Cyber Security & Disaster Resilience Proceedings
PNWER Annual Summit – Big Sky, Montana
July 13, 2015

John Gordnier, Consultant, Practical Solutions Intelligence Law
Eric Holdman, Director, Center for Disaster Resilience, PNWER
Randy Middlebrook, Protective Security Advisor, U.S. Department of Homeland Security

Speakers:
Eric Holdeman, Director, Center for Regional Disaster Security
Randy Middlebrook, Protective Security Advisor, U.S. Department of Homeland Security – Moderator
Brad Richy, Brigadier General, Director, Idaho Bureau of Homeland Security
Nathan Shoop, Physical Security Specialist/Information Security Audit, Zoot Enterprises, Inc

---

Emerging Threats in Cyber Security

Randy Middlebrook brought up the question of how our assets are being protected, not physical security but cyber security. He commented that cyber threats are becoming strong, fast, and impacting a wide range of infrastructures. DHS is looking to foster partnerships to help both sides. They need to be informed of the problem so that they can help you determine solutions. Protecting assets, management and resilience is lateral in government and in the private sector.

Brett stated that the biggest threat he's seen is the human factor, the apathy, denial, and complacency towards cyber security. People aren't following through or holding people accountable. The biggest challenge will be getting the people to work with the tools and programs already implemented to protect their assets.

Nathan Shoop commented that he's seeing everything on the private side being targeted; perimeters must be watched logically and physically, everything needs to be kept in house. Nathan feels the major problems are the technology problems, patching, attacks, and threats. But from the Private side point of view, time, balancing business and security, social engineering, properly training all of your admin, etc. is also a big problem. Everyone wants a secure business but there's also a need to make money and that is a hard line and a tough decision to make every day. Time and training can be working against us. Outside agencies can give private sectors heads up on what's coming and what's going on. Both sides need to always be trying to gather as much information as possible.

Brad Richy stated that personal and business information is being lost, that it's not a question if they have your identity, it's when they're going to use it. Cyber hazards

need to be included in an all hazard approach. He then addressed the question of what makes cyber hazard comparable to other hazards. He replied that there was a time that there were excessive travelers coming through Idaho that over overwhelmed the cell service and thus 911 lines weren't operating correctly. Cyber security brings in the ability to know these issues are going on, it allows gov to communicate on other hazards, taking an all hazards approach. The ability to shut down water supply, electrical supply, etc. all come from cyber disaster, the ability to do that is there and server protection is necessary for that, making cyber an all hazard approach. Looking into the industrial system, all of the automatic systems in your cars can be hacked or affected, what if it's not on star on the other end and you don't know. Working with Micron technology, it's going worldwide, manage and maintain a system. Sharing information, building relationships, growing connections and workshops to get together and talk about the problems in the region and how to prevent them. It's not a question of if. For the state of Idaho, they've recognized the need to get together and work more, expand communication, and get people together to talk about compliance, governance, keeping up to date, educating.

State senator of MT/Prof in IT Iron Corp Labs asked about data level encryption because it seems solutions are digging deeper moats and building bigger walls and trying to figure out how people cracked the codes instead of trying to change the data itself.

Nathan then said it comes down to people developing the software and having the proper coding practices. That is a huge issue, JAVAS and OS's have a lot of vulnerabilities, he then said people are there to find vulnerabilities and people working to code better.

Eric commented on organizations getting better at locking down data and people having the ability to communicate behind the iron wall. Commented on the development of building a system to create better security.

Brett commented on Trojan Horses being used to break through the cyber walls, the person leaving the computer logged in or not paying attention to people not supposed to be around their information. In his experience, there are sharp IT folks who work to build better walls but there's the people who blindly put records at risk, and no one is placing consequences on these people who are opening doors wide open for these people and this poor behavior. He said that employers aren't watching people, allowing them to open up the chance to hack. Time and training issues put all of the coding work to waste. A good password and basic rules for protection could fix this.

Jeff Douglas seconded the opinion, there is a culture of resistance to go into this system. Change management has to be well synchronized and pushed and constant ongoing discipline.

Gail Tarleton commented on people not have a suspicion of risk viewpoint. Interested in General's comment about ideas toward legislative work to help a gov declare a state of emergency around a data security breach. With the health care exchange, massive amounts of public data are a part of this and we're aware of the nature of the risk but we aren't putting in the legislative agenda to help them declare an emergency and a procedure to go about that. She asked if we have something in the works for that type of issue.

Brad replied that most states are behind on developing a plan, but Idaho has started crafting an emergency response plan. State network is addressed but it's a real challenge. When you think about the vulnerability of being unable to operate on your own system because the FBI or secret service has to come in and run forensics on your system, what is that vulnerability and how much with that vulnerability cost you? You have to evaluate your own system.

Randy commented on computer emergency response teams and having a suite of tools to address your security vulnerability.

Matt Reilly commented on the universities, and being ahead on communication of incidence and having national systems to share information and how to respond. They take in a lot of info to protect but also have a view of openness and sharing creating a unique challenge for universities. Commented on using the community to overcome the challenges and using a group in the northwest to do trainings, community building and working together.

Brad added on internal control, who is allowed what access. The universities have all these attendees and it's a real challenge to keep the info protected.

John Gordnier added to think about the way institutions approach privacy; there's privacy notices. You're carrying the privacy of your institution with you whenever you login to any system, iPhone, computer etc. Private and public need to look more at institutional privacy concerns and not just personal concerns. A lot of employees don't understand that they take some of the company home every night. There's a dimension of rethinking privacy from a new standpoint, employees are a huge privacy risk at all times.

Eric brought up who are you going to call when you have a breach? Who and when should you call? You don't want to announce it, but you want to be able to shut down the system. There's a transparency problem, if you've known why take so long to address? When to inform law enforcement, customers, vendors, general public?

Randy responded with: you find out there's a breach, and we can't stop it. From the exercises they have done, you should determine your FBI contact for cyber security and breach. Reach out to them to allow them to help you determine who to involve and how to stop it and prevent it from getting worse. They will be able to help you

over the phone right away. But there is a ton of work to be done in that area, keeping issues private but stopping the attack and addressing the problem.

Brad added that Idaho recently discovered an intrusion into the system and they don't know exactly how far back they have to go to evaluate what has been taken. It happened on t the classified side which brought of the issue of how to notify someone without the clearance of a classified breach. Every state has a fusion center, working with them when the alert was sent to them, but now who to go to? Went back to DHS who came up with information on the unclassified but official use side to determine what agency and a few details, have them then check their logs and how their system was operating on those days. Go back into the system and evaluate the system 24/7 to determine when the breach may have happened, it gets overwhelming but with outside help it can be determined. It's a huge challenge for everyone out there.

Deborah Meyers asked about the importance of the private sector and notifying, what you say now that there's been a breach of 21 million peoples' information. If a private sector, why go to the federal gov if they allowed the intrusion and didn't know how to counter act it? How do you deal with skepticism and gain confidence?

Randy commented on the breach and if you have anyone tell you they're failsafe they're lying because that's not the case. There was a state gov. who asked his state security officer about the state's security and he told the gov. that they weren't protected from a massive breach and that could happen. If you try to protect everything you protect nothing. It's a risk management game, with what's going on to try to keep up, you aren't going to. Gov tries to pick up successful hackers to turn and help us. You just can't protect everything. They were working on that breach for years and years, that doesn't happen in a day. It takes a lot of planning on both sides.

Nathan commented on the gov. having more access than we have, they have more tools that private sectors don't have. They have resources.

Margaret Hodges asked where we're seeing these breaches manifesting in being used and what is being breached. How are we seeing the stolen information playing out in the world?

Brad responded with four types of attacks: data, political annoyance type of attack (like in Ferguson), critical infrastructure, and corporate espionage. Each type comes with its own applications, data is biggest for them. People share their personal information on Facebook every day, your handing out that information. It's no longer personal information. It isn't hard to get social numbers, they say if your passwords are less than 12 characters, they can get into your information.

Drones, Body Cameras & the Law

John commented on body cameras, having the videos as public records is dangerous, they're going to be utilized and they can be altered. They can be used frame by frame to compare actions to policies and proper use of force. If you're going to use body Cameras, think about circumstances and consider polies and procedures to address how that body camera does or doesn't relate to your policies. But folks on the other side have discovered the GoPro. He continued with the idea that the government's body camera will be countered by the Go Pro on the other side of the civil disturbance. Before you decide they will help you, understand that there's huge downsides and you need to explore all those downsides to educate your people on how to use them.
Gael Tarleton stated concern in making sure agencies are estimating the costs of this.
John replied that agencies will always underestimate.
Purge is an enormous problem. You've got to look at and demand that people who take this info have a robust purge policy that you're in control of.
Safety is expensive but can you afford not to take it seriously? If you're going to look at costs you have to consider the costs of inaction as well, that could be so much higher.
Nathan asked about how data is being purged.
John responded that nothing is guaranteed. Know who is in charge of your information, as your people, bring in an outside contractor. Law enforcement can't investigate cybersecurity without outside help.
Canadian professor stated that he's being instructed not to use certain metadata in us jurisdiction, asked to move outside of certain programs like cloud and dropbox. Cloud services for university environments, potential misunderstandings that need to be cleared up, avoiding myths and misperceptions. Using the first task force call to clear up misperceptions and myths between countries.
Brett commented that permission and ability are two different things, so with these myths, the policies may not allow it but that doesn't mean that people who have the ability won't act on that ability.
John added the need to understand metadata, the three how issue. How public and private collect data, how long you have it, how you exchange it/how you use it.
John then stated that everyone's phones and cars and Facebooks are a nonstop record of where you are and what you're doing, GPS is creating that ability. Causing illegal evidence because of accessing the information without a warrant. Accessing information unrelated to illegal activity, violation of privacy. Iphones are creating a need for exploration into privacy boundaries and how they apply and the possibility of an intermediary privacy. The courts don't know where that privacy is yet, it falls between total privacy and total lack of privacy. How do you deal with it? How do you deal with our personal and protect your systems with all of this. The courts will have to begin looking into handling this intermediate privacy from a legal standpoint. The necessity of pinpointing necessary data and ignoring the other data.
Moving on to drones, John explained that they're gathering huge amounts of data most of which about people who aren't the subject that you're interested in. What do you do with all of that excess data? He directed attention to his handout. Why are drones so scary? You can equip them with anything, they can stay in one spot,

photograph, infrared, arm them. The city of Seattle police bought two drones and flying them. Seattle no longer has those drones because they didn't inform anyone that they had them. LAPD bough the drones. Drone policy – each entities on both sides of the border is going to be interested in drones. There's great uses for drones like to survey rail lines or check agriculture, but there's huge privacy concerns here. If you're going to fly a drone over property you have to get consent. Huge hunting and fishing issues, hunters using drones to track game, or anti using a beeper to scare of game so it can't be hunted. Idaho has some drone laws, UT, WA, or, MT, and they're all different laws, and we need some effort to bring those laws together. He brought up the questions of is it better for state to wait for judiciary to resolve issues? No, the legislative side needs to start in on this, get your lawyers privacy educated.
Eric brought up redaction of video, who's editing that video? With this, always, have a third party observer preferable who the court has sworn to talk about how it was redacted. When you provide redacted tape to a news medium, print or TV, make very sure that you know exactly what you disclosed and exactly what you didn't and be prepared to defend what you didn't disclose and why. Sometimes you may find that it's better to disclose that you redacted.
John requested that PNWER do the following:
Send out copy of power point to attendants.
Send out article/handout – didn't have enough copies

Canadian Senate Report on Terrorism

Daniel Lang discussed how the Canadian government is using the intelligence committee to get an overview of the terrorist threats present in Canada. There was some conversation in respect to militancy left over from air India bombing and fundamentalist ideology that is becoming more evident. The threat was there but manageable. It was reported that they lost a soldier, two days later they experience the attack on parliament hill and lost one other. That was the setting that started the course of hearing. There was 318 Canadians who were involved directly and indirectly in these terrorist threats/activities. Interest in other countries coming in and financing indirect the cause of radicalization. Also told that fin track had identified 683 actual transaction where financing had been involved in terrorism activities. Also told by revenue agency that there had been charitable agencies who lost charitable status for being involved in terrorist activities. There were very few, if any, prosecutions taking place, causing a great deal of concern. Canada has gone through a major rewrite of legislation and what kind of authorities agencies have been given to be able to do the jobs we need them to do. Legislation was brought before parliament to direct attention towards cyber threat activity so law enforcement can do the job they're asked to do. Daniel commented then that Canada has discovered that they're facing a political religions movement, an ideology pushing these individuals to do what they're doing. There has to be person to person influence over some period of time to where they may move on into other areas that brings them past radicalization to being a terrorist. This person to person influence needs to be confronted and the real reason why they're doing this needs to

be determined. The report brings forward recommendations to denounce these types of ideologies and teachings and prepares Canada to turn their backs on those people.

Action Items

Form a regional cyber task force made up of cyber planning leads from each state and providence in the PNWER region, with the purpose of sharing best practices in cyber resilience across jurisdictional boundaries.

Brett wants an action item to address the social effect and making the public and employees take it as seriously as they do fires or floods, education and outreach to inform how cyber can cost lives and has life threatening implications.

Host a regular call with the cyber task force in the fall of 2015