# e-Government and Cyber Security: The Role of Cyber Security Exercises.

Art Conklin
*Center for Infrastructure Assurance and Security*
*The University of Texas at San Antonio*
*art.conklin@utse.edu*

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

## Abstract

*e-Government operations are increasing with citizen demand for timely and cost effective services. Security associated with individual systems is similar to many e-commerce solutions. The span of control of e-government and its impact across a community defines a system that is more than a sum of just single systems. To test security issues across the entire system requires a new method of analysis, a community based cyber security exercise. Results from recent community based exercises have provided insight into opportunities for improvement and has demonstrated the value of these events.*

*Information gained from community based exercises permits local governmental entities to better prepare their e-government systems to serve their citizens needs. Although some actions discovered in the exercise may be difficult and resource intensive, numerous low-hanging fruit opportunities for improvement can be discovered and used to improve e-government systems.*

## 1. Introduction

The 'e' revolution has swept through business creating e-business and e-commerce. E-Government follows for much of the same reasons that drove business to embrace the e-revolution. Increased customer access to services drove businesses to move operations to e-business. With this move to a new method of doing business, businesses adapted operating procedures to capitalize on this new distribution channel. In addition to business to consumer (B2C) channels, business to business (B2B) channels changed as well. Internal business operations also became enhanced through the communication channels provided by e-business. Globalization and outsourcing followed enabled by the communication channels and business processes initiated by the change to e-business. E-Commerce is completely different than its predecessor, the brick and mortar world.

e-Government faces the same challenges that faced e-business. Adapting an existing service delivery model to a new delivery means, in this case electronic, carries with it commensurate required changes in policies and procedures. E-Government has its own descriptive categorizations. Some of the common ones are Government to Government (G2G), Government to Citizen (G2C), and Government to Business (G2B). [1]

These required changes present challenges and opportunities to agencies as they move services to new media. A simple example of records security and retention provides illustration to this concept. Assume a couple goes to the county courthouse and fills out a marriage certificate on a piece of paper. In the old model, this piece of paper is processed and filed, eventually being stored in some record, either as paper or possibly microfiche. Record retention and security are physical problems, with long proven solutions. But with these solved problems, in the e-environment new issues arise. Where access was limited by the physical storage and security provisions, access control is significantly more complicated in electronic records. Accessing paper or microfiche records can be an expensive, time consuming issue. In the e-world, the access problem is solved, databases and electronic records make multiple remote accesses a cost efficient process. But with this ease of access comes a new security issue – how to manage access. Who can see the record, and with it being electronic – who can change it? Record retention is also an issue with a new twist, for while 100 year old paper records are common, data format issues can exist in electronic records across only decades. The e-world is not just an electronic version of the previous business model.

Managing a complex environment such as a combined e-world and original business model is a daunting task. Outside evaluation and assistance can be invaluable when analyzing the effectiveness of business processes. Many large businesses have an internal audit function that assists in this effort. At other times outside contractors are brought in to

assist. In the world of e-government, outside evaluation is just as valuable.

E-government has many unique characteristics that increase the level of difficulty for implementers. Differences in access, structure and accountability have been previously studied with respect to e-commerce and e-government comparisons. [2] The characteristics of structure and accountability play a particularly important role in this study of cyber-security exercises and community based government operations.

The aspect of structure and its decentralized, multi-party, dispersed decision making authority associated with governmental entities plays an important role in exercises. This dispersed authority has implications in any cross government initiatives, typically requiring significant resource expenditure on consensus building. [2] The concept of accountability also plays a role in e-government activities with additional resources being expended on efforts of maintaining transparency and good stewardship of the people's money. The concept of accountability can be expanded to include characteristics of cooperation and compliance, key elements in government's efforts to achieve control in a community. [3]

Taking a small local community government and examining its constituency base reveals the following: local citizens, large corporate entities with facilities in the community, and a significant number of government entities. Separate government levels, local city, local county, adjoining city and county when applicable, state, and federal agencies define one method of segregating entities. Within these levels are a variety of government agencies that are in many ways independent. City police, fire and emergency medical services, county sheriff, state law enforcement, federal law enforcement (multiple entities), define just some of the entities involved. If a government entity, such as the city, own or operate a municipal service or utility, you can add in water, gas, electricity, sewer and trash as appropriate.

This milieu of entities should raise some concerns as towards inter-agency communications. A well designed exercise will test not only each agencies policies and procedures, but also the cross agency communication element. The concept of community based cyber security exercises comes from a military exercise model. Exercises allow participants to evaluate what-if scenarios and their responses to the events. This can serve as an invaluable awareness tool and business process model evaluation technique. Adapting this methodology into the e-government community with respect to cyber security can bring some of the same benefits. This paper examines aspects of conducting community based cyber-security exercises involving local government bodies and the local entities that interact with them. The methodology is one of case study form, using information gathered from community based cyber security exercises conducted in three cities, a major metropolitan area, a port city and a border city.

## 2. Cyber Security Issues

Cyber security can simply be defined as security measures being applied to computers to provide a desired level of protection. The issue of protection can be defined using the acronym CIA for Confidentiality, Integrity, and Availability. Confidentiality refers to the property that data should only be viewable by authorized parties. Integrity refers to the principle that only authorized users are allowed to change data, and that these changes will be reflected uniformly across all aspects of the data. Availability refers to the principle that data and computer resources will always be available to authorized users. Using the word simple to describe computer security is misleading however, much as it can be said to be simple to play golf. Just it the ball in the hole in as few strokes as possible. The devil is in the details.

The history of computer security can be viewed as one of regression. Early computer systems offered high security, but relative to today's functionality, very little in terms of availability. As software vendors increased functionality, moving to PCs, then distributed computing and now towards web services, data availability increased by orders of magnitude. But with this increase came issues of confidentiality and integrity. The driving principle behind much of the software being developed was one of features first, other things like security later. In the past few years, an increase in attention to security issues has swept the software industry.

The basic design of the Internet was built around shared access and trust, with security measures being an after thought. There are many protocols in wide use that offer little if any security to their users and instead rely on trust. This model made sense when the Internet was first developed, for the information being transferred was of little value to others than the owners. Today, the Internet is used to transfer information between people, their banks, their brokers, businesses and government entities. This information can be of significant value to others, including criminals, as the current level of cyber attacks, identity thefts and phishing attacks attest.

The state of the environment and the information value has placed significant responsibility on software developers and system designers to maintain

appropriate levels of CIA for their users. This has raised the level of complexity for e-commerce and e-government. When a citizen arrives at the local driver's license office, they can establish their identity by showing their old driver's license when they apply to have it renewed. On-line, proving one's identity to a software program is more challenging. The credit card industry has made changes to their cards, specifically the addition of a printed security code to the card, one that is not electronically encoded on the magnetic stripe, but must be read off the card. Similar changes may be needed to items such as driver's licenses to force possession of the physical document to provide the necessary information for authentication.

Government documents play a crucial role in our society. Government issued documentation acts as the foundational elements supporting a person's identity. Driver's licenses, social security numbers, tax identification numbers, and various entitlement documents are used on a regular basis by people to demonstrate their identity and authorization for various opportunities. Because these documents form the basis for all subsequent documents, their integrity is paramount to many industries. Also because of the importance of these documents, they are targets for criminals and other nefarious agents.

Maintaining a proper cyber security position requires a combination of managerial and technical task executions. Management must determine the appropriate level of risk tolerance and the appropriate set of security requirements. Technical specialists using the security requirements document develop the necessary technical safeguards to insure appropriate levels of protection are deployed. After the development and deployment of security functionality, a testing and audit function is used to determine both correctness of the solution and continued compliance to the stated requirements.

Security failures are high profile events. Several recent incidents, including Card Systems, LexisNexis, Bank of America, DSW and others have exposed millions of records to potential identity thieves.[4] Not only are these events bad PR for the companies involved; they can be bad business, as class action lawsuits and licensing actions can destroy the companies involved. These are marketplace remedies that a capitalist market places on firms that do not perform up to community standards. The same forces do not exist for government entities.

## 3. E-commerce business model

E-commerce is built around a business model that utilizes the ease and speed of communications facilitated by network connectivity. In a marketplace where speed to market is rewarded with market share, firms become very adept at delivering speed. As the marketplace gained competition, agility on the part of firms to develop new services and new opportunities based on this new channel.

e-Businesses come in many sizes, shapes and markets. Whereas Amazon can be viewed as a re-invention of normal business, e-Bay, Yahoo, and Google can be seen as entirely new creations. Each of these firms has had its business troubles, yet has ridden out the tough times and joined the ranks of profitable firms in the business landscape.

Regardless of the industry, the basic business model is one of firms interfacing with suppliers and customers. The number of relationships is bounded in type, but not in quantity. For a firm to double its ability to service its customer base, the driver is mostly just one of capital – just add servers. Compared to the time requirements for adding trained personnel and physical facilities, the advantages with respect to speed become obvious.

The next generation of e-business involved not just automating normal business processes, but enhancing them with new offerings. A prime example would be the integrated financial offerings offered to ordinary people. Bank accounts and investment accounts are electronically linked so that a user can execute trade orders or transfer funds anytime, day or night. Advanced information tools such as charting and analysis functions provide information. Marketing determines business opportunities and business units execute on the plans.

The basic business functions of a normal business exist in an e-business; obtain customer orders, process the orders, manage the development of products sold, new product development, marketing and more. Depending on the level of integration of e-business and standard business, the level of involvement of information technology varies. The actual level of IT involvement is not the critical issue, the level of specific integration and specialization of functionality associated with the e-functionality is the important factor. Specialization and specific integration are resource intensive issues that require significant dedication on the part of the firm to achieve.

Security functionality is one of many items that needs specific attention with regard to unique e-business functionality. Information technology based solutions rest upon electronic information stores. The information stored in the systems has tremendous value and needs appropriate levels of protection to insure its security. The development of specific security controls to accomplish these requirements is of significant concern to e-commerce based

companies and they commit resources to achieve the needed objectives. Information comprises the core asset in an e-business environment and the necessary business processes to properly use and protect it are the keys to success in e-commerce.

Connectivity between customers, suppliers and the firm is what separates e-commerce data from standard business data. In the e-world, access to the data from both customers and suppliers is the norm, with customers and suppliers computer systems interacting directly with the firm's systems. This requires specific levels of access and control, and these form the differentiator in this business model. Speed of execution comes from the direct connection between the information systems of customers, suppliers and the firm's own systems. This direct connection requires both appropriate levels of controls and a method of interface simple enough to facilitate the necessary customer interactions.

An examination of the successful e-commerce firms, their practices and methods, shows significant levels of effort in the interfaces, the back office functions and crucial elements such as security. Although there are differences between the specific implementations of the different firms, the end result is the same, time and effort was applied to develop the appropriate systems to facilitate the desired business objectives in the e-commerce arena.

## 4. e-Government model

Thinking that e-government is a natural extension of e-commerce ignores the basic fact that government operations are different from business operations. Government operations feature a different set of players including a wide array of differing constituents, a diverse collection of different agencies operating in degrees independent of each other, and significant limitations on the ability to raise capital. The lack of competitors can also be seen as a factor limiting creative forces of change.

One of the biggest challenges for e-government is the diverse number of agencies. Not only are citizens and local firms customers, but in many cases, the agencies can be seen as customers as well. But not all customers are equal with respect to level of information sharing; information sharing across networks between the police department and a city operated water department may be done at a different level than the police department and the public citizens of the area. It is important to look at each of these potential interactions as communication channels that need to be defined in terms of trust, and content. These different entities each have a role in the community's response to a cyber-security event, and the exercise is structured to explore this aspect of emergency operations. Managing these multiple independent relationships is a challenge that grows exponentially with the number of channels.

Complicating the communication channel issue is one of central authority. Although government agencies have a defined hierarchal relationship, this does not always manifest itself in terms of interagency coordination. As previously noted, building consensus is a time and resource consuming item, that may or may not be an appropriate use of resources in an emergency response event. In corporate relationships, interdepartmental rivalries are typically quickly resolved by decisive action from higher up the chain of command. What drives this response is the focus of the firm on its mission. Government bodies have too many missions and too many relationships to have similar simple solutions to coordination issues.

When e-business faces opportunity to grow and expand, the needed resource is capital. Capital is grown by successful business operations, hence successful e-businesses develop the very resource needed for more growth. Government agencies do not have this capital development ability. This can severely inhibit e-government's ability to respond to new opportunities and demands by its customer base.

Government entities exist for the purpose of serving society. While commercial firms exist for the benefit of their shareholders, governments serve the communities they represent. This connection to the community is a key factor in government operations. People view commercial firms as a source for specific service or product. Communities view government in a wider view – as a supplier of many different services. The view is not always positive, but instead frequently exhibits a level of asymmetric risk. Citizens expect everything to always be right and at lowest possible cost, even when the cost won't support the desired level of service. [3]

Automation of business functionality, whether for e-commerce or e-government is not free, in fact it is a fairly costly initiative. Significant resources are needed for the hardware and software, and the tasks associated with security are frequently the first to be cut when trimming budgets. Delivery of functionality to the end user drives deployment schedules and budgets and security is frequently only taken seriously after an incident.

The determination of appropriate technical actions to achieve desired business results in an e-government setting has an ally in larger national governmental entities. As these entities have greater resources, they have some of the wherewithal to examine technical alternatives and determine appropriate paths to

success. Entities such as the National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) have published extensively technical and managerial reports that can guide efforts.

Common areas of hardship, such as authentication methodologies have received attention from these national agencies. New solutions suited for e-government, such as knowledge based authentication offer insights into unique e-government challenges. The use of national level resources to tackle some of the more technical issues associated with security provides significant information applicable to individual implementations associated with e-government. Unfortunately these resources are still stovepiped and geared towards separate aspects of technology deployment and not the system level issues associated with deploying them in operation.

Whereas commercial entities have the capital resources necessary to devote to the proper development of business processes to support e-functionality, government resources can be more constrained. Limited financial resources are still available to government entities, the key is in the proper application of them. IT management needs to develop coordinated plans that maximize the application of the limited resources to areas of impacts to information security. One of the keys to management of any activity is this use of measurements to measure effectiveness. Community based cyber security exercises can provide such measurement to management.

## 5. Cyber Security Exercises

*Past experience has shown that preparedness efforts are key to providing an effective response to major terrorist incidents and natural disasters. Therefore, we need a comprehensive national system to bring together and command all necessary response assets quickly and effectively. We must equip, train, and exercise many different response units to mobilize for any emergency without warning.*

— National Strategy for Homeland Security, July 2002

One method of testing operational environments is with a scenario based exercise. Exercises have been used in training and development of actors in a complex open decision environment for decades. Practice makes perfect is a mantra repeated by military units, law enforcement units, fire departments, etc. The US Department of Homeland Security promotes exercises as a method of preparing for and evaluating community preparedness for disaster response. The objective of DHS is to assist communities in their efforts to obtain an objective assessment of their own capacity to prevent or respond to, and recover from, disastrous events.[5]

Using an exercise to test a local government's ability to operate in a less than perfect cyber environment has provided insight into e-government operations and provided the participants an opportunity to determine their strengths and weaknesses. This exercise-based model has been deployed in several communities with remarkably consistent results. The exercise methodology allows local governments to test their existing policies and procedures associated specifically with cyber attacks and combined physical and cyber attacks. The objective of the exercise is to simulate a realistic attack by an adversary targeted to disrupt local government operations, typically using a combination of physical and cyber events.[6] With the continued expansion of systems designed to facilitate a move toward e-government, the importance of examining how cyber attacks can affect a community becomes even more critical.

Communities engage in exercises designed to test their first-responders on a frequent basis. The goal is to examine their ability to respond to physical attacks and disasters. The use of a cyber security component in one of these standard community based exercise can simulate the risks associated with an adversary whose intent is to disrupt government operations using any means available. Combining cyber and physical elements is a method of increasing the effectiveness of disrupting activities. Cyber security represents a weakness in many systems at the local level where cyber security resources are the lowest. This creates a vulnerability for civil disruptions as local government dependence on electronic systems increases.

Community based exercises are just that – community based. Because the scope of e-government operations is community wide, the exercise is inclusive of all sectors of the community. Local government operations are represented, including local law enforcement, emergency operations, and city management. If a local utility is owned or operated by the city, they are represented, as are critical infrastructure firms such as telecomm, medical (local hospital), ports and universities. Other levels of government agencies, such as the US military, or federal law enforcement are represented if they have a presence in the area. Each of these entities has a presence at the exercise.

The structure of the exercise is one where the numerous entities are gathered around tables in a common meeting environment. Each type of entity is given its own table, and generally multiple members from each entity take part in the exercise. The structure of the exercise is based on a table-top based scenario where different aspects of an overall scenario are revealed over time to each table. Each table (entity) is given information that it would normally be exposed to in its normal mode of operations.

The events of the exercise are built around an overall scenario where a group has a hostile intent towards a local entity. A series of actions are performed, some directly associated with the hostile intent, some intended to cover their tracks. Examples of issues brought into the scenario are viruses, intrusions into the electric utility disconnecting power to key officials, denial of service attacks (DOS) attacks, web defacements, shooting at cell towers, and posting flyers with disinformation around town. A mixture of physical and cyber attacks are used, targeted at different entities.

As each clue is revealed to each table, the table answers questions pertaining to how they would react. Who would they contact, do they have a policy, etc. The objective of the questions is to learn how each entity responds, determine how they are interconnected and their self-perceived state of control in a degraded environment.

The key elements that make these community based exercises valuable include the focus on the community level involvement, the active decision making on the part of the participants and the interfaces between entities. The scenario illustrates an attack against an entity in a community, yet the attackers may use several vectors in the community to provide more power in their attack. E-government operations are not performed in isolation, but are activities involved in the community. Active decision making is when participants have to interact with the scenario and determine what course they will follow. The decisions are not framed by "normal" events, but rather by situations where the decision maker is acting with incomplete and imperfect information. Routine decisions can be just replications of previous actions, but the scenario is designed to move decision makers into areas where they may not have practiced or thought through the ramifications of their actions.

Mapping and observing the interactions needed between groups is a key element of the exercise. The scenario is designed to exercise the connections between entities. Some of these interconnections are by design, i.e. a city IT group, and some by local proximity, i.e. loss of cell phones due to tower damage.

Measurement of key indicators is an important element in the management of any business process. Using a community based cyber security exercise to measure the effectiveness of communication across the entire system provides management the information needed to improve operations of the system.

## 6. Results and Conclusions

After performing cyber security exercises in several communities, some common results have been observed.[7] As expected, e-government has significant weaknesses under abnormal or hostile environments. Also as expected, the larger agencies, i.e. Federal agencies, with their larger resource base, frequently have better prepared e-government solutions. E-government solutions based solely on adding IT functions to government tend to have weaknesses associated with operations under non-normal conditions. Poor awareness and a lack of understanding of cyber security issues was seen across the board on all exercises. Although many of the entities had normal communication channels over which they commonly dealt with normal operational details, once issues of cyber security arose, it was common to just defer cyber issues to the IT group and this created a bottleneck.

Local government entities have experience in emergency operations and disaster responses. The differences between cyber security based exercises and normal disaster based exercises lies in the party that is primarily responsible for managing an event. Emergency operations and emergency services, fire, police and medical services, are experienced in responding to emergencies and regularly practice for such events. Even with the dispersed lines of authority and control that are present across government, the limited involvement of a few main players makes decision making and execution effective in 'normal' emergencies. In cyber-security events, where multiple parties within the government are both effected and involved in the response, the dispersed lines of authority and control become an impediment in large scale coordination efforts. This is consistent with principles of structure and accountability as presented by Jorgensen and Cable. [2]

Other identified issues include issues associated with government entities roles and responsibilities during the exercise. Managing e-government resources and maintaining them in an operational state during a cyber attack requires a distributed resource of trained personnel. Identifying gaps in trained resources, coupled with gaps in awareness and panned

responses was common during each exercise. Because e-government frequently connects citizens with several aspects of government, and because electronic communications are growing rapidly across all entities of local government, learning and understanding gaps in inter-agency communication and coordination plans under adverse conditions was an important finding to community leaders in each exercise. This gap is a direct manifestation of technology issues, access issues and accountability issues previously examined. [2]

Inter-agency communication is a key element, as many responses in the event of a disaster require coordination between elements. In the event of physical injuries, citizens may call 911, the 911 operator dispatches EMS services, which transport people to local hospitals and emergency rooms. Police and fire departments may also be involved in this type of situation. If numerous calls arise, then prioritization adds to the communication and coordination issues. Adding the element of citizen confusion if public information outlets such as web pages and emails are tampered with, electronic communications quickly become an issue that aggravates local government efforts to respond to the serious threats.

A positive result is that many of the issues uncovered are relatively easy to resolve. Because the nature of the cyber security exercise led to a self discovery of the weaknesses, the entities were more likely to believe in their findings. Using the exercise as a form of active learning, the participants gained significantly more than they would from reading a report on the same subject. [8]

Self discovery also yielded information into weaknesses not readily apparent to outside observers. An event in the scenario leads to a what-if discussion at one of the tables; the participants, possessing detailed knowledge of their own procedures see other issues and holes that need to be repaired.

Unfortunately some of the findings are not easily fixed, especially those involving resources. Capital is a resource that is not easily increased in government operations. As e-government operations have different resource basis, and one that is more heavily dependent on capital, this makes increasing e-operations more difficult for government than for business. Properly building out e-government structures will require significant resources, resources seen being deployed by Federal agencies, but out of the reach of many local communities.

Through the simulated hostile environment that attempts to stress the operations of e-government, the one key element that continually showed up as a weakness was communication. Developing a strong communication plan, one tied to a previously determined action plan is not a foreign idea to government entities. During the cyber security exercise, at each table of participants, repeatedly the idea of improving communications was broached by members. Emergency service personnel are used to managing key communication aspects under adverse conditions, and they noted the need to extend this idea from intra-group to inter-group.

Technical awareness was also another issue that each table again came face to face with. The members of the groups assembled at the tables during the exercise were technical experts in their specific jobs and responsibilities. These were highly competent people, dedicated to doing the right thing for their community. The challenge they noted was that they did not possess the necessary knowledge to make the proper decision at the time of the event. These people have developed their careers upon the idea of planning for and executing the plans associated with less than perfect situations. Natural disasters, accidents, criminal events, and other extreme situations are activities that government entities are called upon to deal with on the behalf of citizens. To do this effectively, each entity has developed plans, with numerous contingencies based on previous experience to facilitate quick decision thinking at the time of the event.

Community based cyber security exercises attacked this expertise in two directions. First, the nature of the exercise, like the nature of government from a citizen's position, is one of inclusivity [3] – the inclusion of many different entities in an event or decision. Second, a technical nature – cyber security, that is outside the expertise of the participants is the basis of at least some of the issues associated with the overall exercise. Forcing the attendees to work together in an area where they are lacking specific expertise challenges them to learn and improve.

A key lesson learned from observing numerous exercises is that participant's behavior towards incidents is driven by previously planned responses. Determining the proper responses to an incident is a task that is better performed in advance of the event, when time is available for the entities and actors to examine and determine appropriate alternatives. Issues such as e-government and cyber security are not normal topics for these planning steps and hence the preparation for the event was not as high as participants would be used to for most exercises. This is an awareness issue, and one that is fairly easy to begin addressing. The key to successfully addressing these issues requires significant technical expertise, and this is an area where local governments will need to procure resources.

A key antecedent to resource application is the understanding of the need for the resource application. As cyber security issues and e-government issues are relatively new, the experience base for management officials is lacking. Awareness is a challenge in any new innovation diffusion situation. A key to awareness in the adoption of a new innovation is how the adopter perceives the value of the new innovation. Using an exercise format and allowing participants to self discover the value of the innovation (cyber security issues) and this makes the awareness issue personal and lasting. Similar to active learning principles in the classroom, this active discovery of the gaps, and opportunities to be addressed has proven to be a very effective model at initiating follow-on actions.

## 7. Future Work

Currently, exercises associated with e-government operations under adverse or disastrous conditions are being conducted from the top down by the Federal government [6] and from the bottom up by local communities. The next logical step is to conduct exercises in groups of local communities and at the state and regional level. At the top levels of government, the number of direct communication links is relatively limited at the top-most levels. The number of inter-agency communication links, and the number of inter-connected dependencies at regional levels posses the greatest challenge. At the local level, the interaction with the highest levels of the national government is limited and channeled through federal agencies. At the state and regional levels, there are significant communication and dependency links both down to local units and up to national units as well as across state level agencies. Exercises are designed to test the plans, policies and implementation of these tools in the management of operations under adverse conditions. Add the challenge of electronic access, a newer and much less mature environment, and there is a lot of opportunity to learn where the gaps exist, and what needs to be addressed first and what aspects can be ignored.

Looking at these issues at the regional and state level in coordinated exercises that involve numerous communities and numerous levels of government will undoubtedly reveal new issues and opportunities for the parties involved. This is an area of research being examined in the coming year.

A separate challenge is to follow-up on the participants of previous exercise events and determine the level of improvement that occurred from the exercise initiated awareness. E-government is still in its infancy, and like other e-initiatives and all new initiatives, there is a learning and growth period as lessons are learned and better solutions are implemented. In this dynamic environment, a single point in time exercise, no matter how comprehensive is limited in its ability to effect meaningful change to the environment. Over time, repeated cycles of exercises and other management methods of determining gaps will need to be employed in a continuous improvement cycle. Determining the effectiveness of the community based cyber security exercise at initiating this chain of change events is also an area of active research.

## 8. References


1. Carter, L. and F. Belanger, *The utilization of e-government services: citizen trust, innovation and acceptance factors.* Journal of Information Systems, 2005. **15**(1): p. 5-25.
2. Jorgensen, D.J. and S. Cable, *Facing the Challenges of E-Government: A Case Study of the City of Corpus Christie, Texas.* S. A. M. Advanced Management Journal, 2002. **67**(3): p. 15-21.
3. Alford, J., *Defining the client in the public sector: A social-exchange perspective.* Public Administration Review, 2002. **62**(3): p. 337-346.
4. Acohido, B. and J. Swartz, "*ID thieves search ultimate pot of gold databases"*, in USA Today. 2005.
5. Ridge, T., *Homeland Security Exercise and Evaluation Program*, Department of Homeland Security, Office of Domestic Preparedness. Volume I, 2004.
6. White, G., G. Dietrich, and T. Goles. *Cyber Security Exercises: Testing an Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events.* in *Proceedings of the 37th Hawaii International Conference on Systems Science*. 2004. Kona, HI.
7. Center for Infrastructure Assurance and Security, *"Dark Screen A Cyber Security Exercise for San Antonio/Bexar County Final Report"*. 2003, The University of Texas at San Antonio: San Antonio.
8. Felder, R.M. and R. Brent, "*Learning by Doing*." Chem. Engr. Education, 2003. 37(4): p. 282-283.
9. FEMA (May 5, 2003), "TOPOFF 2", FEMA News, Department of Homeland Security, www.fema.gov/nwz03/nwz03_topoff2.shtm