Risk Intelligence

KEEP PEOPLE SAFE, PROTECT ASSETS, AND ENSURE OPERATIONAL EFFECTIVENESS

ON A GLOBAL ANNUAL BASIS, HUNDREDS OF THOUSANDS - IF NOT MILLIONS - OF DISRUPTIVE EVENTS OCCUR.

Organizations have a duty to keep people safe, protect assets, and ensure operational effectiveness. To fulfill this mission, enterprises need a system to detect and evaluate potential threats and a platform that will allow them to easily visualize, assess, and predict which events could hamper or severely threaten their most valuable assets and continuity of operations.

When NC4, a leading global provider of threat intelligence solutions was acquired by Everbridge, the industry's only end-to-end platform for threat assessment, incident communications, and critical event management was created— reducing the impact of internal and external threats to people and assets.

A robust risk intelligence solution requires 24x7x365 global monitoring capabilities to assess and disseminate the risk information that allows enterprises to understand, effectively manage, and mitigate the impact of critical events. Building on the best practices of NC4's 15 years of running intelligence monitoring centers, Everbridge and NC4's recently launched Risk Intelligence Monitoring Center (RIMC) combines thousands of trustworthy data sources with an experienced team of analysts, creating the industry's leading source of verified data and hyper-local threat intelligence.

This white paper sheds some light on how the RIMC provides organizations with unprecedented visibility into the threats and incidents that can impact people and business.
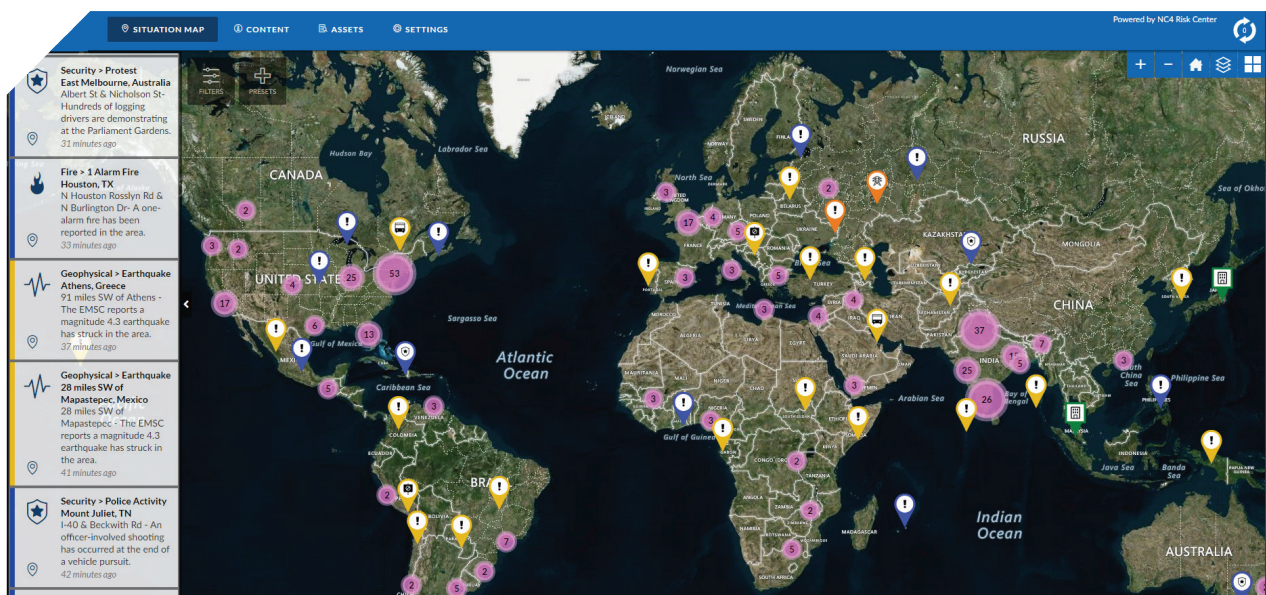

Figure 1. Information in Risk Center.

PROACTIVE RISK AWARENESS

Those tasked with protecting critical infrastructure, physical assets, supply chains, and employees must have access to real-time threat information and predictive analytics in order to execute a coordinated response to mitigate risks around the organizations they serve.

The combination of social media platforms and mobile computing (i.e. smart phones) has turned 1 in every 3 humans (over 3 billion[1] social mobile users, as of 2018) into a potential sensor and reporter of disruptive incidents. Add to that tens of thousands of breaking news reports and stories from traditional electronic outlets and other online media sources and it's a truly massive amount of data to sift through. Deepening the complexity of the challenge are the dozens of languages in which these incidents are reported.

The quantity and type of data is in fact so great that it's impossible for one human being—or even one team— to filter through the noise to find the relevant material needed without wasting time, money, and manpower. Instead, organizations must have a sophisticated set of technologies and methodologies to scan for, detect, and evaluate potential disruptive events relevant to what they care about most. The RIMC provides hyper-localized, highly customizable information. The detailed, contextual, and granular level of intelligence triggers proactive notifications based on alert profiles.
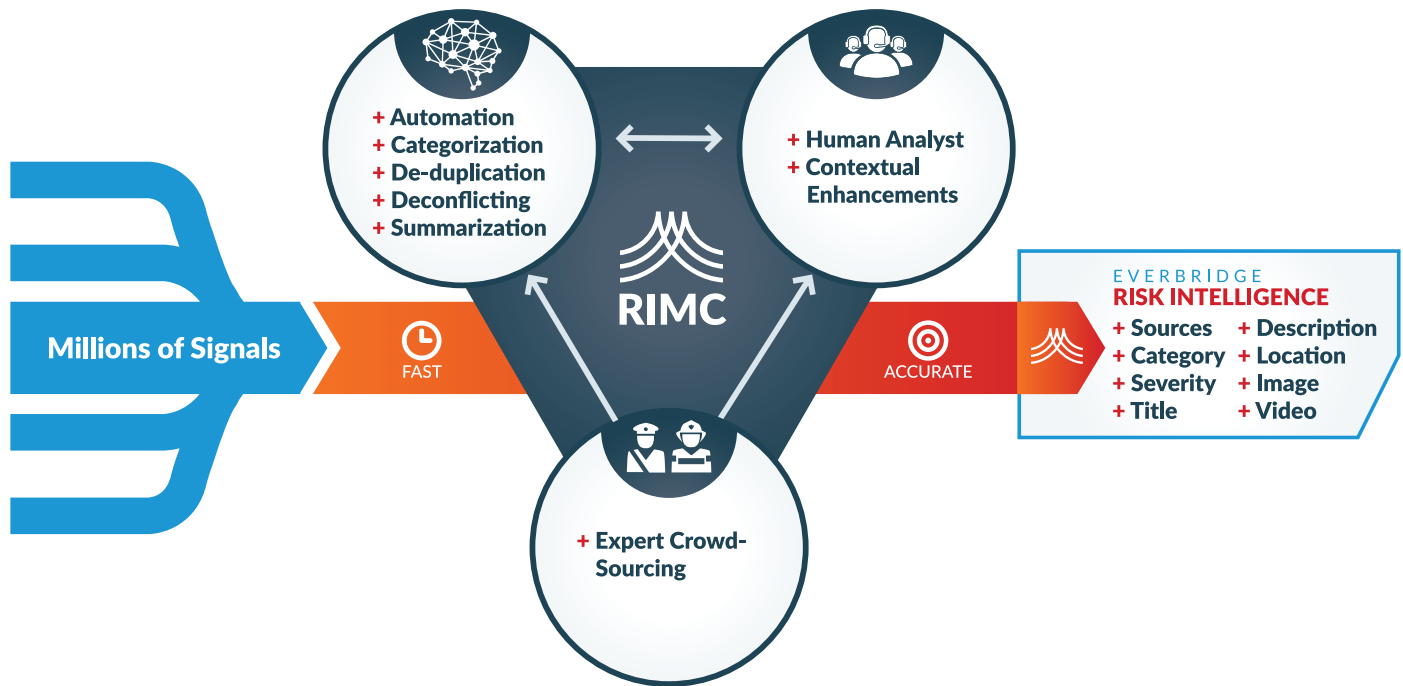
[1] https://wearesocial.com/blog/2018/01/global-digital-report-2018

Figure 2. Millions of Signals Presented with Velocity, Volume, Variety and Veracity ("4Vs" of Big Data); Detected and Processed by Everbridge RIMC

On a 24x7 basis, the RIMC leverages a variety of manual, semi-automated, and automated collection methods to winnow the universe of data signals into those that are likely to correspond to actual relevant incidents.

PROCESSING RISK INTELLIGENCE

Our process for collecting, identifying, evaluating, and disseminating risk intelligence proceeds through the following steps:
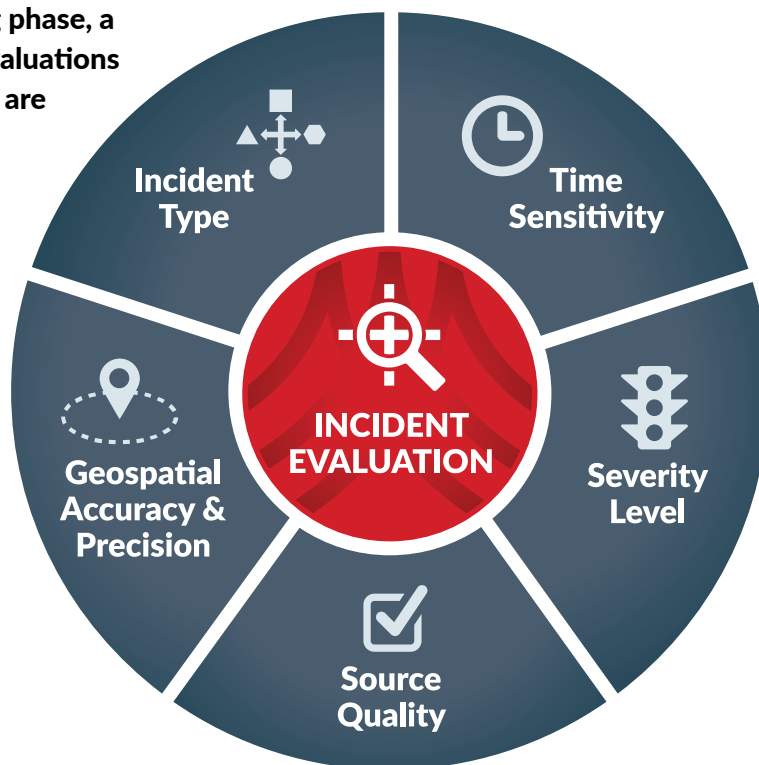
- **Identify:** Intelligence analysts work around the clock to identify incidents around the world, hyper localized to each organization's locations and assets. Various collection platforms leverage a wide combination of sources such as: government agencies, local/regional/foreign media outlets, social media networks, and other systems to identify incidents. The mixture and composition of sources varies by location, but generally the collection platforms target social media, computer aided dispatch systems, public safety scanners, local, national, and global media sources, and informational websites, among others. This provides a layered, contextual perspective for analysts, which is vital when reporting an incident accurately and timely.

- **Filter:** A multi-tier filter process eliminates 'noise' and narrows down the number of source-based reports for analysts to review manually. Analysts, with the help of systems, discard unrelated or less informative reports while allowing priority reports to pass through.

- **Evaluate:** Once these reports are received via the collection platforms, analysts, with the help of some automated and semi-automated processes, evaluate the timeliness, accuracy, and location of each incident report. The time between an incident occurring and the analyst team evaluating is usually extremely fast.

- **Decide:** A robust set of reporting guidelines and tools assist analysts in helping to decide whether the incident is significant enough to be reported.

- **Report:** Many signals lack information that can be used to identify the location with precision and accuracy. Rough locations may be established, but additional information may be required to establish the actual location with a high degree of confidence.

- **Distribute:** Then the analysts enter the data which then triggers alerts to the affected users based on their user profile settings and preferences.

The RIMC reports on a wide range of events; from fires and suspicious packages to natural disasters and terrorism, and everything in between. Our capabilities save lives, protect assets, and help ensure timely, efficient and effective response to incidents thereby mitigating their operational impact.

INDICATOR EVALUATION AND PROCESSING

Once the RIMC has detected a possible threat event, we have mechanisms in place to handle the disambiguation and evaluation (processing) of indicators to deliver timely, accurate, and contextual information to users. This includes a multi-tier filtering process that reduces 'noise' and narrows down the number of concerns each analyst needs to review manually. Once these indicators are received via the collection platforms, our team of analysts, with the help of some automated and semi-automated processes, evaluate the timeliness, accuracy, and location of each potential event. The time between an event occurring and analyst team evaluating it is usually extremely fast.

In the processing phase, a rapid series of evaluations and assessments are conducted:

Incident Type

Time Sensitivity

INCIDENT EVALUATION

Severity Level

Source Quality

Geospatial Accuracy & Precision

- **Incident Type:** To determine the appropriate response, it is critical to properly classify the type of threat event. The RIMC divides events into the following categories: Transportation, Geophysical, Meteorological, Structural, Hazmat, Aviation, Health, Security, Labor, Infrastructure, Fire, Terrorism, and Other.

- **Time Sensitivity:** A multi-tier filter process eliminates 'noise' and narrows down the number of source-based reports for analysts to review manually. Analysts, with the help of systems, discard unrelated or less informative reports while allowing priority reports to pass through.

- **Severity Level:** Characterizing events by explicit degrees of severity allows for more rapid and easy prioritization for customers.

- **Source Quality:** RIMC identifies and catalogues credible and authoritative sources that cover a wide variety of event types; due consideration is given to every source's credibility and ability to deliver accounts of the incident with veracity. For example, incidents are only tagged as confirmed when analysts are able to directly verify the information with an authoritative or primary source. If a primary source is unavailable, secondary source confirmations are often tagged as unconfirmed until further confirmation. For instance, scanner reports are often classified as unconfirmed as there is a very small likelihood that initial scanner communication can be misheard or the extent of an incident can be misstated. As an example, a fire on Beech St may be transcribed as Beach St by the listener and therefore mis-geolocated, or a violent crime with only one victim may be initially communicated as a mass casualty incident until officials further assess the situation.

- **Geospatial Accuracy & Precision:** Many signals lack information that can be used to identify the location with precision and accuracy. Rough locations may be established, but additional information may be required to establish actual location with a high degree of confidence. RIMC has an established set of tools and processes that allow our analysts to identify the location of an event and geolocate it precisely so that it can be placed in accurate context and distance to our clients' assets, personnel, and interests.

Vetted, customized, hyper-local data is essential to proactive risk intelligence. The RIMC focuses on providing actionable, relevant, and reliable information — only what's important. Our processes and our systems reduce the number of irrelevant and incomplete events that need attention. The more granular the data, the higher the likelihood you will receive actionable intelligence for a given asset.

While other risk management platforms may bombard you with initial information when an incident first occurs— a.k.a the "fire and forget" method— RIMC analysts continue to update the incident until the impacts have been minimized. Customers receive these updates as alerts depending on their preferences, customizations, and the particularity of coverage requested.

IMPACT OF SEVERITY

RIMC Thresholds

EXTREME

SEVERE

MODERATE

MINOR

Severity levels allow clients to customize the type of information they receive, empowering them to prioritize relevant incidents that affects them or require action. Severity levels are assigned by RIMC analysts based on close examination of a number of factors, including:
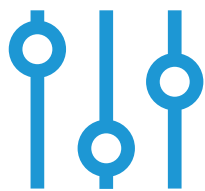
- **Type, degree and extent of impact**
- **Size of the impacted area and population**
- **Potential for escalation of the incident**
- **Context and prior patterns (ex. sensitivity of location)**
- **Estimated time to resolution**

Using hyper-local data to set thresholds, we can bring our clients' focus to incidents that are likely to: 1) yield noticeable disruption to operations; 2) involve multiple assets, or assets away from home facilities (i.e. travelers and or expats); 3) require corporate-level support for the response; or 4) warrant executive attention.

The RIMC uses the following designations to categorize the severity of an incident:

"Extreme", "Severe", "Moderate", and "Minor".

At Everbridge, we have established thresholds and severity gradations for every one of our incident types.

USER-DEFINED AND ADJUSTABLE RISK TOLERANCE

Users can capture (and adjust) their risk tolerance and notification requirements

Every enterprise has a unique risk profile based on a wide range of factors, including: geographic disposition; sector; quality and scope of security and resiliency plans; organizational size and structure; and other factors exposing the organization to threats and disruptions. For example, transportation disruptions may be critically important to an organization that relies on fulfillment centers but have a minimal impact on call center operations.

Everbridge allows clients to configure custom profiles to receive relevant alerts for a broad array of threats and incident types. Leveraging our risk profile tool, users can capture (and adjust) their risk tolerance and notification requirements based on the nexus of incident severity and proximity to identified assets.

ROLE OF RIMC ANALYSTS

Granular intelligence is hyper localized, customizable, and contextualized for each customer

Risk intelligence is not simply a data feed or alerts on your phone or app. Behind the "magic", the talented and dedicated RIMC analysts are evaluating, geo-locating, vetting, analyzing, and reporting on incidents 24/7/365. RIMC analysts are responsible for all aspects of real-time reporting from initial reporting to ongoing monitoring and closing of incidents, as well as conducting time-sensitive interactions with customers.

Monitoring centers are staffed 24/7/365 on both U.S. coasts while other analysts are stationed around the world. The majority of our intelligence team holds advanced degrees, region-specific expertise, and fluency in a foreign language. Through a partnership with CyberTech, an India-based tech company, we also have access to a dedicated team specializing coverage in India.

IN-DEPTH ANALYSIS

Global Insights analytical products reduce the media-driven noise by providing a clear and concise assessment of any situation or event worldwide

The Global Insights Team, an important component of the RIMC, is comprised of expert intelligence analysts—distinguished by their regional knowledge, language skills, and experience—who use thousands of sources to turn raw information into intelligence. The team writes in-depth risk analysis reports to help ensure the safety and security of travelers, facilities, and other assets around the world. Through their work, the team members reduce the media-driven noise by providing a clear and concise assessment of any situation or event worldwide, including emerging threats, major planned events, public health concerns, and more.

The team produces the following types of analytical reports:

- **Global Flashpoints:** Global Flashpoints (GFPs) are concise—two to three sentences—analytical pieces about trending events and developments that are taking place throughout the world and have the potential to impact client operations and travel.

- **Situation Reports:** Situation Reports provide timely, in-depth, contextual information about events that may impact organizational strategic planning, assets, supply chain resiliency, and traveler and corporate security. These reports include the latest developments of tactical and strategic importance on complex events worldwide. Situation Reports may also cover complex, long-term developments around the globe such as terrorism, drug wars, piracy, and civil unrest. Also covered are significant outbreaks of infectious diseases, particularly virulent and widespread seasonal illnesses and health-related developments.

- **Special Event Briefings:** Special Event Briefings address security risks and vulnerabilities for large-scale, high-profile planned events as well as unplanned incidents, such as natural disasters or terrorist attacks. In addition to detailing the immediate impacts of the development, Special Event Briefings could include secondary or follow-on impacts such as roadway closures, associated protests, or airspace closures.

- **Country Reports:** The Global Insights team maintains over 200 Country Reports that contain detailed analysis by country that includes a general overview, crime and security trends, arrival and departure requirements, business highlights, ground transportation guidelines, and health and medical information for travelers.

- **Analytical Briefs:** Focusing on potential near-term risk, Analytical Briefs emphasize the implications of emerging global developments that affect traveler and operational safety, security, health, and productivity. Analytical Briefs are written by Global Insights analysts using primary sources and contain original, forward-looking analysis.

- **Custom Reports:** Custom reports are produced on an as-needed basis in response to a specific inquiry from a customer. This additional service can be delivered through verbal briefings between an analyst and clients via telephone, an email response to specific inquiry, or a custom brief, such as travel report.

STATISTICS

NC4 combines thousands of vetted sources with experienced teams of analysts creating the industry's leading source of verified data and hyper local threat intelligence. We empower businesses and government organizations to collect and disseminate intelligence across a variety of industries: 5 of the 6 largest Aerospace and Defense companies, 8 of the 10 largest commercial banks, 8 of the 10 largest computer software companies, and 5 of the 10 largest pharmaceutical companies.

Types of threats monitored	At least **138** different types through real-time coverage
	At least **22** different types through Global Insights content
Number of data sources monitored	19,000+
Real-Time Incident Reports - 2018	261,829
Unique Real-Time Incidents - 2018	101,089
ActivWeather Notifications – 2018	3,312,183

These statistics reflect a lot of intelligence; but, they are only numbers. The story behind the statistics encompasses breadth of coverage, timeliness, granularity, and performance.

Let us show you how top quality and relevant risk intelligence can make a difference in keeping your people safe and your operations running faster.

Visit **www.everbridge.com** to learn more.

ABOUT EVERBRIDGE

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order to keep people safe and businesses running. With the acquisition of NC4, the company has created the industry's only end-to-end critical event management and threat assessment platform to keep people safe and business operations running. Together now under one company, Everbridge is providing the most comprehensive solution for enterprises and government agencies to reduce the 'time to know' that a critical event has occurred through to remediation, all from a single pane of glass.

Everbridge serves 9 of the 10 largest U.S. cities, 8 of the 10 largest U.S.-based investment banks, all 25 of the 25 busiest North American airports, six of the 10 largest global consulting firms, six of the 10 largest global auto makers, all four of the largest global accounting firms, four of the 10 largest U.S.-based health care providers and four of the 10 largest U.S.-based health insurers. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Beijing, Kolkata, London, Oslo and Stockholm. For more information, visit www.everbridge.com, read the company blog, and follow on Twitter and Facebook.