# Cyber Security Exercises: Testing an Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events

Gregory B. White
Associate Professor
Department of Information Systems
The University of Texas at San Antonio
gwhite@utsa.edu

Glenn Dietrich
Associate Professor
Department of Information Systems
The University of Texas at San Antonio
gdietrich@utsa.edu

Tim Goles
Assistant Professor
Department of Information Systems
The University of Texas at San Antonio
tgoles@utsa.edu

## Abstract

*The digital age has transformed how today's organizations operate. The production and delivery of essential goods and services takes place through complex and interconnected business processes that in turn rely on a set of interdependent infrastructures. These infrastructures and their supporting information systems transcend individual organizations. However, information systems security research is largely under the purview of computer science and engineering departments, and consequently often focuses on technological issues while overlooking the pervasive nature of information systems in today's society. This has generated calls for a new approach to information systems security; one that employs a socio-organizational perspective that includes not only individual organizations but entire industry sectors and government agencies as well.*

*This paper presents one such approach, the use of scenario-based exercises in addressing security issues common to large organizations, industry sectors, and various levels of government. Lessons learned from illustrative examples of such exercises, as well as suggestions to help organizations conduct their own exercise, are discussed.*

Keywords: Computer security, information systems security, security management

## 1. Introduction

A review of the growing number of universities that offer courses or degrees in computer security or information assurance reveals that many of them maintain their research center in either computer science or computer engineering departments. Their goal is to produce technology that addresses specific aspects of information security. This has been true for many years. However, despite several decades of work in this arena we are still experiencing increases in the number of incidents that occur (see the annual CSI/FBI survey from the Computer Security Institute, www.gocsi.com or check the statistics provided by the CERT/CC at Carnegie Mellon University at www.cert.org for more information on the number and trends in Internet attacks). According to one study, as many as 94% of large organizations in North America have deployed firewalls, and 52% have deployed virtual private network solutions [19]. Reasons for the increases include the discovery and use of new vulnerabilities or methods of attack by the intruders, thus evading the existing list of attack signatures contained in current intrusion detection systems. It might also be explained by the fact that even when vulnerabilities are known and patches to fix them are available, individuals and organizations frequently do not patch their systems. [12] The solution to information systems security is obviously not technology alone. The solution has to include the environment in which the technology is deployed, including human and organizational elements [3]. A quote from a respondent to the Deloitte, Touche, and Tohmatsu 2003 Global Security Survey serves to nicely sum up the issue: "Technology can only help reduce risks to a point." [13] This position is reflected in an emerging belief that the bulk of previous information systems security research, although worthy, is too narrow in scope to cope with the increasing pervasiveness and intertwined nature of information systems in all aspects of our individual, organizational, and societal lives [3].

Responding to this call for a more holistic approach to information systems security

0-7695-2056-1/04 $17.00 (C) 2004 IEEE

research, this paper explores the use of scenario-based exercises to identify and test resources and capabilities necessary for preventing, detecting, and responding to cyber security incidents. The remainder of the paper is organized as follows. Section 2 provides an overview of the challenge facing today's organizations in addressing information systems security issues that transcend the organization's boundaries, and some methods that might be used in addressing that challenge. Section 3 expands on one particular method; the use of scenario-based exercises to heighten awareness, provide training, and assess a city's or sector's ability to detect and respond to cyber events. Examples of such exercises are presented in Sections 4 and 5, followed by a discussion of lessons learned in Section 6, suggestions for conducting exercises in Section 7, and concluding remarks in Section 8.

## 2. Challenge and Response

The fact that information systems security issues now extend beyond the organization leads to one of the challenges of managing organizations in the new millennium; that is, creating and assessing security-related policies and procedures that address the interorganizational nature of information systems and business processes [9]. One approach to this is that taken by the United States government. Initially, the government recognized the existence of *critical infrastructures*, defined as "those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [15]. These infrastructures are categorized by industry sector, such as energy, transportation, banking and finance, information and telecommunications, and so forth. In conjunction with the formalization of critical infrastructures, sector-specific *Information Sharing and Analysis Centers* (ISACs) were created. Their mission is to provide a centralized presence that gathers, analyzes, and distributes information related to threats or events that impact a specific critical infrastructure. The ISACs are non-governmental organizations, with each one operating independently. ISACs have now been established in several sectors, including financial services, information technology, and telecommunications. The next step is for the ISACs to assess threats and vulnerabilities to their respective sectors, and formulate plans for a sector-wide coordinated response. Exactly how to do so, however, is not clear. Any investigation of critical infrastructures must take into account their complex and interdependent nature. This interdependency implies that such an assessment must view the infrastructure as a whole, not as a collection of parts that can be reduced or subdivided [16].

Critical infrastructures are linked through, and heavily reliant on, cyberspace – the hundreds of thousands of interconnected computers, information systems, and telecommunications networks that support all sectors of the economy [15]. Thus it is crucial to reduce or eliminate any threats to or vulnerabilities of the cyberspace infrastructure. One possible solution is through programs designed to heighten security awareness and training. Most security practitioners will agree that such programs should include all personnel, and should include not only introductory training but ongoing awareness reminders as well. [4,13] This is a good start and will help to address the human element of security at the organizational level, but does not always include a feedback loop - activities designed to assess the effectiveness of security policies, procedures, and training. Nor do training and awareness programs by themselves address the interorganizational aspects of information systems security.

A promising approach to resolving these issues is through the use of exercises. Many organizations, such as fire and police departments recognize the need to not only train their personnel but also to periodically exercise them. These exercises provide an opportunity to test the ability of the organization to adapt to new situations that may not have been part of their original training. Already some organizations exercise part of their security plan when they test their backup strategies to ensure that they can recover from an event that results in corruption or loss of data. This is important, but does not go far enough – especially when the interconnected nature of the Internet is considered because problems in one sector can have a tremendous impact on other sectors as well. What is required are exercises that test not only an individual organization's ability to respond to cyber security events, but also the ability of related external entities, such as cities and states or other industry sector members, to respond in a coordinated manner. This is where *scenario-based exercises* can be of significant value.

## 3. Scenario-based Exercises

Scenarios, in general, are tools to help organizations deal with uncertainty. They consist of descriptions or narratives of possible future situations or circumstances that might impact the organization and its environment, and are often used for strategic planning purposes [18]. Crisis management scenarios are designed to confront the participants with a convincing representation of a plausible reality, drawing them into the exercise. When expanded to include the external environment, scenario-based exercises depict a reality over which the participant has little or no control, but which significantly affects him. The challenge for participants in such a situation is to manage themselves so that they remain viable, functioning, and effective [21]. This is the essence of interorganizational cyber security exercises.

There are generally three different purposes for scenario-based exercises. Each provides a direction in terms of how a specific exercise may be conducted. The first is to conduct an exercise for awareness. The goal in this case is to bring individuals together to make them aware of possible security events their organization might experience, how to formulate a response, and how involved such a response might actually be. This is especially true for events that may cross the various critical infrastructures and industry sectors. The second purpose for running an exercise is to use it for education and training. The goal in this case is to prepare the participants in response techniques they may be required to perform in the event that a security incident does occur. The third purpose is to actually test their ability to detect and respond in a coordinated manner to an attack or disruption.

Within the information systems security arena, what a scenario-based exercise entails depends on the level at which it is being conducted. Preventing a security event from occurring should obviously be the first goal of a security program. Failing that, the ability to detect an attack when it occurs and to respond to it becomes important. There is little that an individual organization can do to prevent an attack from occurring. There are many steps that an organization can take to make the chances of the attack succeeding much less likely. These steps include the various security best practices that organizations attempt to employ [1,2,10]. The fact that there is no absolute assurance that an attack will not succeed requires that every organization include detection and response capabilities in their security program. Organizations frequently test the effectiveness of their prevention measures when they conduct vulnerability assessments and penetration tests. There are numerous articles and books that describe how to conduct these [5,17] and a quick search of the Internet will yield numerous companies that provide this service on a contractual basis.

A single organization conducting an internal exercise is the most basic form of a cyber-security exercise. At the other extreme is an exercise that incorporates various agencies at the city, state, and federal government level, and involves a scenario that encompasses not just information systems, but other critical infrastructures as well. A recent example is the TOPOFF exercise that occurred in May 2003. It included individuals at all government levels in multiple cities in two different states, including federal government personnel. It demonstrated the understanding that such events are important, and provided the organizations involved with a feeling as to how prepared their organizations were to respond to an incident with widespread infrastructure disruption, including physical damage and casualties [11]

From the information systems security perspective, one drawback to exercises such as TOPOFF is that they tend to focus on the most obvious and immediate dangers – those that involve potential loss of life – and the cyber piece of the exercise can easily be overlooked or ignored. An alternative approach is to conduct a cyber-centric exercise; that is, one that concentrates on the ability of the participants to respond to a cyber-event. This has two advantages over incorporating a cyber aspect into TOPOFF-type exercises. First, it isolates the cyber security aspects of a large-scale exercise, enabling the participants to narrow their focus to information systems infrastructure considerations. Second, the budgetary requirements, administrative overhead, and coordinating efforts, although still significant, are much less demanding than a full-scale exercise. An example of a this type of cyber exercise, named Dark Screen, was conducted recently by The University of Texas at San Antonio's (UTSA) Center for Infrastructure Assurance and Security (CIAS) (discussed in more detail in Section 4).

Another type of cyber-security exercise is sector or industry-level exercises. These involve multiple organizations, including entities external to the organization such as customers, suppliers, peer or competing firms, and assorted government agencies. They are challenging to organize, and require a high degree of cooperation and coordination between entities not accustomed to working together in such a fashion. Cross-sector exercises involving two or more industry sectors obviously require an even higher level of coordination. The need for exercises at these levels, however, is great due to the interdependencies between industry sectors. For example, a disruption in the telecommunications sector can degrade the ability of the financial sector to process transactions, the transportation sector to schedule flights, and the energy sector to monitor and control pipelines and power plants. These problems in turn can have a ripple effect that spreads to other sectors, resulting in a series of second, third, and *n*th order effects [16]. It is recognition of this that has driven the development of the Information Sharing and Analysis Centers (ISACs) mentioned earlier. The ISACs provide a focal point for members of each sector to report cyber-security related events. The ISACs then analyze and disseminate that information, notifying all the sector members of the situation and formulating a coordinated sector-wide response. An example of a sector-level exercise is presented in Section 5.

Since activities in one sector will often affect activities in another, cross-sector coordination is also important in any response to a cyber-security event. Reminiscent of the SLAMMER worm of January 2003, the Blaster worm infected over 330,000 computers worldwide. This incident illustrates how quickly a cyber security event can spread across the Internet, affecting all sectors. [14] Events such as these, however, are in one respect much easier to deal with since they are high profile. A well structured attack conducted over many months and involving many different networks or systems, on the other hand, will be much harder to detect unless coordination between sectors takes place. This is one of the major reasons to conduct cross-sector exercises.

## 4. Dark Screen – a City/County Exercise

Dark Screen is a City/County cyber-security exercise conducted in San Antonio, Texas. While not the first city cyber-security exercise, it did have the distinction of being the first to conduct a community-wide exercise that involved all sectors, not just government agencies. [23] The goal of Dark Screen is to test the ability of San Antonio and Bexar County to prevent, detect, and respond to a cyber-terrorist attack. When the exercise was first proposed, by Congressman Ciro Rodriguez (D-TX), the question as to what exactly should be tested was raised. The desire by some was to make it as technical as possible with live penetration tests of the city's networks as well as the networks of the various infrastructures supporting the city/county. The way this was approached in Dark Screen was to conduct three separate phases for the exercise. The first phase, a tabletop exercise, occurred September 13, 2002. The purpose of the initial tabletop was mostly to bring the various entities together and make them aware of what was possible in a cyber-arena and how it could affect their own organization. Another goal was to bring the various individuals who would be responsible for responding to a cyber-security event together so that they could meet and exchange contact information. The initial phase included not only representatives from the local city and county emergency response organizations but also representatives from the local critical infrastructures (e.g. power, water, communications), local industries, and state and federal agencies. The tabletop lasted 4 hours and consisted of a series of events, presented to the participants in three stages, that represented events leading up to the hypothetical attack, the events representing the attack, and a period to recover after the attack had occurred. Participants were grouped at tables based on what organization they were representing and facilitators guided the discussion of each group as they examined how they would respond to the various events. No actual response was conducted during this tabletop phase of the exercise.

The second phase of the exercise consisted of activities conducted by the various organizations in the city in response to the lessons that they learned during the tabletop phase. One common lesson learned was the need for better communication between agencies and rosters were created so people knew who to contact should an event occur. Another lesson that had been learned was the need to ensure that backup communication mechanisms were in place in case primary methods (such as the Public Switched Telephone Network) were lost. During the second phase vulnerability assessments and penetration tests were also conducted for various organizations representing the critical infrastructures in the city (e.g. water and electricity). A discussion was conducted early in the planning for Dark Screen as to what would be tested from a "live" standpoint. The desire to see if the "power grid could be taken down" was mentioned several times. While this certainly would be glamorous, it was decided that this was neither realistic nor did it fit into the goals for the organization. Actually bringing an operational network down may indeed be the ultimate goal of an attacker but there is no way to effectively test whether this can be done without negatively impacting the city. Obviously the power cannot actually be disrupted without affecting all local residents. The same is true of emergency agencies or the telephone service. It may be argued that it is possible to penetrate a system to the point that "the next keystroke would take this system down" but such actions are dangerous and certain activities cannot be shown to be effective unless they are actually conducted (e.g. a Denial of Service attack – how does one know that it will really be effective or not against an operational network that has some mitigating countermeasures in place, unless you actually conduct the attack to test how well the countermeasures work). Some argue that you can use a separate network configured the same way that the operational network is configured but this only provides a limited ability to test technology, and to possibly train individuals in response techniques they normally would not have an opportunity to work with. The artificiality of the separate network introduces too many factors that make it ineffective in testing the "human element". For example, in a normal operational environment there are many activities being conducted that are legitimate. Interaction with users occurs constantly. Simulating both the valid traffic (network and otherwise) is very difficult in a simulated environment. In addition, in an operational environment those who are tasked with detecting and responding to security events never know when they may occur yet when working with a simulated network they know that they should be at an increased level of alertness since they know that something will be occurring. It was for these reasons that for Dark Screen, what was to be tested during the "live exercise" in the third phase was limited to mostly non-technical issues and instead the second phase included functions such as penetration tests for the various entities.

The third phase was conducted in September, 2003. The purpose of the third phase was to exercise the response capabilities for the entities involved. How well do they respond to indications and warnings of possible pending attacks? How well can they communicate and do they have the ability to communicate and coordinate with other agencies in the city as well as the state and federal government should primary communication methods be lost? The hope was that Dark Screen could help develop a community response to security events and not simply rely on government entities.

Specific results from any of the phases of the Dark Screen exercise are considered sensitive by the participants of the exercise and have not been released. The official reaction of the organizations involved is to acknowledge that the exercise was a success and lessons were learned that have helped prepare the city/county to respond to cyber-security events. One other acknowledged lesson learned was the need to communicate with other local entities. Prior to the Dark Screen exercise, the various organizations involved had experienced one of two types of security incidents. They either were involved in an attack on their organization, which was not communicated with other organizations since it was considered a private matter, or the security event was one of the many events that affected the nation as a whole – such as Slammer. In this second instance the organizations did not communicate with others in the city since they could go to national sources to obtain information about the attack. The Dark Screen exercise illustrated a third type of attack, one aimed at a community where communication between organizations in the community is necessary to effectively address the event. Having to consider this new type of attack forced entities to work cooperatively in a manner they had previously not considered.

## 5. Sector-Based Exercises

Exercising the various sectors that make up the critical infrastructures for the nation is an involved process. The first such exercise, outside of the Department of Defense, was the Blue Cascade Exercise conducted in June, 2002 in the Pacific Northwest involving public officials and industry leaders from several Northwestern states and Canadian provinces. Designed to assess the preparedness of the region's critical infrastructures and how an attack on one would impact the others, this exercise demonstrated that the operators of the critical infrastructures had little understanding of how their infrastructures were interrelated. [20]

A more recent series of exercises has been conducted by the UTSA Center for Infrastructure Assurance and Security. The first of these occurred in March, 2003 for the Financial Services sector in New York. Sponsored by the New York Electronic Crimes Task Force, part of the United States Secret Service, the exercise was designed to bring together high-level managers in the various financial services organizations in New York City to discuss their individual and sector-wide ability to respond to cyber-security events at various levels of threats. The specific results of the exercise, and details about the specific scenarios used in the exercise are considered sensitive and have not been released. Details about the need for such an exercise and how it was conducted, however, can be discussed.

The exercise in New York consisted of 4 scenarios with multiple events presented in each scenario. The scenarios progressed in their level of complexity throughout the day. The first scenario presented several events that could be considered of an unstructured nature and the type of things that are commonly faced by organizations today – events such as viruses, web defacements, and simple network probes. The second and third scenarios presented more complex situations that might be experienced as a result of a structured attack on the organization by an entity such as organized crime. Events in these scenarios included items that might be more expensive and time consuming to conduct including bribing of an insider to perform some malicious activity or the development of special tools to be used in an attack. The final scenario presented situations that might occur as a result of a highly structured attack that could be launched by nation states or terrorist organizations against some aspect of the U.S. infrastructures. Picking up on early indications and warnings became very critical in this last scenario as attacks of this nature may be of the "low and slow" variety which occur slowly over very long periods of time.

The participants for the event were broken into two groups for each scenario. One group consisted of a dozen participants who were taken to a separate room where they were presented the events sequentially. They had the opportunity to ask technical questions of one of the scenario developers who knew the real background of the scenario and all related activities. The participants were to determine what their response would be for the events presented and a spokesperson was selected to present to the larger group left in the auditorium what they had decided.

While the smaller group was working out their response, the larger group of participants were presented the same events but were also asked a series of leading questions to check what their response might be. The nature of the questions inevitably led them to certain conclusions and actually provided additional information that the smaller group would not receive unless they asked the appropriate question of the scenario developer. The larger group had the opportunity to discuss the situation and to ask questions and also had the ability to periodically view the participants from the smaller group as they conducted their discussions. Different participants were chosen each time to be part of the smaller group discussion. The result of this method was to not only provide participants the ability to try and work through a series of events that constituted a cyber-security attack but also to experience how difficult it often is to address such situations with limited time and knowledge of the "big picture". A major theme heard from participants was the necessity to better coordinate and communicate during a security event. This was mentioned not only in relationship to the sector itself but between various sectors and the federal government as well. The importance of organizations such as the ISACs was also discussed and the need for them to provide timely guidance and leadership when a security event occurs. This lesson learned was similar to the one learned during the Dark Screen exercise where participants discovered how better communication between entities was needed to effectively address a cyber security event.

In August a two-day, 6-scenario event was held in Chicago for the Financial Services sector in that region. Again sponsored by the U.S. Secret Service, the event resulted in similar lessons learned as the one previously held in New York.

## 6. Information Sharing

One observation that was repeatedly made in all of the exercises was the need to share information between organizations and sectors. This lesson learned illustrates the need for more than just a technological solution to the computer security issue. Participants in all of the exercises had implemented the standard security solutions found in most organizations today. These included such things as firewalls, intrusion detection systems, and virtual private networks. Despite this technology, organizations were introduced to threats for which technology alone would not provide a solution. In responding to security incidents, communication between organizations is essential. The ISACs were established for this purpose.

Information sharing can take several forms. Some information that needs to be shared between the organizations in a sector is not time-critical. If it takes several weeks or even months to disseminate certain information it will not adversely affect anybody. Other information is more critical and should be disseminated within a few days. The ISACs as currently implemented can accomplish information sharing within these time periods. What they are not able to accomplish is to disseminate information that needs to be received in a few hours or even minutes. The speed of the Slammer worm, which infected more than 90 percent of vulnerable hosts within 10 minutes, [14] demonstrates the speed with which cyber-security incidents can occur. If the sectors that represent the different critical infrastructures want to be able to respond quickly, they need to have a different communication structure implemented.

The military Computer Emergency Response Teams respond to time sensitive threats. The military is a much more monolithic structure which can exert control over its networks in a way that is different than the ISAC's. The ISACs do not have the responsibility or the authority to control the networks of the many different organizations that are members. Again, the sectors face a problem for which a technological solution is not the answer. To accomplish a similar level of control the ISAC will first need to have a 24/7, 365 days/year operation which they use to serve as a focal point for the individual sectors and to receive information from government agencies, the other ISACs and the security industry

The question remains as to where the ISACs receive their information. As originally designed, the National Infrastructure Protection Center (NIPC) sponsored the ISACs and would interface with them. The ISACs are now sponsored by the Department of Homeland Security (DHS). It is the responsibility of the DHS to ensure a coordinated response between and with the ISACs in the event of a cyber-security incident. Since the creation of the DHS, a lot has happened in the organization and operation of the ISACs and their final implementation remains to be seen. The DHS, in turn, has to have mechanisms in place to receive and share information with other government agencies (including the military, law enforcement and intelligence communities) and the security, computer, and telecommunication industries. When organizing the government, the military can again serve as a model where each of the individual services maintains their own CERT. All of these then report to a single Department of Defense (DoD) CERT which can disseminate information to other organizations outside of the DoD or can receive information from outside the military to pass to the individual service CERTs. States also need a similar structure and some states are beginning to form their own centers to coordinate their cyber-security activities. [6]

## 7. Organizing a Cyber-Security Exercise

Creating and conducting a cyber-security exercise is a valuable experience for all participants but can be a major undertaking. Each exercise will vary in its planning and implementation but there are some general steps that will be applicable to all.

### *Determine the scope*

An initial decision that must be made is to determine exactly what is to be exercised. Is the desire to test some level of government response (such as a city/county), or possibly to conduct a sector-based exercise, or is the goal to determine a single organization's ability to respond to a cyber-security incident of some sort? Obviously the larger the scope the more involved and complicated this process. This is not to say that these exercises should be discouraged, on the contrary, it can be argued that all communities should be conducting these exercises just as they conduct exercises to test their emergency fire, police, and medical services. Exercises that incorporate more than one sector are particularly challenging to conduct. Obtaining support from government agencies often is a very political process and eliciting support of senior officials will greatly aid in keeping the planning moving. The importance of obtaining this support cannot be overemphasized and will be critical for the success of the effort.

### *Determine what is to be tested*

Another question that needs to be addressed is what will be tested – is the goal to test the ability to detect an attack or to respond to one? Is the goal to conduct a technical exercise similar to a penetration test or is it designed to test whether the personnel involved understand the procedures they are to follow in the event of a cyber-security incident and know who they should contact? For larger-scale exercises involving multiple organizations there may in fact be different goals for each organization, which the planning must take into account. One organization may want to test their ability to detect an attack while another may only be interested in evaluating their employee's knowledge of security procedures. It is best to let each organization determine what it is they want to test. A little encouragement and some suggestions might be used to help stimulate and obtain the desired responses.

### *Select a scenario planning team*

The creation of a smaller scenario planning team is critical. The team should be no larger than a dozen individuals and should have as broad a representation as possible. This group will be the entity that actually develops the specific events that will be included in the overall master scenario document. Creativity is important but realism is essential. Whatever is created must be based on what is actually in place. It will probably not be possible to have an expert from all sectors on the team so points of contact should be obtained that the team can go to in order to obtain technical information. For an exercise involving only a single organization, the team can be much smaller with no more than four individuals on the team.

### *Choose an overall scenario storyline*

Once the planning team is selected, the overall storyline needs to be developed. Will the incident be a terrorist attack, an attack by organized crime, or some other security incident? What is the goal of the attackers – what is it that they are trying to accomplish? Choosing a realistic attack is critical as this storyline is what ties all of the events together. If participants come away from the exercise making statements such as "that would never happen" then the exercise will be most likely viewed as a failure.

### *Fill in the events that support the story*

There may be several events that occur leading up to the main attack that might provide indications and warnings of the pending attack. Probes of networks or phone calls to individuals asking for certain restricted information might provide advance warning of an inordinate level of interest in the organizations participating in the exercise. The team should create a number of these events that provide the background details for exercise. This is also a good way to encourage communication between participating organizations. Before actually conducting the exercise it is a good idea to have the larger group with representatives from each participating organization review the overall plan and series of events. Each of the individuals that will participate in this review will become a "trusted agent" for the exercise and should agree to not reveal the details before the exercise is conducted. Depending on the size of the exercise, more than one of these review sessions may be necessary.

### *Conducting the exercise*

The exercise can take several forms. It can be a tabletop exercise in which all participants meet at a single location to address the exercise scenario events as a group. The exercise could also be conducted at each of the organizations concurrently. The advantage of a tabletop exercise is that it is much easier to control. The disadvantage is that the participants are only discussing what they would do in response to the events presented, they aren't actually responding to them. Having the exercise spread among all of the organizations provides the opportunity to actually exercise the response capabilities of the organizations but it is much harder to control. Which is the appropriate format depends on the goal for the exercise. Is the exercise designed for awareness or education or is it designed to test actual responses? If the decision is made to test responses, several precautions should be taken. For organizations that still have real-world operations, such as fire and police departments, there needs to be a method to terminate the exercise immediately should an actual incident occur. The same is true of network personnel who may have to respond to an actual cyber incident during the time the exercise is taking place. Observers should be present when certain events occur so that the reactions of the individuals involved can be recorded. The observers, who may be the trusted agents from the organizations, can also make a quick determination as to whether an event is part of the exercise or is a real-world incident and can make the decision to call off the exercise if needed. A central "command post" should be utilized which all participants can call to report real-world events and which can in turn contact the other observers should it become necessary.

The amount of detail required in a script for a tabletop scenario is much lower than what is required to maintain control of an exercise spread among several organizations.

### *Create an "after-action" report*

After the exercise is concluded, a report should be created that describes the original goals, scenario, and the lessons learned from the exercise. Individual organizations should also be encouraged to create their own reports, which would include more sensitive details that would not be included in the larger group report. Both the larger group report as well as the individual organizational reports should include any recommendations for improving the security or response capabilities of the organizations. The report should also include a discussion on conducting the exercise itself and should provide lessons learned and details on how to improve on the exercise when the next one is planned.

## 8. Conclusion

Technology alone is not sufficient to solve the computer security problems the nation faces. The human element is present at many places in our approaches to security and these human elements should periodically be tested to see if they could effectively respond to cyber security events. A series of exercises have been conducted for various organizations to accomplish this task. A common lesson learned throughout all of the exercises conducted is the need for a greater sharing of information between organizations within and between sectors. The ISACs were formed to accomplish information sharing but their current organization does not facilitate the level and speed of sharing that needs to occur for them to be part of a response to security incidents. Additional manning for both the ISACs and their individual members will be required for them to become truly effective.

Regardless of whether the ISACs become a major component in sector-wide security responses, individual organizations, as well as municipal governments, should consider conducting their own exercises to ensure that they are prepared in the event of a cyber-security incident. The communication necessary to effectively address a cyber security event is unusual and organizations currently are probably not considering what is needed to address cyber security events. It is too late to establish the required lines of communication when an event occurs. Instead a cyber-security exercise could serve as the catalyst to bring entities together to discuss how to address this type of event. Conducting an exercise can be a major task but a general outline for accomplishing one has been presented and various organizations exist that are ready to assist in this important endeavor.

## References

[1] Austin, R. and Darby, C. (2003) "The Myth of Secure Computing", *Harvard Business Review*, 81 (6), pp. 120-126.

[2] Avolio, Frederick (March 20, 2000), "Best Practices in Network Security", www.networkcomputing.com/1105/1105f2.html

[3] Backhourse, J. and Dhillon, G. (1996) "Structures of responsibility and security of information systems", *European Journal of Information Systems*, 5 (1), pp. 2-9.

[4] Briney, Andrew and Frank Prince (September 2002), "Training Remains the Weakest Link", Information Security, Vol 5, No. 9.

[5] Cole, Eric (2002) Hackers Beware, New Riders Publishing, Indianapolis Indiana.

[6] Cornyn, John and Bobby Inman (March 25, 2002) "The Texas Infrastructure Protection Center", Report of the State Infrastructure Protection Advisory Committee (SIPAC), Office of the Attorney General for the State of Texas.

[7] DHS (2003) "The National Strategy to Secure Cyberspace", Department of Homeland Security, http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

[8] DHS (2003), "Sharing Information to Protect the Economy", Department of Homeland Security, http://www.dhs.gov/dhspublic/display?theme=73

[9] Dhillon, G. and Backhorse, J. (2001) "Current directions in IS security research: Towards socio-organizational perspectives", *Information Systems Journal*, 11 (2), pp. 127-153.

[10] Dutta, A. and McCrohan, K. (2002) "Management's Role in Information Security in a Cyber Economy", *California Management Review*, 45 (1), pp. 67-87.

[11] FEMA (May 5, 2003), "TOPOFF 2", FEMA News, Department of Homeland Security, www.fema.gov/nwz03/nwz03_topoff2.shtm

[12] Lemos, Robert (January 23, 2001) “Security patches aren’t being applied”, http://zdnet.com.com/2100-11-527502.html.

[13] Melek, Adel (2003) “2003 Global Security Survey” from Deloitte, ,Touche, Tohmatsu, www.deloitte.com/dtt/cda/doc/content/Global Security Survey 2003.pdf.

[14] Morre, David, Vern Paxson, Stephan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, (2003) “The Spread of the Sapphire/Slammer Worm”, www.caida.org/outreach/papers/2003/sapphire/sapphire.html.

[15] Office of Homeland Security (2002) *National Strategy for Homeland Security*, www.whitehouse.gov/homeland/book/nat_strat_hls.pdf

[16] Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001) “Indetifying, Understranding, and Analyzing Critical Infrastructure Interdependencies”, *IEEE Control Systems Magazine*, 21 (6), pp. 11-25.

[17] Scambray, Joel, Stuart McClure, and George Kurtz (2001), Hacking Exposed 2ed, Osborne/McGraw Hill publishing, Berkeley, California.

[18] Schoemaker, P. (1995) “Scenario Planning: A Tool for Strategic Thinking”, *Sloan Management Review*, 36 (2), pp. 25-40.

[19] Sigmond, Stephen and Vikram Kaura (November 1, 2001) “Safe and Sound: A Treatise on Internet Security”, RBC Capital Markets' report.

[20] Sirhal, Maureen (August 13, 2002) “Critical infrastructure operators lack key information”, http://www.govexec.com/dailyfed/0802/081302td1.htm.

[21] van der Heijden, K. (1996) *Scenarios: The Art of Strategic Conversation*, John Wiley & Sons, Chichester.

[22] Verton, D. (2003) “Blaster worm linked to severity of blackout”, *Computerworld*, Aug. 29, 2003, http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,84510,00.html

[23] White, Gregory and Joe Sanchez (January 2003), “Dark Screen Sheds Light on Cyberspace Security Issues”, Signal, Vol. 57, No. 5.