Identifying and Responding to Threats

Incident monitoring and your critical communication strategy

Threats know no organizational boundaries. Hurricanes, bombings, power outages, and infrastructure events remind us that all organizations are vulnerable to both manmade and natural disasters. The key to improving corporate resiliency is identifying and preparing for threats that pose danger to your assets, operations, and people. While risk assessments and risk management plans are crucial to every organization, another key component of any operational risk management process is incident monitoring.

Incident monitoring allows organizations to:

- Improve risk mitigation
- Reduce business impact
- Ensure continuity of business operations
- Protect the health, life, safety and productivity of employees
- Streamline risk-related decision-making processes
- Reduce costs

Global risk and incident monitoring makes this possible, as it allows organizations to obtain timely, targeted, and relevant incident information that helps identify direct risk.

Ongoing and comprehensive incident monitoring provides a level of risk visibility that goes beyond risk assessments and contingency planning. If an organization is proactive in finding out about incidents that impact them, they can begin the mitigation process earlier and reduce the business impact of the threat.

Effective Incident Monitoring: Processes and Technology

Focused, targeted, and timely incident monitoring data improves risk visibility, allowing you to understand what the global threat picture means to your organization and your assets around the world. In order to be successful, incident monitoring processes and supportive technology must adhere to these best practices:

Information must be Timely

Incident monitoring needs to be real-time or as close to real-time as possible. The earlier you can get information the better; if an organization is only informed about a threat once it impacts operations it might be too late. Real-time information allows organizations to be proactive about risk mitigation – both from the perspective of planning your response based on advance notice and reducing impact through effective response management once the inevitable incident occurs. In addition, situations don’t often evolve according to plans; ongoing incident monitoring that provides situational awareness supports a flexible and dynamic response.

In time-critical events, like active shooter scenarios, incident monitoring might be the only way an organization finds out about an incident before its conclusion – local responders and staff are often consumed with responding to the event, and aren't able to relay information about the situation.

Monitoring must be 24/7/365

Threats can happen at any time – they're not limited to business hours. Often the worst incidents with the biggest negative impacts occur in the middle of the night and/or on weekends or holidays. Organizations need to conduct incident monitoring 24 hours a day, seven days a week, 365 days a year. Automated monitoring tools enable organizations to be connected at all times. Even if your organization doesn't operate outside of business hours, incidents that aren't managed properly can have a long-lasting impact, and prevent business from resuming.

Monitoring must be Comprehensive

Many organizations focus only on major events like severe weather, acts of terrorism, or large scale outages. However, it is important to conduct all-hazard incident monitoring, as smaller events could be a threat as well. For example, a water main break or small fire can be just as damaging as a blizzard or a security event. It is crucial to look at everything, as missing – or ignoring – a small event could lead to costly damages.

Information must be High Quality

Information needs to be as accurate as possible, which often means balancing a trade-off between quality and timeliness. If the information provided to an organization isn't accurate it offers no benefit. It is important to understand where the information is coming from, how accurate it is, what the sources are and if it has been verified. To ensure accuracy, use multiple sources to vet all threat information.

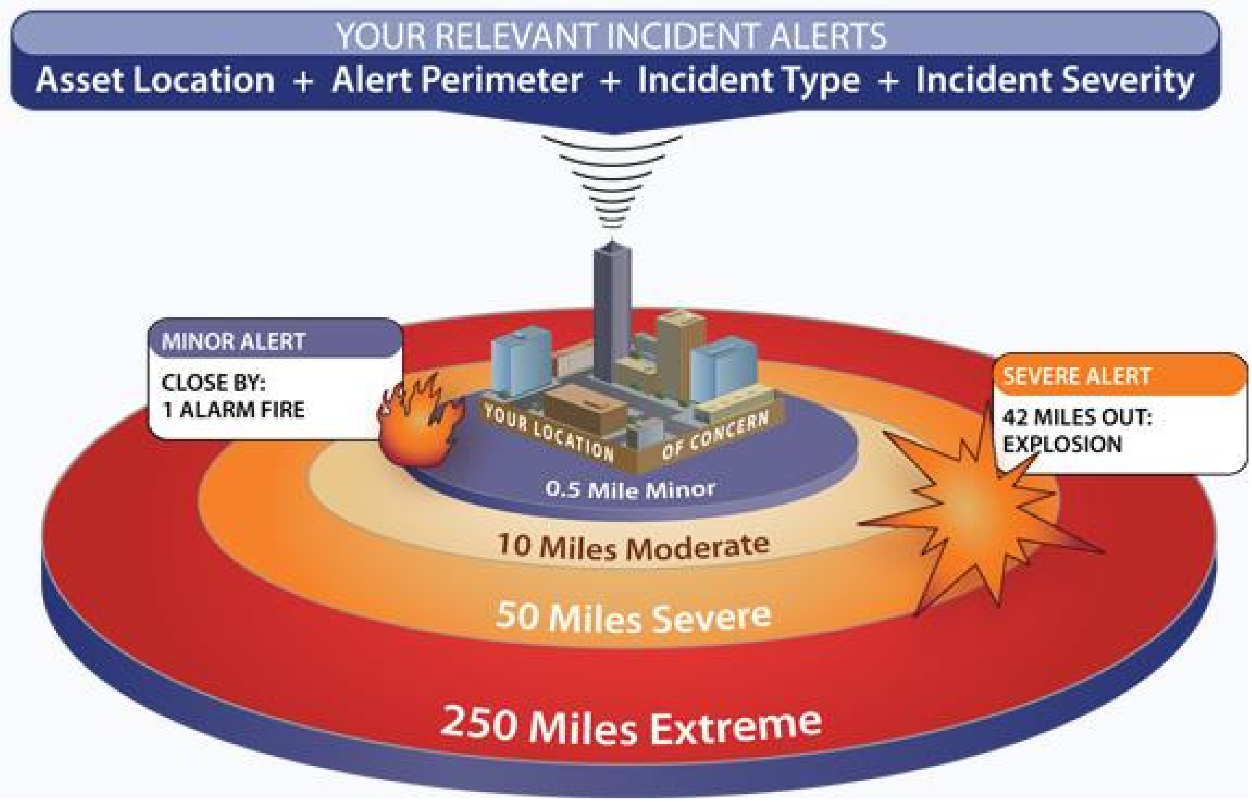
Early, unconfirmed information may be unreliable – but it can still be valuable, providing early warning of developing events and allowing organizations to prepare a response or head off an incident. Organizations should have visibility into "unconfirmed" threat reports, but should plan their response strategy accordingly. For example, if information is received from a police scanner it is likely to be tagged "unconfirmed" until it has been confirmed by a government source (e.g. police department, fire department, etc.) or confirmed by virtue of it being disseminated by reputable media sources. The information could be correct, but cannot be treated as 100% accurate.

Information must be Relevant

One of the most important characteristics of effective incident reporting is relevance. Incident information can be overwhelming unless properly filtered for relevancy. For example, an active gunman in Las Vegas likely doesn't impact business at an organization in Boston. Organizations shouldn't have to decipher which threat information is relevant to them. There are a couple of questions that can be asked to determine relevancy:

- How likely is a threat to affect you?
- How close is it to you? Is the threat local to your organization?

Numerous threats happen around the world every day. They key is being able to determine which threats are relevant that actually pose a risk. Today's technology allows for powerful profiling and filtering capabilities to ensure that incident alerts are as relevant as possible.



Relevancy is Crucial to Effective Incident Monitoring

Image source: NC4

Managing Incident Impact through Threat Monitoring

Minor Incidents Can Have a Major Impact

When putting together your monitoring strategy, it is important to understand the potential impacts of incident types on your organization. In many cases, organizations overlook the fact that, in some situations, seemingly minor threats are just as important as major threats. In fact, a minor incident could end up having a major impact.

In a real life example, a major investment bank lost over 10 million dollars in revenue due to a water main break. The break happened on a Saturday afternoon down the street from one of their facilities, flooding the basement and taking out an electrical transformer. The resulting outage brought down a foreign currency trading system. Only then did the company's IT department become aware of the incident. When the Asian financial markets opened on Sunday, the financial institution was unprepared to process critical transactions and they had to send the trading business to their competitors. Early warning of the water main incident would have provided adequate time to mitigate the impact and prevent the resulting financial losses.

Another example of the impact minor incidents can have is in the telecommunications industry. Major wireless operators manage many locations with unmanned computer and radio switching components controlling their networks. Minor incidents such as small roof fires can cause component failures which often result in dropped calls and customer dissatisfaction. Monitoring incidents at the granular level (1/10th of a mile) can give early warning of fires and other events and provide network operations staff adequate time to re-route call volume around the components before they fail.

Early warnings about this type of incident can help an organization prevent a minor threat from causing a significant amount of damage. The key is to remember that both minor and major incidents can have a lasting impact on an organization if not properly addressed, and included in a monitoring strategy.

Major Incidents Can Have a Major Impact

Of course, major incidents that have wide impacts are important to include in incident monitoring and planning as well. Security incidents occur constantly on a global basis. Incident reporting is extremely useful in the midst of security incidents, especially when lives are in danger.

Major incidents, including terrorist attacks such as the Boston marathon bombing, the Volgograd train station bombing in Russia, or the Kunming attack in China, garner substantial media attention and can have major impacts for organizations with expats or travelers in the vicinity.

Managing the Business and Productivity Impacts of Incidents

Finding out about an incident early can be a huge benefit to managing its impact. Security incidents not only threaten the safety and security of residents, responders, and employees, they can have an economic impact related to lost sales revenue, negative public relations, and missed work.

Even those incidents that don't directly impact the assets of an organization can still be disruptive if not proactively managed. For example, a school shooting may seem unrelated to the operations of an area business. But employees in critical roles, like call center workers, could also be parents with children at the school. When these employees rely on the media for breaking news about the incident, they may receive sensational and inaccurate information. Allowing rumors to spread can negatively impact the productivity of a call center as parents panic and seek information on their own.

In this instance, if an organization can provide its employees with accurate and up-to-date information about the situation, they can proactively manage the impact. Providing relevant facts to employees can identify those who have been directly impacted, allowing them to leave so they can attend to their families. This means that the situation can be managed internally to have a limited impact on productivity.

In all cases, finding out about incidents early is essential, as it puts organizations in the position to better manage the impact. Getting out ahead of an incident allows for better preparedness and repositioning of assets.

Minimize the Impacts of Incidents through Communication

Incident monitoring also plays a vital role in ensuring rapid information sharing during these critical incidents. Once you know about an incident you also need to respond, notifying all the right people and providing clear instructions on what to do.

As part of your incident monitoring planning, build out a plan for communicating around identified threats. Identify threats that could affect your organization or constituents, and plan a communication strategy for multiple scenarios – both minor and major. A prepared, documented communication plan is critical for incidents that are likely to impact the safety, security, and productivity of your contacts.

For each type of threat, identify how you would respond:

- Who is involved in threat response?
- What processes would be followed?
- Who would be impacted?
- What messages would be communicated?

Based on your responses to these questions, you can create message templates to help speed your response during time-sensitive events. Templates should be prepared for multiple event stages (before, during, and after event impact) and should be matched to the anticipated mode of delivery (voice call, SMS, email, etc.).

Your communication plan should also include a process for on-the-fly messaging, for unexpected scenarios or developments. This means that your communication technology needs to support quick creation and quick delivery of messages that may be crafted shortly before they are sent.

In all cases, messages related to incidents should be simple – short, readable, and actionable. The wording and structure of a message can impact reader comprehension and affect successful incident management. A guideline to use when crafting your messages is Dr. Chandler's 3-3-30 recommendation, outlined in his book, *Emergency Notification*:

- No more than 3 message points
- Deliver 3 short sentences
- Keep the key content in the first 30 words

The key to effective response is not only identifying threats before they happen – but also communicating to those who are potentially affected in time for them to minimize the impacts. Effective two-way communication with your contacts, including on-the-scene resources, can help you supplement incident monitoring by gathering front-line intelligence to guide response.

Key Takeaways

- Comprehensive monitoring is critical for risk management.
- Minor incidents can have a major impact, especially if they're close and affect an organization directly.
- All-hazards monitoring is key, as it allows an organization to be aware of incidents ranging from an active shooter to a water main break.
- Incident reporting should be 24/7/365 and requires the best quality information available.
- Relevant information is critical, as organizations need to respond to the right incidents and avoid information overload.

About NC4 and Threat View

NC4 provides revolutionary safety and security solutions that empower government and business with accurate, timely and secure information. NC4 solutions are used in the public sector by federal, state and local agencies in both emergency management and law enforcement disciplines, and in the private sector by companies involved in financial services, high-tech, insurance, manufacturing, aerospace and defense, oil and gas, pharmaceuticals and healthcare, as well as several other industries. NC4 takes a comprehensive and integrated approach to safety and security by providing: relevant global security and travel intelligence, analysis, traveler tracking, and real-time threat alerting to mitigate risks; a common operating picture for fighting crime and managing emergencies; and a platform for secure communication and collaboration.

Everbridge Threat View, powered by NC4, combines the world-class risk assessment intelligence of NC4 Risk Center™ with Everbridge's Unified Critical Communication Suite and global reach, empowering organizations to respond to risks and improve resiliency.

Everbridge Threat View merges predictive, real-time risk intelligence with mass notification, situational intelligence, GIS targeting, and incident management. Users will leverage this comprehensive tool to monitor threats, avoid risk escalation and communicate effectively during disruptive events. This solution brings to market a unique combination and level of risk assessment, mitigation, response, and communication.

Threat View enables organizations to:

- Access NC4 Risk Center global threat assessment information from within the Everbridge interface
- Establish alerts based on proximity, severity, and type of NC4 Risk Center incident
- Visualize on a map active alerts with proximity to Everbridge contacts
- Quickly communicate with potentially impacted contacts using map-based targeting
- Rapidly notify contacts in the surrounding area using phone, email, SMS text, and mobile push notifications
- Identify missing employees and employees in need with real-time polling
- Provide ongoing situation updates to executives as an incident progresses
- Assemble and collaborate with response team members instantly using 'one-click' conference calls

Visit www.NC4worldwide.com to learn more.

About Everbridge

Everbridge provides a unified critical communication suite that helps clients be better prepared, make better decisions, and respond quickly and confidently during disruptive events. When an incident happens, whether it's a natural disaster or an IT service outage, we automate communications to ensure that the right messages get to the right people at the right time.

Widely recognized by analysts as the market leader, Everbridge solutions are trusted by clients in all major industries and government sectors to connect with over 50 million people around the world.

THE ONLY END-TO-END PLATFORM

- **Planning**: Everbridge is easy to set up, maintain, and organize, meaning that you're always ready for a quick, coordinated response. Everbridge ensures that the right messages get to the right people - with the most advanced opt-in portal on the market, streamlined integration with internal and external data sources, and simple group and contact management.

- **Assessment**: When trouble strikes, you need rich insight, presented simply - so you can quickly assess potential impact and make an informed decision to avoid loss. Everbridge offers the only solution on the market that meets these demanding requirements, with the most advanced interactive dashboard in the industry.

- **Response**: In critical situations, ease-of-use can mean the difference between an effective response and a mistake that carries serious consequences. Everbridge is engineered to be simple to use under pressure, with a user interface that accelerates time-to-message and reduces the likelihood of errors.

- **Delivery**: Even during large-scale disruptions, Everbridge stays on. The most advanced platform in the industry ensures that you reach your contacts - every time. And with worldwide coverage and capabilities, including globally local calling infrastructure and data storage, we're ready to support you wherever your people are in the world.

Visit www.everbridge.com to learn more.