Understand and Plan for the Corporate Risk Landscape

Forward-thinking organizations know that risk is everybody's business. It cannot be confined to a single line of business or performed on an ad-hoc basis within operational silos. Ownership of risk must be shared across the enterprise and be deeply collaborative and transparent.

We know this to be true given the current volatility of global markets and the hard-learned lessons from 2020 and 2021, all of which significantly disrupted our economic, business and social ecosystems.

In an ideal world, the real-time information required to effectively manage and mitigate such disruptions and risk—including cyber, business, operational and reputational—would flow into a company and be shared across a well-defined group of stakeholders who work together and are empowered to make quick, well-informed decisions.

While not every organization has achieved this ideal state, it's a goal that all should work toward if they are to successfully navigate our now unpredictable, fast-changing world—and the expanding threat landscape that has materialized as a result.

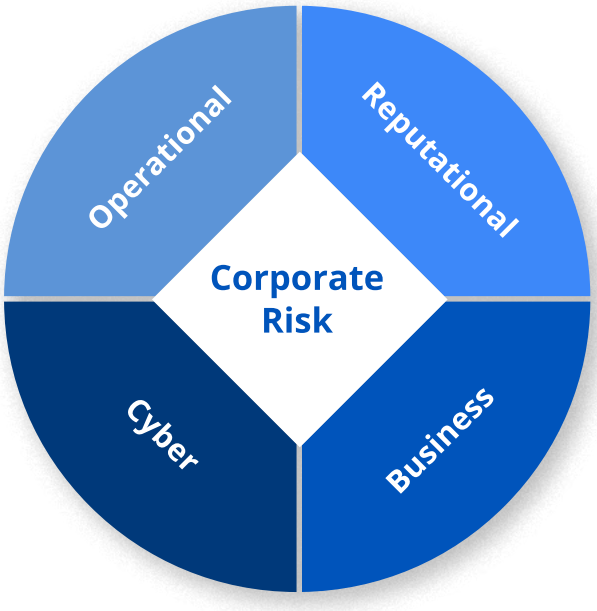
Success depends on building proactive, integrated security and risk management solutions that leverage the systems and processes needed to detect potential risk events, in real time, as they unfold. Here we explore best practices that security and risk leaders can use to do so effectively.

Top 10 Global Risks for Businesses

The latest Dun & Bradstreet Global Risk Report identifies 10 of the biggest threats to businesses globally, including geopolitics, COVID-19 and an energy crisis.

1. Global inflation
2. U.S.-China competition
3. Resurgent COVID-19 waves
4. China's economic slowdown
5. Supply chain difficulties
6. EU politics
7. Europe's energy challenge
8. Political polarization
9. Climate policies
10. Fiscal worries in emerging markets

The New Composition of Corporate Risk



Operational
- Health & Safety
- Asset Protection
- Executive Protection
- Physical Security
- Traveling Personnel
- Delivery Logistics

Repuational
- Delivery Disruption
- Brand Attacks
- Company Controversy
- Media & Commentary
- Social Responsibility
- Public Figure Activity
- Conferences & Events

Cyber
- Data Breaches
- Leaked Credentials
- Phishing
- Ransomware
- Advanced Persistent Threats
- Illicit Sales

Business
- International Events
- Site Selection
- Market Activity
- Political Environment
- Competitive Activity
- Supply Chains

Communicate and Coordinate Risk Across the Enterprise

As risk is a shared exercise among business leaders and teams across the enterprise, all bear some responsibility for identifying, mitigating and communicating potential risks and disruptions. One of the simplest ways to improve collaboration between security and risk management teams and business units is to improve communication between the two.

Increase face-to-face time

Resist the urge to rely on reports as a primary means of communication. While risk reports do have value, there is an enormous benefit to using meetings as a communications channel.

They create a dedicated time and space for focusing on risk, which fosters dialogue and strengthens risk accountability and ownership among lines of business and risk management teams.

Speak in a language easily understood

When communicating with senior leadership, business partners, and other key stakeholders, it's important to speak in a language they can easily understand. Otherwise, your messages won't resonate, it will be harder to gain buy-in and/or critical information could be lost or misunderstood.

Remove overly technical references and explanations from conversations and presentations. Instead, focus on speaking about risk in terms of business goals and outcomes.

Democratize access to risk information

This eliminates information silos and bottlenecks. Start by sharing real-time information on potential risks across the enterprise. Then take it a step further and help heads of business lines and functions understand how to assess if and how the risk will affect their area of responsibility.

This includes helping them to determine specific triggers and thresholds. Look to emerging technologies that increase visibility and use of data to create a source of truth.

Create clear roles and responsibilities

Build security and risk plans that describe clear roles and responsibilities and allow for a coordinated, unified response to risk. This ensures business leaders and teams have clearly defined swim lanes mapped to their spheres of responsibility, so that when a risk occurs, the response is orderly and efficient.

Plans should anticipate probable risks your company will likely encounter in the future, and regularly simulate those risks with stakeholders.

Measure the Right Risks, the Right Way

The number of risk sources has increased exponentially. Today, risk emanates from technology (e.g., emerging tech, legacy systems), supply chains, business operations, employees, regulatory and societal change and more.

But many organizations often only focus on the types of risk that are most relevant to what they do and where they operate, leaving them less agile and unable to pivot and respond to risk as a whole or to new and emerging risks. To effectively measure risks, know your risk triggers and which risks to measure.

Understand risk triggers

Compounding this is a lack of visibility into risk trigger events. If you assume the risk of a terror attack in a specific city has a medium likelihood and medium impact, you can prepare for that. But if you aren't aware that there have been increasing terror attacks in a nearby city, the opportunity to get ahead of the risk will be lost.

This is where real-time information is critical. Dataminr uses its AI platform to detect the earliest signals of high-impact events and emerging risks from more than 250,000 public information sources—social media content, internet-connected sensors, news sites, audio feeds, and the deep and dark web—in real time, often minutes or even seconds of when an event occurs.

Measure risk in business terms

Measuring the right risks is half of the challenge. The other half is measuring risks in a way that is meaningful for the intended audience. Consider the way cyber risk is measured. Usually it's given a qualitative measurement of high-medium-low, red-amber-green, or a rating of 1 to 8. This is problematic as these measurements are subjective and open to interpretation.

To effectively measure risk in a way that can be meaningful and relevant, frame it in a way that aligns to business imperatives. In other words, focus on quantifying risks. Doing so eliminates subjectivity and ambiguity from the risk assessment.

The Power of Real-time Information

Dataminr customers use Dataminr Pulse—a real-time alerting solution that provides the earliest indications of emerging risks, high-impact events and potential crises—to not just continue operations, but to innovate and even save lives.

U.S. Midwest hit by deadly tornadoes: Six U.S. states were hit with catastrophic tornadoes December 10-11, 2021, including one that stayed on the ground for a record 227 miles. Dataminr provided customers with the critical real-time information needed—more than 200 alerts as the situation unfolded—to direct employees to safety, track tornado paths and spot unforeseen risks in their disaster recovery response.

Company protects its brand and reputation: Through Dataminr Pulse, an asset protection team at a metal and mining company learned, in real time, that a news article about a not-yet-public company project had just been published—jeopardizing the organization's planned expansion. The team was then able to proactively mitigate the risk and protect their company's brand and reputation.

Strengthen Risk Leadership

Strong leadership is critical to ensuring organizational resilience—a non-negotiable requirement in today's risk environment. Organizations that have strong risk leadership are those that have established a strong risk culture and successfully maintain it. They also employ a common language and vocabulary of risk, which is understood throughout the enterprise and consists of the following three key components.

Accountability

While risk leaders are responsible for risk management, the board and senior executives are responsible for enterprise risk oversight.

Work to ensure there is commitment from these leaders to set the right tone and clearly communicate the importance of risk throughout the organization—including modeled behaviors and company value messaging.

Awareness

Is risk management at the front-end of the decision-making process? Is it aligned to business objectives? Both are indicators of an organization's risk awareness.

Make risk management policies and procedures available, accessible and part of the business planning cycle. And, ensure they are applied as part of day-to-day decision making and activities.

Attitudes

As mentioned earlier, everyone is responsible for risk management. Work to ensure the value of risk management is expressed through discussions, actions and activities—and that people feel empowered to challenge and escalate.

As we grapple with how to navigate an increasingly volatile world and its inherent risks, the list of those charged with identifying and responding to risk will continue to grow. And so too will the need for real-time information. In fact, real-time data often forms the cornerstone of effective risk management—creating organizations that are more resilient and agile, no matter the type and scope of future risks and disruptions.

Learn More

Learn how organizations like yours use Dataminr's real-time alerting solution, Dataminr Pulse, to effectively navigate today's ever-evolving threat landscape.