Confronting Complexity in Managing a Cyber Crisis
Lessons Learned for Responding at Network Speed

by
Admiral Mike McConnell, USN, Retired
Senior Executive Advisor, Former Vice Chairman
Former Director of National Intelligence, Director of National Security Agency
mcconnell_mike@bah.com

Admiral Thad Allen, USCG, Retired
Executive Vice President
For the unified responses to the Deep Water Horizon spill,
Principal Federal Official for Hurricanes Katrina and Rita
allen_thad@boozallen.com

Mr. Christopher Ling
Executive Vice President
ling_christopher@bah.com

Booz | Allen | Hamilton
delivering results that endure
Corporate leaders recognize that their organizations will likely experience a cyber breach or system breakdown of some nature. But rare is the executive who thinks such an event will lead to an organization-threatening crisis—until it does. Too often, companies are unprepared to address the myriad issues created when intruders gain access to critical networks and data. Given that corporations have come to understand that a network breach is virtually inevitable, why do so many remain ill-prepared to manage the resulting crisis?

Corporate responses that bring too little too late typically suffer from two significant shortcomings. First, despite a growing realization among corporate leaders that a cyber breach can pose serious, broad-based challenges, their response efforts often focus on the technical problems. That is, they concentrate on finding and removing the intruders as quickly as possible, while also ensuring that business operations continue with as little disruption as possible. These activities are vitally important, but the impact of a cyber breach can reverberate far beyond a company's networks and business operations. Depending on the intrusion, it may also create an intellectual capital problem, a customer problem, a legal problem, an operations problem, a policy problem, a lost-revenue problem, and a communications, public relations, and brand problem. Corporations must be prepared to manage the wide range of internal and external issues that may arise. If not handled with speed and effectiveness, these problems can destroy corporate value that took years to build.

The second shortcoming is that many companies respond to a cyber crisis using traditional business problem-solving approaches, as if crisis action planning were the same as strategic planning, which focuses on quarterly and long-term performance. But the issues created by a major breach are too complex for normal planning processes and conventional leadership modes, particularly because a rapidly unfolding cyber crisis demands confident decision making and execution—all at the speed of the network.

Corporate leaders can better respond to cyber crises by applying the best practices of military operational planners and national preparedness agencies. Their lessons learned offer valuable insight into how corporations can prepare for and manage a cyber crisis:

1. **Identify All Potential Cyber Crises.** Rigorously analyze their probable occurrence and severity of impact upon the organization—across all functions—and its external stakeholders.

2. **Create Integrated Response Plans.** Coordinate the organization's many departments and stakeholders so they speak and act as one.

3. **Exercise the Plans.** Practicing your integrated response regularly will improve the response and the plans.

4. **Assign Responsibility for Creating, Exercising, and Executing the Plans to a Single Position.** Institutionalize collaborative decision making, but assign authority to one person who will be held accountable for effectively resolving the crisis.

In today's highly interconnected global economy, a major breach can quickly explode into an extinction-level event for a victimized organization. The key to corporate resiliency is anticipating and addressing the full range of issues that are triggered by the intrusion. The entire enterprise, not just the security team, must be prepared to respond quickly and with unity of purpose to those issues.
How Did Cyber Incidents Become Complex Cyber Crises?

Most corporate leaders today recognize that a cyber breach is inevitable. No matter how strong their security, sooner or later a malicious actor will break into or access their network and systems. In addition to building a strong perimeter, companies are also building proactive threat identification and response capabilities that are aimed at quickly finding and removing cyber intruders, while ensuring that business operations continue with as little disruption as possible. New tools, skills, and approaches—such as continuous monitoring of networks and data analytics that provide a predictive edge to intelligence—are designed to alert security teams to anomalous actors and isolate intruders before they can inflict serious damage.

Despite such efforts to minimize risk, the news is replete with stories of industry and government organizations—many armed with strong cyber defense capabilities—that struggled to contain the unexpectedly harsh fallout from a network breach. As we have seen in numerous cases involving banks and financial institutions, retailers, healthcare organizations, and multinational corporations, a cyber incident can undermine customer loyalty, taint the corporate brand, and damage the bottom line. It can also threaten the jobs of top corporate leaders. These incidents have left many people wondering: How did network intrusions that once posed headaches only for the IT shop grow into major crises that threaten companies with significant, long-term damage?

A number of factors have combined to create the potential for cyber disasters:

- Digital technologies permeate every aspect of corporate life. Corporations are using digital technologies to improve operations, market new products, and boost revenue and profits, but these same technologies have also made it possible for malicious actors to gain access to large stores of sensitive business data and disrupt operations in ways that were virtually impossible in a paper-driven world.

- Criminal hackers, state-sponsored actors, and insiders have become extremely sophisticated in developing new techniques and schemes for penetrating corporate and government networks. They are relentless in their efforts to gain access and often difficult to detect once they are inside.

Exhibit 1 | Number of Data Breaches Continues to Rise

According to the Identity Theft Resource Center, the number of US data breaches reached a record high of 783 in 2014, a 27.5 percent increase over 2013. The medical/healthcare industry experienced the most breaches (42.5%). The organization has tracked data breach incidents since 2005.

• Technology’s increasing complexity compounds these risks. Innovations such as cloud and mobile computing introduce new vulnerabilities and opportunities for malicious actors to penetrate networks and systems.

• The increasing interconnectedness of corporate and government networks increases the risk that cybersecurity problems will be shared, often unknowingly. A foreign supplier located thousands of miles away could be the conduit for an aggressive attack. Moreover, as the Internet of Things becomes more pervasive, the opportunities for attack—and the concurrent corporate risk—grow exponentially.

These interrelated factors have increased the odds that a company will experience a major breach in which sensitive corporate or customer data is stolen or critical operations are disrupted. These developments have also shortened the time that corporations have to respond when a breach is discovered because the longer malicious actors remain on corporate networks and systems, the more damage they will inflict.

**Cyber Crises Unfold at Network Speed**

There’s another important reason that an immediate response to a cyber crisis is needed: The rise of 24/7 news media and the ubiquitous presence of social media and mobile devices. Previously, when a cyber incident occurred, corporate leaders had a small window of time to investigate the problem and formulate their public response. They could even issue a few “no comments” to the media, all with the good intention of offering a full accounting once they identified the problem and developed a solution. That is not possible today. When a cyber breach occurs, silence by the corporation is immediately filled by reporters, talking heads, and interested chatters on Twitter and other social media, forcing the company’s spokespersons to play defense in crisis messaging.

The end result: A cyber breach quickly becomes an enterprise-wide crisis. In addition to tracking down and eliminating the attackers, a company is fielding complaints from customers whose credit card information was stolen. The public relations staff is answering a host of questions from the media regarding the breach and its impact. The legal team is scrambling to understand the company’s liability, as well as to help craft public statements that don’t invite lawsuits. The finance department is calculating the potential costs to repair the damage, such as paying for credit monitoring services for customers whose personal information was stolen. They also are calculating the potential drop in revenue, profit, and stock price caused by the controversy. The marketing department is crafting a strategy to retain and win back customers. Corporate leadership is responding to inquiries from law enforcement or government regulators. And all these activities are playing out in a 24/7 environment that demands constant updates on progress.

It’s clear that a major cyber breach—e.g., one that involves sensitive corporate or customer data—poses more than a technical problem. It’s more than a business continuity challenge. A major network intrusion can create a multidimensional crisis that impacts nearly all aspects of the company’s business, as well as its customers, regulators, and other external stakeholders. A cyber crisis is marked by the complexity of the issues that must be addressed and the speed at which they unfold. For banks, retailers, and other types of corporations, a breach that spirals into an out-of-control public relations disaster can become an extinction-level event. Once customers lose faith in the security of the victimized enterprise, they will take their business elsewhere and never come back.

**Responding Effectively to a Cyber Crisis**

Thriving businesses are typically adept at strategic planning. That’s why they are successful. But too often, corporate leaders approach cyber crisis action planning as if it were a strategic planning exercise. It’s not. There are some similarities between strategic planning and crisis action planning—both call for objective, fact-based decision making—but they also differ in several important respects. A strategic planner
has time to develop forecasts, examine alternatives, create new solutions and, to some degree, pick and choose the market signals to which the company will respond. In contrast, the crisis manager must react to all the problems created by the cyber breach. Immediate situational awareness is essential because the manager cannot choose to address some issues while ignoring others. The crisis manager must make do with available information and resources, while the strategic planner has time to develop both. Once a breach occurs, it’s too late to develop a strategic plan for responding to the crisis. Attackers are operating at network speed. News and social media are reporting at network speed. Consequently, crisis action teams must respond at network speed.

**When a major breach occurs, attackers are operating at network speed. News and social media are reporting at network speed. Consequently, crisis action teams must respond at network speed.**

How should corporations approach cyber crisis management? In preparing an effective response to major cyber crises, corporations can learn from two groups of crisis planners: military operational planners and disaster preparedness planners. Military planners are preparing for specific mission scenarios that require clear communications and precise coordination among numerous actors. Preparedness leaders are preparing responses to a variety of potential disasters, both natural and human-made, which also require effective communication and coordination among dispersed government and nongovernment stakeholders. Our recommendations for corporations are based on our experience in leading major disaster response activities (cyber- and noncyber-related) for government and corporate organizations. In addition, Booz Allen Hamilton provides the military-grade cybersecurity—multilayered threat defense operations and incident response—to the public and private sectors. In fact, Booz Allen is one of just nine companies that have been issued cyber incident response assistance (CIRA) accreditation under the National Security Agency’s National Security Cyber Assistance Program. We have also worked closely with military and preparedness organizations to help them plan for and execute their response plans.

We understand the full range of internal and external issues that need to be addressed, and the best practices for executing a successful response in a cyber crisis.

In developing effective response plans—that is, plans that lead to successful crisis management—corporations should follow four main principles:

1. **Identify the Potential Cyber Crises.** A company should identify in advance the cyber crises that could occur, such as a theft of intellectual capital or personally identifiable information (PII) or major denial of service attack. All possible scenarios should be examined. All stakeholders should be identified.

   This examination should also include a rigorous analysis of how these potential scenarios will impact the various financial, operational, legal, sales, and other activities of the business, as well
as investor relations, customer relations, and other external-facing issues. The estimated impacts may vary based on whether the breach was caused by an insider, foreign state, or criminal hacker. In addition, each type of cyber incident will have varying impacts across the organizations. This in-depth examination is essential because many companies fail to appreciate the effects that cyber breaches can have on the entire enterprise.

2. Create Integrated Response Plans. A company should develop response plans that address each scenario and integrate the actions of the individual departments and actors within each plan. In the military, “joint planning” enables the different directorates or functions—manpower and personnel, logistics, operations, intelligence, etc.—to prepare to work together effectively. Similarly, a company’s integrated plans should provide mechanisms for coordinating the company’s response activities, so the different players speak and act in unison. Wargaming can provide insights into the anticipated cyber incidents and planned responses, helping companies refine their plans and identify all of the capabilities required for effective response.

Companies will not have the resources to create plans for every possible scenario. Consequently, the selected plans should reflect the probability that the crisis will occur and the potential damage it could inflict. Companies will still want to plan for a cyber incident with a small likelihood of occurrence if its impact would be extremely severe.

3. Exercise the Plans. Response plans should be exercised regularly, perhaps once per quarter, to ensure that responders understand their roles and practice carrying them out. This is essential to enabling unity of effort—that is, a well-integrated response—when an incident occurs.

Here again, wargaming is an important preparedness tool. Many companies have developed robust incident response and threat defense operations at the technical level. That is, their cybersecurity teams have put in place security operations centers (SOCs), incident response and digital forensics, security information and event management (SIEM) systems, malware analysis, and other capabilities. Many have become very adept at responding to attacks and breaches, and at keeping operations running while they hunt down and eliminate intruders. An effective wargame will help them practice these technical activities in concert with the corporation’s crisis responders who will be addressing legal, customer, financial, public relations, and other nontechnical issues. As just one example, the security team may advocate that the company refrain from public comment until the cyber intruders are found and eliminated, but the communications team knows that, even if this is a good strategy from a security standpoint, it will increase the probability of customer dissatisfaction, lawsuits, and long-term harm to the corporate brand. And so the two groups must work out an approach in advance that best addresses and minimizes all potential risks, not just the technical risks. Exercises and wargames will help corporations develop an integrated response capability that effectively coordinates activities among its diverse responders.

Remember: Having a plan is not the same as being prepared. Training is essential.


Having one person oversee this task is essential to success. Too often, these functions are dispersed among different players, leading to lack of coordination in planning and preparation, and lack of effective execution during the cyber crisis. A company needs a single person or function that oversees the technical and nontechnical aspects of preparing for and responding to cyber crises. This person would understand how the technical aspects of a breach can impact the entire enterprise, including the risks it would pose, and, therefore, could direct the preparation and response in the context of mitigating enterprise risk.
Chief Executive Officers (CEOs) often want to manage the crisis themselves. Some are good at it, but many are not. We have seen many examples of CEOs who took charge of a cyber crisis only to see it spiral out of their control. Some ended up losing their jobs. The problem wasn’t that they were unengaged or poor leaders or lacked strong managerial skills; rather, they lacked the specific skills and training needed to manage a cyber crisis, which calls for a different temperament and capabilities than those needed to run a corporation. Moreover, even the most capable CEOs may become too caught up emotionally in the problems to make objective decisions, particularly if they fear being held responsible for the crisis. This also holds true for other high-level executives.

In contrast, the person chosen to lead the company’s crisis planning, training, and management will be specifically trained for the position. Among this person’s most important competencies will be the ability to lead joint decision making by calling together the various corporate functions, so the crisis leader can gather insights and recommendations to guide crisis action planning and execution. In addition, this position should not be one that shares blame for contributing to the cyber crisis. This will allow the crisis manager to focus his or her efforts on guiding the company through the crisis.

Not every company may have the size or resources to establish a separate position for managing a cyber crisis, but it’s a best practice where possible. This person would report directly to the CEO during the crisis, and would be accountable for managing the crisis effectively.

By following these four principles, corporations can put into place what the military calls a “command-and-control” model for operations. The Department of Defense defines command and control as “the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.” In the corporate world, once a cyber crisis hits, the executive or manager tasked with managing the crisis would become the company’s designated commander with authority to direct the various players and activities in the execution of the company’s crisis plan. It should be noted that while the command-and-control model gives ultimate decision-making authority to the commander, this approach relies heavily on joint decision making among all the relevant functions to ensure realistic appraisals of options, collaborative action planning, and the highest probability of success.

Of course, there is a cost to cyber crisis planning and management, but it pales in comparison to the measurable risk and potential cost of trusting that all of the affected components across the enterprise will quickly come together to develop and execute a unified crisis action plan when a major breach is uncovered.

Making the Case for a Crisis Task Force Officer

The need for cyber crisis planning, combined with the effectiveness of the command-and-control model for planning execution, raises one more salient point: It may be time for large corporations to consider appointing a Crisis Task Force Officer (CTFO) to guide the planning, training, and management of corporate crises. This position could encompass all potential crises and disasters, but it’s the dramatic rise of severe cyber crises that is driving the need for a high-level position.

A CTFO’s activities and responsibilities would be similar to those of a joint task force commander in the military. The CTFO would be selected and trained to confront complex, potentially catastrophic problems, pull the organization together, and manage the crisis in real time. CTFOs would also lead the crisis planning and training activities. As part of their responsibilities, these leaders would spend time getting to know and understand each of the company’s functions—financial, legal, operational, etc.—so they would know how decisions ripple through the enterprise. Once a crisis hits, CTFOs could call on pre-planned action.
modes that have been exercised and perhaps wargamed as well. They also would have broad command-and-control authority across the enterprise to direct the company’s response.

The CTFO might report to the Chief Risk Officer or Chief Information Security Officer during planning and training but, when a crisis occurs, would report directly to the CEO. Although the CTFO would not be held responsible for causing the crisis, the CTFO would be responsible for managing the crisis. The CTFO is the person who gets fired if the crisis response is mismanaged.

Establishing a Crisis Task Force Officer within the company would have many benefits. It would mitigate cyber-related insurance costs. It would demonstrate for insurance companies, regulators, and industry partners that the company values security and resiliency. Most importantly, it would enable the organization to pivot swiftly and effectively to crisis management when a crisis occurs, reducing risk and damage while the organization regains its footing in the brief but fierce storm.

**Conclusion**

For a number of years, particularly since the 9/11 terrorist attacks, companies have been establishing resiliency plans that put policies and procedures in place for continuing operations during a major disaster. Too often, they have handed off different planning and management tasks to different departments, hoping it would all come together during a crisis, though lacking urgency or belief that the planned response would actually be needed.

In recent years, we have seen a seismic shift in the corporate risk environment, due primarily to the increasing risk of a major cyber breach. Responding effectively to modern cyber breaches has proven to be difficult because of the complexity of the cross-organizational issues created by the breach, and because of the speed with which the entire organization must respond to these issues. In short, the challenge isn’t just knowing what to do; it’s also doing it at network speed. Traditional management skills and approaches that are well suited to running a business do not necessarily translate well to managing a major cyber crisis. The new risk environment requires new thinking about how to plan for and manage a major crisis.

The principles that guide military operational planning and execution, as well as disaster preparedness and management, offer important insights into how corporations can effectively prepare for and manage a major cyber crisis. Corporations should start by identifying the cyber crises they may face, as well as the full range of impacts—internally and externally—that could result. Once the potential crises and impacts are known, corporate leaders can develop integrated response plans that unite the different responders across the organization in coordinated action. The plans must also be exercised to ensure that they are effective and that everyone understands their roles within the enterprise-wide response. The final building block for corporate resiliency is assigning clear responsibility for planning, training, and managing the crisis. Of course, having strong cyber threat defense operations remains essential for minimizing the probability of a breach and responding quickly when a breach occurs. However, cyber operations must be coordinated with other response activities as part of an overall strategy to mitigate enterprise risk. These principles create a command-and-control model that enables the entire enterprise to respond quickly, effectively, and with unity of purpose when a cyber crisis hits.
About the Authors

John M. (Mike) McConnell
Senior Executive Advisor

Mike McConnell is a Senior Executive Advisor and former Vice Chairman of Booz Allen Hamilton, where he led Booz Allen’s rapidly expanding cyber business. After retiring from the Navy in 1996 as a Vice Admiral, he led Booz Allen’s Information Assurance business and the firm’s Intelligence business focused on policy, transformation, homeland security, and intelligence analytics. As a pioneer in the evolution of cyber, Mike has served as an industry leader advising Fortune 50 companies.

Upon being asked to become the second Director of National Intelligence (DNI), Mike left Booz Allen after 10 years and served as the DNI for 2 years under Presidents Bush and Obama. He developed the concept and became the chief architect for the $17 billion Comprehensive National Cybersecurity Initiative (CNCI) for securing America’s digital infrastructure.

Mike was instrumental in the modernization of the Foreign Intelligence Surveillance Act (FISA), which updated the national policy to keep pace with the evolution of communication as changed by the internet.

As the Director of the National Security Agency (DIRNSA) under Presidents George H.W. Bush and Bill Clinton, Mike led the development of a portfolio of innovative technologies in cyber capabilities to exploit the “growing data at rest” created by the internet in addition to the traditional methods of collecting “data in motion”.

As the Intelligence Officer from 1990 to 1992 for the Chairman of the Joint Chiefs of Staff, Mike created the first Joint Intelligence Operations Center (JIOC), which allowed real-time synchronization of intelligence collection with real-world operations, enabling predictive analysis in support of decision making.

Mike has twice received the nation’s highest award for service in the Intelligence Community. He has also served as the Chairman and CEO of the Intelligence and National Security Alliance (INSA). He is the 2011 recipient of INSA’s William Oliver Baker Award, for sustained and excellent service in intelligence and national security.

Mike holds an M.P.A. degree from George Washington University, is a graduate of the National Defense University (Global Telecom), the National Defense Intelligence College (Strategic Intelligence), and holds a B.A. degree in Economics from Furman University. In addition to being a member of Phi Beta Kappa, Mike has also been awarded three Honorary Doctorate degrees, including from The George Washington University.

Contact Information:
Mike McConnell
Senior Executive Advisor
mcconnell_mike@bah.com

Thad Allen
Executive Vice President
booz-allen_thad@bah.com
703-902-6755

Christopher Ling
Executive Vice President
ling_christopher@bah.com
301-313-7230

Thad Allen
Executive Vice President

Booz Allen Executive Vice President Thad Allen is a leader in the firm’s Departments of Justice and Homeland Security business in the civil market. He leads the development of thought leadership and client engagement regarding the future direction of law enforcement and homeland security.

He is known for bringing together government and nongovernment entities to address major challenges in a “whole of government” approach. Thad completed his distinguished career in the US Coast Guard as its 23rd Commandant.

President Barack Obama selected Thad to serve as the National Incident Commander for the unified response to the Deepwater Horizon oil spill in the Gulf of Mexico. Working closely with the US Environmental Protection Agency, DHS, the Departments of Defense, Interior, Commerce, and Health and Human Services, state and local entities, and BP, he sought to bring an integrated response to operations.

Prior to his assignment as Commandant, Thad served as Coast Guard Chief of Staff. He was designated Principal Federal Official for the US government’s response and recovery operations in the aftermath of Hurricanes Katrina and Rita throughout the Gulf Coast region.

Other Coast Guard assignments included Commander, Atlantic Area where, in 2001, he led the Coast Guard’s Atlantic Area forces following the September 11 attacks. He previously served as Commander, Seventh Coast Guard District, where he oversaw all operations in the southeastern United States and in the Caribbean.

He is a Fellow in the National Academy of Public Administration and a Member of the Council on Foreign Relations. Thad also currently serves as a director on the Coast Guard Foundation and Partnership for Public Service.

He is a 1971 graduate of the US Coast Guard Academy. He holds a master’s in Public Administration from The George Washington University—where he received the Alumni Achievement Award in 2006. He also holds a master’s in Science from the Sloan School of Management at the Massachusetts Institute of Technology.
About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for 100 years. Today, Booz Allen is a leading provider of management consulting, technology, and engineering services to the US government in defense, intelligence, and civil markets, and to major corporations and not-for-profit organizations. In the commercial sector, the firm serves US clients primarily in financial services, healthcare, and energy markets, and international clients primarily in the Middle East.

Booz Allen helps clients achieve success today and address future needs by applying functional expertise spanning consulting, analytics, mission operations, technology, systems development, cybersecurity, engineering, and innovation to design, develop, and implement solutions. The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 23,000 people, and had revenue of $5.48 billion for the 12 months ended March 31, 2014. Over the past decade, Booz Allen’s high standing as a business and an employer has been recognized by dozens of organizations and publications, including *Fortune*, *Working Mother*, *Forbes*, and *G.I. Jobs*. In 2014, Booz Allen celebrated its 100th anniversary year. More information is available at www.boozallen.com. (NYSE: BAH)
Principal Offices

Huntsville, Alabama
Montgomery, Alabama
Sierra Vista, Arizona
Los Angeles, California
San Diego, California
San Francisco, California
Colorado Springs, Colorado
Denver, Colorado
District of Columbia
Pensacola, Florida
Sarasota, Florida
Tampa, Florida
Atlanta, Georgia
Honolulu, Hawaii
O’Fallon, Illinois
Indianapolis, Indiana
Leavenworth, Kansas
Radcliff, Kentucky
Aberdeen, Maryland
Annapolis Junction, Maryland
Lexington Park, Maryland
Linthicum, Maryland
Rockville, Maryland
Troy, Michigan
Kansas City, Missouri
Omaha, Nebraska
Red Bank, New Jersey
New York, New York
Rome, New York
Fayetteville, North Carolina
Cleveland, Ohio
Dayton, Ohio
Philadelphia, Pennsylvania
Charleston, South Carolina
Houston, South Carolina
San Antonio, Texas
Abu Dhabi, United Arab Emirates
Alexandria, Virginia
Arlington, Virginia
Chantilly, Virginia
Charlottesville, Virginia
Falls Church, Virginia
Herndon, Virginia
McLean, Virginia
Norfolk, Virginia
Stafford, Virginia
Seattle, Washington

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com