Understanding and Planning for the Corporate Risk Landscape

Dataminr®

It's all hands on deck inside the situation room at a major American retailer. A Category 5 hurricane is cutting up the Gulf of Mexico, and is projected to make landfall in the U.S. within hours.

Real-time information flows into the room, and gets delivered to the group at the same time, serving as the catalyst for quick, coordinated decisions. Leaders from every responsible department are here, with clearly defined roles and a common goal: Mitigate risks to people and assets, predict business needs, maintain operational continuity and recover as quickly as possible.

Think back to the last time your company mitigated an emerging risk. Did it resemble a well-oiled situation room, or was the experience a disjointed blur of actions? More importantly, is your company prepared to handle its next crisis?

The average large enterprise mitigates multiple risks every year, borrowing elements from the situation room—real-time information flows into the company and is shared across a small group of stakeholders, who work together and are empowered to make quick decisions.

Modern risk management is a highly collaborative exercise. Forward-thinking companies know that risk management cannot be confined to a single department or performed on an ad hoc basis inside operational silos—ownership of risk must be shared across the enterprise.

COVID-19 EXPOSES RISK MANAGEMENT GAPS

In early 2020, the COVID-19 pandemic plunged the planet into the first global, simultaneous risk management exercise since the dawn of the information age. Companies experienced risk vectors from multiple angles, requiring coordinated decisions from across the organization:

- How do we protect the health of our employees and customers?
- When do we close our offices?
- Do we have the IT infrastructure in place to support a rapid shift to remote work?
- Do we lay off nonessential employees? Furlough workers, or ask employees to take pay cuts?
- When do we close our retail locations, contact centers and warehouses?
- How do we pivot our business model to preserve cash flow?
- How do we maintain business continuity, and continue to serve our customers?
- How do we maintain supply chains amid mandatory quarantines?
- How do we protect the enterprise against cybercrime and pandemic-related ransomware?
- When do we reopen, where do we reopen and how?
- How do we stay informed about the federal, state and local regulations related to COVID-19 in the geographies that we operate in?
- Do we renegotiate our leases? Break our leases? Sell assets? Apply for loans?
- How do we protect our channel partners?
- How do we foster employee engagement and productivity amid unprecedented personal tragedy?
- How do we protect our brand reputation?

COVID-19 continues to serve as a good test of every company's risk management framework. Evaluating your company's response today can help you put the policies in place to better prepare for future risks.

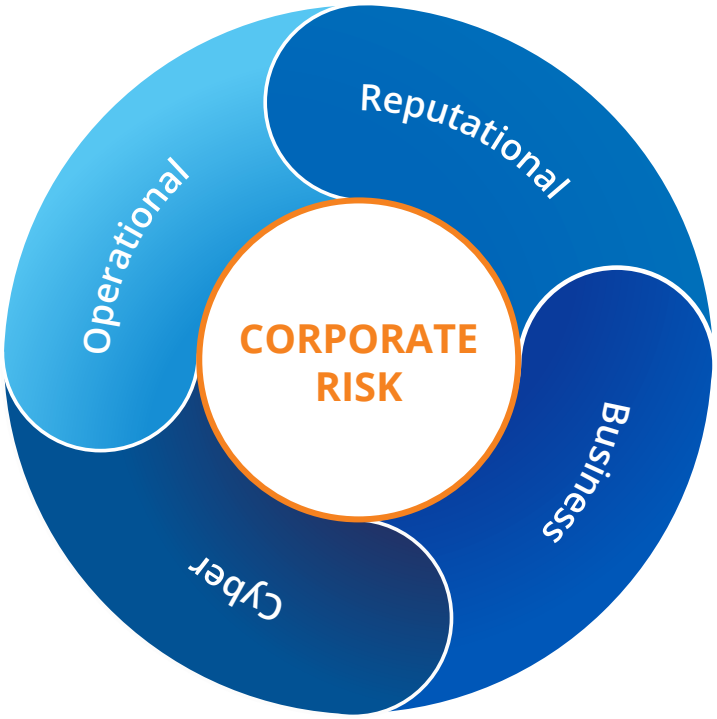
NAVIGATING THE CORPORATE RISK LANDSCAPE

Modern corporate risk can be broadly categorized into four segments: Operational risk, reputational risk, business risk and cyber risk.

Inside each quadrant, additional sub-categories of risk exist. For example, inside the operational risk quadrant, there's asset protection, executive protection, physical security, travel safety, human health, risks to logistics and deliveries, and more.

Risk management is a shared exercise, reaching into every corner of the company. Every department has clearly-defined ownership of their area of responsibility, allowing for rapid, coordinated response during a crisis.

Real-time information about potential risks must be shared across the enterprise, allowing functional owners to assess risk from their unique point of view. Eliminate information bottlenecks by democratizing access to information about emerging risks.



THE VALUE OF COORDINATED RISK MANAGEMENT

From the outside, well-coordinated risk management looks seamless and unified: A company experiences a risk event, communicates clearly about its impacts and action plan, acts on the plan and reports back once the risk has been mitigated.

Anyone who has worked on a corporate crisis team will tell you that the work behind the scenes is complex, fast and deeply collaborative. Crisis response plans need to be tested regularly. Uncoordinated responses are glaringly obvious to the public, and can permanently damage a company's brand reputation.

Consider the case of 7-Eleven Japan, which invested a considerable amount of time and money building and marketing a new mobile payments service, in a country where four out of five transactions are still paid for in cash.

In July 2019, the company launched 7Pay at some 21,000 convenience stores across the country, signing up 1.5 million people in its first few days. But the service contained serious security flaws , and within hours, people took to Twitter to warn others not to sign up for the app.

Despite those early warnings from the public, it took 7-Eleven Japan two days to act, temporarily taking 7Pay offline and halting new user signups. By that point, hackers had compromised the accounts of 808 people, stealing ¥38 million (roughly US $353,000).

The company's president apologized, and 7-Eleven Japan permanently closed the app a month later, amid a crisis in consumer confidence in the technology.

BEST PRACTICES

Build risk management plans that describe clear roles and responsibilities and coordinate a unified response to risk

Risk management must evolve beyond ad hoc actions taken by individual departments, toward a holistic view of risk that involves multiple stakeholders inside the enterprise. Individual departments must have clearly defined swim lanes mapped to their spheres of responsibility, so that when a risk occurs, the response is orderly and efficient.

Build plans that anticipate probable risks your company will likely encounter in the future, and regularly simulate risks with stakeholders.

Real-time information forms the cornerstone of effective risk management

Relevant, up-to-date information is a crucial input to risk mitigation. No matter what the crisis, getting an accurate picture of the size and scope of the crisis is necessary to making better-informed business decisions.

Especially for global enterprises, information on an event breaking thousands of miles from headquarters could help influence a critical decision that affects operations in multiple countries and regions. But for those employees and clients in the immediate vicinity of a breaking event, a hyperlocal view of the incident as it unfolds is also crucial for sound decision-making.

This is particularly important for travel safety during a quickly-developing emergency. Corporate security teams use real-time alerts—which are often significantly ahead of official reports—to discover unpredictable, emerging threats, and communicate with employees and executives nearby who might be affected by the incident.

Dataminr delivers real-time alerts on emerging risks to hundreds of the world's largest companies, journalists and public agencies. The company's artificial intelligence platform processes billions of units of public information every day, searching for early indicators of potential risk.

Democratize data access, allowing functional owners to assess risk from their unique point of view

Make sure the functional owners of risk inside your company have equal and consistent access to real-time information. In many companies, information is gathered and processed in silos, creating artificial bottlenecks to action.

Security operations centers are often at the forefront of incoming information, picking which alerts to surface internally. In practice, that results in slower response times and a lack of alignment inside the enterprise.

Every department should get real-time information that's tailored to their specific business needs, sharing the responsibility of risk detection across the enterprise.

To illustrate the impact of an information bottleneck in action, consider the case of the credit reporting giant Equifax, which discovered evidence of a serious cybersecurity breach on July 29, 2017.

On Aug. 1, four senior Equifax executives, including the company's chief financial officer, sold $1.8 million worth of shares. The company launched an internal investigation that guaranteed an embarrassing outcome no matter what they found—either the executives had engaged in insider trading, or had not been notified that a serious cybersecurity breach had occurred.

The board ultimately found that information about the breach had not been universally shared across the leadership team. The four executives in question had no idea that their company was in trouble when they ordered the stock sales.

Every organization navigates their risk landscape differently, depending on the organization's size, industry and the nature of the crisis they're facing.

Emerging risks can pose profound operational challenges when not managed proactively. Risk management needs to be a shared responsibility across the enterprise. Teams must share a common view into the specific details around a crisis, and use real-time information as a group to make better business decisions.

Learn more at
https://www.dataminr.com/corporate-risk

Dataminr®