Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

.edu, Partner or Pariah:

A New Paradigm for University/Community Partnerships in Cyber Security

Gregory White, Ph.D. and Timothy Goles, Ph.D., The University of Texas at San Antonio

Abstract – All too often colleges and universities are viewed in the security community as weak links that are easily exploited by those intent on causing harm or disruption to networks connected to the Internet. As such, they are often viewed as Internet pariahs, outcasts on the Internet not conforming to the accepted rules of behavior in terms of securing their infrastructures. This does not have to be the case, however, and colleges and universities can actually become community leaders in security. This paper discusses how an academic institution can take a prominent role in the community through leadership in a community cyber security exercise. The paper describes the Dark Screen exercise conducted in San Antonio, Texas and the university's role in conducting this and other exercises.

Index terms – Security, partnerships, exercises

I. Introduction

For many years, colleges and universities have been considered a weak link in the security chain. They have been viewed as an open environment and many feel they are not concerned about security and are full of networks just waiting to be exploited. Attackers have often used colleges and universities as platforms from which to launch attacks on other organizations connected to the Internet. Frequently academic institutions have used their desire to foster open communication as the reason that they do not enforce more stringent security requirements on their users. As a result, the security community generally views these institutions as pariahs and breeding grounds for anti-social Internet activity.

This does not have to be the case. In many academic arenas universities are viewed as pillars in the community, fostering intellectual curiosity and innovation, and frequently spinning off new business ventures. The same can be true for security. There are many ways an academic institution can take a leadership role in helping to secure cyber infrastructures in the community. One of the most visible is in conducting training and awareness activities to help make the community more aware of the threats and the possible methods to address potential cyber attacks on the community and its infrastructures. Training and education has always been in the purview of academia and is an obvious avenue to take in developing a leadership role in security. There are many different formats that education and awareness activities can take. One with the potential for a particularly tremendous impact is to lead the community in conducting a cyber security exercise.

Gregory White serves as the Interim Director and Technical Director for the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA) where he is also an Associate Professor of Information Systems. Timothy Goles is an Assistant Professor of Information Systems at UTSA.

II. Exercises as Educational Tools

At the heart of the issue is the question of how can organizations, both individually and collectively, better prepare to prevent, detect, and respond to incidents that threaten the community? Exercises have been used by a variety of different organizations for many years as awareness tools valuable in educating participants on new techniques, procedures, tactics and tools. Exercises are also frequently used to conduct drills to determine the level of preparedness for participants in the specific domain of interest. The military, for example, uses exercises for training its personnel and to evaluate the effectiveness of its technology (weapons), tactics, and procedures in responding to simulated attacks by an adversary. Force-on-force exercises are frequently used to provide soldiers with an environment as close to actual combat as possible. Fire departments conduct exercises to provide opportunities for their personnel to respond to and deal with various types of fires that they may not on a regular basis have the opportunity to address. Cyber security exercises can be conducted for similar purposes. They can be used to increase understanding of vulnerabilities, identify opportunities for improvement, help develop and refine operating procedures and technology, and to develop lines of communication between organizations that will need to respond in the event a cyber incident occurs. As part of an exercise,

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

penetration tests, designed to see whether attackers can gain unauthorized access to computer systems and networks, can be performed to evaluate the level of effectiveness for an organization in terms of detecting and responding to an attack. Penetration tests and exercises can also be used to provide personnel with an opportunity to respond to attacks which are possible but which they may not have had to deal with before.

In addition to technical and procedural issues relating to the ability of organizations to prevent, detect, and respond to cyber incidents, exercises can also address broader issues with economic, legal, and political ramifications. These issues are often poorly understood because of the interconnected and interrelated nature of today's information infrastructures. Exercises are an effective way to highlight the interdependencies between the various critical infrastructures and sectors. Simulating the loss of an infrastructure before it actually occurs allows other sectors to evaluate their level of dependence on the sector whose loss has been simulated and to determine their level of preparedness in terms of alternatives for the infrastructure that was lost. Exercises can also increase awareness of the importance of information systems security across the many sectors found in a community. In a manner similar to the way sectors were made aware of their dependence on other sectors, the simulated loss of information systems can provide an organization with an understanding of how much they rely on computer systems and networks and how prepared they are to operate should these systems be lost.

A number of cyber security exercises have been conducted at a variety of different levels. The majority of the exercises have focused on the technical side of computer security. Events such as the Air Force's Black Demon Exercise have pitted a defending force against attackers who attempt to gain unauthorized access to computer systems and networks or to disrupt their operations. In the Black Demon exercises, the second of which was conducted recently in March 2004, the Air Force tested and evaluated the effectiveness of their operational procedures against concerted network attacks, reconnaissance, denial of service, the loss of network-defense tools, insider threats, malicious logic and the loss of a network's firewall.[1] Over 200 individuals participated in the two-week exercise which was designed to train participants in network security operations. A range network was used to simulate actual Air Force operational networks in order to allow participants to experience attacks that would have been disruptive to operational networks had they been conducted against them.

The type of technical exercise that Black Demon represents is useful for organizations such as the Air Force, which has a highly developed set of procedures supported by technology and professionals who have been trained to handle attacks as they occur. For organizations without a similar highly developed set of security technology and procedures, such as what can be found in most industry organizations as well as local governments and infrastructures, this type of exercise would be less useful. In the vast majority of communities a Black Demon type of exercise would help very little in preparing the various community organizations to prevent, detect and respond to attacks as the communities do not have the refined environment present in the Air Force. Instead, what communities need are more exercises aimed at awareness and training instead of exercises designed to drill organizations and evaluate the effectiveness of established procedures, technology and personnel. An example of a community oriented scenario-based exercise is Dark Screen.

III. Community Information Assurance Exercises

Dark Screen was a three-phased community information assurance exercise conducted between March 2002 and September 2003 in San Antonio, Texas.[2] The first phase of the exercise consisted of a tabletop scenario designed as an awareness tool to help participants better understand the threats that cyber attacks could pose to a community. Over 200 individuals came together to participate in the five-hour event that brought together representatives from the military, local government, representatives from state and federal agencies, local critical infrastructures, industry, and academia.

The exercise consisted of a series of events revealed sequentially according to a master schedule maintained by the discussion facilitator for each table. The events were broken into three segments: pre-attack indications of a possible future cyber attack, the events that constituted the attack itself, and events that might occur in the aftermath of the attack. Participants were divided into groups, based on the organization that they belonged to. Similar organizations were grouped at the same table so that there was, for example, one table for individuals from the various city utilities, another table for representatives from state agencies, a separate table for representatives from federal agencies, and so forth. Recorders at each table took careful notes so that responses from the different organizations could later be compared to see if discrepancies existed between the responses provided by the various organizations. If, for example, one organization stated that it would rely on obtaining information from another organization the recorder for their table would make a note which could be compared with the other table's notes later. If the participants at the second table stated that based on the given situation they would not share the information they had with anybody, a similar note was made by that table's recorder. Later the

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

notes from these two tables could be compared and the discrepancy noted and passed on to both organizations so they could discuss the differences and potentially modify their individual procedures accordingly.

At the end of the first phase, participants had a better understanding for where their organization could improve its security plans, procedures, and capabilities. Participants also gained knowledge regarding the interrelated and interdependent nature of the community's cyber infrastructure and information systems. In addition, the managers and IS professionals present were able to improve and expand their interorganizational contact network so that they had current contact information for individuals and organizations to call in the event of a cyber security incident. Finally, the entire community gained a heightened sense of awareness concerning its dependence on the information infrastructure and the importance of information systems security.

The second phase of the exercise commenced immediately following the first, as participants returned to their organizations and began to improve their security posture based on the lessons learned in the tabletop exercise. During the second phase, organizations also had the opportunity to take a technical look at their security perimeter as vulnerability assessments and penetration tests were conducted by several of them. This helped these organizations prepare for Dark Screen's third phase, another scenario-based exercise. During the third phase, however, the exercise was not simply a tabletop exercise but rather consisted of both live and simulated network events. The exercise was conducted over a two-week period but simulated an attack that actually would have taken place over just a few days. The exercise was spread out to ensure that control was maintained as many different organizations were involved with a limited number of exercise coordinators to maintain control of the significant number of disparate simulated events.

The largest number of participants in Dark Screen were from the City of San Antonio, Bexar County, and the Air Force's Air Intelligence Agency. These are the most prominent organizations in the area and would most likely bear the brunt of any cyber attack on the community. The exercise was conducted, however, by individuals from the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA). From the beginning, CIAS personnel played a prominent role in the development and organization of the exercise. Early during the planning of the exercise a scenario development committee was formed with representatives from the various key organizations in the community. The initial goal was to develop a high-level outline for the exercise events. This outline basically provided the "story" behind the exercise events which explains why the community is being attacked and what the goals of the attackers are. Building upon this outline, CIAS personnel developed the scripts used in both the tabletop and live exercises. CIAS personnel also conducted penetration tests on two of the cities infrastructures during the second phase of the exercise. In this way, the university and its security research center assumed a leadership role while working closely with the city and county's emergency management personnel.

The benefit in conducting a community information assurance exercise is not unique to San Antonio and its surrounding region. The type of threats and the possible attacks simulated in the Dark Screen exercise exist for all communities in the nation. As part of the exercise, the CIAS collected information in order to develop a template that might be used to guide exercises in other communities. The first attempt to apply the lessons learned in Dark Screen to another community occurred in February 2004 when the CIAS conducted a tabletop scenario in Corpus Christi, Texas. Though a bit smaller in scope, the exercise included many of the same elements. Lessons learned in this exercise are now being applied to modify the template so that it is more broadly applicable. The goal is to conduct additional exercises in other communities in order to gain further information that could make the template valuable to as many communities as possible. A key factor in Corpus Christi was to include other academic institutions so that they could assume a leadership role in the later phases. Individuals from Delmar Community College and Texas A&M University-Corpus Christi attended and participated in the exercise. The CIAS will work with these institutions to help steer them during the second and third phases of the exercise.

IV. Sector Exercises

While Dark Screen was designed as a community-based exercise, many of the lessons learned can be applied to other environments as well. In particular, the various critical infrastructures and the sectors they represent are all heavily dependent on information systems in their daily operations. Cyber security exercises can be used as a valuable awareness and training tool for the various sectors just as they were for the San Antonio community. After the success of the initial phase of the Dark Screen exercise, the CIAS was asked to put together an exercise for the financial services sector. A tabletop exercise, focusing on the issues for this sector, was conducted in March 2003 in New York. The exercise highlighted the different types of attacks that might be experienced as a result of unstructured, structured, and highly structured threats. Most industry countermeasures are designed to address the unstructured threats, so the discussions on the structured attacks were extremely valuable to the participants. Again, the goal was for participants to leave

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

the exercise with an idea about what they would need to do to enhance their own organizations' security posture. The success of this exercise led to additional sector-based exercises, all similar in format, in Chicago, San Francisco, and Houston. These exercises were each designed to address the specific sector's security concerns and allowed for a more in-depth examination of possible sector vulnerabilities.

While it may at first seem that there is little connection between the sector- and community-based exercises, this is not the case. Communities all include elements of the various sectors. There are, for example, financial services organizations in all major cities in the nation. While the community-based organizations include an examination of the communication channels necessary in the community to respond to a cyber attack, they do not provide an opportunity to examine communication that would occur within a specific sector. The sector-based exercises provide an opportunity for an examination of intra-sector communication. Additionally, community exercises are focused on attacks on the community and the interdependencies between the different infrastructures, and do not go in depth on any one sector. The sector-based exercises can explore focused attacks on individual sectors and can examine more closely the affect that a loss of one sector might have on another. The exploration of the interdependencies between sectors is critical for their defense.

All of the sector-based exercises were conducted by the CIAS for the U.S. Secret Service in conjunction with the Guidry Group, a Houston-based security organization. Representatives from other academic institutions have been present at all of these exercises. Again, this is an area where academia can take a leadership role in the community and for the nation. Other institutions have already conducted other cyber exercises such as the Livewire exercise developed and conducted by Dartmouth's Institute for Security Technology Studies (ISTS) in October 2003.[3]

The Livewire exercise involved both community and sector representatives and was a cross between the sector-based and community-based exercises. Its main emphasis was on testing the responses of the telecommunications, banking and financial services, and energy sectors to a potential physical and computer terrorist attack. As was discovered during the Dark Screen and the individual sector-based exercises, Livewire showed the need for better communication between the various sectors and between the sectors and the federal government before and during a cyber attack. Livewire also featured another aspect also found in the community and sector-based exercises previously performed, the combination of physical and cyber attacks. Including both physical and cyber attacks in an exercise is important no matter what the major emphasis is for the exercise. If the exercise is designed to concentrate on cyber response aspects, physical attacks can be used to enhance the cyber attacks by destroying key components of a network or the telecommunications mechanisms the network relies on. If the major thrust of the exercise is a physical attack, a cyber attack can be added to create further confusion to the initial attack and to disrupt the responding organizations' ability to effectively communicate. The leadership displayed by the ISTS at Dartmouth during this national-level exercise provides another example of how an academic institution and its components can play a key role in cyber security training and awareness.

V. Other Community Programs

Providing a leadership role in conducting cyber security exercises is one way that academic institutions can become a valuable security partner for communities, but it certainly is not the only one. There are a number of professional organizations such as the Information Systems Security Association (ISSA), American Society of Industrial Security (ASIS) and the FBI sponsored InfraGard that have local chapters in many cities in the nation. Each of these organizations needs a place for their local chapters to hold their meetings, and all have local boards that frequently need members and advisors. Academic institutions can provide assistance and leadership to these organizations by having faculty members attend and volunteer for board positions and participate as members. Academic institutions can also provide places for these organizations to meet, speakers for their meetings, and can encourage students to participate and join. The networking aspect of the meetings can prove a valuable experience for students who often will be faced with the prospect of searching for appropriate jobs in the community upon graduation.

Organizations such as ISSA have as part of their goals the continuing education of their members. This is an area that academic institutions can again directly participate in as a valuable partner. Luncheons, workshops, and seminars can be organized by faculty and organization members to address current security needs of the community. Often these organizations can also provide adjunct instructors for security courses that the university may wish to offer but may not have the faculty to support. Thus, relationships of this sort can be valuable for both entities.

During the second phase of the community information assurance exercise format, a series of penetration tests are conducted on various local government and infrastructure organizations. Most governments do not have the funds to contract with security consultants to provide in-depth tests of their cyber infrastructure. This is another area in

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

which academic institutions can assist their communities – by providing the technical expertise to perform penetration tests of critical local assets in order to determine what additional countermeasures might be appropriate. This can be done as part of an exercise, or as a class project. For example, a graduate information systems security class at UTSA has conducted vulnerability assessments for several local organizations including small local companies, non-profit organizations, and local government entities. The experience is valuable for both the organization receiving the assessment and the students who have the opportunity to evaluate real-world networks and observe the challenges organizations experience on a daily basis. This course has been taught for three years at UTSA without a complaint from any of the assessed organizations. In fact, several organizations have requested a repeat assessment the next time the course is offered.

Another way that academic institutions can partner with the local community is illustrated by the creation and support of the Information Technology and Security Academy (ITSA) in San Antonio, Texas. ITSA is a program aimed at juniors and seniors in high school. For half of their school day, participating students attend courses on information technology or security taught by local community college faculty. By the time the students graduate, they can have earned up to thirty hours of college credit. This results in several benefits for the community. First, it encourages students to consider continuing their education after graduation from high school by attending either a community college or four-year institution. If the student elects to do so, they already essentially have one year of coursework completed. A second potential benefit of this program applies to those individuals who may elect not to continue their education. Instead of entering the workforce with only a high school education and few marketable skills, individuals participating in the ITSA program will have gained valuable high-tech skills that may qualify them for better jobs. As such, the ITSA is serving as a workforce development program as well as a program to encourage students to attend college. When specific high schools are targeted, this can result in encouragement of individuals from families who have never had a college student. Finally, this program raises the overall community awareness of and appreciation for information systems security not only from the standpoint of its importance to the protection of the community but its impact on the local economy and workforce as well.

Programs such as the ITSA play a valuable role in reaching out to the community. Other community outreach initiatives fostered by universities could include in-service lessons targeted for teachers in the local school district who may use computers as part of their coursework. Frequently these individuals do not have a real understanding of current security threats. Lessons designed to help them better protect their own school's networks would almost certainly be greatly appreciated. Providing short lessons for these same individuals that they could present to their own students covering methods to protect their own home computers would also be likely met with much appreciation. While discussions of this nature are valuable to students in high school, teachers and students in lower grades could also be provided with lessons and instruction on issues such as personal privacy, Internet safety, and protection of intellectual property (e.g. music and movies). For example, UTSA developed a security awareness program for teachers in grades K – 12 that covers such topics as online safety and etiquette, cyber security and ethics, and tools that can be used for cyber security awareness.

VI. Benefits to Academia

There are a number of beneficial reasons for universities to become more active in community cyber security issues, not the least of which is to help shed the pariah image that so long has plagued them. An obvious benefit is the fact that the academic institution itself, as well as the employees of the institution, are all members of the community being protected. Whatever affects the community and its infrastructures will affect the university, its employees, and their families.

Students frequently express concerns as to whether what they are being taught is really applicable to the "real world". Lending their expertise to the community in conducting exercises or performing penetration tests provides real-world exposure for security instructors. This not only provides experience that can directly benefit classroom lecture, it also provides a glimpse into possible areas requiring research and may lead to security research initiatives at the academic institution. In addition, as previously mentioned, students may benefit from hands-on involvement through class projects, This synergy between experience, teaching, and research is a valuable reason for institutions to become involved in the community. As the trusted relationship between the academic institution and community organizations increases, this sort of opportunity can provide additional benefits for the academic program, supplying not only the instructor with real-world experience but the students with similar lessons as well.

VII. Conclusion

Colleges and universities have in the past been frequently associated with poor security and have been viewed as a breeding ground for computer attackers. As such, they have often been viewed as security pariahs–organizations not concerned with security and organizations that cause

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

others connected to the Internet a great deal of trouble. This does not, however, have to be the case. Academic institutions can take a positive leadership role in the community and nationally by conducting any of a variety of security related training and awareness programs. The most intensive of these programs involves developing and conducting a security exercise for the local community, one or more of the various sectors, a state, or the nation. Exercises are an extremely valuable training tool but there are many other less intensive programs, such as security awareness training for local industry or school districts, that could be conducted which would ensure the university's role as a security partner and allow it to shed the security pariah image.

VIII. References

[1] Masao Doi, "Air Force conducts network-defense exercise", April 1, 2004, AFPN, available from http://www.iwar.org.uk/news-archive/2004/04-01.htm

[2] Final Report, "Dark Screen: A Cyber Security Exercise for San Antonio/Bexar County", September 26, 2003, available from http://www.utsa.edu/cias/Papers/DarkScreenFinalReport.pdf.

[3] Tim Spellman, "Expert: U.S. at risk of cyberterrorism", The Dartmouth Online, April 19, 2004, available at http://www.thedartmouth.com/article.php?aid=2004041901010

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE