BITSIGHT®
The Standard in SECURITY RATINGS

How Continuous Monitoring is Revolutionizing Risk Management

CONTENTS 2

INTRODUCTION 3

EXPANDING CONTINUOUS MONITORING 4

VENDOR RISK 6

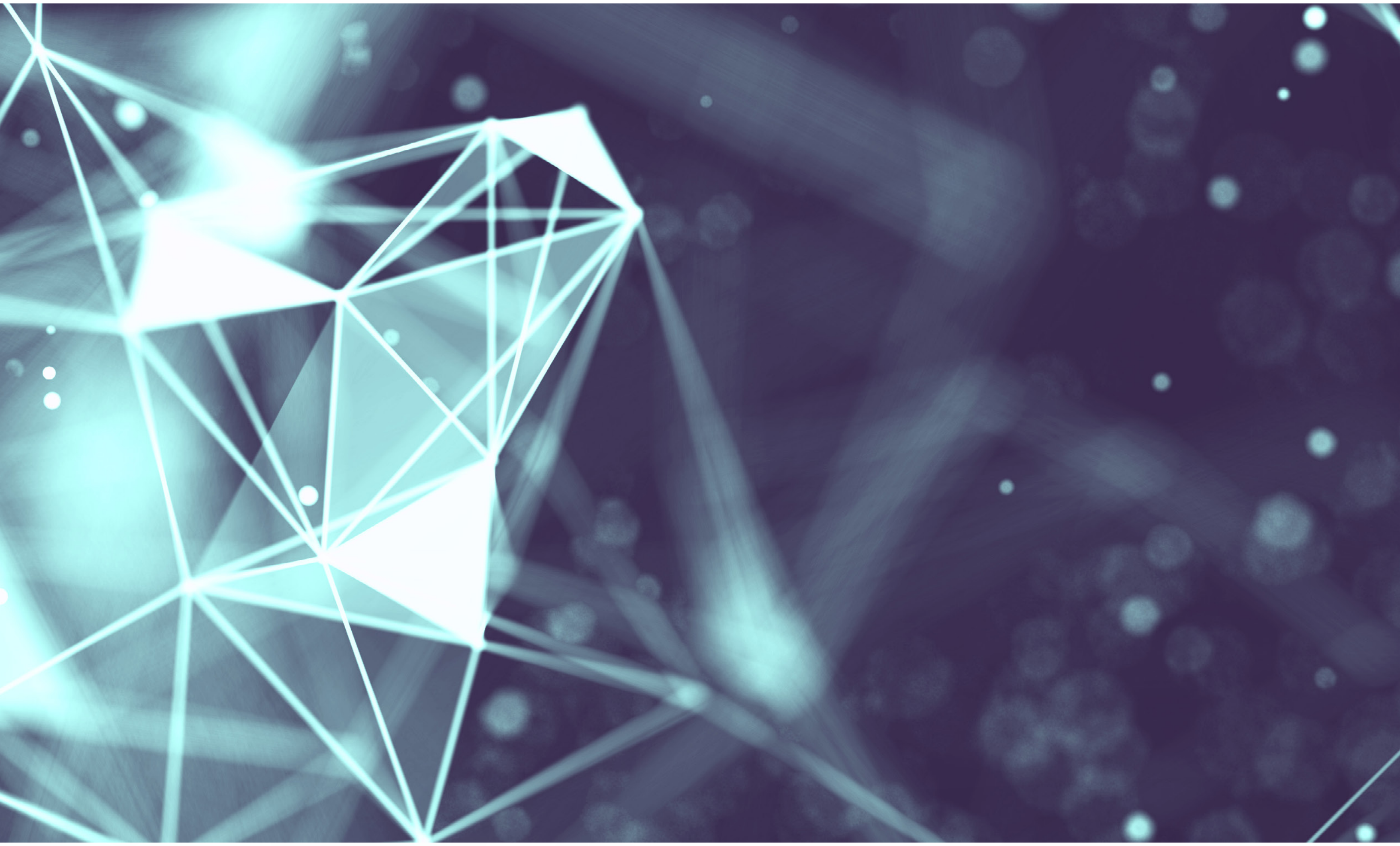
REPUTATIONAL RISK 8

STRATEGIC RISK 9

OPERATIONAL RISK 10

ENVIRONMENTAL RISK 12

CONCLUSION 13



INTRODUCTION

In the past, the job of a risk analysis professional went a little like this: Spend the workday reviewing as much data as you can get your hands on. Analyze that data for common themes and ideas. Draw conclusions based on these ideas. Make or suggest decisions based on these conclusions.

The data on these risk managers' desks might have come in the form of monthly, quarterly, or annual reports. Depending on the risk category, perhaps they were financial reports, strategic analyses from major consulting firms, or manufacturing equipment inspection results. In each of these examples, data was aggregated over the long-term, analyzed using time-consuming processes, and deliberated over in order to reach decisions.

Modern business no longer allows for this kind of slow-and-steady risk management workflow. Thanks to the rise of big data and artificial intelligence, organizations are able to assess and respond to risk faster than ever before.

However, modern business no longer allows for this kind of slow-and-steady risk management workflow. Thanks to the rise of big data and artificial intelligence, organizations are able to assess and respond to risk faster than ever before.

Here's how it works now: data is aggregated from millions of devices, sensors, and users in every moment. This unprecedented volume of data is often combined with other data sources, then analyzed by software employing machine learning algorithms and other state-of-the-art technology. The software produces conclusions that are being constantly updated based on real-time changes to the data set. Risk management professionals review the conclusions for trends and anomalies, then weigh this information against their company's risk tolerance to make strategic decisions.

A process which previously took days, weeks, or months is now happening in a second — and beyond that, it's happening every second, so that the most up-to-date information is always just a click away.

This is called continuous monitoring, and it represents a paradigm shift in risk management.

New technologies have made it possible to continuously monitor different aspects in a wide variety of risk categories. In this Ebook, we'll explore the latest continuous monitoring technologies that are making an impact in five of them: vendor risk, reputational risk, strategic risk, operational risk, and environmental risk.

EXPANDING CONTINUOUS MONITORING

Continuous monitoring is not a new concept. In some areas of risk management, like cybersecurity and finance, it's already left its mark in a big way.

Take cybersecurity for example. In this field, continuous monitoring has become no less than necessary. Many businesses have internal security operations centers whose personnel are tasked with monitoring the network for incoming threats, then deciding on appropriate remediation measures and neutralizing them as soon as possible. Many other businesses outsource this work to managed security service providers.

Cyber risk professionals rely on continuous monitoring solutions like security information and event management (SIEM) software to keep tabs on cyber threats and incidents on their networks — networks which are becoming increasingly complex thanks to the proliferation of internet of things (IoT) devices.

Continuous monitoring is so important to effective cyber risk management that it's even part of the NIST Risk Management Framework, a widely-adopted standard for securing information systems.

So, at least in some areas, continuous monitoring is nothing new. What is new, however, is the ability to use continuous monitoring to identify and remediate risk outside of established spaces like cybersecurity and finance.

> NIST
>
> *[The NIST Risk Management Framework] promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes.*
>
> *Source:* NIST Special Publication 800-37

The reason? Continuous monitoring requires massive data sources, which a computer network or a financial market were always able to provide. Now, the advent of big data has introduced vast amounts of data from a variety of other sources, from social media posts to weather sensors.

DISCLAIMER

Although we'll be mentioning specific technology products in this Ebook, BitSight does not necessarily endorse the use of these specific solutions.

VENDOR RISK

According to Gartner, “Vendor risk management (VRM) is the process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance.”

In other words, whenever vendors, suppliers, or other third parties have access to your data, there is a risk that something bad might happen to it. In order to mitigate the risk of data breach via third parties, most large organizations engage in vendor risk management activities.

At many organizations, vendor risk management processes are time-consuming and resource-intensive. Risk and IT professionals send questionnaires and surveys to their vendors once or twice a year. Vendors fill out the questionnaires to the best of their ability and return them. Then, Risk and IT teams use the questionnaires to make decisions about whether or not these vendors present any risk that is unacceptable to their business. This whole process can take a while — according to a recent study conducted by Forrester Consulting on behalf of BitSight, it takes **88%** of organizations over two weeks to assess a vendor’s cybersecurity posture.

For organizations with hundreds or thousands of vendors, this kind of manual risk management becomes problematic very quickly. When an assessment is months old, it does not accurately reflect the current risk a company is exposed to by a vendor. Even fresh questionnaires can contain errors, omissions, or inaccuracies.

Some businesses spend millions building security operations centers that continuously monitor their own networks for cyber threats while effectively ignoring the cyber risks they’re being exposed to by third parties. And this risk is very real — according to Deloitte, **20.6%** of business leaders report having dealt with a situation where sensitive customer data has been breached through third parties.

> *Some businesses spend millions building security operations centers that continuously monitor their own networks for cyber threats while effectively ignoring the cyber risks they’re being exposed to by third parties.*

Companies with a BitSight Security Rating of 500 or lower are ***nearly five times more likely to experience a breach*** *than those with a rating of 700 or higher.*

For a long time, questionnaires were one of the only ways to gather IT security information about third-party vendors. In the last few years, however, some companies have begun aggregating and analyzing externally observable cybersecurity risk factors that finally enable the continuous monitoring of vendor risk.

BitSight is a notable example. BitSight Security Ratings are numbers that reflect the cybersecurity posture of an organization based on risk factors like botnet infections, out-of-date devices, TLS/SSL certificates, file sharing behavior, and more. These ratings have been proven to correlate with the risk of data breaches. In fact, companies with a BitSight Security Rating of 500 or lower are nearly five times more likely to experience a breach to experience a breach than those with a rating of 700 or higher.

With security ratings, Risk and IT professionals can maintain a real-time understanding of the risks they're being exposed to by every vendor in their portfolio. Best of all, BitSight Security Ratings are updated daily, empowering decision making based on near-real-time data. Leveraging this technology, organizations can monitor and protect the data living outside their network in nearly the same way they monitor and protect internally stored data.

REPUTATIONAL RISK

Warren Buffett is quoted as saying "It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."

Most large and mid-sized organizations understand that their reputation is an enormously important asset. For this reason, many organizations hire reputational risk management (RRM) professionals to help protect them from the perils of public opinion.

Among the various categories of business risk, reputational risk might just be the most volatile. Public reactions are difficult to predict, and tracking every threat to a business's reputation is almost impossible. On top of that, the correlation between an incident and its effect on overall reputation depends on a variety of external circumstances. In a risk arena with so many variables, one thing remains certain: the bigger they come, the harder they fall.

Because these technologies are continuously monitoring social media for reputational and digital threats, RRM professionals can be alerted early and possibly divert crises before they even begin.

Threats to reputational risk can be anything from unfortunate incidents to data breaches to long-term rule-breaking to the misbehavior of CEOs. Unfortunately, threats to a business's reputation don't even need to be based on fact. With the ubiquity of social media and online review sites, anyone can say anything about an organization and potentially gain traction.

Of course, the first step in managing reputational risk is limiting behaviors that might threaten a company's reputation in the first place. Avoiding unethical business practices, protecting sensitive data from hackers, and implementing company-wide training programs are all good places to start.

The work of most RRM professionals, however, is concerned with the other side of the equation — listening in on the public conversation and recommending actions based on what they hear.

For large organizations, the volume of conversation happening around their brand at any moment is staggering. In order to stay ahead of reputational threats, these companies must hire a staff of people to scrape the internet looking for signs of trouble, or pay consulting firms huge sums for similar services. When threats inevitably slip through these manual monitoring procedures, large organizations typically rely on PR firms to limit negative repercussions.

With the advent of artificial intelligence, however, everything has changed. Companies like Dataminr read millions of communications across the internet and report back with posts, tweets, and reviews that contain potentially damaging content. Because these technologies are continuously monitoring social media for reputational and digital threats, RRM professionals can be alerted early and possibly divert crises before they even begin.

Some continuous reputational risk monitoring tools like Recorded Future can even scan the dark web — that hidden side of the internet beyond the reach of search engines. By actively monitoring chatter on these sites, continuous monitoring technologies can alert reputational risk management teams of potential illegal activity involving their company, like the trade of sensitive data obtained via hacking or phishing.

STRATEGIC RISK

SRM professionals are using big data and machine learning to keep a finger on the pulse of politics in other countries without leaving their office.

Deloitte defines strategic risks as "risks that affect or are created by an organization's business strategy and strategic objectives." Any time an organization decides to move into a new market, expand a service offering, change its pricing structure, or make any other major decision, it is exposed to a certain amount of strategic risk. The job of a strategic risk management (SRM) professional is to research and analyze that risk in order to determine whether the strategy is worthwhile.

More so than the other categories in this list, strategic risk remains a human-driven enterprise. Strategic decisions require weighing so many distinct variables that software can't be relied upon to return perfect answers to strategy questions (at least not yet). However, when it comes to researching and analyzing certain strategies, continuous monitoring technology has become a huge asset for SRM experts.

For example: Company A wants to establish a manufacturing facility in a foreign country that is currently offering excellent business incentives. However, that country's government has been historically unstable, and Company A doesn't want to move in if there's a significant risk that the current administration will fall out of power. Company A's SRM team needs the latest information on the political situation in this country in order to make the most informed decision about whether or not to proceed with the plan.

Understanding the politics of a foreign nation might previously have required staying within its borders for an extended period of time, gathering impressions from powerful people, and speaking with various consultants and experts. Now, however, SRM professionals are using big data and machine learning to keep a finger on the pulse of politics in other countries without leaving their office.

Companies like Geoquant offer up-to-the-minute analyses of geopolitical risk. By aggregating data from social media, news outlets, and other sources, then running that data through language analysis software and machine learning algorithms, Geoquant claims to be able to update political risk indicators in near-real time. Other companies are turning to internally-developed technology solutions to measure political sentiments from all over the globe.

The kinds of threats that affect strategic decision making are highly dynamic. Politics, pricing, disruption, and more — they all move at a speed that can make yesterday's analyses obsolete. By arming themselves with continuous monitoring tools, SRM professionals can improve decision making and help steer their organizations toward success.

OPERATIONAL RISK

A business is exposed to operational risk by its procedures, processes, systems, and third- and fourth-party relationships. The more opportunity these vectors have to disrupt the flow of business, the greater their operational risk.

Operational risk is easy to visualize in a manufacturing environment, where the failure of one element can bring the entire production process to a dead stop. To effectively mitigate operational risk in this space, manufacturers must regularly inspect every piece of equipment for signs of wear. However, these inspections also require delays in production.

By attaching sensors to factory equipment that continuously monitor performance and track the symptoms of potential failure, manufacturers can cut down on the need for production stoppages and drastically reduce operational risk.

Outside of manufacturing, operational risk affects organizations in a similar way, though it may be more difficult to visualize. Just as each machine in a factory is linked together in such a way that one broken link can break the whole process, many organizations are linked to third and fourth parties in supply chains, IT vendor relationships, and more.

Because all of the businesses in these chains are linked, you don't just need to worry about your vendors — you need to worry about your vendors' vendors as well.

Reducing operational risk in this sense requires a two-fold approach. First, it's necessary to choose partners based on their levels of risk. Second, operational risk management (ORM) teams need to develop backup plans in case there are issues with a third or fourth parties' operations.

Before the digital revolution, developing these plans of action was relatively simple. However, the proliferation of digital services has exploded the number of vendors ORM professionals need to account for, and increased the likelihood that these vendors might experience unexpected downtime.

In other words, because all of the businesses in these chains are linked, you don't just need to worry about your vendors — you need to worry about your vendors' vendors as well. A single cyberattack that shuts down your ecommerce platform's cloud services provider could have huge ramifications on your bottom line.

Luckily, there are tools available to help ORM professionals map these complex relationships in order to develop backup plans to reduce the risk of business interruption. BitSight Discover leverages the power of continuous monitoring to identify common service providers and technologies in your supply chain. It lets users see at-a-glance ratings that indicate each of these vendors' cybersecurity posture, and it provides quantitative measurements of how important each relationship in the network is to each vendor.

From this comprehensive vantage point, operational risk management teams can identify their riskiest relationships and focus their efforts on creating effective remediation plans should one of those relationships break down.

ENVIRONMENTAL RISK

As we've explored, big data has enabled businesses to proactively respond to all kinds of risks. With continuous monitoring tools, companies can make smart remediation decisions at the first signs of trouble, instead of cleaning up after threats have already done their damage.

In a testament to just how powerful continuous monitoring technologies really are, there are now solutions designed to help organizations proactively respond to the one thing we've always assumed we couldn't really predict: the weather.

Of course, environmental risk management (ERM) professionals always had the ability to turn on channel 4 news and see the chance of precipitation for that afternoon. What sets continuous environmental risk monitoring tools apart is their ability to combine several sources of forecasting data with data on infrastructure outages, the historical impact of weather events, compliance factors, and even a company's own operations.

Here are a few examples:

Riskpulse offers logistics professionals the ability to track the environmental risks to product shipments. These risks are quantified on a scale from 1-25 and take into account the exact details of each shipment. The risk calculations are continuously updated and integrated into dashboards for deeper analysis.

Envirosuite continuously monitors the output of noise, odor, water pollutants, and air particles from factories and processing plants and compares these numbers against up-to-date weather models to help these organizations remain in compliance with environmental regulations. When a complaint is received about a pollutant, envirosuite maps how that pollutant would have traveled in current weather to pinpoint exactly which part of a plant is at fault.

AIR Worldwide provides models of the potential damage caused by environmental disasters to help insurance underwriters determine appropriate rates for their customers. They combine historical data with advanced computer models and current weather forecasts to give their clients the best possible idea of the real risks of natural and unnatural disasters.

These continuous monitoring tools can help businesses service their customers when they need it most — like when retailers are trying to get shipments of supplies to an area before a hurricane.

CONCLUSION

In a 2018 risk study, PwC asked over 1,500 senior risk executives about their risk management programs. The ones who identified their programs as "very effective" or "somewhat effective" were classified as "Adapters." One of the key differences between Adapters and Non-adapters was the degree to which they had adopted continuous monitoring.

As we've demonstrated, many risk categories have components that can be continuously monitored. For risk professionals who are not currently engaging in continuous monitoring activities, the trick is to discover those components before the competition does.

Where will continuous monitoring take risk management in the future? Many organizations are taking steps to integrate continuous monitoring tools with traditional GRC and ERM solutions to synthesize various risk management platforms into central locations.

Risk management professionals will always be responsible for making judgements about which risks to avoid and which opportunities to seize. However, thanks to the expansion of continuous monitoring technologies, they are becoming less responsible for the tedious tasks of data collection, aggregation, and analysis. Organizations that equip their best risk management personnel with continuous monitoring tools will put themselves in a position to make more informed decisions that help their businesses succeed.

> *To adapt their capabilities to influence and enable their organizations' innovation strategies, Adapters are much more likely to say they add new risk-related skill sets, expand continuous risk assessment, and use new technology for more real-time information.*
>
> *Source:* PwC 2018 Risk in Review Study