

Leading Through Crisis: A Guide for Security Leaders



In today's complex threat landscape, security leaders across industries and functions—physical security or cybersecurity—must step into the role of crisis leaders to ensure resilience and continuity.

According to a report by the [Business Continuity Institute](#), 75.1% of organizations had to activate their crisis management team over the past 12 months, demonstrating the prevalence of risks faced by businesses. This has underscored the need for organizations to build operational resilience for today and tomorrow.

As a result, leaders now have expanded mandates and are more focused on improving business resilience. To ensure their organization can thrive amid disruption and uncertainty, they must move from managing to leading crises. Here we explore three ways security leaders can do so effectively.

Delegate and communicate effectively

During time-sensitive and disruptive events, CSOs and CISOs must communicate multiple messages—up, down and across the organization—quickly and often with incomplete or ever-changing information. It's important to be transparent about what is known and what is not. Senior leadership and employees need to be able to trust security leaders, their teams and the communications they receive—even if the news is bad or if security leaders have to admit they don't yet have the answers.

The tone of communication is also critical. During an emergency, it is crucial to use a calm and people-centered approach. While emotions always run high during a crisis, avoiding unnecessary panic will allow employees to respond to directions appropriately and make rational decisions.

In addition, a crisis leader's superpower is delegation. Learn to delegate to the point of discomfort and then delegate a bit more. This means also learning to trust and empower your team to make tough decisions. Help them to do so successfully by first creating a long-term view with a clear link between the now and what will be. The picture you paint of the future state should be as vivid and whole as possible, so that your team can see how they as individuals play a role.

Continually reinforce the post-crisis vision and establish principles around the decision-making process. This will help clarify what should be prioritized and allow the team to make well-informed decisions. Then, communicate that same vision to the broader organization to help prepare for the changes ahead. The key here is knowing how to refine the volume of data and intelligence and differentiate between information that is directional, must be actioned and requires a decision.



3 questions security leaders should ask when facing a crisis:

1

What do I know?

Facts are the bedrock of risk and crisis management; you will need to be as informed and as current as possible. Rely on your human and technical networks. AI-powered technology, such as real-time alerting solutions, can help you and your team maintain situational awareness of unfolding events.

2

What do I need to know?

There will be gaps in your knowledge and understanding of any crisis. Look to your team to identify what those gaps are and determine, as quickly as possible, how to fill them. The board will also give you critical information requirements. It's your job to provide answers, which may not be readily available without the help of additional resources or frameworks.

3

What do I think?

Making smart assumptions about what is going to happen next—and its likelihood—is fundamental to any crisis leadership and planning function. You must be clear in communicating those assumptions and the data underpinning them.

Understand your risk landscape

Watch for internal and external risks

We know crises are inevitable. But when a crisis does occur, many security leaders tend to focus inward, when research has shown that the most effective crisis leaders will place an equal emphasis on the internal and external environments. They understand that they don't operate in a vacuum. Their security operations are inextricably tied to both internal organizational partners, such as legal, risk and HR, as well as external stakeholders like customers, regulators, suppliers, and vendors.

Remember that external partners have a vested interest in your success, and the strength of those relationships is a key part of building resilience. Establish those vital relationships now so that you can lean on and/or influence them during a crisis. At the same time, stay informed about your third-party risk exposure to protect yourself from potential cascading effects should your external partners face a crisis.

Maintain situational awareness of threats

Whether managing a corporation, a government agency, or a nonprofit, understanding the risk landscape is critical to building resilience. High-performing CISOs and CSOs understand the threat landscape and how both macro and micro risks—be they global, regional, or local—might affect the business.

Effective security leaders are also those who implement advanced technologies to maintain situational awareness of risks at all times. For example, AI-powered tools, such as real-time alerting and intelligence systems, are invaluable for leaders across industries, from safeguarding critical infrastructure to ensuring public safety. Dataminr's [Intel Agents](#)—a new form of agentic AI developed specifically for security teams—uncover and deliver the most relevant context about any global event, threat, and risk in real-time. Armed with real-time intelligence, security leaders can move from identifying the 'what' of a situation to understanding the 'so what' in seconds. This allows them to quickly determine the impacts on their organization and respond more effectively.

"A lot of times we don't know there's a crisis right away. By using Dataminr... we're able to see stuff going on well before many of our competitors and many of our folks out in the field, and before you hear about them in the news."

Doug Russell,

Sierra Nevada Director of Security and Safety Data Integration Strategies

Read more: [Sierra Nevada Improves Crisis Management With Dataminr Pulse](#)

"Before Dataminr First Alert, we could not react to [an incident] until it was already happening. Now, we're able to proactively identify key priorities based on [public safety] trends. It's allowing us to save a ton of lives,"

Commander,

Defense

Read more: [The Total Economic Impact™ of Dataminr First Alert](#)



Top 5 global risks of 2025

1. State-based armed conflict
2. Extreme weather events
3. Geoeconomic confrontation
4. Misinformation and disinformation
5. Societal polarization

Source: [World Economic Forum](#)

Organizations' top 5 drivers of crisis activation

1. Extreme weather
2. Third-party failure
3. Cyber attack
4. Civil disorder
5. Health and safety incident

Source: [Business Continuity Institute](#)

Top 5 areas where AI can help within crisis management

1. Data analysis and decision support
2. Real-time alerts
3. Predicting potential crises
4. Automating response protocols
5. Communication and coordination during a crisis

Source: [Business Continuity Institute](#)

Run the personal stress test

Crisis leadership requires not only strategic thinking but also personal resilience. Leaders across sectors and functions must prepare themselves to remain calm and decisive under pressure. However, if you don't yet know how you will react in times of crisis, it's difficult to set yourself up for success. Learning to stay calm in a high-pressure environment may prove the most challenging obstacle to achieving a desirable outcome: minimize disruption and maintain business continuity.

The best way to do that is to put yourself in stressful situations—just as you would test your risk and security protocols. Practice making tough, strategic decisions in as realistic an environment as possible. How do you react? What are your weaknesses? Your strengths? There are psychometric tools that you can use to stress-test yourself; some firms use them for crisis leadership training. The goal is to understand what happens to you when faced with a crisis.

You'll also need to master other aspects of effective crisis leadership, which demands a mix of hard and soft skills such as: maintaining situational awareness; when and how to be directive; and managing complexity and multidisciplinary teams.

Being an effective crisis leader also calls for defining and honing your leadership style. Here are three styles that can prove useful in a crisis:

1. Transformational leadership.

Focuses on team-member growth through collaboration and communication. When done right, the result is valuable, positive change within individuals, and better team performance, retention and morale. The goal is to develop followers into leaders.

2. Cognitive leadership.

Calls for understanding the environment that you are leading and then applying whichever leadership style, tool or skill is needed for the situation.

3. Transactional leadership.

Focuses on the role of supervision, organization and group performance. Also known as managerial leadership. Whereas transformational leadership fosters growth and innovation, transactional leadership helps ensure operational efficiency—both are critical in navigating crises across industries and functions.

Learn more

Discover how [Dataminr Pulse for Corporate Security](#), [Dataminr Pulse for Cyber Risk](#), and [First Alert](#) enable CSOs and CISOs across private and public sectors to stay ahead of critical events and risks, better manage crises and maintain their organization's resilience.

This ebook has been updated from the original, published on October 7, 2021, to reflect new events, conditions or research.

