A Grassroots Cyber Security Program to Protect the Nation

Gregory B. White, Ph.D.
Center for Infrastructure Assurance and Security
The University of Texas at San Antonio
greg.white@utsa.edu

Abstract

As governments increasingly move to automating various government functions and as the movement to implement e-government increases, an important element that must be considered is security. Numerous communities have learned what can go wrong if security is not addressed as numerous cyber incidents have been experienced. While dependence on cyber infrastructures increase, nations have increased their efforts to prepare for a national cyber incident. Unfortunately for communities, nations are overlooking the need for local governments to be prepared for incidents. This is not only true for incidents that might impact or target only a single community, but it also includes national incidents that will have an impact on every community. Even if an incident is being addressed by organizations at the national level, cities still need to function and if they are not prepared to respond to a cyber incident they may find that they are not able to properly meet the needs of their citizens while relying on the government at the national level to address the incident. This paper addresses a model that has been developed to help communities develop a viable and sustainable cyber security program. By doing so, this paper describes a model which can help secure a nation by working from the “bottom up” in a grass-roots initiative.

1. Introduction

Many lessons were learned from responding to the attacks of September 11, 2001. This was an event that affected the nation and ultimately had a global impact. While the U.S. federal government was attempting to deal with the impact of the attacks, one lesson that was being learned was that while the event was an attack on the nation, it was the local first responders that had to deal with the immediate effects of the attack. Since that time the nation has spent a considerable amount of money improving the ability of local and state governments and their first responders to deal with an attack of this nature. The lessons that have been learned by the first responder community are equally applicable to the cyber security community. A critical lesson to learn is that while there are numerous cyber events that might have a national level impact, they will also have an impact on state and local entities and local government leaders and cyber first responders need to be prepared to address cyber events that may occur which will have a negative impact on the community.

This is a critical lesson. At the same time that governments are learning this lesson, another movement is occurring that will be directly affected by the ability of governments to secure their systems. Governments across the world at both local and national levels are increasingly introducing various aspects of e-government. As they do so, they must consider how a cyber attack or event could impact the operation of the various government entities and how their citizens might be impacted. This paper examines several cyber incidents that have occurred at the local and state levels that illustrate how communities are increasingly becoming reliant upon the various cyber infrastructures and how a cyber event can have a negative impact on the community. This leads to the obvious conclusion that something must be done and the paper will introduce a model to help communities develop viable and sustainable cyber security programs. The implementation of this model will be discussed and results based on feedback from state and local officials will be presented. The paper will conclude with an examination of the future of the model.

2. Threats to Communities

There are many benefits and reasons for introducing electronic-government at the local level. Governments see increased access, convenience, customer support, lower costs, and more access to information as reasons to increasingly rely on computer systems and networks to provide services to their citizens. [1] While all of these are benefits, the increased reliance on networks, and in particular the Internet, introduces a potential weakness as any of a
variety of cyber security events can impact the delivery of the services. There are numerous examples of government entities at various levels experiencing a problem.

In February, 2009 a virus infected almost 500 of the city of Houston’s computer systems. [2] The infection caused the city to shut down part of its municipal courts system including suspending arrests for minor offenses. In addition, the Houston Emergency Center was forced to disconnect from the city network for several hours and forced 3000 people to have their court appearances rescheduled. [3] The impact of this temporary interruption of services was felt by citizens, as expressed by one individual who simply wanted to pay a fine for a traffic violation:

Christian Navarrette, an art teacher, left his job early to get down to the courthouse to pay a speeding ticket. He said he was turned away when he tried to pay the ticket, which is due by Monday. “They told me if I pay it now, it may not post by Monday because of the computer problem,” he said. “They told [me] that I could face more fines if I pay it today, or I can just come back to pay it Monday. I guess I’ll have to leave work early Monday, too.” [3]

While it could be argued that the impact of this incident was minimal – only affecting 3000 citizens already in the system plus allowing a small number of individuals who had committed minor infractions to avoid arrest – other incidents had considerably greater impacts. In April, 2009, a fiber optic cable was deliberately cut in several locations in Silicon Valley. This resulted in, among other things, loss of 911 access for thousands of customers. [4] In addition, tens of thousands of citizens found they had lost Internet access as well as landline and wireless phone service. [5] The loss of 911 service is obviously much more critical to a community. An example of another potentially significant security issue that would be of tremendous importance to governments at all levels is the security of electronic voting systems. There has been quite a few studies on this subject, including one event in 2010 in which the Washington D.C. election board invited groups or individuals to attempt to break into the city’s voting system. One group was soon successful in gaining sufficient control to be able to both view and change votes. [6] While this was a public test, it is easy to imagine the potential implications had this flaw not been exposed at that time.

Other incidents illustrate additional events that threaten governments at various levels. In May, 2011, MSNBC posted a story regarding a security researcher penetrating the computer inside a police cruiser. The level of access obtained allowed the researcher to compromise telnet and ftp services as well as to view the current feed from the car’s camera and its stored videos. [7] In another well publicized incident, the state of Virginia was the target of an extortion attempt by an attacker who claimed to have broken into a patient database and encrypted millions of records maintained by the Virginia health agency. [8] The attacker, who claimed to have encrypted the data and then deleted the original file, demanded a $10 million ransom for the password that would decrypt the file. The ransom note provided undoubtedly left officials in a quandary. Specifically, the note stated:

In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh 😐

For $10 million, I will gladly send along the password. You have 7 days to decide. If by the end of 7 days, you decide not to pony up, I’ll go ahead and put this baby out on the market and accept the highest bid. Now I don’t know what all this [expletive] is worth or who would pay for it, but I’m bettin’ someone will. [expletive], if I can’t move the prescription data at the very least I can find a buyer for the personal data (name, age, address, social security #, driver’s license #).

Now I hear tell the [expletive] Bunch of Idiots ain’t fond of payin out, but I suggest that policy be turned right the [expletive] around. When you boys get your act together, drop me a line at hackingforprofit@yahoo.com and we can discuss the details such as account number, etc.

Until then, have a wonderful day, I know I will 😎” [9]

Since every state and community will likely have multiple files or databases with sensitive information about its citizens, this incident illustrates the potential harm that might occur should sufficient security not be provided. It also shows that there are individuals that are willing to target states and communities and to attempt to extort money from them.

The types of issues seen in these examples from U.S. states and communities are not confined to the
United States. In July, 2010, the website of the Mumbai Cyber Crime Cell was hacked, embarrassing the cyber crime department of the city’s law enforcement agency. [10] The group claiming responsibility for the hack also claimed to have “tampered with the information about most wanted criminals, which included some suspected terrorists.” [10] In another incident in Queensland Australia, a disgruntled individual attacked the computer control systems that managed the city’s wastewater. He was able on numerous occasions to divert the flow so that as much as 1 million liters of raw sewage was dumped onto the grounds of parks, waterways, and a local tourist resort. [11] All of these examples serve to show how the various cyber systems, networks used in the daily operations of the various critical infrastructures in a community, can be attacked and cause mild to severe disruptions in the community. In order to address this, communities need to establish their own cyber security programs and cyber incident handling processes and procedures. Unfortunately, very few communities have such programs and in fact few even have an idea of where to begin.

3. Initial Efforts to Establish Programs

After the physical attacks that occurred September 11, 2001, many state and local governments placed an increased emphasis on preparing to deal with terrorist attacks using any of the traditional weapons of mass destruction. This included attacks using chemical, nuclear/radiological, biological, or explosives. No real effort was placed on cyber security at the local level. At the national level, discussions were widely held (and had in fact been held for a number of years) regarding the possibility of a cyber terrorist attack. Efforts were under way at various federal agencies to determine ways to secure the national cyber infrastructures. These efforts were focused on cyber events that would impact the entire nation (or a major portion of it) and involved discussions on how the various federal agencies would interact with industry to address the incident and work towards a resolution. Industry was recognized as a key component of a national response because the majority of the Internet was under the control of industry and not the government. State governments were only minimally considered – basically through the establishment of the Multi-State Information Sharing and Analysis Center (MS-ISAC). No efforts were undertaken to help prepare local governments to address a cyber incident. The problem with this was twofold. First, as has been discussed, should a national cyber event occur, just like the events of 9/11, it is a national incident but state and local officials will be impacted and will need to be able to handle their own response to it. Second, a national strategy that didn’t include a state and local piece completely ignored the possibility of an incident that would have only a local impact (such as was discussed in the section on community cyber incidents).

The Center for Infrastructure Assurance and Security (CIAS) decided to address this gap in the plan to secure the nation’s cyber infrastructures by creating a grass-roots level program that would help to secure computer systems and networks at the local and state level, coordinating with federal agencies when appropriate. The first step in this effort was the creation of a community cyber security exercise for the city of San Antonio. Called Dark Screen, this exercise was conducted in September, 2002 and involved over 200 participants in a tabletop format. The event was a success in terms of making various leaders in the community more aware of the potential for disruption that a cyber incident could cause. The participants included not just local city and county government leadership, but members from the local utilities, federal agency representatives, and industry. All were more aware as a result of the exercise of the need to share information and to work together in the event of a cyber incident. As a result of the success of this event, the CIAS obtained funding to conduct similar events in other cities around the country. This occurred from 2003 through 2005.

At each community that the CIAS delivered an exercise in, the event seemed very successful in making the leadership more aware of the potential problems a cyber incident would cause. After moving on to the next city, no further work was conducted with the city where the exercise had just been completed and the after action report delivered. After two years, the CIAS began to take a look at the communities in which exercises had been conducted. What was discovered was that while the individuals in the community were aware that cyber incidents could be an issue, the communities had not taken any real step toward establishing a cyber security program. The cities were aware of the issues posed by cyber incidents, but they didn’t know what to do in order to secure their own critical cyber infrastructures. This was not what had been expected and the CIAS determined that a new approach had to be taken.

4. Development of the CCSMM

The problem in the communities was, as stated, that the leaders still were aware that a cyber incident could have a negative impact on the community, but they didn’t know what to do in order to prepare for one or to
address one should it occur. The first attempt to address this was to develop a course that would be provided to the community before the exercise. After the exercise, it was decided to provide some hands-on assistance to communities so that issues raised during the exercise could be addressed. These two additional events proved to be a tremendous step forward in helping communities as it helped them better understand what was needed. These two additions, however, were not enough as communities really needed a roadmap that they could follow to be able to build a viable and sustainable cyber security program. As a result, CIAS researchers came together and created the Community Cyber Security Maturity Model (CCSMM) to address this need. The model, as shown in Figure 1, was designed to accomplish three things:

1. Serve as a yardstick so that communities can determine where in the model they currently are (i.e. how mature their security program is)
2. Serve as a roadmap so that a community knows what it needs to do in order to advance to the next level of the model.
3. Provide a common point of reference so that different communities can discuss their respective programs and plans from a common perspective.

The model as shown describes the characteristics of communities at five levels of maturity. The first level basically describes a community that has not established cyber security program. Unfortunately, in the experience of the CIAS, this has been the level that all communities have been at. The next level, “advanced”, describes a program that has advanced in its program and has established the basics for a continued program. While the characteristics described at this level do not seem extremely difficult to attain, a community displaying all of these characteristics has actually taken a very large step toward establishing a cyber security program. The subsequent levels each build upon the basic characteristics as depicted here until at level 5, a community not only has a mature program but it is also serving as an example and helping other communities attempting to establish their own programs. After several years of working with communities, it has been shown that it is possible for communities to establish programs based upon the model, but it will take years for a community to attain level 5. There is some debate, however, whether it is necessary for all communities to reach the top level of the model and the general consensus among researchers is that it is not needed. There are some communities – those that because of their location, size, or organizations that exist within their boundaries – that are a more natural target and might therefore need more security than a smaller, less visible community. Generally, the CIAS tells communities that their long-term goal should be to attain level 4 of the model.

One axis of the model shows the different levels a community can attain. The other axis describes what a community should have implemented in each of four characteristics. The first of these is awareness and describes how widespread the understanding of what the impact of a cyber incident might be on the community. The second is information sharing which describes what mechanisms are in place within the community to share information about and analyze cyber security events and what fusion efforts are performed to tie what may seem to be disparate pieces of information into a unified threat picture. The third characteristic describes what processes and procedures are in place in various organizations within the community to address cyber security. It also addresses what testing/exercise/practice is accomplished to evaluate the procedures that have been developed. The final characteristic describes to what extent cyber security is considered in the community’s disaster planning process and what incident response steps have been implemented to cover a cyber incident.

5. Expansion of the CCSMM

The initial model developed as depicted in the previous section was a tremendous first step in developing a model to help communities establish viable and sustainable cyber security programs. Unfortunately, it soon became obvious that there was
something that was still missing. The main problem was that it was quickly realized that for a community to be mature enough in its program to reach the higher levels of the model would require a certain maturity for organizations within the community. In other words, for the community to be secure, the individual organizations within the community needed to also have a certain level of security. This also works the other way. For a community to reach the upper levels of the model, it needs to be able to rely on entities above it to provide certain assistance and information pre- and post-incident. Thus, for a community to be secure requires that the state also have a certain level of maturity in its security program. What this basically meant was that the model was not a two-dimensional model as depicted in the Figure 1. But should actually be a three dimensional model as shown in Figure 2. This figure does not depict the intricate dependencies that exist between levels (i.e. it does not show what level the state needs to be at or that individual organizations need to be at for a community to attain a specific level). Instead, it simply shows that, just like a community, organizations and states also have multiple levels of maturity their programs can be at. The model’s name was not changed, even though it now encompasses more than just a community, because the focus is still on securing the nation from a grass roots level defined to be the community.

![Figure 2. The expanded 3-D model](image)

6. Implementation of the CCSMM to Produce Viable and Sustainable Programs

The CCSMM describes various things that can be done for a community to not only establish a program but to grow the program in its ability to address increasingly complex types of cyber incidents. While the model provides a description of the characteristics and addresses metrics, training, and technology as well, it does not specifically lay out a single path that can be followed to reach the various levels. In truth, there is no single path as often it will simply not matter which course is taken first from a list of courses or which technology or policy needs to be acquired first from a long list that are ultimately needed. That said, in the experience of the CIAS, the initial level of the model, which is arguably the most important as it is the one that will start a community on its path to developing a cyber security program, there is a specific sequence of events that has proven very effective. This sequence was developed to help communities in a specific state to start developing their own programs at the same time that the state also is developing its own program. What has been seen is that most states already have started a cyber security program, but the programs are designed to address the state as a single entity. In other words, the program addresses the various state agencies and departments. It views the state as simply the aggregation of the agencies and departments and the government that they report to.
What the state programs don’t do is to address the state from the perspective of an entity that consists of a number of smaller entities (e.g. cities or towns). The sequence of events that the CIAS has used in the states that it has implemented the program in does just this – working with the state to help it develop its ability to act as a focal point to help communities address their own cyber security issues. The sequence of events that the CIAS has developed are as follows:

- Initial contact meeting with community leadership
- Leading Cyber Security (LCS) course
- Exercise I Initial Planning Conference (IPC)
- Final Planning Conference (FPC)
- Community Cyber Security Exercise
- After Action Report (AAR)
- Community Workshop
- Voice and Data Security Course
- Cyber Security Solutions Workshops
- Exercise II IPC
- LCS course (expanded participation)
- Exercise II FPC
- Community Exercise II
- After Action Report
- AAR Workshop
- State Exercise IPC
- State Exercise FPC
- State Cyber Security Exercise
- State Exercise AAR
- State Exercise Workshop

This is admittedly quite a sequence of events, but it has shown to be successful and it is needed to address the many elements that will make up a community’s cyber security program. At the first level, much of the effort revolves around making community leadership aware of the potential problems and issues and in providing a common point of reference for individuals at all levels of the community to work from. This will prove valuable for them as they implement the program and attempt to talk to others not only in their own chain, but in other organizations that they need to deal with due to factors such as interdependence of resources.

It should be mentioned that the researchers recognized that at this point, especially considering the fiscal constraints being experienced in states across the nation, that few if any communities have a budget to help develop a cyber security program. As a result, expecting too much at the lowest level of the model will do nothing but forestall efforts by communities to embark on the process to develop a program. This will do nothing to improve the level of security and does not help meet the goal of establishing a grass roots program. As a result, the things that are expected of a community at this lowest level are all designed to be available at no-cost or at a low-cost. This will allow communities to start on the process and as their program develops they will have sufficient time to budget for the elements that will require funding.

It should also be noted that the steps outlined above, and the model itself, are designed to help a community to develop a coordinated program. There are many things that an organization (or community) can do that will appear to help better prepare the community. There are, for example, dozens of training courses that can be taken that address many aspects of cyber security. Each of these courses can be valuable, but taken by themselves and not as part of an organized program will result in disparate “point products” and not a solution to developing a security program. Without a plan that addresses cyber security from a comprehensive point of view, individual classes and technology may only provide the façade of security and not lead to actually adequately protecting the community.

7. Impact of the CCSMM

The implementation of the CCSMM as described in the previous section has begun in five states in the United States. In each of these states, two communities have been selected to initially implement the program. The states who have participated in the program so far include Delaware, California, Texas, Illinois, and Louisiana. In addition, North Carolina is in the initial planning stages of the program and two additional states will soon be chosen to add to the list. As was explained in the previous section, tabletop exercises have served as key events that focus the communities on the program and additionally provide an opportunity to measure the effectiveness of the initial efforts. Participant surveys have been utilized to measure the effectiveness of the various parts of the program utilizing a 5 point scale ranging from 1 (strongly disagree) to 5 (strongly agree) with a variety of statements. The exercises average around 75 participants. The results have been very encouraging.

A number of the questions asked deal with the effectiveness of the presentation and the individuals who have delivered the material. These are less important to the topic of this paper. There are, however, four questions in particular that relate directly to the materials and the impact they have on the participants and the program. These questions are:
1. This event increased the group's understanding of cyber security.
2. This event increased my understanding of the need for community interaction and cooperation.
3. This event raised relevant issues about the community's ability to interact in an actual emergency/disaster/incident.
4. The information I received can be put to practical use.

For the eleven communities (two communities per state with five states participating and with one extra community in one state), the scores for the average scores ranged from 4.53 to 4.75 with an overall 11-community average of 4.65. The second question produced averages ranging from 4.44 to 4.80 with an overall average of 4.58. The third question resulted in averages from 4.00 to 4.59 with an overall average of 4.44. Finally, the fourth question produced averages that ranged from 4.32 to 4.58 with an overall average of 4.48. This indicates that the participants generally felt fairly strongly that the exercises were valuable experiences and that they led to better awareness of the cyber security issue. In addition, the exercises seem to have provided information that the participants could use to help develop programs in their own organizations and within the community. The after action report that is provided for each of these exercises detailed for each community specific steps that they could take to continue the process and the after action report workshop provided the communities the opportunity to begin to assign tasks to specific individuals in order to accomplish these tasks.

8. Computer Security Pipelines

A concept that is frequently discussed in security circles is the need to establish an effective pipeline in academia to provide the number of cyber security professionals that are needed. The media has latched on to several different numbers that are frequently seen such as the need for 10,000 cyber security professionals in the government. Articles often then discuss the inadequate “pipeline” that exists starting in our high (or even middle) schools, going to 2- or 4-year schools, and possibly on to graduate schools. The general comment that is made is that we need to be producing more security professionals in order for the nation to become secure.

The researchers at the CIAS agree with the statement that more security professionals are needed but feel that the picture is bigger than that. In order for communities (and ultimately the nation) to be secure, every individual who has a high speed Internet connection needs to take a certain amount of responsibility upon themselves and secure their own systems. Citizens need to assume some responsibility in this effort. This is not an unreasonable expectation. Citizens generally understand the concept of physical security and understand that if they don’t take a minimum amount of responsibility to secure their own property, they may lose it to theft. In addition, their car which may be stolen because they left it unlocked with the key in it could then be subsequently used in the commission of another crime. The same is true in the cyber arena. A computer system and home network which is left unsecured with no or an easily guessed password, and with no encryption for the wireless connection, may result in a successful “hack” by an intruder and the system may then be subsequently used in the commission of another “hacking” event. A program to educate citizens on their responsibilities and that can help them learn what they should minimally be doing to secure their systems should be part of a community security program.

Returning to the issue of a professional security pipeline, schools should not just be looking at developing programs that will lead to the creation of security professionals but should be including cyber security at all places that it is appropriate. This includes not just computer programming courses found in computer science or information systems programs but in basic computer familiarization courses where individuals may learn the basics of picking secure passwords or turning on encryption for their home and office wireless networks.

9. Conclusion

The Community Cyber Security Maturity Model, whose implementation has begun in five states within the United States, has shown to be a valuable tool in helping communities to take an organized first step in establishing viable and sustainable cyber security program. The model serves as a yardstick to determine the current level of maturity for a community, a roadmap for the community to follow in order to improve their security program, and as a common point of reference so that individuals in different communities can discuss their individual programs and share experiences and lessons learned. An expanded, three-dimensional version of the model actually illustrates the fact that the model can be expanded beyond the individual community perspective to encompass individual citizens, organizations, the nation, and multiple nations. Results from efforts in the five states the model is currently being
implemented in have been very positive and participants in the various events that make up the program to implement the model have indicated that the information they have acquired in the program can be used to help implement programs within their organization and their state.

Much has been accomplished in developing the model and the states that are implementing it are finding many positive results from doing so. Much still needs to be done, however. Five states are significant, but just as it takes securing individual organizations with a community to ensure the security of the community, in order to secure the nation the individuals elements that make up the nation (e.g. the states) need to be secured. Thus, it is important for the United States to continue adopting the model and to see that all states embark on the process to establish their own programs.

While much of the model has been developed, there still remain unknowns at the higher levels (since no community is currently at that level). In particular, the technology that will be required to ensure the security of a community in terms of its ability to effectively share information in a timely manner while maintaining the privacy and confidentiality of its citizens and organizations within the community is essential. Without sharing of information, the ability to detect in advance a pending attack will be significantly impacted. The goal should be to prevent attacks from occurring and not just responding to them. This will require a level of information sharing not currently present.

The next step for this program is for additional states to begin adopting the model and for the researchers to take a critical look at the states that have started to determine its effectiveness. While initial indications are positive, the long-term impact of the program has not been determined since the program is still in its infancy. If communities are not able to sustain momentum then it must be determined what can be done to modify the program to ensure its effectiveness.

10. References


