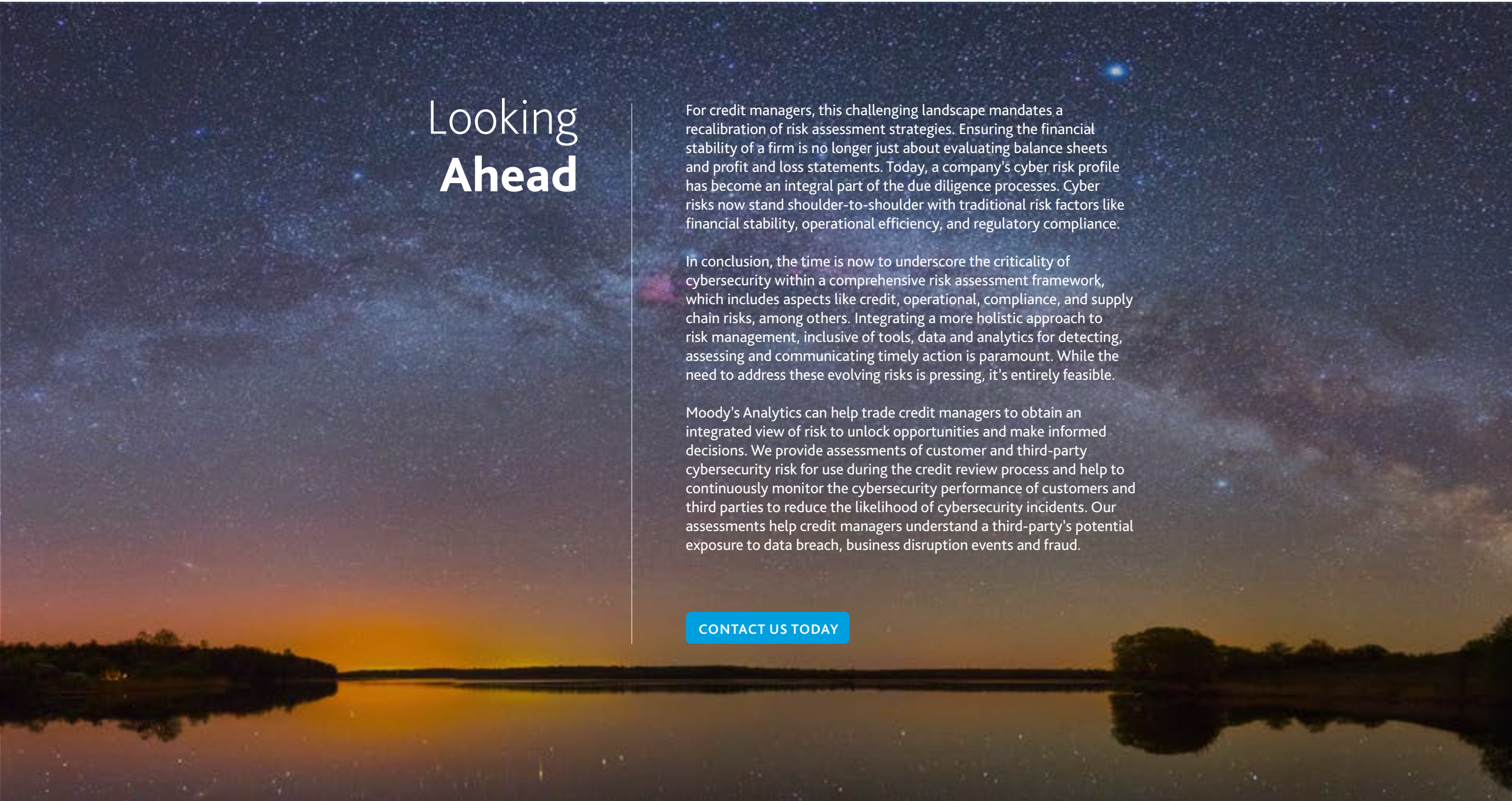
A cyber incident can disrupt relationships with suppliers and customers. Suppliers may require stricter payment terms after a breach. Customers may delay or cancel orders, impacting cash flow. The converse is also true - a cyber incident from a supplier could also impact the company and its ability to meet its own obligations to customers.

Looking at the broader landscape, the connection between a company's cyber hygiene and its creditworthiness becomes evident. Companies that don't take preventive cybersecurity measures can exhibit higher risks of payment defaults, establishing a direct link between their cybersecurity postures and financial stability. Such patterns make cybersecurity not just an IT concern but a significant driver of corporate governance and managerial competence.

Our recent whitepaper, authored by Alejandra Caro Rincon and Gustavo Ordonez, titled **'The impact of cybersecurity management practices on the likelihood of cyber events and its effect on financial risk'** [5]**, found that:**

1. There is a strong correlation between the quality of cybersecurity practices and the probability of a reported cybersecurity event
2. Certain industries, such as Finance, Healthcare, and Technology exhibit relatively higher risk of cyber related financial losses
3. Larger companies face an elevated risk and impact of security events compared to smaller
4. Significant negative effects of cyber incidents on firm value, include severe events leading to persistent negative equity returns over a 12-month period
5. Potentially material financial implications of cyber risk, highlights the importance of cybersecurity in a complete integrated risk assessment

[5] *The impact of cybersecurity management practices on the likelihood of cyber events and its effect on financial risk*



Looking **Ahead**

For credit managers, this challenging landscape mandates a recalibration of risk assessment strategies. Ensuring the financial stability of a firm is no longer just about evaluating balance sheets and profit and loss statements. Today, a company's cyber risk profile has become an integral part of the due diligence processes. Cyber risks now stand shoulder-to-shoulder with traditional risk factors like financial stability, operational efficiency, and regulatory compliance.

In conclusion, the time is now to underscore the criticality of cybersecurity within a comprehensive risk assessment framework, which includes aspects like credit, operational, compliance, and supply chain risks, among others. Integrating a more holistic approach to risk management, inclusive of tools, data and analytics for detecting, assessing and communicating timely action is paramount. While the need to address these evolving risks is pressing, it's entirely feasible.

Moody's Analytics can help trade credit managers to obtain an integrated view of risk to unlock opportunities and make informed decisions. We provide assessments of customer and third-party cybersecurity risk for use during the credit review process and help to continuously monitor the cybersecurity performance of customers and third parties to reduce the likelihood of cybersecurity incidents. Our assessments help credit managers understand a third-party's potential exposure to data breach, business disruption events and fraud.

CONTACT US TODAY

Moody's
ANALYTICS