Gap Analysis

I feel there are large gaps in information sharing amongst small business and our school systems. I feel that the Department of Homeland Security can do a better job at sharing information to small businesses and our school systems. School violence unfortunately is a problem we must live with and wonder if this type of incident can happen at my child’s school. Not every school has the same budget nor do they have the same type of threats that others have. But as citizens of this country we must not live in a country where our schools, a place where our kids learn not have the same type of security measures as other schools just because they are located in better state, city or neighborhood. I recently read an after action report, this report covered an Active Shooter exercise which occurred on January 25, 2011. Though this report was found on a secured website, school representatives, law enforcement personal and any one with a need to know can have access to this report. Items that were identified may not be a requirement or governed by any regulation, but without these measures we risk the lives of not only our children but our staff as well. Items that were identified included:

(AAR/IP, 2011)

• Providing building schematics to the ?????? Police Department to expedite their response

• Training with the ????? County Sheriff’s bomb dogs to familiarize them with the campus

• Joint training with the ?????? Police Department for personnel and facility familiarization

• Obtaining Radio interoperability with OPD to minimize communication issues

• Participating in the creation of Safety Watch and Cadre to help identify behaviors that may be concerning

• Purchase a Mass Notification System to expedite message delivery in cases of emergency

(AAR/IP, 2011)

Each of these measures were identified as being a critical factor not only for responding forces but also proactive measures that can identify behaviors of future suspects. After reading these countermeasures and excellent advice, I assume these after action items were released to other schools and colleges advising them that these measures were a result of an exercise that was conducted. Some cities or states don’t have the resources to conduct an exercise of this magnitude. So I contacted a few principles and a superintended and ask them that if they ever receive security information from any reliable sources. Both principles and the superintendent replied that the only information they receive is either from their Resource Safety Officer (RSO) or any information they look up. Not that I don’t feel that our law enforcement don’t have the knowledge to implement these ideas or find this type of information and share it. So I contacted the local police department and educated them that there are numerous sites that need to be analyzed and researched so that they can learn from others. This type of information should not be coming from a father, concerned citizens or third party, this information should be coming from state and city law enforcement agencies.

Recently in Philadelphia, Janet Napolitano said the federal government and the private sector must improve the way they share information to prevent and respond to cyber threats. She further indicated Cyber Attacks have increased significantly over the past decade. (Walters, 2012) She also indicated that the cyber threat is costing tax payers 114 billion dollars a year and it’s only getting higher, she pointed out the private entities own majority of the utilities which include pipe line gas systems and water treatment facilities. Napolitano indicated that the private sector needs to remove barriers that make it difficult to share information. (Walters, 2012) I understand private companies don’t want government involvement, they feel they give the government an inch they will take a mile. That is not the case, the government has access to resources private companies do not have, allowing them collect the right threat intelligence that can directly affect the Department of Defense. There are hundreds of private companies that provide services and goods to the Department of Defense, which can be a huge vulnerability when it comes to the insider threat or cooperate espionage.

Small businesses are at greater risk due to multiple reasons. First they feel they aren’t at risk of being a target, which is wrong, small business are highly considered to be an easy target for adversaries due to inadequate security they practice. Hard target vs. Soft Target has always been a topic people and especially small businesses do not understand. For example, if I were targeting a large company like Northrup Grumman or Lockheed Martin, I would never directly target those entities for a couple of reasons. The security at those locations are expected to better trained and equipped and a lot more layers of defense are implemented and practiced making them a harder target. Now a large company like Lockheed Martin deals with a lot of third party vendors which depending on the reconnaissance I conduct I can choose one that does not adhere to security principles that a larger company would. Let us say Lockheed Martin utilizes a third party for their shred. A well-established shred policy is very important to a company trying to reduce the possibility of losing critical information. Critical information is any information that is not classified, sensitive or requires any special type of storage. Critical information is all of the above, critical information is information if put together with the right information can cause damage to a company. Critical information can be different depending on the type of service or product you provide. Each section will create a critical information list (CILs) and post

it near their workstation so they are reminded about what can and cannot be released. Critical information should be shredded; there are three types of shred; Strip shred, crosscut shred and micro shred, micro shred is preferred and recommended. Having a third party shred services creates issues due to not knowing how your information is going to be disposed of. Now I don’t recommend this practice for a company like Lockheed Martin or Northrup Grumman due to the US proprietary technology.

Living in Kansas I feel our critical infrastructure is at risk because we have not implemented certain security measures recommended by the Department of Homeland Security. Our Supervisory Control and Data Acquisition (SCADA) are at risk by physical and IT adversaries. I think this gap in information sharing is a serious issues involving our critical infrastructure. (Rashid, 21012) Our utility system and power grids are running on a system that that’s almost 30 years old and was only suppose to last 40. These systems are old and have numerous vulnerabilities which need to be mitigated soon before we find ourselves in the dark ages. To give you an example of how easy it was to bring down the Iran nuclear power plant and send them back a couple of years. It took a simple thumb drive that was plugged into their Supervisory Control and Data Acquisition system. It didn’t take any special operators or high tech equipment, just a thumb drive loaded with malicious code. The vulnerabilities that excess within SCADA systems since there so old is unlike regular operating systems like windows or MACs. These systems cannot be taken off line or re-booted, they require to be running 24 hours a day 7 days a week. The issues SCADA faces are unlike other systems, when a SCADA system are compromised it indicates a valve is malfunctioning or not closing. The virus at the Iran power plant overheated the system almost causing a meltdown.

These are gaps in information sharing that the Department of Homeland Security aren’t taking care of. I covered information that Janet Napolitano said earlier about small businesses needed to reduce the amount of barriers allowing government entities more access to there information or systems. I feel the Department of Homeland Security fails to communicate with smaller businesses.

I feel the Department of Homeland Security needs to establish a point of contact in all major cities allowing small businesses to get information. Depending on the service or product the company offers will dictate how much assistance that small business will receive. I understand the Department of Homeland security have their hands full with other obligations and this might not be an option for them. Another recommendation is having individuals like myself who have degrees in security administration help those small businesses in need. With schools needing security to reduce the risk of active shooters, cyber bulling and drug use, having someone with direct access to the Department of Homeland Securitys tools and resources can help them plan, collaborate and reduce risk in every state, city and neighborhood.

Conclusion

In closing I’ve discussed the gaps in information sharing from the department of Homeland Security in two specific areas. Our schools and small businesses are facing threats that could potentially be devastating to our public school system and critical infrastructure. I covered how FEMA has a great lessons learned website offering numerous tools and resources to help any company small or big reduce risk or assist in emergency planning. The site offers up to date information concerning all agencies under the Department of Homeland Security to include the Coast Guard, Customs and Borders Patrol and Immigration and Custom Enforcement. The Department of Homeland security also has the Federal Emergency Management Agency which responds to all natural disasters or any other incident that requires some type of relief. I know this is going to be an uphill battle to change the way information is shared, but with persistence and drive hopefully we can change the way information is shared.

Works cited

AAR/IP. (2011). After Action Report for Active Shooter Functional Exercise. Orange: Chapmen University.

Agency, F. E. (2012, September 16). Lesson Learned Information Sharing . Retrieved from Federal Emergency Managment Agency: https://www.llis.dhs.gov/member/home.do

ARA. (2012, September 10). Are small businesses protecting themselves from a data breach? Retrieved from Mysuburbanlife.com: http://www.mysuburbanlife.com/westmont/community/blogs/biz-bits/x2131921425/Are-small-businesses-protecting-themselves-from-a-data-breach

Greenstien, R. (2005, September 19). Katrina Relief and Federal Spending and Deficits . Retrieved from Center on Budget and Policy priorities: http://www.cbpp.org/cms/?fa=view&id=534

Kamien, D. G. (2006). The Mcgraw-Hill Homeland security handbook. New York: professional Publishing.

Rashid, F. Y. (21012, Feburary 12). State of SCADA Security Worries Researchers. Retrieved from EWeek.com: http://www.eweek.com/c/a/Security/State-of-SCADA-Security-Worry-Researchers-234517/

Walters, P. (2012, September 10). Napolitano: Cooperation needed on cybersecurity. Retrieved from SFGate: http://www.sfgate.com/news/article/Napolitano-Cooperation-needed-on-cybersecurity-3853020.php