MIS QUARTERLY EXECUTIVE

DARK SCREEN: AN EXERCISE IN CYBER SECURITY[1]

Tim Goles
The University of Texas at San Antonio

Gregory B. White
The University of Texas at San Antonio

Glenn Dietrich
The University of Texas at San Antonio

Executive Summary

The digital age has transformed how organizations function. The production and delivery of essential goods and services is now highly dependent on the global information infrastructure: the complex and interconnected telecommunications networks and information systems owned and operated by a multitude of discrete organizations. Yet, this amorphous entity is beyond the control of individual organizations. This paper presents Dark Screen, a scenario-based exercise for identifying and assessing resources and capabilities useful in protecting the information infrastructure.

One community's experience with Dark Screen offered three main observation: (1) there was a low level of awareness regarding information infrastructure interdependencies and vulnerabilities among the exercise participants, (2) the participating organizations had no process or mechanism for coordinating interorganizational responses to a cyber security incident, and (3) the communications channels for disseminating information before and during a cyber security incident were ill defined.

In today's environment, organizations need to broaden their view of cyber security. The self-protection model, where each organization only deploys a perimeter defense around its own boundaries, is no longer adequate. The three recommendations for management from the Dark Screen exercise are: (1) view cyber security as a business issue, not a technology issue, (2) broaden your cyber security mindset to include the information infrastructure your organization depends on but does not control, and (3) join collaboration efforts to coordinate cyber security regionally, if not nationally.[2]

THE WORLD RELIES ON CRITICAL INFRASTRUCTURES

In January 2003 a small data packet was sent to a single SQL server. That data packet, consisting of only 376 bytes of code, infected the server with the Slammer worm. The worm then launched itself onto the Internet. In just 30 minutes it had infected 78,000 machines worldwide. This pattern was repeated in August 2003 with the spread of the Blaster and SoBig worms.

These destructive computer programs saturated the Internet, shutting down servers and interfering with vital communications and services. The impact was widespread. Air and rail transportation was delayed and, in some cases, cancelled. Production and delivery of electrical power were interrupted. Customers could not withdraw money from automated teller machines. Emergency services call centers were shut down. The ripple effect of these and other disruptions had immediate and severe consequences for a wide range of economic transactions and human services.

[1] Jack Rockart is the accepting Senior Editor for this article.

[2] The authors would like to gratefully acknowledge Peter Todd for his helpful suggestions on improving this paper. Funding for this research was provided by the Center for Information Assurance and Security (CIAS) of the University of Texas at San Antonio under a grant from the United States Air Force. An early version of this paper was presented at the SIM Academic Workshop on December 13, 2003, in Seattle, Washington.

These incidents illustrate the interconnected and interdependent nature of today's world. Advances in technology have transformed production and delivery of goods and services. Company-centered, often centralized, hierarchical structures and workflows have given way to complex and interdependent systems and processes that permeate society. These *critical infrastructures*[3] depend on the *information infrastructure*:[4] the interrelated information and telecommunication systems, technologies, and capabilities to gather, process, and disseminate information both within and among organizations.

The information infrastructure transcends organizational, geographical, and national boundaries. It has become so large, complex, and widespread that it is beyond the direct management or control of any single entity. Thus, a firm, no matter how diligently it implements security policies and procedures, has a potentially fatal exposure that is beyond its direct control. Further complicating matters, recent turbulence in social, political, and commercial environments, coupled with ongoing technological advances, has given rise to new threats to the information infrastructure. These threats raise the question, "How can organizations – individually and collectively – prevent, detect, and respond to incidents that threaten the information infrastructure?"

One promising approach to uncovering answers is to use *scenario-based exercises* to identify and test resources and capabilities aimed at protecting the information infrastructure. This paper presents one such exercise: Dark Screen. Lessons learned from the exercise highlight the need for individual firms to extend their information security envelope beyond traditional organizational boundaries to improve their cyber security posture. Two associated issues surfaced by Dark Screen are potential disclosure of sensitive information to others when adopting a more open and integrated approach to cyber security, and the role of government in protecting the information infrastructure.

WHY BE CONCERNED ABOUT OVERALL INFORMATION INFRASTRUCTURE SECURITY?

The information infrastructure "consists of technologies and capabilities for gathering, handling, and sharing information … depended upon by multiple organizations, whether within a single enterprise, a critical infrastructure sector … the nation as a whole, or transnationally."[5] The information infrastructure is both part of and apart from the other critical infrastructures. It is obviously part of the other infrastructures because it enables the exchange of mission-critical information, and it facilitates the operation and control of essential processes in individual industry sectors. It is apart from the other critical infrastructures in that it cuts across all levels and sectors of industry, government, and society. It connects critical infrastructures to one another via cyber links, adding another layer to the already tangled web of infrastructure interdependencies.[6] In the event of a disruption in the information infrastructure, the other critical infrastructures would grind to a halt, severely disrupting the daily flow of commerce.

The information infrastructure faces many threats and vulnerabilities (Figure 1). *Threats* are impending dangers or menaces that can originate from any actor with the capability, opportunity, and intent to do harm.[7] *Vulnerabilities* are weaknesses in the design, implementation, or operation of the information infrastructure. As Figure 1 indicates, these threats and vulnerabilities do not fall neatly within existing institutional responsibilities, "but rather sprawl messily across many of the vertically integrated political, social, and economical structures."[8] The alignment of threats and vulnerabilities leads to *risks*, or potential damage to the information, activities, and technologies used in the other critical infrastructures. This interconnectedness furnishes a compelling incentive for firms to address information infrastructure security.[9]

[3] Critical infrastructures provide the continued supply and support of energy, utilities, manufacturing, food, telecommunications, financial services, transportation, public health and safety, and national security. They are discussed in depth in the 1997 report of the President's Commission on Critical Infrastructure Protection (http://www.timeusa.com/CIAO/resource/pccip/PCCIP_Report.pdf).

[4] Much of the material in this paper concerning the information infrastructure comes from *The Cyber Security Research and Development Agenda*, published in 2003 by the Institute for Information Infrastructure Protection (I3P). The I3P is a consortium of research organizations focused on cyber security and information infrastructure protection. The Agenda may be found at http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf.

[5] I3P, Section 1.2, p. 2

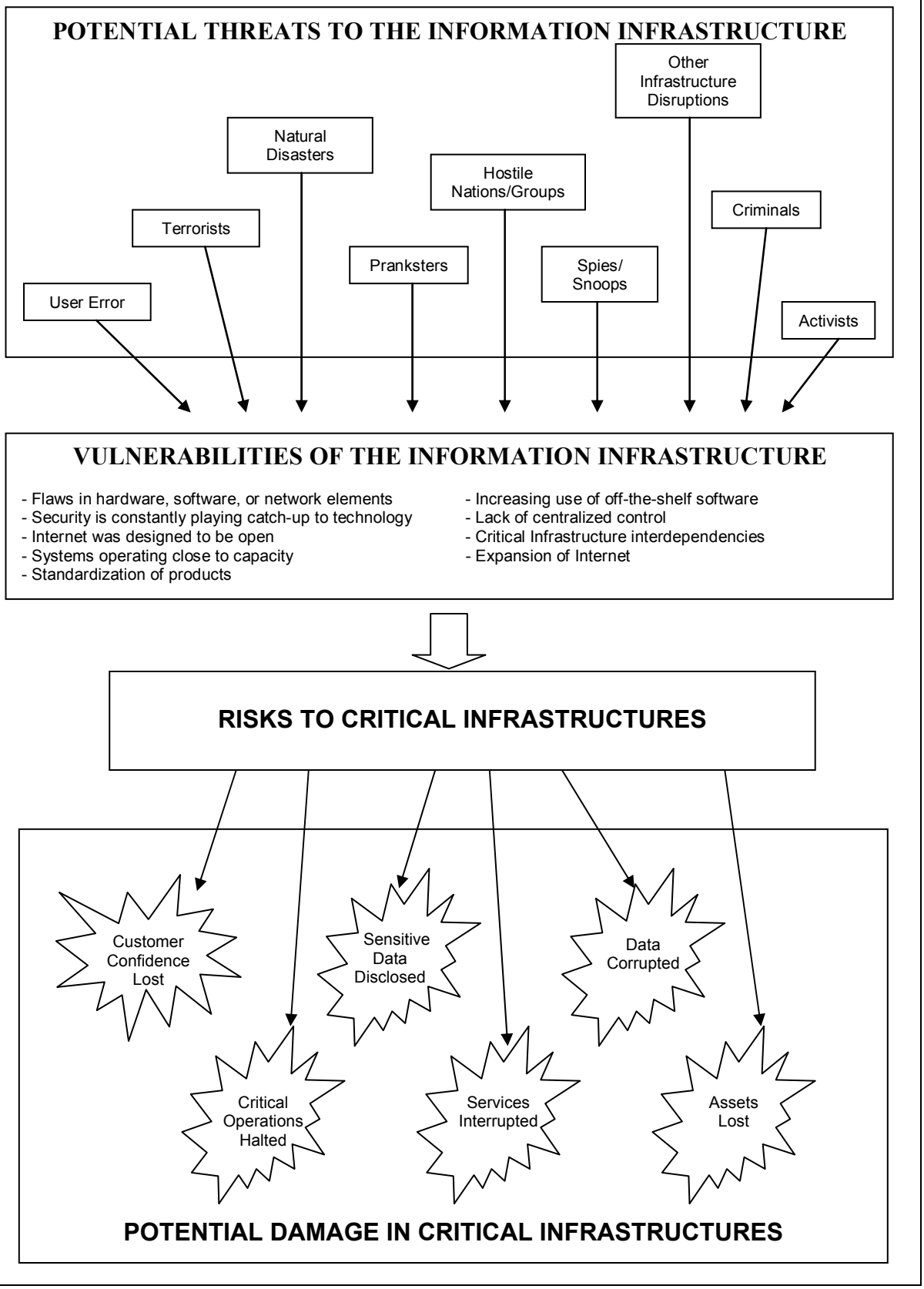
[6] For a comprehensive discussion of critical infrastructures and their interdependencies, see Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K., "Critical Infrastructure Interdependencies," *IEEE Control Systems*, (21:6), Dec. 2001, pp. 11-25.

[7] Institute for Defense Analysis (IDA): "National Strategies and Structures for Infrastructure Protection: Report to the President's Commission on Critical Infrastructure Protection," 1997, available at http://permanent.access.gpo.gov/lps19700/NationalStrategiesStructures.pdf.

[8] Rathmell, A., "Protecting Critical Information Infrastructure," *Computers & Security*, (20:1), January 2001, pp. 43-52. Quote is from page 46.

[9] Based in part on Figure 1, p. 23, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities," April 2001, GAO-01-323, http://www.gao.gov/new.items/d01323.pdf

Figure 1. Information Infrastructure Threats, Vulnerabilities, and Risks



At this point a natural question is, "If every organization adequately addresses its own cyber security, why should we concern ourselves with overall information infrastructure security?" The answer is threefold:

1. We do not live in an ideal world
2. It may be more cost-effective to pool security resources
3. Due diligence requires firms to assess risks that extend beyond organizational boundaries

We do not live in an ideal world. It is unreasonable to expect every organization to implement best security practices. Large firms have the resources and technical expertise to attain a high level of security, but small and medium-sized firms often do not. Their lower level of security makes them potential weak links in supply and distribution chains.[10]

The information infrastructure also has inconsistent levels and types of technologies, ongoing organizational and environmental turmoil (e.g., mergers, acquisitions, reorganizations, new regulations), and a growing number of increasingly sophisticated threats.[11] Information systems and technologies do not always perform as their designers intended, nor do their users always fully understood them. These system-based and user-based security vulnerabilities are compounded by each organization's need to interface with diverse types of hardware, operating systems, and communications systems. In such a situation, the ability of individual actors to respond to threats is limited. Identifying and resolving problems or threats requires collaboration and cooperation with other entities. For example, the coordinated response of private firms and government agencies to the Code Red virus minimized its potential disruption and damage.[12]

It may be more cost-effective to pool security resources. This pooling is reflected in calls to protect the 'global information commons' through collective action.[13] For example, the attacks of September 11, 2001 in New York City revealed that, although individual Wall Street firms thought they had redundant and diversified information systems and communications networks, once the networks left the firms' boundaries, they were routed by the telecommunications carriers through a central switching office. That central office was severely affected by the attacks, resulting in a total regional network failure. Consequently, the financial industry, telecommunications carriers, and the city are jointly taking steps to strengthen their infrastructure security by building true redundancy into the regional telecommunication network and sharing the cost.[14]

Due diligence requires firms to assess risks that extend beyond organizational boundaries. The convincing reason for firms to address information infrastructure security is the legal concept of *due diligence*. Due diligence has recently been expanded to include the responsibility of individual firms to assess IT-related risks and vulnerabilities that extend beyond their traditional organizational boundaries. A firm that experiences an infrastructure-related interruption in critical business functions or services may quite likely be perceived as negligent or incompetent, regardless of whether or not the firm is at fault. For example, a denial-of-service attack launched from outside the firm will, in all likelihood, disrupt transactions and communications between the firm and the outside world. This disruption can lead to a loss of customer confidence and good will. It can also result in higher insurance premiums, reluctance or refusal of other companies to do business with the firm, and rapid devaluation of the firm's stock price, with a corresponding decrease in the firm's market value.[15] The firm and its executives will be exposed to significant corporate, and possibly even personal, legal liability if they do not exercise due diligence in protecting the firm's computers and networks. In fact, there is legal precedent holding that network attacks have become so common that they should be anticipated.[16]

[10] Wearden, G. *ZDNet UK Insight*, 11 November 2004, http://insight.zdnet.co.uk/specials/networksecurity/0,39025061,39118368,00.htm.

[11] I3P, Section 3; http://www.cert.org/stats/cert_stats.html.

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

[13] Lukasik, S., Greenberg, L., and Goodman, S. "Protecting an Invaluable and Ever-Widening Infrastructure," *Communications of the ACM*, (41:6), June 1998, pp. 11-16; Lukasik, S. "Protecting the Global Information Commons," *Telecommunications Policy*, (24:6), Aug. 2000, pp. 519-531.

[14] Junnarkar, S. "Keeping Networks Alive in New York." *CNET News*, Aug. 22, 2002, http://news.com.com/2009-1001-954796.html; Seifert, J. "The Effects of September 11, 2001, Terrorist Attacks on Public and Private Information Infrastructures: A Preliminary Assessment of Lessons Learned." *Government Information Quarterly*, (19:3), pp. 225-242.

[15] For more information on the business and legal consequences of failure to exercise cyber security due diligence see: Cavusoglu, H. "The Economics of Information Technology Security," *Eighth Americas Conference on Information Systems*, 2002, pp. 2481-2485; Cook, W. "Dangerous Waters," *CSO Magazine*, August 2004. http://www.csoonline.com/read/080104/flashpoint.html; Dutta, A. and McCrohan, K., "Management's Role in Information Security in a Cyber Economy," *California Management Review*, (45:1), Fall 2002, pp. 67-87; Lipson, H. F. and Fisher, D. A., "Survivability – A New Technical and Business Perspective on Security," *Proceedings of the 1999 New Security Paradigms Workshop*, September 1999.

[16] For a primer on these and other IT security-related legal issues, see: Volonino, L. and Robinson, S. R., *Principles and Practice of Information Security: Protecting Computers from Hackers and Lawyers*, Pearson Education, Inc., Upper Saddle River, NJ, 2004.

Figure 2: Dark Screen Participating Organizations

Alamo Area Council of Governments
Bexar County
- Emergency Operations Center
- County Judge
- District Attorney's Office
- Department of Information Resources

Bexar Metro 911 Network District
BexarMet Water District
CACI
City Public Service
City of San Antonio
- Emergency Operations Center
- Mayor's Office
- Fire Department
- Police Department
- Department of Information Technology Services

Greater San Antonio Hospital Council
Federal Bureau of Investigation
Frost Bank
San Antonio Water System
SBC
State of Texas
- Attorney General's Office
- Department of Information Resources
- Texas National Guard

The University of Texas at San Antonio
United States Air Force
United States Army
Veridian

SCENARIO-BASED EXERCISES

Scenarios are tools to help organizations deal with uncertainty. They are built around descriptions or narratives of possible future situations or events that might affect the organization and its environment. They are often used to help firms address complicated and murky situations with a large number of unknowns, such as in strategic planning or crisis management situations.[17]

Scenarios can be orchestrated using an exercise format. Exercises, in general, are rehearsals designed to increase the probability that an entity will successfully fulfill its mission. The intent of a *scenario-based exercise* is to envelop the participants in a convincing portrayal of a plausible reality, drawing them into the setting. When broadened to include external entities and the environment, scenario-based exercises depict a reality outside the direct control of the participants which nevertheless has significant implications and consequences for them.[18]

In the case of the information infrastructure, what is required is an approach that tests not only an individual organization's ability to respond to a cyber security event but also the ability of related entities (organizations in the same and different industries, government agencies) to respond in a coordinated manner. Achieving this broad view is the essence of a scenario-based cyber security exercise.[19] This paper uses a case study of one such exercise, Dark Screen, to explore the issues involved in information infrastructure assurance.

THE DARK SCREEN EXERCISE

Dark Screen was a yearlong three-phased cyber security exercise conducted in San Antonio, Texas. It was designed to help representatives from the private sector, along with federal, state, and local government agencies, identify and test resources and capabilities to prevent, detect, and respond to a cyber security incident. It had its genesis in the summer of 2001, when pockets of security professionals in San Antonio and the surrounding county (Bexar County) began discussing security issues related to the regional information infrastructure. The events of September 11, 2001 in-

[17] The process of scenario planning and development is described in: van der Heijden, K., *Scenarios: The Art of Strategic Conversation*, John Wiley & Sons, Chichester, 1996. The use of scenarios for strategic planning is explained in: Schoemaker, P. J. H., "Scenario Planning: A Tool for Strategic Thinking," *Sloan Management Review*, (36:2), Winter 1995, pp. 25-40.

[18] The use of scenario-based exercises to address security issues common to large organizations, industries, and various levels of government is discussed in: White, G. B., Dietrich, G., and Goles, T., "Cyber Security Exercises: Testing an Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events," *Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004.

[19] This approach has been successfully used elsewhere to investigate infrastructure security issues. *Blue Cascades*, held in June 2002, was co-sponsored by the Pacific NorthWest Economic Region (PNWER), the US Navy Critical Infrastructure Protection Office, FEMA Region 10, and the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness. It focused on infrastructure interdependencies that could make a region vulnerable to cascading impacts in the event of an attack or disruption. A follow-up scenario-based exercise, *Blue Cascades II*, took place in the fall of 2004 (http://pnwer.org/pris/bluecascades.htm). *Livewire* was a national-level scenario-based exercise conducted in October 2003 that involved over 300 participants representing more than 50 organizations across federal, state, and local governments and the private sector. It focused on cyber interdependencies across infrastructures (http://www.us-cert.gov/policy/ testimony_liscouski_mar3004.html). A series of scenario-based exercises similar to Dark Screen has been held in the financial, IT, and energy industry sectors (http://www.csoonline.com/read/100104/simulation.html).

creased their motivation to address these issues. The final impetus came from Congressman Ciro Rodriguez (D-TX), who proposed in March 2002 that the city and county conduct a cyber terrorist exercise to evaluate the region's cyber security status. At the organizing meeting, the University of Texas at San Antonio's (UTSA) Center for Infrastructure Assurance and Security (CIAS[20]) was chosen to lead the planning and conduct the exercise. Participants are listed in Figure 2.

Phase I

Phase I took place in September 2002. More than 220 individuals from 18 organizations participated. They included not only representatives from the technical and security areas of the organizations but also highly placed executives and government officials. These senior, involved, and knowledgeable executives included department and division heads, operations directors, chiefs of staff, and CIOs familiar with interorganizational communications channels and crisis management procedures. The fact that the exercise was instigated by an influential congressman and fully supported by the mayor and other regional political figures ensured participation from the highest levels of local organizations.

Phase I was a tabletop exercise[21] consisting of a series of scripted events presented in three modules:

1. Module 1 set the stage, outlining the pre-incident situation and presenting a series of seemingly unrelated events leading up to the cyber incident.
2. Module 2 consisted of events representing the actual incident.
3. Module 3 dealt with recovering from the incident.

Each module had built-in "stops" where participants answered questions and discussed their actions and responses to the scripted events.

The participants were grouped at tables according to type of organization and industry. There was no communication or exchange of information between tables. Each table was supplied with a scenario script unique to its participants' organization type or industry. The scripts described only the incidents and events that affected those participants. Some information was common to all the participants, but that overlapping information was limited to information about incidents or events affecting organizations at other tables. Each table's discussions and responses to the scripted events were recorded as the scenario unfolded. Figure 3 presents an abbreviated excerpt from Module 1.

The main purpose of this pre-event phase was to investigate how well each table could recognize patterns or the significance of the events and whether each table could determine appropriate communication channels and responses. For example, did they detect a coordinated and widespread attack, or did they only see a series of isolated and unconnected incidents? Who would they call for more information or assistance? Would they notify any other group or organization? From whom would they expect to receive information?

Immediately following Phase I, the responses were analyzed, and a report was prepared and distributed to the participating organizations. This report served as the basis for Phase II.

Phase II

While Phase II was not directly scenario-driven, it did draw on the individual organizations' responses to Phase I. Phase II was divided into two stages.

1. Stage One consisted of a series of meetings and discussions between exercise officials and individual organizations to assess each organization's responses to Phase I and to formulate recommendations to improve the organization's security. The objective was for the participants to apply the lessons learned from Phase I. After a suitable period of time (generally 3 months), follow-up meetings were held with each organization to evaluate its implementation of the recommendations.
2. Stage Two was a series of vulnerability assessments conducted on several of the major participants. The goal was to evaluate in detail the level of security preparedness of each one in response to threats to the information infrastructure. Overall, several common recommendations for improving security at individual firms emerged. (These are presented shortly.)

Phase III

Phase III of Dark Screen took place one year after Phase I, starting on September 15, 2003 and ending on September 25, 2003. It consisted of a series of scenario-based exercises conducted at selected individual organizations. Each organization created *a red team*. Each red team was composed of skilled individuals who worked on behalf of the organization, seeking to

[20] Designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency, the University of Texas at San Antonio houses the CIAS. CIAS is a multidisciplinary research center designed to bolster research and educational initiatives in the information systems and infrastructure security field. It is a partnership between academia, the private sector, and government that explores technical, behavioral, organizational, and policy issues related to information assurance and security.

[21] A tabletop exercise is a process based on a written scenario that involves the participants in a group discussion through the use of problem statements, directed messages, and prepared questions. It is designed to evaluate plans and procedures, and explore issues of communication, coordination, and responsibility.

Figure 3. Dark Screen Exercise Excerpt

MODULE 1: PRE-EVENT PREPARATION

The World Banking Funds Summit (WBFS) will be held in San Antonio, Texas, the weekend of September 13-15. Similar recent events have seen vocal protestors demonstrating about U.S. involvement in world monetary matters. The generally accepted belief is that the event in San Antonio will likely attract similar protestors. There have been rumors that certain terrorist or criminal elements may try to disrupt the summit as a result of actions taken by the U.S. government to seize their assets.

Monday, August 26, 2002 – 10:00 AM

A forensic cyber investigation has uncovered multiple probings of utility and telecommunications sites in Texas, California, and Wyoming. The probes were routed through telecommunications switches in Saudi Arabia, France, and Pakistan and focused on emergency telephone systems, electrical generation and transmission facilities, and natural gas pumping stations and pipeline control facilities. The intruders were able to assemble a detailed map of each system and possibly intercept and modify SCADA commands without detection.
(SCADA is an acronym for Supervisory Control And Data Acquisition, a generic term covering computer-based systems used to monitor and control physical processes and environmental conditions in a wide variety of plants and systems, including energy, manufacturing, water, utility, and telecommunications applications. SCADA systems are often accessed remotely.)

Question: (To computer security firms and government agencies)
What would be done with this information?
Who would be notified?
How would this information be transmitted to the various utilities?
Who decides on the information release?

Monday, September 2, 2002 – 3:00 PM

Monitoring of hacker chat rooms shows unusually high levels of participation over the last 48 hours. Discussions seem to have centered on a possible new vulnerability in a widely used Remote Access Service (RAS) software package that might allow possible escalation of privileges and crashing the system.

Question: (To computer security firms and government agencies)
Whom do you contact with this information? When?
How would this information be transmitted to the appropriate parties (CERT, vendors, other government agencies, etc.)? When?

Friday, September 6, 2002 – 7:00 AM

CERT releases an advisory on a new vulnerability in the Remote Access Service (RAS) software package that could allow possible escalation of privileges and crashing of the system.

Question: (To all participants)
How does your organization normally receive such warnings?
What does your organization do with this information?
How do you know if a new vulnerability applies to systems in your organization (i.e. how do you know if you have the OS or application in question)?

Friday, September 6, 2002 – 11:00 AM

CNN runs a story on the new vulnerability announced by the CERT. One individual who has in the past demonstrated insider knowledge of the hacker community mentioned hearing of a new virus being written to exploit the vulnerability and set to be released next Friday, the 13th. The virus, nicknamed Black Cat, disables the system and displays a solid black screen – a Dark Screen.

Question: (To all participants)
What steps would your organization take to verify/learn more about this virus/worm?
What steps would your organization take to protect itself from this event?
How does your organization know if it might be vulnerable? (i.e., how do you know what hardware and software your organization has, what version it is, and whether or not it is exposed to this threat?)

Figure 4: A White Card Example

THIS IS A DARK SCREEN EXERCISE MESSAGE

White Card # _____ Date:09/15/03
Participant: Bob Jones Time: 1500 hours

A Denial of Service attack has been launched against your organization's Internet-connected network (IP address XXX.XXX.XXX.XX). This DoS attack has at least been temporarily effective, blocking Internet traffic to/from the network. Internal network traffic is unaffected. What actions will you take in response to this activity?

THIS IS A DARK SCREEN EXERCISE MESSAGE

uncover the vulnerabilities in the organization's information systems that an attacker might exploit. The teams consisted of CIAS staff and a few *trusted agents* from each participating organization (a trusted agent is an individual from the target organization who is privy to the details of the exercise, who is present during the exercise, but who functions primarily as an observer and does not assist the target organization's personnel during the exercise). The red teams were subdivided into two groups. One group was at an offsite location and conducted the actual attack. The second group, including the trusted agents, was onsite.

The mission of the trusted agents, usually mid- and senior-level managers, was threefold:

1. They ensured the scenario was executed according to plan by legitimizing the presence of the red team members and interacting with the 'non-trusted' personnel to provide additional information, if necessary.
2. They functioned as observers to note the organization's response.
3. They served as a fail-safe mechanism; in the event of an unforeseen problem, they could terminate the exercise.

The trusted agents also helped finalize the proposed plan of attack. The plan itself called for live scans and probes of the organization's operational systems and networks. The purpose of the probes was to exercise the organization's capability to detect and respond to indications and warnings of an imminent attack. The probes sent suspicious network traffic to the target company. They were initiated from a pre-arranged IP address so that the trusted agents could ascertain whether or not any truly suspicious traffic occurred during the exercise.

While the probes were underway, a simultaneous *white-card exercise* was held to simulate events or activities that would be too disruptive to daily operations to actually be performed (for example, launching a denial-of-service attack), but which were valuable in assessing other aspects of the organization's response capabilities. The white-card exercise gets its name from the index cards used in the exercise. Each card contained a narrative description of the simulated event. The cards were handed to various personnel on duty during the exercise. These individuals were instructed to respond as if the event were actually occurring. This white-card approach allowed individuals to respond to a specific situation without actually interrupting service at the company. Figure 4 contains a sample white card.

The probes and white-card events were coordinated to provide a single storyline, or scenario, that exercised not only each individual organization's internal response capabilities but also how well the participating organizations worked together to address the security incidents. Key questions in Phase III included asking each organization how they responded to the incident, whom they turned to outside the firm for assistance or more information, and whom they notified about the incident. As with Phase II, a number of frequently recurring issues was observed.

OBSERVATIONS AND RECOMMENDATIONS FROM DARK SCREEN

The three phases of Dark Screen led to two sets of findings. One set contains 3 observations regarding

interrelationships among organizations and with the information infrastructure. The second set consists of 7 recommendations for improving the security posture of individual organizations.

Observations Regarding Interrelationships

1. Overall, there was a low level of awareness regarding information infrastructure interdependencies and vulnerabilities. The participants displayed little understanding of interdependencies between their organization and other organizations. The participants were also, for the most part, unaware of the vulnerabilities and capabilities of other organizations and how those might affect them.
2. There was no process or mechanism to coordinate interorganizational responses to a cyber security incident. Most participants assumed that their organization's security procedures would be adequate for preventing, detecting and responding to cyber incidents. As a result of the tabletop exercise, however, they realized their assumption had been based on viewing their organization as a stand-alone entity. It did not take into account the interrelated and interdependent nature of the information infrastructure.
3. The communications channels for disseminating information before and during a cyber security incident were ill defined. Although some participants were part of small, informal information exchange networks, these networks were based on personal relationships. There was a lack of understanding concerning what capabilities and information each organization had access to and how to share it. After the exercise, one participant summed up the general feeling: "Exchanging business cards before an event occurs is much better than exchanging them during one."

Recommendations for Individual Organizations

1. Designate an individual or group to be responsible for the organization's overall information systems security. Ensure that security-related policies and procedures are current and widely publicized. Develop and implement procedures outlining how the organization would respond to a cyber security incident. Implement a process that ensures the procedures are periodically re-evaluated and modified. Cyber security education and training initiatives should be extensive and ongoing throughout the organization.
2. Create and deploy incident response teams. These teams should identify both "first responders" to cyber events as well as ad hoc members that might be called on to lend specific technical or other expertise.
3. Create a current contact list of individuals and organizations (both internal and external) to contact when a real or suspected cyber security incident occurs. Periodically test and update this list. Many organizations had not compiled a list of people or resources to contact in case of a cyber security question or incident. This oversight impedes the flow of relevant information, hampers advance notification, and thwarts a coordinated response. When compiling this list, encourage managers to thoroughly and creatively search within and outside the firm. Consider, for example, local chapters of professional organizations, such as the Information Systems Security Association (ISSA), or education and research centers, such as Carnegie Mellon University's CERT Coordination Center or The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. URLs for these and other resources are listed in Appendix 1.
4. Sanitize discussions and descriptions of your organization's technical environment.[22] In more than one case, technical information regarding an organization's operating system, network management software, and other internal systems was posted on the organization's Web site, in listservs (mailing lists), or on online help forums where IT personnel had posted questions or comments.[23] Disclosure of this information enables attackers to utilize tools and techniques known to be effective against these particular systems.
5. Insist that critical security patches be installed as soon as they are available. In many cases, the assessment teams' internal scans found known vulnerabilities that were several months to one year old. Default passwords and shared accounts were also frequently found. Firms should stringently require that *all* passwords be changed regularly, including default administrative and system-level passwords. Shared accounts should be prohibited.
6. Do not rely on just a few individuals. Several organizations were able to respond to various events because specific individuals in the organization knew what should be done. Frequently, these indi-

[22] Managers should especially take note of the dangers posed by social engineering, as illustrated in Mitnick, K. D., "Are You the Weak Link?", *Harvard Business Review,* (81:4), pp. 18-21.

[23] This was usually done when trying to obtain help for a technical problem, or to help someone else. Although no malice was involved, and for the most part organizations were not directly identified by name, it was still possible in most cases to identify the company or agency (e.g., "I work for the water utility of a large Texas city…").

viduals were informally anointed security gurus. If these individuals had not been present, the organization's ability to respond would have been severely hampered, resulting in an incorrect or ineffective response.

7. Monitor critical security indicators frequently, ideally in real time. Several organizations reviewed critical security indicators (such as firewall logs) weekly, or less frequently. Such infrequent reviews makes timely identification of potential threats problematic and can slow or prevent effective response. In addition, it hinders organizations from correlating their threat-related information.

DISCUSSION OF THE FINDINGS

The purpose of Dark Screen was to highlight cyber security issues within the information infrastructure, and to help organizations become more adept at preventing, detecting, and responding to threats to the infrastructure. Portions of the exercise pointed out opportunities for individual firms to improve their internal security posture. While this is a necessary first step, it is not sufficient to provide a thorough defense against the full gamut of cyber threats and risks, which in the current environment "are not focused on individual companies, but on regions and industries."[24] Therefore, the next step is to expand the security envelope to include the information infrastructure. To that end, after the conclusion of all three phases of Dark Screen, high-level aggregate findings were compiled. These findings fall into four general categories:

- The overall mindset toward the information infrastructure
- Command, control, communications, and intelligence (C3I), the four aspects of managing information infrastructure security
- Disclosure and trust issues
- The role of government.

Moreover, there were some intriguing consequences, both intended and unintended, that emerged in the aftermath of Dark Screen.

Mindset

"This (Dark Screen) is an education process as well as an exercise."

CIAS Exercise Director

Perhaps the greatest benefit of an exercise like Dark Screen is the role it plays in raising the collective awareness of both the public and private organizations regarding information infrastructure interdependencies and vulnerabilities, the need for interorganizational information sharing and coordination, and the lack of understanding of the nature and value of cyber security. In a cyber security context, Dark Screen findings relating to mindset included the following:

Low level of awareness. Initially, there was a low level of awareness regarding the interdependencies and vulnerabilities of the information infrastructure and how they affected individual organizations. Several organizations had comprehensive security policies and procedures in place, including firewalls, intrusion detection systems, virtual private networks, and business continuity plans. However, these firms were surprised at the extent of their dependency on the information infrastructure, their vulnerability to threats or disruptions to the infrastructure, and their lack of contingency plans to cover disruptions to the infrastructure.

Lack of understanding. Compounding the low level of awareness was a widespread lack of understanding concerning the evolving nature of cyber security in an era of ubiquitous computing. Most of the firms in the exercise focused on internal security issues, overlooking external entities and issues. This internal focus was exemplified by a manager from a participating organization, "My department doesn't rely on our internal IT department. We have 'virus protectors'…."

This comment also highlights another facet of the lack of understanding regarding cyber security. Most organizations are only familiar with two types of cyber events: an event that strikes the organization alone (e.g. an intrusion into its network) or an event that is more global in nature (e.g. a worm or virus, such as Slammer). In both cases, the organizations only focus on erecting a barrier or perimeter. This view of protection is analogous to barricading a castle while leaving the surrounding countryside unprotected. The barricade may protect the inhabitants from immediate harm, but it does little to ensure long-term security and prosperity. Similarly, it does little good to fortify a single organization if the supporting infrastructure is degraded to the point where critical operations and processes are impeded.

Finally, there was a tendency to think of cyber security as a goal, as opposed to a process. For example, several firms took a 'checklist' approach. Once they had checked off all the items on their security checklist, they sat back, assuming their organization was secure. This approach overlooks the dynamic and constantly evolving nature of ubiquitous computing and cyber security.

[24] The quote is from one of a series of Gartner research reports on infrastructure security (Caldwell, F. "What's Critical in Critical Infrastructure Protection," http://www3.gartner.com/DisplayDocument?doc_cd=114165).

Viewing cyber security as a nuisance and overhead. Cyber security is still, to a certain extent, perceived as a nuisance and an overhead. In practically all instances, the organizations in the exercise suffered from resource constraints, which led to a lack of training and expertise at multiple organizational levels, from end users to IS and network security specialists to mid-level and senior managers.

C3I (Command, Control, Communications, and Intelligence)

> *[We need] "... a more integrated and formal internal approach to dealing with cyber incidents, as well as increased communication with external sectors regarding cyber security issues."*
>
> *Senior Manager, San Antonio City Public Services*

C3I governs the timely and effective deployment of resources to accomplish a given mission. It involves designating the individual or unit responsible for identifying and assigning the activities necessary to achieve objectives (command), and those responsible for managing those activities (control). Command and control are facilitated by timely information sharing (communication) and information management (intelligence, which involves collecting, analyzing, and disseminating the relevant information). In a cyber security context, Dark Screen findings relating to C3I included the following:

Unclear command structures. Within individual organizations, security-related duties and responsibilities were not always clearly defined. In many instances, security was "tacked on" to an individual's other job responsibilities.

When multiple organizations were affected by a cyber incident, it rapidly became apparent that there was no centralized agency, facility, or mechanism for planning, organizing, leading, and controlling interorganizational activities. Furthermore, the roles, missions, and authorities of the various government agencies were unclear. As one individual at the public sector table stated, "No one seems to trust the initial (government agency) report. Their first move is always to verify that information."

Nonexistent control procedures. A number of the participating organizations did not have current policies and procedures for responding to cyber security events that threatened their organization. Few had guidelines or protocols regarding what might constitute a threat, impending cyber security incident, or actual event, nor when to notify other at-risk organizations. Fewer still had formed cyber incident response teams.

No defined communication channels. Information sharing is critical when dealing with cyber security events that can have a devastating effect literally within minutes. There was no effective clearinghouse or communication channel for reporting cyber incidents. Methods to facilitate the timely sharing of information were ill-defined, both prior to a cyber security incident (threat notification) and during one (coordinating activities and responses, communicating with the general public). Similarly, the mechanism implemented by the federal government to communicate cyber-threat information to private sector organizations and state/local government agencies is relatively new, unknown, and unproven.

No intelligence facilities. Dark Screen highlighted the need for a cooperative approach to collecting, analyzing, and disseminating information among local organizations, government agencies at multiple levels, and industries at regional and national levels. This coordination is critical for crafting plans, structures, and mechanisms that can actually prevent or detect a cyber security incident. Coordination is paramount when formulating a coordinated response to an incident.

Disclosure and Trust

> *"I recognize that participating in this exercise may raise concerns about the privacy of individuals, proprietary business information, classified information and existing vulnerabilities, and these issues will be fully examined and addressed."*
>
> *US Congressman Ciro Rodriguez (D-Texas)*

In a cyber security context, Dark Screen findings relating to concerns about disclosure and trust included the following.

Concern about disclosing sensitive information. One concern raised during the exercise relates to the need to balance public access to government information against the obligation to protect that same information from inappropriate disclosure. Both state and federal laws govern this issue. For example, information garnered during Phase II (vulnerability assessment and penetration testing) might conceivably be subject to requests for disclosure under the federal Freedom of Information Act and the Texas Public Information Act. However, disclosure of this information obviously is not in the public's best interest. Thus, federal legislation has been introduced to protect firms against potential antitrust liability and Freedom of Information Act (FOIA) disclosures when they

share information with each other and the government (the Cyber Security Information Act, H.R. 2435 in the House, and the corresponding Bennett-Kyl bill in the Senate).

Lack of interorganizational trust. Closely related to the disclosure issue is trust. Several of the organizations were reluctant to disclose aspects of their internal security to outside entities. However, given that the information infrastructure is beyond the direct control of any one organization, or even a small group of them, leaders in the private sector should devote attention to fostering interorganizational trust and overcoming barriers to information sharing. Of course, steps must be taken to ensure that such disclosures are made only when appropriate and that the information disclosed is appropriately safeguarded. This sharing might include, for example, prescreening or sanitizing sensitive data and information and using relatively secure technologies, such as virtual private networks or encryption.

The Role of Government

Participation in Dark Screen by a number of local, state, and federal government agencies spotlighted government's role in ensuring security of the information infrastructure. Currently, the role of the federal government is in flux. There are several roles government can play.

Provide high-level guidance. Originally, the responsibility for ensuring the security of the information infrastructure fell to the National Infrastructure Protection Center (NIPC). However, in June 2003, NIPC was replaced by the National Cyber Security Division (NCSD), which is part of the Department of Homeland Security. Many NIPC personnel opted not to transfer to NCSD, resulting in a shortage of experienced personnel. In addition, there has been turnover at the top: three different directors of NIPC/NCSD within a two-year period (Richard Clark, Howard Schmidt, and Amit Yoran). This instability has led to a lack of high-level guidance for overall cyber security efforts.

Coordinate public and private efforts. Although the federal government called for voluntary participation from the private sector, initially there was limited response. Industry-based Information Security and Analysis Centers (ISACs) were established to be cooperative ventures run by private firms, with limited government involvement.[25] However, private firms were reluctant to share information to the extent necessary to make the ISACs effective. After this reluctance became apparent, the United States-Computer Emergency Readiness Team (US-CERT) was created in 2003. Formed in conjunction with Carnegie-Mellon's Computer Emergency Response Team (CERT-CC), US-CERT is intended to function as the coordination point to bridge public and private sector institutions and to aggregate and disseminate cyber security information.[26]

Another government-supported effort is the National InfraGard Program. This program is designed to leverage contacts between the government and the private sector to share information about cyber incidents and infrastructure vulnerabilities and threats. InfraGard pulls together the federal government, state and local government agencies, and business and academic institutions at a local level through local InfraGard chapters throughout the country[27].

Develop policies and programs. In addition to US-CERT, the National Cyber Security Partnership (NCSP) was also created in 2003. Comprised of representatives from industry, academia, and government, NCSP's objective is to develop policies and programs to protect the information infrastructure. To date, NCSP has issued reports calling for a National Cyber Security Early Warning Contact Network and a National Crisis Coordination Center, both to be managed and supported by the Department of Homeland Security and US-CERT[28].

Government initiatives to secure cyberspace are discussed in Appendix 2.

Summary of government's role. The role of government in cyber security in its formative stage was hamstrung by uncertainty and tentativeness. In addition, it was predicated on voluntary participation from private industry, which did not materialize. As a result, the initial efforts to form a partnership between the public and private sectors floundered. However, more recent initiatives, such as US-CERT and the National Cyber Security Partnership, coupled with a renewed emphasis on the ISACs and InfraGard, seem to indicate that both sides recognize the necessity of government-industry cooperation to protect the information infrastructure. While these indicators are encouraging, it is still too early to assess their effectiveness.

One final item regarding the role of government in protecting the information infrastructure is worth mentioning. Although this discussion is centered on U.S. government actions, protecting the information infrastructure is not the province of a single nation. This view is noted in The International Critical Information Infrastructure Protection (CIIP) Handbook, published

[25] For more information see http://www.isaccouncil.org/about/.

[26] For more information see http://www.us-cert.gov/index.html.

[27] For more information see http://www.infragard.net/.

[28] For more information see http://www.cyberpartnership.org/about-overview.html.

by the Center for Security Studies (CRN) at the Swiss Federal Institute of Technology (ETH Zurich), Switzerland. The Handbook is an inventory of the information infrastructure protection policies of fourteen countries, and provides the basis for an international dialog on information infrastructure security risks and vulnerabilities.[29]

CONSEQUENCES OF DARK SCREEN

One of the intended consequences of Dark Screen was a heightened awareness among decision makers and IS professionals regarding vulnerabilities and interdependencies of the information infrastructure. An unintended, and positive, consequence was the emergence of an informal group of these individuals. Coming from different organizations, they self-organized into what one member calls a "loose collaborative effort" dedicated to strengthening overall cyber security in the San Antonio area. The group is characterized by the members' mutual concern for the information infrastructure. This group serves as the basis for a 'community of practice' that shares expertise and information regarding new threats or developments that might impact their organizations and the information infrastructure.[30] Calling themselves the Infrastructure Advisory Panel, this community prods local firms and government agencies to communicate more openly and share more information.

At the operational level, the group has disseminated early indications of potential probes or disruptions ("we just noticed xxx on our intrusion detection system – has anyone else seen something like this?"), shared assessments of new products, publicized unanticipated interaction effects between various software packages and patches, and sustained an informal contact database that people can turn to for information, opinions, and advice.

At the management level, the group has facilitated an ongoing dialog, which has resulted in enhanced problem-solving (more people looking at a given problem), expanded benchmarking of security metrics, broadened perspectives on risk assessment, and propagation of security best practices.

On a strategic level, the benefits accruing to organizations with members on the Infrastructure Advisory Panel have included increased visibility and networking opportunities in the regional marketplace, a heightened reputation from being perceived as a good corporate citizen, and a competitive advantage over non-members that comes from having an enhanced security posture.

Collectively, this community of practice has benefited the San Antonio area in several ways. It has contributed to the success of local organizations in obtaining funding and grants for local infrastructure protection initiatives. It led the effort to substantially upgrade the capabilities of the regional Emergency Operations Center to respond to infrastructure disruptions. It has boosted the influence and legitimacy of other, more formal groups (e.g., the local InfraGard and ISSA chapters, and the Technology Committee of the Greater San Antonio Area Chamber of Commerce). Currently, the Infrastructure Advisory Panel is contemplating creating a regional Security Information Network modeled after the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Pilot Program in Dallas, Texas.[31]

RECOMMENDATIONS

After reflecting on these findings, one overarching theme emerges: In today's environment, organizations need to approach cyber security differently. The self-protection model, built on each organization deploying a perimeter defense around its own boundaries, is no longer adequate.

Following are three recommendations on how to view cyber security differently.

View cyber security as a business issue. Senior management must recognize that information security is not a technical issue; it is a business issue. Security practices need to be integrated into the business, via the following three initiatives:

Make cyber security an integral part of corporate governance. Cyber security should be reviewed and understood by all CXO-level executives. The organization's security posture should be reviewed during board meetings. Corporate officers and directors should be educated on the cyber security implications of recent legislation, including the Sarbanes-Oxley

[29] For more information see http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf.

[30] Communities of practice are informal groups bound together by a common interest. They share knowledge, ideas, and experience to foster creative new approaches to problems. See Wenger, E. C., and Snyder, W. M., "Communities of Practice: The Organizational Frontier," *Harvard Business Review*, (78:1), January 2000, pp. 139-145.

[31] In June 2004 the U.S. Department of Homeland Security, in partnership with local private sector organizations and the Federal Bureau of Investigation, launched a pilot program intended to strengthen infrastructure security information exchange between the private sector and local government. The Homeland Security Information Network-Critical Infrastructure (HSIN-CI) will first be implemented in Dallas, Texas, and followed by other locally operated pilot programs in Seattle, Indianapolis, and Atlanta (http://www.dhs.gov/dhspublic/display?content=3748).

Act, the Gramm-Leach-Bliley Act, and the Health Care Insurance Portability and Accounting Act.

Realize that security is a process. Technology is constantly evolving, as is an organization's business environment and objectives. To remain current and effective, security policies and procedures likewise need to change. This need implies that, much like quality improvement, cyber security is a continuous process, not an end product. Managers should therefore adopt a structured process approach that takes into account the dynamic nature of cyber security.[32]

Institute cyber security best practices – that is, controls, objectives and procedures to comprise an effective cyber security program. Such a program provides the foundation for securing the organization's cyber assets and creates the starting point for addressing security issues that transcend organizational boundaries. Compilations of effective security practices are readily available from several sources for little or no charge (see Appendix 1). These practices can be used as the starting point to develop additional practices based on one's own business and technical environments. Ensure that adequate resources are available to implement and maintain these practices.

Broaden your cyber security mindset. Due to the changes in the business environment and social fabric, coupled with constantly evolving technology, cyber threats are no longer narrowly focused on individual companies. Rather, they are spread across regions, industries, and the information infrastructure. The new cyber security mindset needs to entail cooperation, collaboration, and coordination among organizations and between the private and public sectors.

Thus, the most significant action executives can take is to recognize that their organization is critically dependent on a web of suppliers, vendors, and customers, all connected through the information infrastructure. Take this dependence into account by expanding the firm's security focus beyond the organization's boundaries.

Join collaboration efforts. An effective way to broaden one's cyber security mindset is to support outreach programs that facilitate mutual information sharing and foster collaborative efforts to secure the information infrastructure at local, industry, and national levels.

Local actions include supporting regional chapters of organizations such as the Information Systems Security Association (ISSA) and InfraGard, or creating a cyber security advisory panel consisting of regional firms, government agencies, and academic institutions. Such a panel could help guide local policy decisions and facilitate information sharing about cyber events in the community.

From an industry perspective, managers should satisfy themselves that the cyber security of external supply and distribution systems linked to their systems is adequate to protect their own organization. Managers should return the favor by sharing appropriate information so that these external entities can, in turn, be confident that the managers' organization also provides an acceptable level of security.

On a national level, organizations should become involved with the National Cyber Security Partnership (NCSP) and the appropriate industry sector Information Sharing and Analysis Center (ISAC). Links to these organizations are provided in Appendix 2.

Finally, organizations should encourage their elected representatives – local, state, and federal – to provide resources and institute meaningful and effective cyber security policies and programs.[33]

CONCLUSION

The information infrastructure has become indispensable to the smooth functioning of today's world. As technologies in the information infrastructure evolve, a host of new security threats and issues arise. One way to explore these issues is through scenario-based exercises such as Dark Screen. As a result of Dark Screen, the San Antonio community is better prepared to prevent, detect, and respond to cyber security incidents. It is worth noting that the challenges and threats faced by the San Antonio community are not unique. Other organizations and communities face them as well. In this sense, Dark Screen can serve as a model for other communities to assess and improve their cyber security capabilities.

Dark Screen also brought to light the need for a new way of thinking – a new approach – to cyber security: communities need new modes of cooperation and collaboration that transcend traditional organizational boundaries. Enlightened self-interest dictates that organizations should work together, and with government agencies, to protect the information infrastructure. The realization that cyber security is an open-ended and constantly evolving process, necessitating interorganizational cooperation, is the true legacy of Dark Screen.

[32] An example of one such approach is presented in: Rees, J., Bandyopadhyay, S., and Spafford, E. H. "PFIRES: A Policy Framework for Information Security," *Communications of the ACM*, (46:7), July 2003, pp. 101-106. .

[33] *CSO Magazine*, a sister publication to *CIO Magazine*, has launched a series of articles that provide an in-depth look at U.S. government cyber security activities, plans, and related issues. The series began in the March 2004 issue, and is available online at http://www.csoonline.com/read/030104/dhs.html.

ABOUT THE AUTHORS

Tim Goles

Tim Goles (tim.goles@utsa.edu) is an assistant professor of information systems at the University of Texas at San Antonio. He earned his Ph.D. in MIS from the University of Houston. He has over fifteen years of management experience in the information technology arena, including responsibility for internal controls and business resumption planning; the evaluation, development, and implementation of strategic and operational information systems; and outsourcing contract management. His work has appeared in several IS and management journals and been presented at a number of international conferences. His current research interests include managing interorganizational relationships, IS outsourcing, and information systems security.

Gregory B White

Gregory White (greg.white@utsa.edu) currently serves as the interim director and technical director for the Center for Infrastructure Assurance and Security and is an associate professor of computer science at the University of Texas at San Antonio (UTSA). He has been involved in computer and network security since 1986. He spent 19 years with the Air Force and is currently in the Air Force reserves. He obtained his Ph.D. in computer science from Texas A&M University in 1995. His current research initiatives include an examination of organizational issues affecting computer security, high-speed intrusion detection, infrastructure protection, and methods to determine a return on investment from security.

Glenn Dietrich

Glenn Dietrich (glenn.dietrich@utsa.edu), CISSP, is chair of the Department of Information Systems at the University of Texas at San Antonio and was the founding director of the Center for Infrastructure Assurance and Security at UTSA. He received his Ph.D. in information systems from the University of Texas at Austin. His research interests include information assurance, technology transfer and business strategy. Prior to his academic career, Dr. Dietrich worked as a consultant in information systems, working primarily with the U.S. Department of Defense building and securing large databases.

Appendix 1: Cyber Security Resources and Best Practices Starter Lists

Disclaimer: Information and links provided here are for informational purposes only. This list is intended to be an example of resources available for further information on the subject of cyber security, not a comprehensive listing of all organizations or sources providing cyber security information or products. Nor does this list imply any recommendation or endorsement of these resources.

"Best Practices"

ISO 17799

http://www.iso.ch/iso/en/prods-services/popstds/informationsecurity.html

NIST Special Publications 800 Series

(especially 800 – 14)

http://csrc.nist.gov/publications/nistpubs/

Defense Information Systems Agency

http://iase.disa.mil/eta/ (select Product Description Page pdf link)

National Security Agency

http://www.nsa.gov/isso/index.html

Other Resources

Carnegie Mellon CERT/CC

http://www.cert.org/

CERIAS

Center for Education and Research in Information Assurance and Security

http://www.cerias.purdue.edu/

Chief Security Officer (CSO)

http://www.csoonline.com/

National Institute of Standards and Technology page of links to security resource sites

http://csrc.nist.gov/csrc/professional.html

National Cyber Security Partnership

http://www.cyberpartnership.org/

InfraGard

www.infragard.net

Managers will also find the following two articles useful in gaining an understanding of issues related to cyber security in today's interconnected world:

Austin, R. D. and Darby, C. A. R. "The Myth of Secure Computing," *Harvard Business Review*, (81:6), June 2003, 120-126.

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

Appendix 2: Government Cyber Security Organizations

In recognition of the fact that over 80% of critical infrastructures are controlled by the private sector, the U.S. government's approach to safeguarding them has been to provide a variety of means for private firms and individuals to voluntarily and proactively undertake protective measures.

Information Sharing and Analysis Centers (ISACs)
http://www.isaccouncil.org/about/

ISACs are designed to enable firms to share security-related data within certain industry sectors. Each sector's ISAC gathers, analyzes and disseminates information to its members for an industry-level integrated view of vulnerabilities, threats, and incidents. ISACs also promote the sharing of security best practices and solutions to common problems among members.

ISACs provide valuable information but their data collection methodologies vary from sector to sector, leading to an uneven analysis of security risks and solutions. Funding also varies from sector to sector. Some ISACs are funded with federal money, some with private funds, and others with a combination of federal and private funds. Consequently, the effectiveness of the individual ISACs varies by industry. By most accounts, the Financial Services ISAC is the most effective, followed by the Telecommunications and Information Technology ISACs.

InfraGard
http://www.infragard.net/

InfraGard's mission is to improve and extend infrastructure security-related information sharing between individuals and private firms, and the government. The idea began in the Cleveland field office of the Federal Bureau of Investigation (FBI) as a local effort to enlist support from information technology practitioners and academicians for the FBI's investigative efforts into cyber crime. The program has since expanded in scope, both geographically (it is now a national program) and organizationally (in addition to the FBI, InfraGard partners now include the National Institute of Standards and Technology [NIST], the National Center for Manufacturing Sciences [NCMS], and the Small Business Administration). However, InfraGard still retains a heavy local orientation and strong ties to the FBI. This results in its effectiveness varying from location to location.

United States Computer Emergency Readiness Team (US-CERT)
http://www.us-cert.gov/

US-CERT is a partnership between the Department of Homeland Security and the public and private sectors. Its mission is to protect the nation's Internet infrastructure and by improving readiness and response capabilities. It does so by analyzing cyber threats and vulnerabilities, disseminating information, and coordinating incident response activities. It also provides a forum for individuals, private firms, and other government agencies to communicate directly with the U.S. government on cyber security matters. Affiliated with the CERT® Coordination Center at Carnegie Mellon University, US-CERT is a valuable resource for the latest technical information regarding cyber threats. In addition, it provides links to other sources of cyber security information and resources.

National Cyber Security Partnership (NCSP)
http://www.cyberpartnership.org/about-overview.html

The NCSP is a public-private partnership established to develop strategies and programs to enhance security over the information infrastructure. Primary members include the Information Technology Association of America (ITAA), the Business Software Alliance (BSA), TechNet and the U.S. Chamber of Commerce, along with CEOs, federal government agencies, industry experts, and academicians.

The NCSP has established five task forces. The task forces will issue high level strategies and recommendations for addressing key challenges of cyber security: 1) Awareness for Home Users and Small Businesses; 2) Cyber Security Early Warning Systems; 3) Corporate Governance; 4) Technical Standards and Common Criteria; and 5) Security Across the Software Development Life Cycle.

