ONTIC

WHITEPAPER

Improve Business Continuity with Proactive Threat Management

A COMPREHENSIVE APPROACH FOR SECURITY TEAMS TO PROTECT PEOPLE, ASSETS, AND INFRASTRUCTURE AND ENSURE BUSINESS RESILIENCY

Turn the page to dive deeper into the following themes:

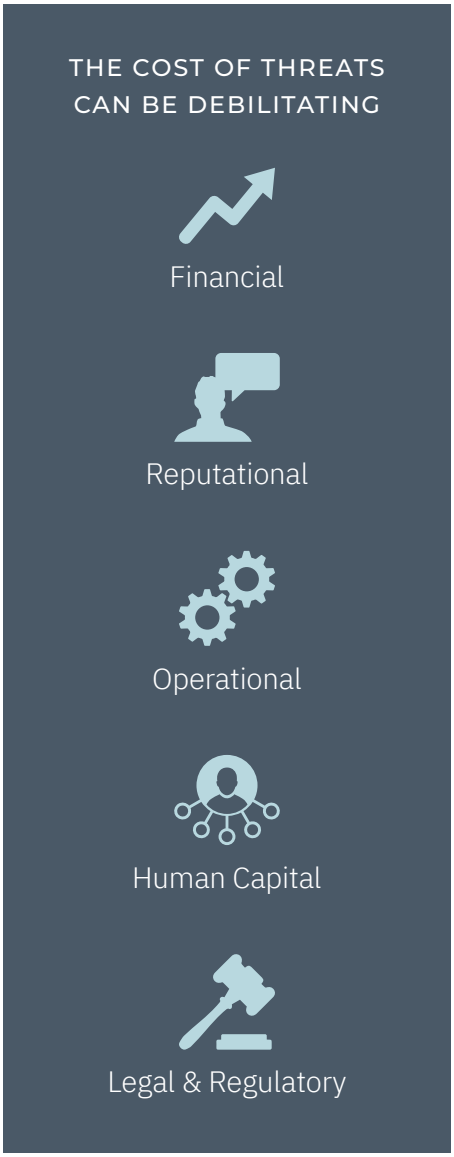
Executive Summary

Organizations face greater risk exposure than at any other time in history. Not only do these threats seem to occur more frequently, they are also more complex and often have global reach. Threats from cybercrime, extreme weather, geo-political events, fraud, activism, and workplace violence are impacting business operations and supply chains, shifting industries in the process. The impact is not limited to business operations — many of these threats also have the potential to directly impact employees, customers, and business relationships.

What do these extreme threats teach us? Organizations need a comprehensive approach to managing risks and threats that will support business continuity. Teams must be able to proactively identify, understand, forecast, and manage risks in all areas of their operations, so they can make quick decisions when disruptions are anticipated and more quickly protect their personnel, assets, operations, and reputation.

The interconnectedness of the threat landscape requires an approach that goes beyond using only traditional risk management strategies such as insurance plans and emergency response playbooks. Today, corporate security, legal, and compliance teams can use a variety of tools to bridge the gap between recovering from risks and proactive threat management, helping to prepare their teams to be more agile and resilient when risks become reality. Using these tools, potential threats can be identified before they cause disruptions to business continuity. With a plan to monitor real-time information about critical threats and vulnerabilities across the enterprise, organizations can make quick adjustments to their operations and security posture as needed to protect the business.

Business continuity plans should be much more than set-it-and-forget-it standardized procedures. Organizations that make the shift to a mindset of proactive threat management will be in a better position to protect their personnel, minimize business disruptions, and support the bottom line.



Common Threats to Business Continuity

All businesses are concerned with internal and external financial risks to their operations, but often threat management is narrowly focused on only those threats deemed high risk. In reality, there is a wide spectrum of threats that could have a substantial impact on business continuity and company value.

EXTREME WEATHER / CLIMATE / NATURAL DISASTER

- Earthquake
- Extreme weather (hurricane, flood, snow)
- Wildfire
- Climate risk

HEALTH & SAFETY

- Epidemic / pandemic
- Food-borne illness
- Infectious disease
- Duty of care

WORKPLACE VIOLENCE

- Any act or threat of violence or abuse against employees, clients, customers, or visitors to the worksite including targeted attacks on corporate leadership

ACTIVISM

- Activism Demonstrations
- Union

GEOPOLITICAL UNREST

- Acts of war / terrorism
- Civil disorder
- Political instabilities

INSIDER THREATS

- Breach or incident
- Theft
- Fraud
- Sabotage
- Espionage

CYBERCRIME

- Cyberattacks against internal or supply chain systems by malicious outsiders

OPERATIONAL

- Power or water outage
- IT failure
- Supply interruption
- Data corruption
- Production loss
- Market trends

COMPLIANCE

- Regulations
- Background checks
- Policy enforcement

Threats may be isolated or may cascade. For example, an extreme weather event could destroy critical infrastructure introducing supply chain delays. Further, any impact on an employee's own health and safety could affect operational capabilities or introduce duty of care requirements — those legal, moral, and ethical obligations to care for the safety and wellbeing of employees.

What is Proactive Threat Management?

Many organizations are already engaged in active risk management plans for several parts of their business.

Typically, the approach outlines various threats that could impact business operations, quantifying the level of risk associated with that threat and the creation of resilience systems for both prevention as well as recovery. This approach can be very effective in ensuring the organization is aware of the risks that it faces and is intentional about making decisions of how to manage each risk, whether they choose to avoid, mitigate, transfer, or accept the risk. However, even when risks are being actively managed, the risk of disruptions to business continuity remain.

To ensure a business can be resilient to the many types of challenges it may face, an organization must also create a complete business continuity strategy that includes both proactive and reactive resilience.

Floods, cyber-attacks, IT breakdowns, supply chain issues or loss of skilled staff are just some of the possible threats to the smooth running of an organization. If not addressed effectively, they can cause disruption or even business failure.

ISO 22301

PROACTIVE RESILIENCE
Activities designed to identify and mitigate threats to business operations

\+

REACTIVE RESILIENCE
Activities initiated after a crisis to maintain communication, minimize the impact of events, and recover operations

=

BUSINESS CONTINUITY
The capability of an organization to continue delivery of products and services amid a disruption

Traditionally, risk management tools and processes have been narrowly focused on cybersecurity and fraud, or corporate security teams charged with executive protection and violent threat mitigation. Today, executives must widen the aperture across their enterprise and bring the same mindset of how to proactively foster resiliency before adversity strikes to an ever-growing set of risks and threats to business operations. The goal of complete business continuity planning is to make every stage of threat management actionable.

Our 2022 State of Protective Intelligence research released from the Center for Protective Intelligence suggests that 88% of organizations are experiencing a dramatic increase in physical threat activity compared to early 2021, with more than 41% of security practitioners reporting they expect to miss more than half of these upcoming threats.

Organizations can use a variety of tools and techniques such as those below to effectively mitigate risks to business continuity — activities that help protect the interests, assets, and physical safety of all stakeholders in an organization.

- Visitor management systems (VMS)
- Connected devices (cameras, access control systems)
- Public record research
- Social media and dark web monitoring
- Cyber threat intelligence tools (insider threat monitoring, intrusion detection, endpoint protection)
- Fraud detection software

In this era of extreme risk, leadership teams are looking to proactive threat management to help anticipate and manage disruption. Preparing your organization to understand and respond to threats before they occur can be the difference between minor disruption and catastrophic loss.

DATA SOURCES

VMS

Customer relationship management systems (CRM)

LPR cameras

HR systems

Access control systems

Collaboration tools

Manual web & social searches

Public records

Registries & official watch lists

The Argument for Comprehensive Threat Monitoring

While many organizations have systems and processes in place for assessing, reporting, and tracking threats to an organization's personnel and operations, too often this data is gathered from a variety of disparate sources, sometimes manually and sometimes using purpose-built tools.

Once it's collected, it's usually held in silos within the organization. Too often when the information is updated, it may be tracked manually in a spreadsheet or on paper, supported by email communication and manual reports, with the collectors independently analyzing the results. Even when the results are shared with other stakeholders, it's difficult to integrate the data into a more holistic picture of the organization's risks. The result is:

- Slow, disjointed communications
- Difficulty identifying connected events
- Lack of a common understanding of threats between physical security, cybersecurity, HR, legal, and compliance
- Delays in investigating and managing active threats
- Potential for missed threats
- Inadequate paper trail and reporting

In fact, the Center for Protective Intelligence recent survey notes that while 95% of organizations are actively adopting new threat intelligence, monitoring, and alerting solutions for physical security, cybersecurity, human resources, legal, and compliance, these intelligence tools remain siloed without a comprehensive strategy for holistic data analysis and reporting.

Today's threat environment demands cross-functional communication and information sharing. Security teams need to be in constant contact with other corporate functions including HR, legal, IT, and Environment, Health, and Safety (EHS) and they need a common point of reference to work together to support business resilience.

A Modern Approach to Security

Elevating your security efforts to prepare your organization for more sophisticated threats requires a dynamic, cloud-based solution that collects and connects the critical intelligence needed to investigate, assess and act on threats to keep employees, executives, and physical assets safe. Consider a platform that combines data with integrated assessment tools to identify, score, and rank potential threats against your enterprise.

INTERNAL SYSTEMS
Visitor management systems (VMS), customer relationship management (CRM), license plate reader (LPR) cameras, HR systems, authentication services, collaboration tools, & more

PROACTIVE LISTENING
Social media, RSS feeds, real-time news, dark web, weather, geo risks

INTEGRATED RESEARCH
Identity, public records, arrests, incarcerations, release, civil records, federal court records, sex offender registries, terrorist watch list, and more

OPEN API
Secure integration with any tools (hardware or software) across your organization

BEHAVIOR INDICATORS
Pre-incident indicators such as suspicious behavior, complaints, or active threats

Moving from static data to an always-on approach to collecting intelligence, it's imperative that security teams have a way to both capture critical signals as well as to curate that data into actionable intelligence. For example, signals can be captured from multiple sources including weather, social media, real-time events (for geopolitical risks), human interactions and technology systems, displayed on real-time interactive maps to help establish situational awareness, to identify potential threats to the business, and support a coordinated, proactive response.

Protective Intelligence Use Cases

Protective intelligence provides enterprises with a proactive way to manage threats from many sources including unrest, workplace violence, climate events, pandemics, and other common threats to positively impact corporate governance, security, logistics, HR, and other critical business functions.

PRO·TECT·IVE IN·TEL·LI·GENCE
Protective intelligence is an investigative and analytical process used to proactively identify, assess and mitigate threats.

Below are several key examples of how protective intelligence can be used to improve proactive resilience against the most common threats facing organizations today.

EXTREME WEATHER, NATURAL DISASTERS & CLIMATE RISK

In just over one year, from March 2020 to August 2021, extreme weather events across the world affected at least 139.2 million people in at least 433 unique events, including 17,242 fatalities, according to data collected by the International Federation of Red Cross and Red Crescent Societies. Climate change is likely to make these crises more frequent and intense, combining to create new supply chain pressures, a particularly serious concern when global supply chains are already strained.

$343B

Global economic losses, natural disasters, weather & climate events

In Canada and the northwestern US, for example, unprecedented heatwaves in 2021 were responsible for extreme wildfires and hundreds of deaths, followed by an extreme atmospheric river event. The situation had a catastrophic impact on agriculture, infrastructure, and the supply chain both into and out of the Port of Vancouver, impacting the deep water port, road transportation, and railways for several weeks.

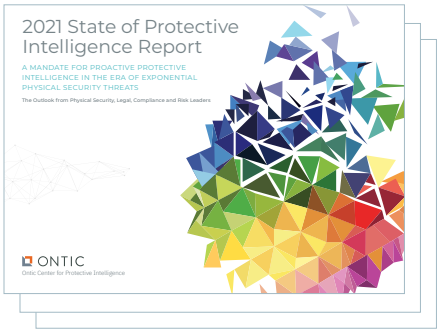
To help mitigate these threats, organizations can examine their supply chains with a particular focus on identifying the most critical nodes where disruptions due to climate change, extreme weather events, or natural disasters would cause the most significant business impact. Once the most critical areas have been identified, protective intelligence techniques can be used to monitor for potential disruptions, while businesses also work to identify suitable alternate options for these nodes if disruptions occur. Just as important is to identify their most critical suppliers and understand their plans for mitigating similar disasters, ask questions about where suppliers are getting their own inputs or how they are mitigating against climate change, extreme weather events, and manmade disasters. For travel security professionals, this same information can be used to inform travel plans or to manage the evacuation of business travelers from impacted areas.

HEALTH & SAFETY

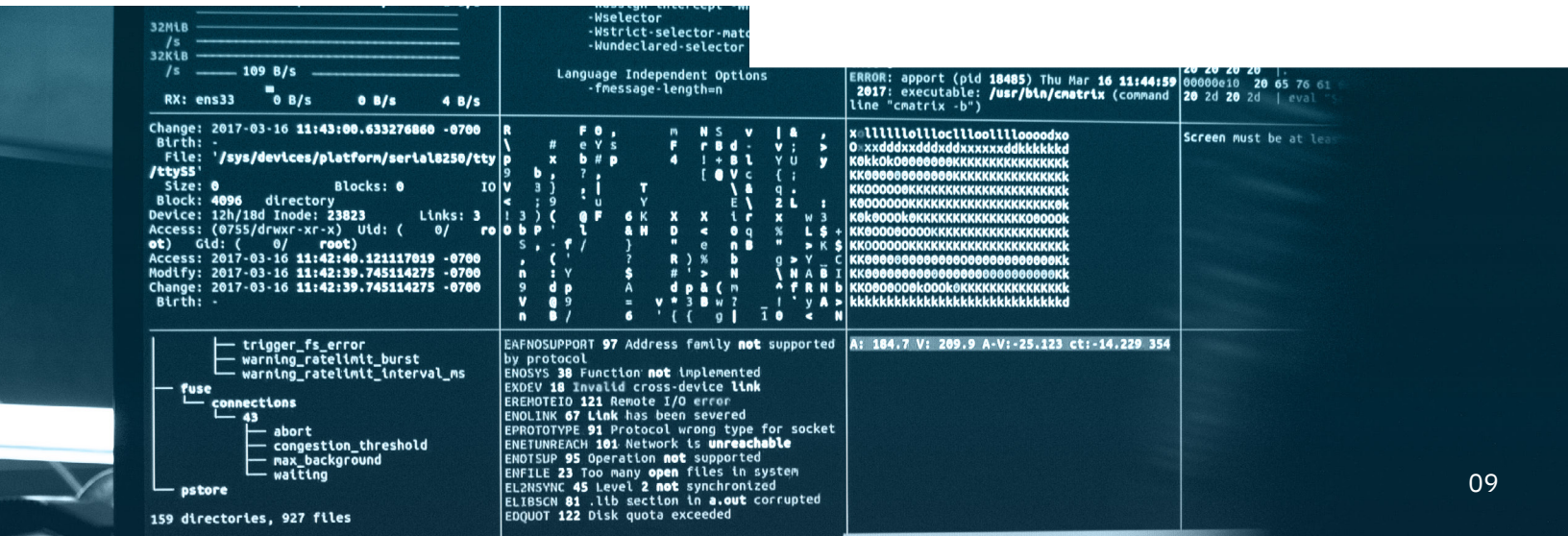
Security managers say they're receiving increasing reports of physical threats against employees in the workplace. Corporate leadership is under more pressure than ever to ensure their personnel are safe, not only for financial and liability reasons, but also to protect their corporate reputation. Monitoring of health and safety issues, including potential problems with employee mental health has become both a standard duty-of-care measure and a prudent course of action to prevent insider threats and workplace violence incidents.

Many companies are already experimenting with technology solutions to monitor their global health and safety concerns. In January 2020, a small team at a global financial services technology company began closely watching early warning signs of a new disease outbreak in the regional capital of Wuhan, China. By combining reliable media sources with historic outbreaks, the team was able to take action early: stopping executive travel, investing early in protective equipment, and swiftly transitioning to remote work. Intelligence-gathering capabilities make it possible to monitor threats in real time to help shape executive decision-making and take action to prevent tragedy.

Business continuity is at the heart of physical security concerns, and 69% say their leadership would agree it will be impossible for their company to recover financially and reputation-wide were a fatality to occur as a result of missed physical threats.



2021 State of Protective Intelligence Report



WORKPLACE VIOLENCE

As a subset of health and safety, workplace violence management often requires specialized knowledge and tools to keep employees safe from harm while in the workplace, working remotely, or while traveling for business. Executives are at increased risk of violent activity and may need specialized protection against stalkers, kidnappings, physical attacks, or the management of violent and non-violent protests.

Violence in the workplace is estimated to cost billions of dollars a year in lost work time and wages, reduce productivity, medical costs, workers' compensation payments, and legal and security expenses according to the FBI. It has impacts not just on a particular victim, but it damages trust, community, and sense of security in the workplace. While mass shootings in the workplace receive a lot of media attention, and are overall on the rise, they still represent a small percentage of the 20,870 workplace violence instances reported each year. Attacks on corporate leadership have also been on the rise, 69% of which target CEOs, mostly by strangers. Read more in our brief on Executive Targeting.

Categories of workplace violence

The FBI, in its coordination with occupational safety specialists and other analysts, defines workplace violence in four categories:

UNCONNECTED CRIMINAL

- No relationship to the workplace or any employee

CUSTOMER OR CLIENT

- Legitimate relationship (e.g. customer, client, patient, student)

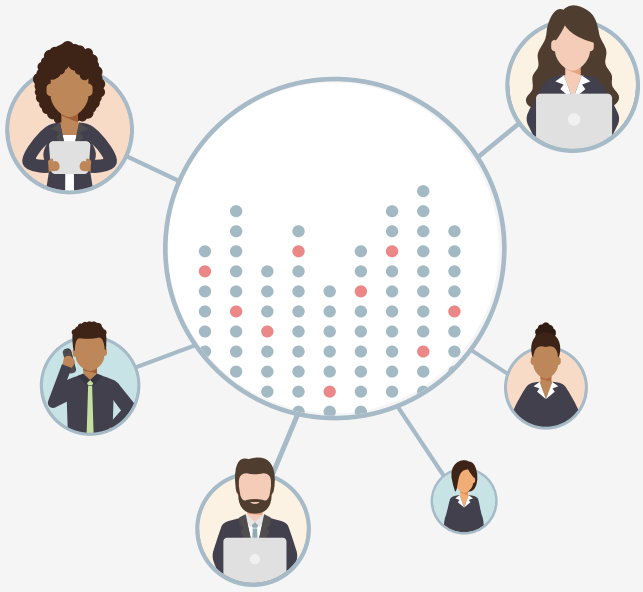
CO-WORKER

- Current or past employee

DOMESTIC VIOLENCE

- No relationship to the business but relationship with intended victim

According to OSHA workplace violence is "any act or threat of physical violence, harassment, intimidation, or other threatening disruptive behavior that occurs at the worksite," ranging from threats or verbal abuse to physical assault or homicide against employees, clients, customers or visitors to the workplace.



In 2021, Santa Clara VTA employee Samuel James Cassidy entered the rail yard and opened fire, killing nine people before committing suicide. The gunman had a history of insubordination and verbal altercations but faced no disciplinary action.

Experts agree that workplace mass shootings often follow a similar pattern and often involve past or current employees, opening the possibility for threat identification and risk mitigation efforts. The same is often the case for other categories of workplace violence.

Workplace violence prevention solutions help teams proactively manage security threats, complaints, terminations, policy violations, and suspicious behavior to detect, evaluate and investigate behavior signals needed to help prevent workplace violence and avoid costly legal activity. By integrating research tools and end-to-end case management solutions, security teams can take swift action when employee concerns or threats of violence arise.

With fully integrated, in-house solutions to investigate potential workplace violence signals, security teams can complete threat assessments and create consistent, compliant incident reports with recommended actions to address misconduct, helping to prevent escalations and while keeping employees and the company reputation safe.

ACTIVISM

Formal and informal activism represent a potential threat to both operations and security. In the wake of Russia's war on Ukraine, the vast majority of multinational brands quickly moved to withdraw their operations from Russian markets. Economist Mary Lovely notes, "Pretty much no company, no multinational, wants to be caught on the wrong side of U.S. and Western sanctions." In an era increasingly focused on corporate responsibility, environmental stewardship, political bias and equality, values are increasingly tied to the bottom line.

Similarly, shareholder activism has become more prevalent in recent years, with groups of shareholders using their status as owners to influence corporate behavior or strategy. For example, environmental activists have joined forces with shareholders of energy extraction companies to change their emissions targets.

However, not all activism that impacts organizations is directly tied to the actions of the impacted organizations. For example, the Canadian Trucker Convoy blocked key trade routes, shutting down production of auto manufacturing at Ford, G.M., Honda and Toyota.

Protective intelligence tools can help corporations monitor threats from activist organizations that are working within specific industries or geographic areas. By coordinating this information with other stakeholders, the company can create a unified approach to understanding activist demands and likely actions. Monitoring these issues can also help corporate security teams to understand when a threat of activism might be morphing into a physical security concern for executives.

GEOPOLITICAL UNREST

Political, economic, social and religious unrest has become a serious business concern, both inside the United States and around the world. In recent years, political unrest inside the U.S. has introduced substantial uncertainty into business activities, increasing business continuity concerns both directly and indirectly through the market and the global economy. In many areas, levels of unrest can be quantified by security teams to help benchmark security measures and countermeasures that should be taken to mitigate these threats to employees and operations.

Corporate security teams need more efficient deep listening tools to monitor known threats, identify changes to geopolitical stability, identify social unrest, especially when it is directed at a brand or executive members, and be alerted to local changes that could impact employee health and safety or business operations. Security teams need tools that allow them to stop searching social and news sites one by one and instead leverage a consolidated listening tool to help quickly surface risk signals from multiple sources that can then be investigated. Such tools can also be utilized by travel security teams to understand when unrest is emerging that could threaten expat employees or travelers, or when known unrest is escalating to unacceptable levels of violence, necessitating employee departure or evacuations.

INSIDER THREATS

An insider is any person who has or once had knowledge of or authorized access to an organization's resources, including equipment, facilities, information, personnel, networks, and/or computer systems. Insider threats include both negligent and malicious behaviors that lead to a security incident or breach, fraud and abuse, theft, sabotage, espionage, or other forms of behavior that harm the business. Further, cybercriminals prey on insider vulnerabilities to gain access to protected systems.

Malicious insider threats can often be linked with documented employee behavior indicators including interpersonal conflicts or control issues, reports of inadequate performance, misuse of travel and expense funds, unapproved changes to computer systems, or other reported infractions. For example, in 76% of fraud cases, at least one red flag was documented before the fraud incident was identified.

Companies are already employing many technical and non-technical controls to detect or prevent insider threats in the digital realm, including stronger access controls, multi-factor authentication (MFA), risk monitoring, and automated expense reviews. However, gaps remain in insider threat monitoring, especially methods to monitor and share information about suspected insider threats within the physical realm, like theft of physical property, sabotage, and fraudulent activities.

$11.45M
cost of insider threats

5%
of revenue lost each year to fraud

92%
of sabotage linked with negative work event

Many organizations will benefit from implementing a proactive insider threat program, automating the capture of internal triggers, unusual behavior or concerning activities, and continuous monitoring of the signals the security teams believes are the most likely early indications of potentially malicious activity. Early signal detection allows teams to quickly activate workflows to investigate the situation more thoroughly, possibly including court records, public records, user behavior patterns supplied by the cybersecurity team, and other internal data.

In organizations where fraud is a traditional problem, it may be especially beneficial for the corporate security team to keep detailed profiles on individuals or groups who are suspected of involvement in fraudulent schemes. When a high-profile financial institution leveraged Ontic's embedded research tools, it was able to scour the dark web and public records to establish ties between profiled individuals, helping to identify a fraud ring. The company passed details of the investigation to law enforcement for further investigation.

Cybercrime

As organizations accelerate their digital transformation, significant investments have been made in threat intelligence, monitoring and alerting solutions for cybersecurity. However, cyber intelligence generally remains siloed within the cybersecurity team.

Potential exists to bridge the gap between cybersecurity and physical security, creating a more interconnected system designed to support the modern threat landscape. For example, security, human resources, legal and compliance teams can combine pre-incident indicators from cybersecurity systems with insight from HR to spot insider threats or with the investigative capabilities to connect person of interest profiles with cyber attacks.

37%

of physical threats originate as a cyber threat

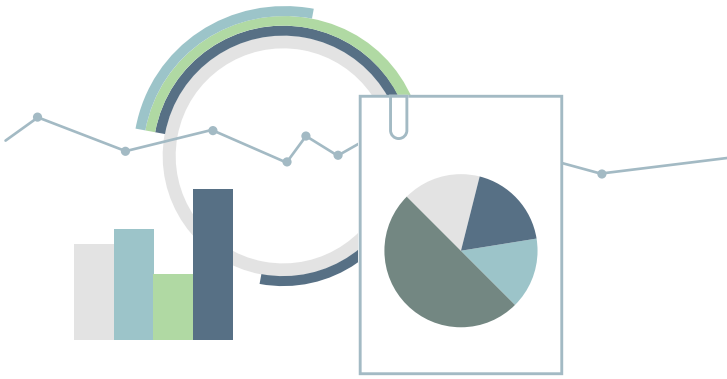
Ontic's 2021 Mid-Year Outlook State of Protective Intelligence Report

Operational

Operational risk involves a failed internal process, system, or human resource or relationship that results in a direct or indirect loss to the business. Common examples of operational risk include a hardware or software failure, utility outages, supply chain disruptions, or breakdowns in business relationships.

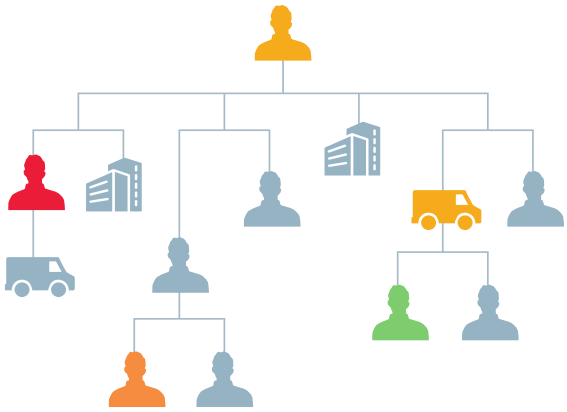
Many organizations utilize risk management principles to track their operational risk vulnerabilities implementing a variety of controls where possible. However, most of these measures remain disconnected from other intelligence gathering teams within the organization. This situation is particularly problematic because many operational threats have significant overlap with other risk functions within an organization, sometimes leading to duplicated efforts or threats that fall through the cracks.

A more interconnected, business-specific approach to managing operational risks can leverage predictive intelligence across many parts of the organization to better understand, identify, and mitigate against risk. Using protective intelligence tools to monitor the most critical operational concerns will help to bridge the gap between fulfilling risk management obligations and ensuring continuity of business operations.



COMPLIANCE

To meet the increased need for instant gratification driven by COVID-19, businesses have ramped up delivery logistics and last mile driver hiring. Major enterprises that employ hundreds of thousands of drivers have a legal and ethical obligation to ensure the safety of these employees, contractors and the customers with which they may interact. Negligent enterprises expose themselves to significant brand, financial, legal, safety and compliance risk, each of which poses challenges to business continuity.



Imagine you are an employer hiring a new contractor, and without doing the appropriate vetting, you hire a company that has committed fraud while operating under another name. On top of that, one of their employees driving your truck isn't properly insured. The cost of investigating and terminating this contract, as well as any legal or settlement costs, are going to far outweigh the expense of conducting an initial onboarding assessment of the company. That's why it's necessary to address these issues proactively. For every bad operator that can be stopped at the gate, a company can save upward of $50,000-$100,000 per incident.

Modern organizations use protective intelligence platforms in several ways to ensure their compliance requirements are met, while also improving business continuity by monitoring any status changes. For example, organizations use protective intelligence platforms to validate information provided by business partners and contractors against public records to verify, identify or licensure. Civil and criminal records at the state and Federal level can be leveraged to ensure the safety of employees and customers, with the possibility of monitoring recent civil and criminal records or even media coverage for activities that could endanger personnel and business operations. A similar process can be used to manage the compliance of critical business partners and suppliers, especially in cases where previous screenings have uncovered unexpected problems, uncovering potential problems before they become a business continuity problem.

Takeaway

Against a rising tide of threats to business continuity and today's hyper-connected environment, leading organizations are leaning into proactive resilience across a wider spectrum of threats. When your team can anticipate threats and vulnerabilities and take steps to minimize their risk, you can help to protect the business from potentially devastating losses — or, at the very least, work to minimize disruptions.

Today's security teams are well-positioned to be at the center of a proactive, technology-led threat detection and assessment program. With a modern, complete business continuity solution, security teams can paint a more cohesive picture of risk intelligence, assessment, mitigation and operations across the enterprise and share those risks with the appropriate stakeholders quickly and effectively.

Platforms like Ontic's cloud-based Protective Intelligence Platform provides early access to emerging threats, pre-incident indicators, and vulnerabilities from real-time data sources, social listening, and internal systems to gain greater understanding of risks to the business. When a critical signal emerges, security teams can conduct immediate investigative research to surface additional details to put the problem in context. With this integrated approach, security teams can help facilitate a connected strategy that brings together every functional area across the organization to act quickly and adjust operations to minimize risk to employees and business continuity.

While you can't prevent every incident, you can boost your proactive threat management and resilience with protective intelligence technology.