Developing a Community Cyber Security Incident Response Capability

Natalie Granado
The University of Texas at San Antonio
Center for Infrastructure Assurance and Security
Natalie.granado@utsa.edu

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

Abstract

Much has been written on cyber incident response and there are many documents that address the process an organization should follow in the event of a cyber attack or incident. What is not addressed, however, is what the response process should be in the event of a cyber attack on a community. Community leaders do not have direct control or authority over the many disparate organizations within a community but may reasonably be expected to direct the response to such an attack. This paper addresses this issue and makes various recommendations for what communities can do in preparing for a community response to a cyber attack or incident.

1. Introduction

Cyber threats that face a community and the nation come in many forms. There are cyber vulnerabilities that have the potential to be exploited impacting day to day operations and daily routines. Communities face vulnerabilities that potentially impact systems such as power, water, transportation, communication and other critical infrastructures. Over the past years theories of how cyber attacks could impact a community were derived from attacks on single organizations. The attack on the nation of Estonia has confirmed many of the theories and has made believers of many skeptics.

Reports concerning the cyber attacks on Estonia describe the crippling of Internet services. The strike impacted multiple sectors including government agencies, financial services, media outlets and schools. [1] [2] This nation was impacted to the extent that officials are considering adding the Internet to their list of national critical infrastructures requiring protection. This digital siege confirmed the fact that a Community Cyber Incident Response capability must be developed and implemented to accommodate a multi-lateral response capability in cities, towns and metropolitan areas throughout our nation.

There are a number of documents and guides that are available to help an organization with developing its own incident response capability. Within a single organization with an incident response plan, the response will generally be controlled through a single entity such as an incident response team. The team will report to a single individual, such as the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or Chief Executive Officer (CEO) for industry organizations. Government organizations will have a similar reporting chain that ultimately may lead to the cabinet secretary for the federal agency or state official for state agencies. The teams and the reporting individual together have the authority to obtain whatever information is needed to conduct response activities, direct appropriate response activities, and to make decisions which may adversely impact the operation of the organization but which at least may appear to be necessary to address the incident at hand.

A similar situation is not present within a community. The local government, as an entity itself, may have an incident response team identified and may have response processes and guidelines created for itself – as a single entity. As a single entity, however, local government is not very different from any other organization. What is not commonly seen, however, is a plan for the community to respond to an attack on the entire community. Such an attack could involve attacks on many different organizations within the community including entities within the power, water, emergency services, banking, and transportation infrastructures to name a few. Attacks on these entities that disrupt their computer operations would have an adverse impact on the community but there is no single individual within the community that has the authority to direct activities within all of these infrastructures. A community leader, such as a mayor, is a logical choice to lead such a response but the individual will have to do so without any real authority over the operations of the different sectors. Without such control, the leader will have to rely on what information is willingly shared and can only make suggestions as to measures that can be taken. This is a much more difficult task.

In order to develop a computer security incident response capability for a community, it is useful to look at recommendations for individual organizational incident response. These recommendations can then

be examine to see how they can be expanded or adapted to a community response capability.

2. Organizational Incident Response

The creation of an incident response capability for individual organizations has been widely written about. At the CIO Perspectives conference held in Palm Springs in 2001, the audience was encouraged by the U.S. Attorney for Los Angeles to report cyber security incidents to the appropriate law enforcement agency. [3] While this may have sounded like a simple and reasonable request, the problem as was pointed out by a CIO at the conference is that organizations get hit on a constant basis. If they reported the thousands of hits they got on a monthly basis the law enforcement agencies would not be able to handle the volume. What was needed was better guidance on what, and how, to report incident information to law enforcement agencies. The *CIO Magazine,* with input from law enforcement and industry professionals, took the challenge and developed some guidance to help organizations respond to the request to do a better job of reporting cyber security incidents. This guidance also included some excellent advice on how an organization could develop a cyber security response and reporting capability.

One of the most significant recommendations from the CIO Magazine is the need for organizations to develop an incident response plan and to designate the individuals who will be responsible for carrying out the plan. The recommendation also itemized a minimal list of things which the plan should provide details on. This list included the processes to:

- Detect the incident
- Analyze the incident
- Contain or eradicate the problem
- Provide workarounds or fixes
- Prevent re-infection
- Log events
- Preserve evidence
- Conduct a post-mortem and apply lessons learned

Those familiar with computer incident response will recognize these elements, they are common to many similar lists by other authors. The list is at some level fairly obvious – there are probably few surprises in it. At the same time, however, the list describes processes that are sometimes labor intensive, often involve specific technology, and may require varying degrees of expertise. Detecting an incident, for example, is sometimes not an easy matter. In the case of a "global" incident such as a virus or worm that is affecting the entire Internet community, organizations can turn to a number of resources for help and may in fact find out that there is a problem from entities such as the US-CERT or even by watching the media which has become more involved in reporting large cyber incidents. An incident that affects only the organization, however, may not be as easy to detect unless it affects the operation of the organization (such as what may occur during a denial of service attack. An intrusion, especially by a talented attacker, may not be so easy to detect and an attack by an insider may even be more difficult. The organization will need to be monitoring systems and the network using logs from devices such as firewalls and intrusion detection systems in order to be able to determine what is normal activity so that abnormal activity – which might indicate an attack is underway or has occurred – is may be spotted. Should an incident be detected, the next step is to analyze it to determine what its impact may have been. Again, this requires a certain level of expertise in order to accomplish. Once the situation is analyzed, the problem should be contained and if possible eliminated. Hand-in-hand with this is making any changes so that the same thing will not happen again. This may involve fixing/patching systems or it may involve developing some other way to mitigate the problem. This is important so that re-infection doesn't occur or additional attacks are not successful. The next two steps are critical if the organization is going to consider prosecution of the perpetrators. A log of all events needs to be maintained – both what was detected as well as what was done to address the event. Preserving these log files, as well as any other pertinent files will be key and careful consideration must be made to maintaining a chain-of-custody accounting for any important evidence. As the organization develops this portion of their incident response plan it will be very useful to consult with local law enforcement personnel familiar with computer crime or examine guidance on preserving computer evidence that has been developed by other law enforcement agencies and made available to the public (see, for example, what is available from various agencies such as the New Jersey Division of Criminal Justice [4] or the CERT at Carnegie Mellon [5]). The final process that needs to be established is to conduct a post-mortem to determine what operational processes might need to be modified or additional ones developed to better prevent a similar incident from occurring or to better respond to one. This step is often overlooked as organizations return to normal operations and the inevitable "catch-up" occurs as a result of lost time. Organizations should ensure that this final process is in place, however, to prevent it from being forgotten.

A second recommendation from the CIO Magazine to organizations addresses the need to educate users to raise security awareness and promote security policies. It does no good to develop a great set of policies and processes to follow in the event of an incident if nobody knows that they exist. It is therefore important that pertinent individuals are trained on their part of the incident response plan and that all users understand what they should do if they detect something they believe to be suspicious.

The third recommendation was to build a centralized incident reporting system. This is valuable for several reasons. Confusion can occur if there are multiple paths that a user can take to report an incident. In addition, it is important that computer incident reporting is not a completely separate entity but should be incorporated into the organization's overall security plan as well. The reason for this is the need to be able to correlate both physical and cyber events which may have a common goal (of attacking the organization). An inordinate interest in the organization, either from cyber or physical channels, could indicate an imminent attack from the other channel.

The next recommendation from the CIO Magazine is to establish escalation procedures that lay out actions the organization should take if an attack turns out to be protracted or particularly damaging. Incident response in this case begins to roll into disaster recovery planning. The organization needs to be prepared to address issues of long term disruption of computer or network assets.

The CIO Magazine's next recommendation is to make sure that service-level agreements include provisions for security compliance, and that they spell out reporting requirements and the maintenance of systems is covered for cyber security events. This recommendation is simply a reminder for organizations to consider any contracts that they may have with service providers and to ensure that in these contracts the service providers are prepared (as the organization is attempting to do) for a cyber security incident.

The next recommendation is a key one. Organizations should decide, in advance of an actual attack or incident occurring, what the circumstances are that will prompt officials in the organizations to call local authorities (e.g. law enforcement agencies). Cyber incidents occur at an extremely rapid pace. There is simply no time for an organization to conduct a discussion of whether authorities should be contacted or not when the incident is occurring. It may seem like the simple response is to always contact local authorities but, as was previously discussed, this is probably not the right answer as it would mean that law enforcement agencies would be inundated with reports and would not be able to address the really important ones because of the volume of reports they received. For organizations in certain industries or certain locations, there may be the additional issue of legislation that mandates reporting of certain types of incidents.

In a similar manner to the previous recommendation, the organization should also determine in advance what the plans are to inform employees, customers, partners, and the general public when an incident occurs. Again, certain industries and geographical regions may introduce legislation that may dictate when reporting must occur. This obviously must be followed but in addition, or for those that are not governed by such legislation, it is important to have determined in advance what procedures will be followed in the event of an incident. Handling customers correctly is important to ensuring their continued status as customers. Informing employees, customers, and partners can be accomplished in a quiet manner without alerting the general public of the incident, but there are times that this too must be considered. Having a plan for dealing with the media will also have a strong impact on how well the incident will affect the organization in the media.

In addition to the previous list of recommendations that covered plans and processes, the CIO Magazine also provided a list of recommendations that addressed the "people side" of the issue. The first of these recommendations was that an organization should have a single individual (or office) that suspicious events should be reported to. This will avoid confusion on the part of employees and will mean that multiple individuals are not attempting to respond to the same incident with the possible result of interfering with each other.

Along with this idea of having a single individual who employees report incidents to, the recommendation was also made that the organization has a single individual identified who will be the person that will report incidents to entities external to the organization itself. This will avoid the possibility of multiple reports being made which could also cause confusion (is it a single incident, or multiple incidents?).

A key recommendation that is fairly simple to accomplish but that may need frequent revision is to maintain a list of the incident response team members along with their titles, a method to contact them at any time during the day, and their role on the team. Related to this is a companion recommendation to also maintain a similar list for vendors and the contact information for individuals who can be contacted in case of an incident for companies such as the ISP that is used by the organization. The first list is easier to

maintain and keep updated since the organization has information on when employees leave but may not know immediately when an employee at a vendor leaves.

In a similar manner as the lists for employees and vendors, the organization should also maintain a list of contact information for its major customers and clients who could be affected by an attack on the organization.

One of the most important contact lists to maintain is the contact information for any law enforcement agency who might have jurisdiction over an incident at the organization. This will normally include not just the local agencies but the nearest office for the FBI and possibly the closest Secret Service office as well. In recent years the importance of computer crime has risen in the FBI and more agents are now devoted to this problem. This information should be readily accessible by the individual the organization has designated as being responsible for contacting the agencies should an important enough incident occur.

While many of these recommendations can be accomplished at little initial cost outside of employee time, it is important to realize that there is a cost associated with maintaining an incident response capability. The time to invest in this capability, however, is before an incident occurs because the damage that can be caused, both in terms of actual destruction/loss of data as well as financial damage or damage to an organization's reputation, can be many times more expensive than the cost of maintaining the incident response capability. The cost of the incident will be even greater if there is no response capability as it may take considerably longer to determine that an incident is occurring and to take the appropriate actions. In an environment where catastrophic events can occur in very short periods of time, an organization can't afford to not be prepared in advance.

3. A National Imperative

The National Strategy to Secure Cyberspace discusses the need to improve information sharing on cyber security matters as well as the need to improve cyber investigative and forensic capabilities at federal, state, and local levels. [6] It also discusses the need for training to help develop these capabilities.

While there is increasing concern about the potential for a "cyber Pearl Harbor" [2], the documents that discuss the efforts needed to prevent such an occurrence or that are needed to prepare to respond are similar in scope to the national strategy – they focus on what must be done at the federal level to address this issue. They also address the need for improvement in cyber security for federal agencies. Discussions of local level involvement are generally in relationship to law enforcement and information sharing.

The problem with this is the belief that ultimately when an attack occurs, it is the local first responders that are required to deal with the emergency. This has been generally recognized in the non-cyber world and much effort has been placed on preparing state and local officials to deal with terrorist attacks such as the ones that occurred on September 11, 2001. While the attacks on that day had national implications, it was the local officials that had to deal with the immediate effects of the attack.

The general belief in the cyber world has been that any cyber attack can be dealt with differently – at a national level by organizations such as the US-CERT. The belief seemingly exists that since the Internet is international in scope, an agency such as the US-CERT will be able to potentially detect a cyber attack that is occurring somewhere in the nation and that they will be able to address it. While there is certainly some truth to this, and that for many of the incidents that have occurred in the past this may be the case, it is not universally true. For incidents that are indiscriminate in nature – that do not target a specific organization but are designed to take advantage of a vulnerability in a protocol or application program across the Internet, entities such as the US-CERT are well placed to deal with it. An example of the type of incident that falls in this category are the viruses and worms that have made major headlines in the media over the last few years. It was such an incident (the Morris Internet Worm) that prompted the original creation of the CERT after all. For attacks that target a specific sector (such as the banking and finance sector or the oil and gas industry) the thought is that organizations such as the individual Information Sharing and Analysis Centers can serve as coordinating entities between individual organizations and federal agencies. This, again, is true for attacks that are of this type. The question remains, however, what needs to be done to prepare for a potential cyber Pearl Harbor if the attack (possibly conducted by a terrorist organization) is actually conducted on a geographical target (such as a specific state or community) and not on a sector or national agencies? Such an attack would have a tremendous impact on the state/community and if successful would have the desired affect of garnering international attention. Another issue that must be addressed is to determine who will respond to a blended or coordinated attack. A blended or coordinated attack is a cyber attack that is used in conjunction with a physical attack. Security incidents are typically categorized as physical or cyber. A physical attack is viewed as gaining access to an assest or facility. A cyber attack is viewed as a way to gain access to a computer or networked system via the

internet. Combining these two attack vectors can enhance the overall impact of the attack. The Russian – Georgian conflict is an example of how a cyber attack used to coincide with military operations can result in devastation that extends across all sectors. Who is tasked with detecting and responding to such an attack? What information sharing mechanisms are in place within a community to provide the data necessary to analyze seemingly disparate information and recognize the correlation between them? The responsibility certainly does not lie at the national level since, as has been mentioned, the volume of incidents that occur on a daily basis would quickly incapacitate the ability of any federal agency to respond to them. The answer lies in the development of state and local community incident response capabilities.

4. Community Incident Response

The purpose of the previous section on an organizational incident response capability was not intended to provide a detailed discussion of what an organization needs to do to prepare for a cyber incident. Instead, the goal was to provide a quick discussion of the things that an organization must do to develop an incident response capability. This allows us to draw parallels to the much better understood organizational situation so that a discussion can occur on community incident response – a topic which has not been addressed previously. Each of the recommendations for individual organizations has a parallel in a community environment. The specific implementation, however, may vary greatly from that seen in an organization.

The first recommendation for organizations from the CIO Magazine was to develop processes to

- Detect the incident
- Analyze the incident
- Contain or eradicate the problem
- Provide workarounds or fixes
- Prevent re-infection
- Log events
- Preserve evidence
- Conduct a post-mortem and apply lessons learned

All of these are as applicable to a community as they are to individual organizations. To accomplish them for an entire community, however, is potentially a much more difficult task. The reason for this is the span of control difference. An attack on a community can encompass attacks on multiple targets in different sectors. Unlike a single organization, there is no single entity that has authority over all entities within a community. Community leadership is responsible for management of other disaster situations but cyber incidents have not fallen into this category as of yet – and may never. Since an attack on a community will involve attacks on multiple targets within the community, the ability to detect the attack in its early stages (which becomes the goal if prevention efforts are not successful) will rely heavily on the ability to correlate seemingly disparate incidents and recognize that a pattern may indicate a larger objective than an attack on a single organization. In order to accomplish this, however, information sharing between the various organizations within a community and community leadership is required. It's not just the reporting and sharing, however, since if an analysis is to occur it implies that there is an organization that is trained to conduct the analysis and that it is this entity that at a minimum receives the shared information. Within the last few years there has been a push by homeland security professionals to establish state and regional fusion centers to perform an analysis on threat information to determine when other types of attacks may be imminent. The need to expand these fusion centers to also include cyber security events has been proposed in the past. [7] Whether a community fusion center is needed or if a state's fusion center with feeds from communities can suffice has yet to be determined.

After an incident/event that targets the community has been identified, the main function of the community incident response capability will be to coordinate the response activities between organizations. Many of the other processes that were identified for organizations to produce are not applicable at the community level. Since the community does not own the systems, individual organizations do, it is not appropriate to assume that the community should, for example, contain or eradicate the problem, prevent re-infection, log events, or preserve evidence. The community can, however, help to coordinate between organizations and can help provide guidance on how organizations may accomplish these activities.

The second recommendation from the CIO Magazine is to raise awareness and educate users. This has direct applicability to the community as well. All organizations within a community will need to be made aware of the possible effects a cyber attack on a community may have. Most IT professionals understand at some level what effects an attack may have on their organization. At the same time, however, most probably have not thought about how their organization fits within the larger scope of the community and what needs to be done to coordinate defensive cyber activities within the community. Awareness is the first step. The second is to then train IT professionals on their individual responsibilities.

Some organizations (those related to the various critical infrastructures) may have more responsibility to the community as the loss of their services would adversely affect the community itself. Others need to be involved simply because they might be able to provide early warning of inordinate interest in systems within the community. All need to know what is expected of them in terms of reporting and information sharing and need to know how and when to conduct these activities.

Both of the first two recommendations allude to what the third recommendation entails. This is to develop a centralized incident reporting system. This task is hard enough within an organization. To implement one in a community is a considerably more difficult task. Communities have not considered the need for such a function and don't have assets allocated toward it. This will most likely have to be incrementally implemented in a phased approach. The initial step would be to identify specific items that should be reported and keep these to definite indicators of pending or occurring attacks. Initially, there may not be a single individual or organization that the information gets reported to. Instead, a group of individuals within the community that have been identified in key cyber security or emergency management positions could receive the reports of security-relevant information. The group as a whole can be used to share information and to conduct some level of analysis.

The next recommendation was to establish escalation procedures that lay out actions the organization should take if an attack turns out to be protracted or particularly damaging. This is also applicable to a community but should be constructed in a manner to identify the state and federal entities that should be contacted in the event an incident is definitely identified as an attack on the community. Procedures should also be laid out to create different levels of reporting and activity within the community as early indicators lead to more evidence which may lead to definite identification of an attack.

The next recommendation, which addressed service level agreements, has less applicability to a community capability than it does to incident response capabilities for individual organizations. The recommendations after that concern determination of who to contact when an incident occurs and when contact should be made. This is as applicable to the community as it is to an individual organization. Communities need to know who to report to at both the state and federal levels and should also be cognizant of points of contact within the various sector ISACs. Preplanning and coordination should be accomplished to establish at what points these entities should be contacted, how they should be contacted, and what information they will need. Along the same lines, the community should set up the procedures and guidance for community leaders to know when and how other organizations, the media, and the general population should be notified if an attack is occurring. This is true for non-cyber incidents, but in the case of cyber incidents is especially pertinent. An individual citizens' home computer system may be usurped to be part of a botnet which could be used in a denial of service attack within the community. As a result, it becomes particularly important that procedures and guidelines are in place to know when to make a general announcement to the community. Since it does not do much good to release information that an attack is occurring without any specific details on what is expected of individuals, as much general guidance on steps that a citizen can take to ensure their computer is not being used as part of a botnet should be prepared in advance. Specific details related to the current attack can be added as needed.

The recommendations dealing with the non-technology related "people issues" within organizations are also applicable to communities. Points of contact for individual organizations and for the community leadership should be identified in advance and this information disseminated to those who will be part of the process. There may be multiple levels of individuals within the community who have a role in a community's incident response capabilities. There may, for example, be an advisory group established consisting of local security experts who can advise the community leadership on trends and issues that should be of concern to the community. These individuals, however, may not be the ones that would receive reports of actual incidents (though they may be the points of contact for the organizations that they are employees of). The actual team identified that would be called upon to provide guidance and response options to community leaders could be made up of different individuals with appropriate representation from the law enforcement community. The individuals who are identified to be part of the information sharing mechanism and for the analysis capability could form an entirely different third group. There is obviously a significant chance that there will be an overlap between these groups, but the function and purpose of each group is separate and each plays a different but important role in the overall community incident response capability. The point of this discussion is to state that whoever these individuals are, the list of them should be created and contact information distributed to other members of the groups and throughout the community as appropriate.

As a final note, since the power of an individual computer system has grown so dramatically over the last decade, and the level of connectivity has expanded, the possibility that an individual citizen might become aware of a possible pending attack is also increasing. With the number of computer hobbyists who frequent chat rooms and participate in blogs expanding, there is a chance that a single individual may become aware of a groups' intention to conduct an attack on the community and thus it may become necessary at some point to also include a mechanism in the community for individual computer users to submit a report of suspicious activities to local authorities. Since this has a tremendous potential to be abused itself (and thus to possibly result in its own type of denial-of-service attack on the incident response process itself), care must be taken in its implementation.

5. Community Cyber Security Maturity Model

The need for an established community security capability beyond what is needed to protect systems and networks owned by local government has been discussed for several years. During the first Cyber Storm national cyber security exercise conducted by the Department of Homeland Security in 2006, there was minimal involvement at the state level and nothing below the state level. The second Cyber Storm exercise conducted in 2008 saw an increase in the number of states that were involved and simulated a certain degree of community-level inputs. Plans which have already begun for the third exercise, scheduled for 2010, already call for a much increased local capability. In addition to this, a Community Cyber Security Maturity Model (CCSMM) has been developed. [8] This model provides both yardstick for communities to measure their level of cyber security preparedness against as well as providing a roadmap for communities to follow. This model identifies five levels of preparedness for communities and identifies the characteristics of communities at each level. In addition, the technology, information sharing, training, and testing mechanisms that are needed for communities to conduct community-level security are also discussed. The various levels of the CCSMM are shown in figure 1.

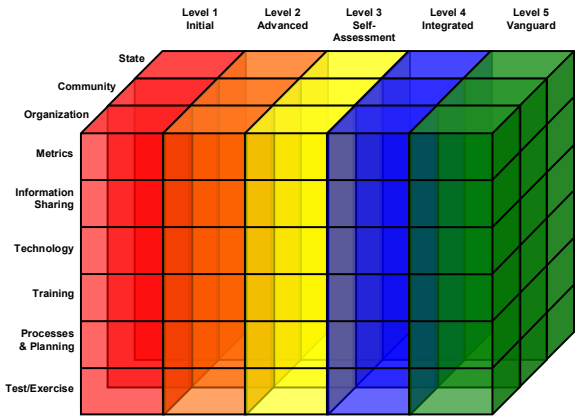

Figure 1. The Community Cyber Security Maturity Model

The three-dimensional version of the CCSMM depicted in Figure 1 implies the linkage already discussed in this paper between communities and the organizations within them as well as with ties to the state. A key component of the model which will provide the ability to gauge whether a community (organization or state) is under attack are the metrics which are gathered at each level. Work on identifying metrics for individual organizations has been underway for several years. Determining what is appropriate to measure for communities, states or the nation is a more involved process. At the lowest levels of the CCSMM these metrics mirror the ones that exist at the individual organizational level and are supplied, in a sanitized form, by the individual organizations within the community. These can then be aggregated for the community to provide an overall picture of hostile cyber activity within the community. In a similar manner, information from communities can be aggregated at the state and federal levels to provide a picture activity within the state and nation respectively.

At the lowest level of the CCSMM, the focus of organizations is on two things. First, the organization must be doing those things it needs to in order to protect itself. It should be applying guidance such as that supplied by the CIO Magazine in order to establish not only an incident response capability but a viable security program as well. The second focus for organizations is on what they need to supply for the community to be able to conduct community-level incident detection and response. Since there are very few communities in which a community cyber security program has been instituted, the focus of most organizations is only on the first of these two aspects.

The CCSMM is currently being used by the DHS cyber training partners to help communities determine what cyber training the community needs. DHS has funded cyber training for states and communities for

several years. In addition, there are a number of communities that have conducted community cyber security exercises to help make community leaders aware of the potential for disruption in the event of an attack. These are part of the model, establishing plans for incident response and continuity of operations is another which communities should also be actively pursuing.

6. Recommended Community Steps

The recommendations for the community don't have to be implemented all at once. There are things that can be done first at little or no cost and others added as time, expertise, and budgets allow. This is important because few communities have a robust budget for cyber security and none have planned for the types of activities and capabilities described in this paper. Communities will need time to implement them and to build their cyber security program as outlined in the CCSMM. At the same time, however, communities need to get started on something and can't simply sit back until a budget is obtained to implement the entire program. They should start with the "low hanging fruit" and establish those portions that can be done at no cost. Several communities have already taken the initial steps in the model and have embraced some of these simple activities.

One of the first steps a community should take would be to establish an advisory board for community leaders on cyber security issues. There are active chapters of professional organizations such as ISSA and ISACA in many cities throughout the world. If the community does not have a chapter of either of these, or other organizations such as Infragard, the community should actively encourage security professionals to establish a chapter. For small communities, regional chapters can be established made up of members from several small communities in the area. The members of these organizations are prime candidates to help advise community leaders on the current threats and issues that might impact the community. The board should meet with community leaders on a regular basis – at least quarterly – and can communicate with (or meet) with each other on a more frequent basis.

The second step communities can take is to take advantage of the training that has been paid for by the Department of Homeland Security (for communities within the United States – similar training is available on a commercial basis for communities within other countries). The DHS sponsored training is free and covers both technical security courses (to include forensics training for law enforcement personnel) as well as awareness-level training for community leaders.

There are many free sources of information available to organizations and communities. The US-CERT produces five different products that are made available to the public (similar advice can be obtained from the different CERTs that exist in other countries as well). These products can be used to help both community leaders and the technical leads within organizations stay current on trends and activities in the cyber world. These products are [9]

Current Activity – Notifies users of the most frequent, high-impact types of security incidents currently reported to US-CERT.
Technical Cyber Security Alerts – Provide timely information about current security issues, vulnerabilities, and exploits.
Cyber Security Bulletins – Summarize information that has been published about new vulnerabilities.
Cyber Security Alerts – Alert non-technical readers to security issues that affect the general public.
Cyber Security Tips – Provide information and advice for non-technical readers about a variety of common security topics.

It is important to note that these products include both technical and non-technical information so both managers and IT staff can benefit from them.

The community's cyber incident response team should also be identified at the early stages of the community's cyber security development. At first these may be advisors for the community's regular emergency operations center. At later stages, computer security professionals may be identified to be part of an emergency operations team. As soon as these individuals can be identified they should begin regular meetings and should take advantage of the types of information and training that is available that has already been mentioned.

As soon as possible, communities should consider conducting a community cyber security exercise to help with awareness and training. DHS is currently developing tools that can aid communities in the creation of such an exercise and has also sponsored exercises in various communities around the United States (the Department of Defense has also sponsored several of these exercises in communities in which there is a significant DoD presence). There is also free guidance on developing security exercises of both a cyber as well as non-cyber nature available from DHS

as well as the National Institute of Standards and Technology.

7. Conclusion

The need for communities to have a viable cyber security program is growing. This is especially true as the e-Government movement increases. As more and more government functions become available to citizens online, the potential for the disruption of these services also increases. The lessons learned from the attacks in Estonia showed how critical cyber resources were to the daily functioning of the nation. E-Government can't exist without e-security and even if the government is able to secure its resources, communities could still be at risk if the other critical infrastructures in the community have not secured their assets.

There is a lot of guidance on developing an incident response capability for organizations. This guidance, though not directed at community-wide responses, provides a glimpse into the types of activities that a community should be involved with in order to be secure. A helpful model for communities is the Community Cyber Security Maturity Model which can serve as a roadmap for both states and communities in their efforts to build a cyber security program and capability.

There is a cost associated with the creation of an incident response capability as part of a cyber security program. This cost at first may be in terms of time that individuals will spend in addressing security matters for the community. As the capability evolves the expense will also include technology components as well as additional personnel not currently employed by local governments. While there is a cost, it is an expense that must be planned for and supported by local and state government because the alternative (no security and the possibility of a cyber attack) are even more costly.

While there is a cost associated with establishing a security program in communities, there are many resources that are available that are free or of very low cost. This paper suggested several steps that communities could take that would not require increasing local budgets but that would start the community on the way to establishing an incident response capability and a security program which would enable them to potentially prevent or detect, respond to, and recover from a cyber security attack.

8. References

[1] Gadi Evron, "Battling Botnets and Online Mobs", *Georgetown Journal of International Affairs*, Winter/Spring 2008, pp121-126.

[2] Jason Miller, "Feds take 'cyber Pearl Harbor' seriously", FCW.COM, May 28, 2007, available at www.fcw.com/print/13_17/news/102825-1.html

[3] CIO Magazine, *CIO Cyberthreat Response and Reporting Guidelines*, available from http://www.cio.com/research/security/incident_response.pdf

[4] Department of Law and Public Safety, New Jersey Computer Evidence Search and Seizure Manual, available from http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf

[5] Georgia Killcrece,et al. *State of the Practice of Computer Security Incident Response Teams*, available from www.cert.org/archive/pdf/03tr001.pdf

[6] The White House, The National Strategy to Secure Cyberspace, Feb 2003, available at www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[7] Natalie Granado and Gregory White, "Cyber Security and Government Fusion Centers", *Proceedings of the 41st Annual Hawaii International Conference on Systems Sciences*, Waikoloa, Big Island, Hawaii, January 2008.

[8] Gregory White, "The Community Cyber Security Maturity Model", *Proceedings of the 40th Annual Hawaii International Conference on Systems Sciences*, Waikoloa, Big Island, Hawaii, January 2007.

[9] US-CERT Quarterly Report, available from http://www.us-cert.gov/press_room/trendsandanalysisQ208.pdf