The National Cybersecurity Preparedness Consortium

Gregory White, Ph.D.
UTSA/CIAS
greg.white@utsa.edu
210-458-2166
October 2013
Center at The University of Texas at San Antonio

- Small, agile and non-profit, founded in 2001

Focus areas

- Cyber Security Training

UTSA is an NSA / DHS National Center of Academic Excellence in Information Assurance Education with security programs and courses in the colleges of Business, Science, and Engineering.
What’s the issue?

- Cybersecurity is a growing concern for the nation.
  - Increased number of attacks
  - Potential for cyber terrorist attacks growing
  - Incidents at the state and local levels on the rise

- Similar to physical attacks, when an event occurs, while it may be viewed as a national incident, individuals at the state and local levels need to be prepared to respond.

- States and local communities are NOT prepared with viable and sustainable cyber security programs.
“Power grid vulnerable to attack, report warns; Experts: U.S. needs to act now to protect infrastructure”
USA Today; McLean, Va.; Tim Friend Jun 25, 2002

“Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system”

“…talented hackers in many parts of the world are willing to peddle their expertise for the right price or political cause . . . We have evidence of Russian hackers selling their skills to radical Islamic groups”
“The Battle Against Cyber Terror”, Network World, 29 November 2004
Attacks are Not Limited to Attacks on the Nation

Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen  March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin’s High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership’s four Austin-area lots.

“We initially dismissed it as mechanical failure,” says Texas Auto Center manager Martin Garcia. “We started having a rash of up to a hundred customers at one time complaining. Some customers complained of the horns going off in the middle of the night. The only option they had was to remove the battery.”

The dealership used a system called Webtech Plus as an alternative to repossessing vehicles that haven’t been paid for. Operated by Cleveland-based Pay Technologies, the system lets car dealers install a small black box under vehicle dashboards that responds to commands issued through a central website, and relayed over a wireless pager network. The dealer can disable a car’s ignition system, or trigger the horn to begin honking, as a reminder that a payment is due. The system will not stop a running vehicle.
2009 Virus hit Houston, shut down court system

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

2009 Fiber Optic Cable cut in Silicon Valley
**2009 State of Virginia, extortion attempt**

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

“For $10 million, I will gladly send along the password. You have 7 days to decide. If by the end of 7 days, you decide not to pony up, I’ll go ahead and put this baby out on the market and accept the highest bid.”
FBI acknowledges more SCADA attacks, increases cyber budget

Join thousands of others, and sign-up for Naked Security's newsletter

by Chester Wisniewski on December 13, 2011 | Comments (4)
FILED UNDER: Featured, Law & order, Vulnerability

At a recent security conference Michael Welch, the deputy assistant director of the FBI's Cyber Division, gave a speech where he discussed the issue of SCADA security.

Information Age magazine reported on his speech and quoted Welch as saying:

"We just had a circumstance where we had three cities, one of them a major city within the US, where you had several hackers that had made their way into SCADA systems within the city,"

We don't know which cities Welch is referring to, but this does bring more light to a subject that has been mired in confusion of late.

Many argued that the security of SCADA systems was being exaggerated after it became public that the water treatment attack in Springfield, IL was a false alarm.

That of course ignores the attack by proF on the City of South Houston's systems and these other three referred to by Welch.

It's great that Welch acknowledges the work we have to do in this area and even went so far as to suggest the FBI will double the size of their Cyber division in the next 12 to 18 months.

Sound too good to be true? Then it probably is.

A story on PoliceLedintelligencer.com shows the FBI's budget for Cyber will increase by $19.6 million, or approximately 12 percent.

The majority of the funding increase will be used to expand their operation from 8 hours/6 days to 24 hours/7 days.

They even explained this to Congress, justifying their need for the funds.
Incidents Impacting States and Communities

Anonymous attack on the City of Orlando (June 2011)

The computer hacker group Anonymous — credited with crashing the websites of Visa and MasterCard in support of Wikileaks — launched what it called "Operation Orlando" on Tuesday, disabling a tourism website and the mayor's own campaign site.

In news releases and emails to the Orlando Sentinel, the loose-knit group issued a "declaration of war" and promised to bring down a different Orlando-related website every day. One hacker told the Orlando Sentinel the group may target Orlando police officers, state lawmakers and the Florida Democratic Party.

Incidents Impacting States and Communities

2012 Data Breach in South Carolina

Data breach at the South Carolina Department of Revenue exposed millions of state taxpayers to identity theft.

- 3.8 million Social Security numbers, 3.3 million bank account numbers and information for nearly 700,000 businesses stolen
- Occurred after a Department of Revenue employee opened a phishing email giving the hacker access to the department's data system
- During a period of weeks hacker scoured the department's system by remote access then, over a two-day period zipped 74.7 gigabytes of data which was then downloaded.

State officials learned of the breach Oct. 10, 2012 from the U.S. Secret Service

Cost so far is $25 million, including $12 million going to Experian to cover a year of state-paid credit monitoring.
But why is Cyber security a Community Issue?

Would your community’s LE and Emergency Management personnel know the significance of these images?
Possible War Driving

During a routine stop for speeding, a police officer notices the occupants of a truck that was stopped have laptops and what appears to be oversized antennas mounted on the vehicle and connected to the laptops. When questioned about the equipment, the occupants (two males in their mid 20s) reply that the equipment is “just computer stuff”. The occupants agree to let the officer search the vehicle, but the officer does not find anything illegal – just handheld global positioning systems and maps of the community and surrounding area. They were driving around facilities owned by the local power company.

Would the State EOC want to know about this?
What about now?

Saturday, 15 April 2006, 1:40 p.m.  
(Dallas Police Department)  
Possible War Driving

During a routine stop for speeding, a police officer notices the occupants of a truck that was stopped have laptops and what appears to be oversized antennas mounted on the vehicle and connected to the laptops. When questioned about the equipment, the occupants (two males in their mid 20s) reply that the equipment is “just computer stuff”. The occupants agree to let the officer search the vehicle, but the officer does not find anything illegal - just handheld global positioning systems and maps of the community and surrounding area. They were driving around facilities owned by the local power company.

Would the State EOC want to know about this?
Saturday, 15 April 2006, 1:40 p.m.
(Plano Police Department)
Possible War Driving

During a routine stop for speeding, a police officer notices the occupants of a truck that was stopped have laptops and what appears to be oversized antennas mounted on the vehicle and connected to the laptops. When questioned about the equipment, the occupants (two males in their mid 20s) reply that the equipment is “just computer stuff”. The occupants agree to let the officer search the vehicle, but the officer does not find anything illegal - just handheld global positioning systems and maps of the community and surrounding area. They were driving around facilities owned by the local power company.

Would the State EOC want to know about this?
If you could step back and view what is occurring around the state – would you be interested if you suddenly could plot all of these and similar occurrences?

Does this now paint a picture that you’d be interested in seeing?

Friday, 14 April
Saturday, 15 April
Monday, 17 April
The National Cybersecurity Preparedness Consortium (NCPC) has been funded by the Department of Homeland Security under a Competitive Training Grant.

- It will address cyber security issues in states and communities.
- It is designed to be a “Grass Roots” program that will link with and assist in national cyber security programs.
- It will coordinate with efforts in other disaster fields with the National Domestic Preparedness Consortium and the Rural Domestic Preparedness Consortium.

The goal is to help states and communities establish viable and sustainable cyber security programs.
Who is Part of the Consortium?

- Initial membership includes universities with existing cyber security exercise/training relationships with DHS
  - Proven track records and existing programs
    - Work already underway, no long lead time needed to get started
  - Initially, the Universities included are:
    - The University of Texas at San Antonio
    - Texas A&M University System (TEEX)
    - The University of Arkansas System Criminal Justice Institute
    - The University of Memphis
    - Norwich University
  - Additional interested universities may be added to provide additional capabilities needed by the consortium.
The Community Cyber Security Maturity Model (CCSMM)

- Consortium organized around the CCSMM.
- Based on 11 years of working with states, communities, and sectors to build cyber security programs.

The model is designed to:

- Provide a **yardstick** to measure a community’s current cyber security status;
- Provide a **roadmap** for states to improve their current cyber security status;
- Serve as a **common point of reference** for individuals in different states and communities to discuss ongoing efforts to improve their cyber security status.
Adding to the Model

- All of the resources needed to implement the CCSMM have not yet been developed.
- The consortium will look for existing programs and resources that can become “part of the solution”.
  - The cyber security problem is huge, as is illustrated by the size of the CCSMM.
  - When appropriate, the consortium can be expanded to incorporate entities with unique capabilities that supply a solution to some aspect of the model.
  - Partnerships can be established with organizations that have an answer to some aspect of the model and that have resources that can assist states and communities.
    - A good example of a potential partner is the MS-ISAC.
Goal for the Nation

To bring states, territories and communities to a minimally acceptable level of cyber security preparedness.

This equates to Level 4 of the Community Cyber Security Maturity Model

This will be accomplished through a coordinated effort between states, communities, and the NCPC.

The NCPC will become a source of training, exercises, tools, and resources that states, territories, and communities need.
Why Level 4?

Level 4 is the point at which communities and states / Territories have established a program to actively assess their on-going cyber security status and have integrated cyber security with other emergency operations.

A community at level 4 has the following characteristics:

- Leaders and organizations promote awareness; citizens are aware of cyber security issues.
- A formal info sharing and analysis, internal and external to the community exists; A formal local fusion and metrics program established.
- Autonomous cyber exercises with assessments of formal info sharing/local fusion are conducted involving live play/assessments.
- Cyber is integrated in COOP; mentor externals on COOP integration; formal blended incident response and recovery program exists.
Cyberterrorism Defense Initiative (CDI)

Participants Trained

- AR: 202
- CA: 533
- CO: 110
- CT: 39
- DE: 52
- FL: 258
- GA: 122
- HI: 69
- IA: 38
- ID: 28
- IL: 76
- IN: 105
- KS: 32
- LA: 29
- ME: 50
- MD: 97
- MA: 94
- MI: 34
- MN: 30
- MS: 40
- MO: 28
- MT: 40
- NE: 30
- NV: 54
- NH: 29
- NJ: 85
- NM: 49
- NY: 367
- NC: 180
- ND: 20
- OH: 142
- OR: 107
- PA: 67
- PR: 52
- RI: 29
- SC: 32
- SD: 28
- TN: 71
- TX: 509
- UT: 202
- VA: 150
- WA: 160
- WV: 45
- WI: 30
- WY: 12

[Map showing completed training and exercises]
Questions?

The National Cybersecurity Preparedness Consortium

Gregory B. White, Ph.D.
Director
Center for Infrastructure Assurance and Security and Security (CIAS)
The University of Texas at San Antonio
greg.white@utsa.edu
210-458-2166