WWW
(WorldWideWeapon): What to Do About Cyber Crime

Moderator: Jerry Dike
DMV Consultant
jldike@aol.com  512-751-0574

Tuesday, Aug. 26, 11-12 a.m.
INTERNET THEFT

1.2 billion + records stolen

Cyber Crime
Data Security, personal DMV data
Russian cyber crime gang reportedly hacks over a billion passwords  August, 2014

4.5 mill. hospital: Names, SSNs, Home addresses Birthdays Telephone nos.

Community Health Sys.  28 states
Brian: Sierra Snow Camping w/son
Dad: WW II Vet
10 Children
Dedicated to church and community

Brian like his dad

Charcoal by son
“Merchants” experiencing data breaches in the last 10 months:

Brian Soublet
March 22, 2014 blog report:

Five financial institutions confirmed a Master Card notice of compromised cards used for charges bearing the notation “California DMV INT.”
California DMV
Credit Card Breach

- DMV as the “common point.”
- Payment Card Industry Forensic Investigation (PFI)
- Law Enforcement Involvement
- Control Agency Reporting
- Remedial Actions Taken
- Results of the PFI
- COSTS
- Rules to Live By
Rules to Live By:

\[ P + D + R = S \]

- Prevention
- Detection
- Remediation
- Sleep at night.
Bill Britton, VP Parsons
At 50, Bill found his siblings.
Motor Vehicle Systems in Cyber Attacker Crosshairs

Bill Britton, VP Parsons
Bottom Line Up Front

- 20 years ago, the cyber security for AAMVA and your customers was not an issue.

- Today, highly integrated, computer and network reliant utilizing COTS architectures and open standards to communicate.

- Threats are real and carry a huge responsibility!
Cyber Attacks - the Numbers

Source: Symantec Internet Security Threat Report XVIII, April 2013
Cyber Crime

“DOJ brings first-ever cyber-espionage case against Chinese officials”

The Justice Department announced a first-of-its-kind criminal cyber-espionage case against Chinese military officials, accusing them of hacking into major U.S. companies to steal trade secrets...

...For the first time, we are exposing the faces and names behind the keyboards in Shanghai used to steal from American businesses...

Year 2014

- Pakistani Man Sentenced in Counterfeit Viagra® and Cialis® Case (May 2, 2014)
- Olathe Man Pleads Guilty To Computer Fraud (April 30, 2014)
- Alleged “Anonymous” Computer Hacker Charged with 18 Counts of Cyberstalking (April 29, 2014)
- Pennsylvania Man Who Sold Counterfeit Military Goods Sentenced to 21 Months In Prison (April 17, 2014)
- Jury Convicts Christian County, Kentucky Man For Stealing Trade Secrets From His Former Employer (April 16, 2014)
- Donna Man Charged with Hacking into Multiple Local Servers (April 10, 2014)
- Ridgeville Man Charged with Trafficking in Counterfeit Products (April 9, 2014)
- Defendant Called “The Hacker” by Law Enforcement Sentenced to 68 Months and Ordered to Forfeit over $470,000 (April 7, 2014)
- Local Man Sentenced on Computer Hacking Charges (March 27, 2014)
- Maine Resident Sentenced for Engaging in Cyber “Sextortion” of New Hampshire Victim (March 13, 2014)
- Springfield Man Pleads Guilty to Trafficking Counterfeit Goods (March 6, 2014)
- Sacramento Woman Gets 18 Months in Prison for Conspiracy to Traffic in Counterfeit Viagra and Cialis Via Craigslist (March 6, 2014)

“Hacking is far different than the type of intelligence gathering conducted by governments around the world, in that this involved cyber-espionage for the sheer purpose of gaining the commercial upper hand against U.S. businesses.”

– Attorney General (May 19, 2014)
The Threat

• **Who**
  – Insiders, Terrorists, or Activists
  – Hackers or Cyber Criminals
  – Nation- or State-Sponsored Cyber Actors

• **Specific Vectors**
  – Email or Instant Messages, Attachments
    • Spearfishing, Watering Hole,
  – Downloaded Files
  – Infected Web Pages
  – Pop-Up Windows
  – Social Media

• **Targets**
  – Critical Infrastructure
  – Social Engineering, Physical Insertion, Brute Force
  – Surveillance and Reconnaissance
  – Transfer - results covertly sent
  – Instruction Executed
“Approximately 67% of websites used to distribute malware were identified as legitimate, compromised websites.”

-Symantec ISTR 2014 Report
DMVs in the Crosshairs

- New York fake DMV Site


- Historical – Malware “embedded” in our systems
  – Chewbacca Trojan
Motor Vehicle Systems Targeted

- DMV Databases Driver Records
- Commercial Drivers License Information System
- Vehicle Registration Information
- Problem Driver Pointer System
- License Plate Reader Information
- National Motor Vehicle Title Information System (NMVTIS)
- Toll Collection Systems
- Personal Information
- Special Registration Data
What is on Your Site worth taking?

Source: A DMV Business Process – found documented on line
Anatomy of Session Hijacking
Economic Impact

• 40 million – The number of credit and debit cards thieves stole from Target between Nov. 27 and Dec. 15, 2013.
• 70 million – The number of records stolen that included the name, address, email address and phone number of Target shoppers.
• 46 – The percentage drop in profits at Target in the fourth quarter of 2013, compared with the year before.
• 200 million – Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards — about half of the total stolen in the Target breach.
• 100 million – The number of dollars Target says it will spend upgrading their payment terminals to support Chip-and-PIN enabled cards.
• 0 - The number of people in Chief Information Security Officer (CISO) or Chief Security Officer (CSO) jobs at Target (according to the AP).
• 18.00 – 35.70 - The median price range (in dollars) per card stolen from Target and resold on the black market (range covers median card price on Feb. 19, 2014 vs. Dec. 19, 2013, respectively).
• 1 million – 3 million – The estimated number of cards stolen from Target that were successfully sold on the black market and used for fraud before issuing banks got around to canceling the rest.
• 53.7 million – The income that hackers likely generated from the sale of 2 million cards stolen from Target and sold at the mid-range price of $26.85 (the median price between $18.00 and $35.70).
Cyber Security Regulatory Compliance

- **Directives**
  - Driver’s Privacy Protection Act, 18 U.S.C. §§ 2721-2725

- **Guidelines**
  - PCI-DSS - Payment Card Industry Data Security Standard
  - NIST 800-12 – An Introduction to Computer Security: The NIST Handbook
  - NIST 800-26 – Security Self-Assessment Guide for Information Technology Systems
  - NIST 800-53 – Generally Accepted Principles and Practices for Securing Information Technology Systems
  - ISA/IEC-62443 – Security for Industrial Automation and Control Systems
Key Security Attributes
Risk Based Approach to Cyber Security

- **Risk Management versus Risk Avoidance**
  - You can’t completely eliminate all risk
  - Apply resources where needed most
  - Accept some reasonable level of risk—residual risk

- **Build Security In—Don’t Bolt it On**
  - It costs far less to secure the system before it goes online
  - “Pay me now or pay me later”

- **Effective Cyber security is dynamic—not static**
  - Security needs to be checked periodically
  - New threats and vulnerabilities occur over time
  - Security needs to be checked periodically
  - New threats and vulnerabilities occur over time
Specifically What DMVs Should Be Doing

- Thorough assessment of your network, controls, and contingency plan

- Secure funding, develop process and policies for implementing a strong cyber profile

- Practice, practice, practice
  - Communication
  - Coordination
  - Conditions
Thank You

Primary Contact

- Bill Britton, VP – Cybersecurity Director
  - (703) 988-8512
  - bill.britton@parsons.com
FBI
Thank you for attending

Please record your attendance using the Sign In Sheet

Moderator:

Jerry Dike
jlddie@aol.com
DMV Consultant
512-751-0574
Questions for Presenters