

# Cyber Crisis Management



**Readiness, Response, and Recovery**

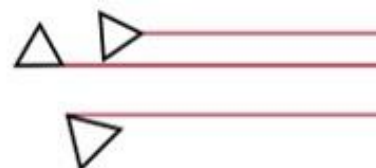
CSG TECHNOLOGIES

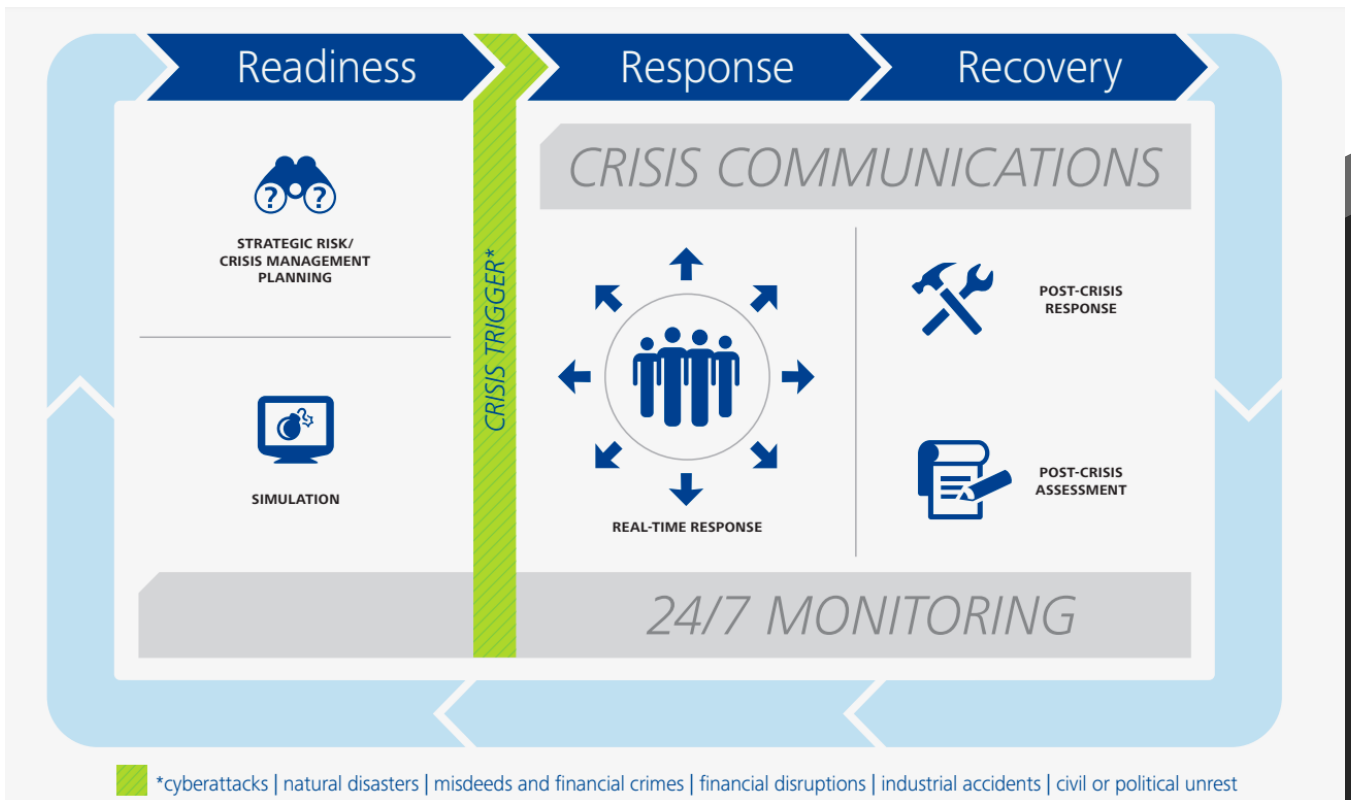




Hacked devices, crashed websites, breached networks, denials of service, copied emails, stolen credit card data, and other cyber incidents have become commonplace. It's enough to leave one thinking—correctly— that no organization can achieve totally assured cybersecurity.

Most organizations have therefore developed some level of cyber incidence response (CIR) capabilities.





# The Need for Crisis Planning

CBS.com notes that 1.5 million cyberattacks occur every year, which translates to over 4,000 attacks every day, 170 every hour, or nearly three every minute.<sup>1</sup> While few attacks succeed, the high probability of cyber incidents dictates that every organization needs to be prepared to respond effectively.

Effective preparation addresses the entire crisis management lifecycle of readiness, response, and recovery.

Each phase of this lifecycle presents opportunities to protect the organization from risks, costs, and damage emanating from an incident—and to strengthen the organization’s defenses going forward

# Readiness

Readiness equates not only to vigilance, for example in the form of 24/7 Monitoring, but also to readiness of resources. A well prepared, multifunctional team must be poised to deal with all aspects of an incident or crisis. In addition, crisis simulation and wargaming enables management to understand what can happen, which steps to take, and whether the organization is truly prepared.



# Response

Management's response can either contain or escalate an incident; indeed, a poor response can even create a crisis. Vigorous, coordinated responses to incidents limit lost time, money, and customers, as well as damage to reputation and the costs of recovery. Management must be prepared to communicate, as needed, across all media, including social media, in ways that assure stakeholders that the organization's response is equal to the situation.



# Recovery

Steps to return to normal operations and limit damage to the organization and its stakeholders continue after the incident or crisis. Post-event steps include assessments of the causes and of the management of the incident or crisis, and promulgation of lessons learned.

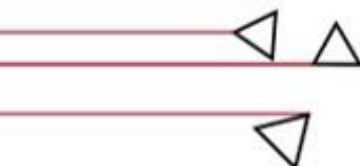


Effective crisis management extends beyond preparing for any specific event to development of broad, flexible capabilities that enable response to a wide range of events along various dimensions. From the standpoint of cybersecurity—the main deterrent to cyber incidents—the goal is to develop a secure, vigilant, and resilient organization.

IT and digital assets now drive a huge portion of enterprise value. Knowing this and understanding system vulnerabilities, attackers target organizations repeatedly and from various angles. Therefore, the risk that cyber crises pose to reputation, brand, operations, and customer and supplier relationships will continue to increase, as will the associated legal and financial effects.

No board of directors or senior executive team can credibly deny the seriousness or the likelihood of cyberthreats. So, the time to prepare a highly effective cyber crisis management plan is before a cyber incident occurs.





# Are you ready?

Most organizations will lack the resources to develop and maintain all necessary incident and crisis response capabilities in-house. The expertise required, the evolving risk landscape, and the resources of cybercriminals render it impractical for most organizations to do it alone. Thus, an outsourced or co-sourced approach with a provider of managed cybersecurity and response services may be the best option for most organizations.