Developing Organizational Capabilities to Manage Cyber Crises

Gabi Siboni and Hadas Klein

The increasing number and complexity of cybersecurity incidents have led many organizations to develop procedures and capabilities to manage them. These include real-time response capabilities, technological capabilities, and the formation of teams charged with maintaining organizational information systems. These efforts are liable to be insufficient, however, because they sometimes fail to consider managerial aspects and the skills and tools required of the technological teams to manage crises while trying to confront a cyber incident. This might result in the situation rapidly spiraling out of control, thus becoming a severe crisis with financial, legal, and reputational ramifications, which affect the assets of the entire organization. This essay analyzes the way to develop capabilities to allow organizations to effectively manage crises in information, telecommunications, and cyber.

Keywords: Cyber, cyber crisis, cybersecurity, recovery, crisis management, business continuity

Introduction

In May 2017, British Airways experienced a severe crisis. According to the company, a mishap at the server farm, caused by an electrical surge that stemmed from turning the system on and off, paralyzed the company's ability to operate its flights for several hours. Consequently, many flights were

Dr. Gabi Siboni is the head of the Cyber Security Program at the Institute for National Security Studies. Hadas Klein is a research associate with the Cyber Security research program at the Institute for National Security Studies.

cancelled, and more than 75,000 passengers were stranded. The damage to British Airways became even worse because the various professionals had failed to understand and fix the actual error so as to minimize the effects on the company and its customers.[1] As a result, the harm to the company, in terms of the bottom line and its reputation, was and remains vast.

This incident was a reminder of the tremendous importance of setting up and drilling a crisis management system in companies that rely upon computer infrastructures in order to function. At present, most managers understand that cyberattacks are inevitable. No matter how professional the organization's cyber defense team, it is highly probable that, sooner or later, the organization will find itself under a cyberattack and attempts will be made to breach its computer systems and/or damage them. Therefore, companies and organizations are investing a great deal in proactive defensive capabilities designed to identify attacks in the early stage before they become full blown and cause real damage. Furthermore, organizations are also investing in new approaches and tools, such as cyber intelligence, continuous network monitoring, and tools detecting anomalous behavior. However, despite all means of defense, organizations must continue to ensure they have the capabilities to handles crises stemming from severe cyberattacks.

In recent years, several cyber crises besetting different sectors developed into significant events, sometimes because of failures in crisis management. Cyber crises of this kind can easily damage customer trust and the company's revenues, reputation, and more. Cyber crises can also threaten managers personally and lead to their resignations or dismissals. An example of a failure in crisis management because of improper preparation was experienced by TalkTalk, the British communications provider, in October 2015. TalkTalk managed the crisis in a confused, opaque, and inconsistent manner, leading to the conclusion that the company did not have any clear crisis management plan in place.[2] Two days after the attack had been discovered, the company still was unable to isolate the damage, assess its scope, identify the attacker, or even put its finger on the reason for the attack. The crisis cost TalkTalk an estimated £60 million in direct and indirect losses in terms of damage to

1 Nicola Harley, "British Airways IT Crisis Mystery as Energy Suppliers Say There Was No Power Surge," *The Guardian*, May 31, 2017.

2 Lucas Fettes, "What Lessons Can All Organizations Learn from the TalkTalk Security Breach?" November 12, 2015, http://www.lucasfettes.co.uk/what-lessons-can-all-organisations-learn-from-the-talktalk-security-breach.

reputation, loss of customers, and more. About eighteen months after the incident, following an investigation by the British regulatory agencies, the company's CEO was dismissed. The report of the regulatory agencies clearly stated that the CEO was responsible for the company's lack of preparedness to manage a cyber crisis.

Unlike TalkTalk, the US infrastructure company Dyn, which in October 2016 experienced one of the worst denial-of-service attacks to date, succeeded within a few hours to repel the attack and prevent an escalation to the point of crisis. Company employees said that they constantly had drilled and prepared for such scenarios, and that the drilling focused not only on technological aspects but also on articulating situation assessments, making decisions under pressure, and communicating with management.[3]

Building organizational capabilities to handle a computer and cyber crisis is a crucial component in the overall construction of every organization's defensive and business continuity capabilities. This essay analyzes the theoretical background of crisis management and suggests examining the development of four basic components that allow an organization to successfully face computer and cyber crises: creating an organizational concept for dealing with a computer and cyber crisis; cultivating the human factor and organizing the personnel into a crisis management team; acquiring or developing technological tools and organizational processes that can help realize the organizational concept; and assimilating all this through drills, exercises, and simulations.

Clausewitz famously noted that "war is the realm of uncertainty."[4] This is also true for crises in cyberspace because the uncertainty—the "fog of war" —and the difficulty in formulating a situation assessment hamper making decisions and implementing actions that can resolve the crisis and generate a quick recovery. Developing these capabilities will undoubtedly lead to more effective handling and managing of any crisis as well as better outcomes for the organization.

---

3 Christopher Roach, "Lessons Learned from the Dyn Attack," *CFO.com*, February 9, 2017, http://ww2.cfo.com/cyber-security-technology/2017/02/lessons-learned-dyn-attack.

4 Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret, vol. 1 (Princeton: Princeton University Press, 1976), p. 101.

Theoretical Background: Crisis Management Strategy

In cyberspace, like elsewhere, there is no single definition of "crisis" and no single criterion for applying the term; often, the concept is overused. Not every cyber incident in an organization necessarily leads to a functional crisis requiring special attention; most cyber incidents are managed by routine processes, such as handling malware infections, repelling weak denial-of-service attacks, and so forth. Usually, such incidents do not damage the organization in the short and long term, and cyber security and information security teams manage them as a routine part of their job. Severe cyberattacks, however, can cause lasting damage to an organization's ability to function and provide service to its clients and customers. These cases are indeed crises requiring special attention.

Olga Kulikova and her colleagues have analyzed the purpose of exposing a cyber crisis in an organization.[5] They claim that such exposure entails four important aspects: First, it improves protection and the ability to articulate a situation assessment; second, the exposure will help the company meet regulatory demands and standards; third, the exposure might damage the organization's financial resilience; and fourth, the organization's reputation might suffer as a result of a crisis, which in turn could affect the business results of the organization.

One model analyzing the process of managing a crisis is the bow-tie model developed in 1979.[6] It positions the incident at the center and characterizes the defenses and controls designed to prevent it, as well as the steps that must be taken to minimize the damage once the incident occurs. Diagram 1 below illustrates this model in the context of a cyber incident:

5 Olga Kulikova, Ronald Heil, Jan van den Berg, and Wolter Pieters, "Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information," *International Conference on Cyber Security (CyberSecurity) 2012* (2012): 103–112, https://doi.org/10.1109/CyberSecurity.2012.20.

6 Steve Lewis and Kris Smith, "Lessons Learned from Real World Application of the Bow-tie Method," (paper presented at the American Institute of Chemical Engineers, Sixth Global Congress on Process Safety, San Antonio, Texas, March 22–24, 2010).

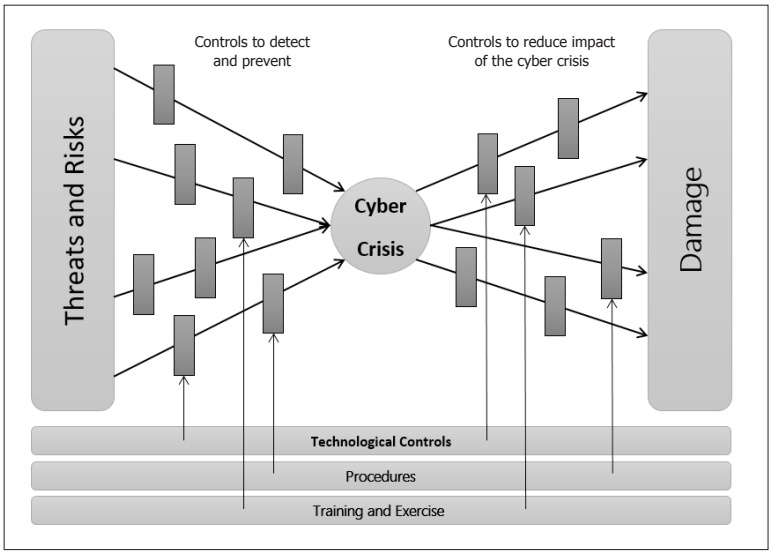

Diagram 1: Bow-Tie Model in the Context of a Cyber Incident

The process of managing cyber crises requires building capabilities that will make it possible to formulate situational awareness throughout the crisis. This process requires constant tracking of a crisis' developing parameters. "Situational awareness" is a term used during crisis management to describe the best possible assessment of what is taking place at any given moment, the possible ramifications of this crisis, the degree of uncertainty of the assessment, the organization's ability to contain the crisis, the way the crisis could develop and further deteriorate, and what could occur later. Situational awareness also describes the organization's active and available defenses against threats. Situational awareness is the foundation for a situation assessment, which is needed to make operational decisions, prioritize events, and handle them based on their threat/risk level and their inherent potential for damage.

The importance of the process of constructing situational awareness is described by Ali Rashidi and his colleagues[7] who analyze the process during a cyber incident as a critical component in the ability to make informed

7 Ali J. Rashidi, Kourosh D. Ahmadi, and Mostafa Heidarpour, "Cyber Situational Awareness Using Intelligent Information Fusion Engine (IIFE)," *Cumhuriyet Science Journal (CSJ)* (Cumhuriyet University Faculty of Science) 36, no. 3 (2015): 3218–3229.

decisions. The authors suggest a model for information fusion to allow a continuous process of providing updates while relying on expert systems.

Barford and his colleagues analyze the phases of the process of building situational awareness.[8] The first phase requires an understanding of what is happening at that moment. This phase is activated after initially categorizing the warnings received and analyzing existing data. The process continues with the goal of understanding the meaning of the incident and the extent of its impact on the organization's critical processes. At the next phase, the authors suggest to comprehend the process of development of the incident and finally to understand how it happened. All these phases are preliminary to the process of making a situation assessment, the purpose of which is to determine the actions to take in order to contain the incident and minimize its damage.

The dimension of time adds further complexity. Often, it is difficult to define the transition from a low-intensity cyber incident, which only requires the routine intervention of the technological team to ensure it remains localized, to a high-intensity cyber incident, which develops into a crisis that has significant ramifications for the entire organization and requires the intervention of non-routine and additional capabilities. One may describe the transition point from a routine cyber incident to a cyber crisis as follows: At first, a hidden gap is created between how the computer systems are functioning and how they are supposed to function according to the organization's service definitions. At this phase, routine intervention is applied. If the situation deteriorates and the gap widens and accelerates and could spread to other areas, more extensive and in-depth efforts are needed.

The Bank of Israel's Directive 361 defines several phases in handling a cyber incident:[9] the detection phase, when there is an initial investigation of the cyber incident; the analysis phase, which refers to a comprehensive and in-depth investigation of the cyber incident in order to determine the possible avenues of action to stop the attack; the containment phase, which is designed to gain initial control of the incident in order to stop the crisis and prevent further deterioration; the eradication phase, designed to neutralize the

8 Paul Barford et al., "Cyber SA: Situational Awareness for Cyber Defense," *Cyber Situational Awareness*, ed. Sushil Jajodia, Peng, Liu, Vipin Swarup, and Cliff Wang (Boston: Springer US, 2010).

9 The Supervisor of Banks, Directive 361, Proper Bank Procedure [1] (3/15), *Cyber Defense Management*, March 2015 [in Hebrew].

event in order to minimize the damage as much as possible; and the recovery phase, during which the organization returns to full and proper functionality.

The capabilities required to manage a crisis can be characterized according to its chronological phases. The first is the preliminary phase of the routine, during which an organization should carry out actions to reduce the probability that a crisis could develop and increase preparedness for managing a crisis, should one occur. In his book *Crisis Management Strategy: Competition and Change in Modern Enterprises,* Simon Booth lists several parameters affecting an organization's ability to manage a crisis, which, he says, must be developed beforehand. The first is planning. At the preliminary phase, organizations should invest resources in planning how to face a crisis.[10] Once an organization finds itself in a crisis, it transitions to the second phase—managing the actual crisis—in which the organization needs a variety of different capabilities to confront the crisis and minimize its damage. The third phase is the post-crisis recovery, which includes an investigation of the incident and drawing conclusions and learning the lessons of the crisis. These phases presented along an axis of time are shown in the following chart:

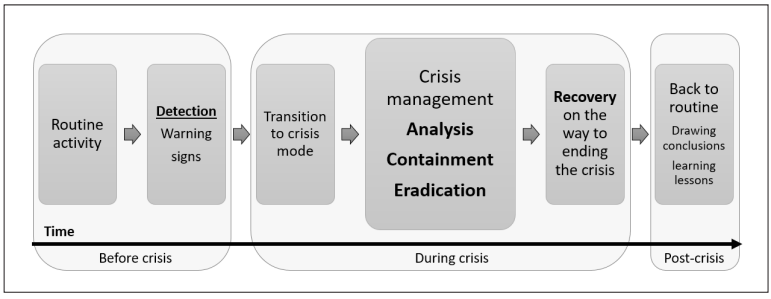

Diagram 2: Chronological Phases of Managing a Crisis

Developing an Approach to Crisis Management

The first milestone is developing an organizational approach to crisis management. Such an approach must include several basic components, the first which relates to determining measures for reasonable downtime and the levels of functioning required for all the computerized systems of the organization. This process requires the organization to rely on an analysis of

10 Simon A. Booth, *Crisis Management Strategy: Competition and Change in Modern Enterprises* (London, New York: Routledge, 1993), p. 13.

its computerized systems and their degree of criticality to the organization's overall functioning. This analysis, called the business impact analysis (BIA), is one component in building a business continuity plan. By using this tool, it is possible to analyze and determine the scope of functioning of each system and the time needed restore it to full operational mode. Such an arrangement reflects the resources for managing the organization's crisis, because an organization that can afford to suspend contact with customers for a few hours differs radically from a bank that suspends its online service or an airline forced to cancel flights, which is liable to cause financial losses and damage to its reputation

The development of such an approach is needed also for the sake of defining what constitutes a crisis and in creating a common language and clear rules for managing it. Determining that a crisis is underway and assessing its severity have immediate ramifications on the resources the organization should allocate to manage it. These resources should relate to the scope of the team managing the crisis, the skills and expertise of the team members, the technological and other means required for the team to operate, and lastly, the extent of training and drilling that the team undergoes. After defining crisis situations, the approach needs to determine the working processes of the organization in its usual, pre-crisis routine and during the crisis itself, and finally determine the post-crisis investigation and learning processes. Furthermore, the approach should determine the responsibility of office holders in the organization during crisis situations.

The development of the approach and the complexity of cyber crises and organizational crises in general require the input of many factors in the organization in addition to the teams providing the technological response to computerized and communications services. Their involvement requires coordination and management of several disciplines, including the management of the legal ramifications related to the operation and safekeeping of databases; management of the regulatory obligations that go into effect the moment a crisis is declared; management of the damage to the organization's reputation; the involvement of the risk management personnel and those in charge of cyber defense in law enforcement agencies, and more. Therefore, as part of preparing for a cyber crisis, it is critical to establish an organizational cyber crisis management committee, which includes the organization's senior

managerial team, such as the chief executive officer, the chief financial officer, the legal counsel, and the director of public relations.

The obvious advantages of including senior management in the cyber crisis management committee are the ability and authority to operate at two complementary levels: The committee should routinely examine regulatory and legal aspects in various crisis scenarios and define financial aspects related to crisis management; validate escalation plans up the managerial chain and contingency plans for managing various media and communications channels when crisis strikes; and during a crisis, the committee should help balance what takes place within the organization and outside of it in order to maintain its reputation and minimize any legal obligations that might occur during the crisis, while maintaining objectivity and ensuring processes of prioritization.

Developing Manpower and Organizing Personnel in a Crisis Management Team

One of the advantages of training an intra-organizational team to handle crises is the ability of such a team to optimally analyze the array of possibilities and courses of action. It is safe to assume that no external party—no matter how experienced—knows the organization as well as the professional teams, business process managers, and senior management. Moreover, intra-organizational team members usually have professional authority and are recognized as such, a factor that can facilitate their work when they must manage a crisis.

To take advantage of the organization's internal resources and realize the organizational approach, it is necessary to train personnel. The process of selecting the various personnel requires a clear definition of the range of functions, the responsibility of the crisis management team, and its interface with stakeholders within the organization and outside of it. It is also necessary to define the skillsets required of these professionals as well as the knowledge and experience they must possess. At the next phase, it is necessary to define the managerial skill and expertise that a member of a crisis management team must have to be able to do his or her job. Such a definition must answer the question: "What skills and expertise are needed to manage a crisis effectively and what does a team member need in order to act effectively?" At the third phase, it is necessary to define the knowledge

and experience required of all members of a crisis management team. Each one should be intimately familiar with the business environment—not just the technological environment—and should therefore be familiar with the organization's business activities, at least at a level of basic understanding. This knowledge can provide team members with the ability to prioritize the management of the crisis based on understanding the criticality of the business processes that have been damaged.

The organization's technological team will face a range of challenges during a cyber crisis, including formulating an up-to-date situational awareness, usually on the basis of partial information, and an optimal response in order to recover rapidly and return to reasonable functioning. When a cyber crisis generates immense public pressure, the organization's managers must provide answers to customers and other stakeholders, further increasing the pressure to which the professional parties are subjected.

The technical cyber crisis management team is the body charged with handling the technological aspects of the crisis. It is also the body that directs the professional parties how to deal with the crisis in a way that will reduce damage and harm to the organization's reputation. Ideally, the technical team is also able to leverage the crisis to the organization's benefit. The team's tasks also include making an initial damage assessment, conveying the current situation and its business ramifications, formulating an action plan for the business processes managers and management, declaring an emergency situation, and managing the incident. These are complex tasks that go beyond comprehending the technological aspects and the organization's computerized and communications systems; rather they demand also a broader understanding of the business, legal, and PR-related effects of a cyber crisis.

When facing a crisis, the crisis management team is subjected to a great deal of pressure, which might impede its functioning. The feeling of pressure intensifies as the gap grows larger between the means and skills needed to confront the crisis and the ability and resources available to the team in practice. It is possible to characterize two types of skills the team should possess: professional/technological skills that involve an intimate familiarity with the organization's technological and managerial systems and soft skills that concern the development of personal and group abilities helpful in the crisis management process.

Developing the professional/technological skills is a process requiring training and professionalization in a range of the organization's technological systems, including the infrastructures and communications systems, the data servers, and the end applications. This should be accompanied by a profound understanding of the management structure, including decision-making processes, the structure of authority and sources of knowledge, as well as all the critical systems and processes at a level that will allow for an analysis of the incident and a mapping of the entities relevant to handling it. To improve the business and organizational understanding of the crisis management team, we recommend brief meetings with the managers of the organization's critical business processes so that the team can come to appreciate the complexity, importance, and challenges inherent in those processes.

The head of the crisis management team should be a member of the organization's management, and it is critical that he or she possess thorough and precise knowledge of the technological aspects and their impact on business processes. Hays and Omodei have determined that the head of a crisis management team should possess a certain combination of personal and interpersonal qualities, including a high tolerance for pressure, self-awareness, and mindfulness of every member of the team, in addition to good communication skills.[11]

A crisis management team should include a member charged with all aspects of coordinating the crisis with the business units. This team member must have a good knowledge of the organizational structure and the administrative aspects required for organizational functioning. The team should also include technological personnel who possess cumulative knowledge of the organization's infrastructures, communications, servers, applications, and databases. When a crisis affects several of the organization's sites, it is important to station representatives of the crisis management team at every site affected, while ultimate coordination must be centralized.

As noted above, the personal characteristics of the crisis management team should also include soft skills, such as interpersonal communications, the ability to listen, emotional intelligence, persuasiveness, creativity,

11 Peter A. Hays and Mary M. Omodei, "Managing Emergencies: Key Competencies for Incident Management Teams," *Australian and New Zealand Journal of Organizational Psychology* 4 (February 2012): 1–10.

precision, problem solving, team work, the ability to make decisions under pressure, and more. These can be developed and improved and eventually implemented during the crisis management process.

Technology

Many tools can help manage cyber incidents. As part of its approach, the organization must decide, depending on its needs, whether to use off-the-shelf tools or develop custom-made ones. Technological tools are extremely important in supporting an organization's crisis management process. They should provide a response in its many stages, such as formulating a current understanding of the situation and carrying out a situation assessment, supplying a supportive system for crisis management—including the ability to preserve and retrieve information from databases from previous incidents, whether they occurred within the organization or in other settings—and the ability to document for the sake of drawing conclusions for the future. The crisis management system allows for mechanical surveillance of the various procedures and processes and emphasizes the priorities in managing the incident by means of previously entered scenarios based on critical business processes. The system also enhances intra-team and intra-organizational communications during an event.

Overall, a crisis management tool is meant to respond to several fundamental needs:

- To create an operational log that is organized as a table and breaks down the process of the crisis. Use of the operational log enables the team to document the cyber incident from the moment it happens and reflect upon it as it occurs. The log's purpose is to help understand the situation, support decision-making processes, and investigate once the crisis ends. The log must include the exact times of the incidents, descriptions of testimonies, facts, and operating assumptions.
- To serve as a platform for communication among key personnel in the organization and stakeholders during the crisis. Rarely do key personnel find themselves all together in the crisis management room; therefore, it is necessary to provide them with a tool that allows them to communicate and understand the developing situation from any location at any time.

- To create one central virtual space for concentrating all the information about the cyber incidents. Creating such a space ensures that the technological teams and the decision makers are operating on the basis of the same facts.
- To help understand the unfolding situation using a range of different cause-and-effect interpretations that are characteristic of the world of information systems, while handling the full volume of cyber incidents and their rapid rate of development.
- To help reduce pressure to allow for objective decision making and a structured use of processes whereby the handling of the crisis is passed up the management chain.
- To support communication based on the organization's matrix of communication and escalation. Crisis management systems make it possible to feed in advance the communications matrix and automatically send updates when previously defined conditions are realized.
- To help understand the significance of events so that the bits and pieces of information gathered from different sources are pulled together to create a full picture, all while assessing the quality of the information, and sorting and organizing it in a way that makes it easily retrievable later.
- To support the process of formulating a possible course of action on the basis of known data while interpreting and analyzing the relevant facts in order to understand how the situation may develop.
- To examine the analysis of the situation and its ramifications given the actions taken. At this stage, a new phase begins, namely that of formulating an updated understanding and assessment of the situation, based on the changes that have occurred due to the actions taken and new data from outside the organization.

The use of technological tools that can help the above-described processes significantly will enhance the efficiency of the work of the crisis management team. Diagram 3 below is a schematic representation of the process that the technological systems must be able to support:

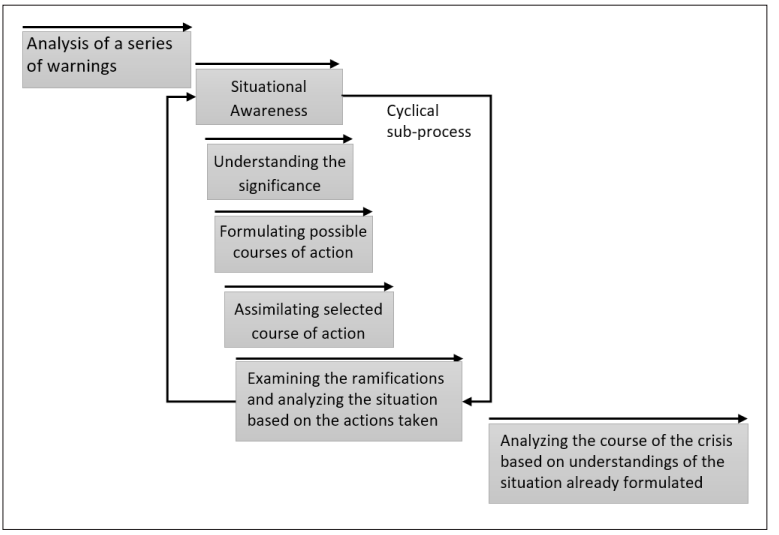

Diagram 3: Representation of the Processes that the Technological Systems Should Support

Another group of technological tools relates to learning from previous cyber incidents both inside and outside the organization. During a crisis, the crisis management team cannot be expected to analyze in-depth why the incident occurred. Such analyses must be carried out in an investigation following the cyber incident as part of the organization's efforts to draw conclusions and learn from the crisis. During the crisis, the focus should be on stopping and eradicating the incident and rapidly recovering the organization's systems to their pre-crisis functioning while setting clear priorities. Sometimes, a temporary fix is needed; at other times, using means that bypass the problem until it is resolved is the right thing to do.

An important tool in diagnosing a crisis is a database of all historical cyber incidents and crises in the organization, a similar index describing cyber incidents in the organization's business sector, with as much detail as possible, as well as those that have occurred in the organization's geopolitical environment. For example, a bank would be wise to maintain a listing of all extreme cyber incidents that have taken place in other banks all over the world. This tool allows the crisis management team at the bank to identify familiar problems and errors caused by similar incidents in the past, thereby gaining information on ways to bypass the problems when they are identified.

This is an automated, structured tool that must include a smart data retrieval engine, including data written in free text format.

Crisis management tools should also document the crisis and the work processes as it occurs so that it can be input into the organizational learning system and used during the current crisis and future ones. The documentation should include the development of events, a description of the warnings issued and their reporting, and the decisions made at every stage. This documentation is significant in various ways should a similar scenario develop in the future or in case the crisis is not yet over despite the steps taken, including the formulation of a current understanding and a situation assessment. In addition, a summary report should be prepared and distributed to all internal stakeholders—including the management and other relevant parties—and to external stakeholders, as per the relevant regulatory directives.

Assimilation: Training, Practice, and Drills

Improving abilities and attaining a high level of preparedness are largely based on training, exercises, and drills as being an integral, structured part of the process of realizing the organization's approach to crisis management. Several components of the assimilation process are involved.

The crisis management team usually includes employees with extensive training and knowledge in computerized systems and the organizational cyberspace. Their role in the team is in addition to their routine jobs. Nonetheless, before becoming a member, all candidates for the crisis management team should undergo some basic training, which should cover the organization's crisis management rules and principles, crisis plans and procedures, and understanding both the business environment and the organization's technological tools for crisis management. The training should also include aspects of identification, documentation, classification, and prioritization; initial diagnosis of the crisis; investigating its development; means of communications and escalation (i.e., passing the handling up the management chain); the organization's existing sources of information and information gathering; and finally, ways of concluding a crisis, investigating it, and learning lessons from it.

In addition to this basic training, exercises should routinely be carried out, including so-called "tabletop exercises" and crisis management team drills under conditions as real as possible, as well as large-scope exercises

that also incorporate the organization's management. The purpose of tabletop exercises is to analyze relevant reference scenarios in the absence of the regular work environment's pressure. Such exercises greatly add to the crisis management team's knowledge, expand the team members' common language, and increase cooperation among them. In these exercises, it is possible to encourage team-thinking processes and focus the team members on dealing with a range of scenarios and controlling the directions in which they develop, while expanding internal and external communications and interactions with stakeholders and improving the mutual understanding of team members' responsibility and authority. Such exercises also make it possible to validate the organization's policy and procedures.[12] It is best if they include professional guidance[13] aimed at increasing the motivation and willingness of the team members to participate in the exercise and allow them to succeed.[14] The set of exercises encourages the crisis management team to consider failed patterns, such as thinking in terms of concealing or minimizing the crisis or giving an immediate solution in order to extinguish the fire.

In addition to tabletop exercises, it is necessary to hold broader-scoped exercises and drills simulating reality as closely as possible. Several principles should be realized while holding them:

- **Formulating the scenario's nature:** Formulating scenarios of glitches, crashes, and other acute problems in the organization's critical systems, while relying on an analysis of the business continuity plan and the business impact analysis. Doing so ensures the handling of the operational core of the organization's cyberspace. We recommend that exercise scenarios be formulated in a way that the crisis management team is exposed to scenarios of increasing complexity.
- **Creating a technological environment:** Constructing a technological environment for the exercise scenario makes it possible to simulate

12 Brent D. Ruben, "Simulations, Games and Experience-Based Learning," *Simulation & Gaming* 30, no. 4 (1999): 498–505.

13 Tim Urdan, "Intrinsic Motivation, Extrinsic Rewards and Divergent Views of Reality," review of *Intrinsic and Extrinsic Motivation: The Search for Optimal Motivation and Performance*, ed. Carol Sansone and Judith Harackiewicz, *Educational Psychology Review* 15, no. 3 (September 2003): 311–325.

14 A. J. Faria and W. J. Wellington, "A Survey of Simulation Game Users, Former Users and Never Users," *Simulation & Gaming* 35, no. 2 (June 2004): 178–207.

reality as closely as possible, while minimizing the exercise's effect on the organization's operational functioning. The technological environment for the exercise must allow communication, event streaming, and the establishment of an environment of sensors for the computerized systems and technological infrastructures.

- **Constructing the scenario:** The exercise should be constructed on the basis of events that reach the crisis management team from the operational systems and their operators. The crisis management team must try to identify the source of the incident by examining the events and the technological sensors at its disposal (e.g., an overload on computing resources, a glitch in copying data or log files, and so forth). The scenario must include the backstory and events streamed during the exercise, some of which are simply noise unrelated to the incident directly.
- **Adjusting the exercise:** The crisis management team and the supporting system of management must identify the source of the problem in the computer systems and the essence of the cyber incident they are supposed to handle. To make this possible, it is necessary to prepare a bank of events to be streamed, based on the development of the handling of the scenario, in order to maximize benefit from the exercise and ensure optimal training for all involved.
- **Controlling and mentoring:** It is critical to maintain a control system in tandem with the exercises. As an exercise unfolds, this system can note the strengths and weaknesses of each team member and of the team and thus focus the learning process and enhance the professional development of both members and the group. During an exercise, it is important to calibrate basic existing capabilities and use the data gathered in order to set measures for necessary improvements and the success of future exercises. The results of the exercise make it possible to focus the program of professional seminars and training for the members of the team.

In addition to the training of the technological team and as part of the process of preparing to handle a crisis, it is also important to hold exercises for the organization's management. This is critical for building a common language, understanding the constraints in sharing information with external stakeholders during a crisis, and giving the technological team peace of mind and the space it needs to handle a crisis without management pressure. Such pressure does not help, and in most cases, it only gets in the way.

Conclusion

The growing number of cyber incidents and crises has greatly increased the need of organizations to develop their capabilities to handle them. Proper handling of a cyber crisis can reduce damage and lead the organization to rapid recovery, while failure to handle a crisis is liable to lead the organization to its collapse.

Cyber event management is an organizational task involving many of the organization's employees, from the cyber and information security personnel to the members of the board of directors. How the organization handles an incident has just as much impact as the technological capabilities the organization has at its disposal. Including a cyber crisis management policy reflecting the organization's needs and goals as part of the organization's overall cyber strategy is vitally important.

An organization's ability to handle a crisis largely depends also on its ability to improvise and function under pressure. These abilities are commonly attributed to Israel's management culture, but they are far from sufficient in the complex reality and chaos generated in a cyber crisis and in which a crisis management team is supposed to function. It is therefore wise to rely on orderly methodologies of cyber and computer crisis management and on a qualified array of personnel that has trained for such an event in its day-to-day work. As such, we recommend that organizations formulate a plan to develop tools and skills as described in this essay and set up an orderly program for training, simulations, and drills.