From: Shwedo, Kevin A <Kevin.Shwedo@scdmv.net>
To: Pitts, TedTedPitts@gov.sc.gov
Stirling, BryanBryanStirling@gov.sc.gov
Soura, ChristianChristianSoura@gov.sc.gov
CC: Sanderson, Jeffrey RJeffrey.Sanderson@scdmv.net
Dolder, Rolf PRolf.Dolder@SCDMV.net
Date: 7/19/2013 6:59:34 PM
Subject: Network Assessment (For Official Use Only -- Sensitive Information)

Gentlemen - Per our previous conversation (sorry it took me a couple of weeks to get back with you – I wanted to ensure it contained sufficient detail to make the report meaningful) -- we conducted a thorough review of our network operations in light of the Department of revenue data breach. Our effort was designed to determine what we were doing prior to the breach and then compare those measures against those since the breach. Below is the summary.

Prior to the breach: The agency focus prior to the breach was in building a strong exterior firewall (dual firewalls referred to as the DMZ) against external penetration. We also had known security vulnerabilities in the areas of encryption and in our server farm. We began working on migration to an Oracle 11G data base well before the breach in order to give us data encryption capabilities for both data-at-rest and data-in-transit. Additionally, we purchased and installed an interior firewall segregating server data and precluding a hacker from running rampant behind the firewalls. All of this was necessary due to the amount of external firewall penetration attempts we were receiving worldwide. At one point we were averaging over 200 penetration attempts monthly causing us to begin collaboration with the local FBI cyber security team. We continue to provide the FBI team with a record (down to IP address level) of all external firewall penetration attempts.

Since the breach: Since the DOR breach, we have conducted a holistic threat assessment. From that assessment, we have concluded that our greatest threats in order are: internal security threat, mal-ware threat, and finally external firewall penetration. The possibility of a disgruntled employee, who already has access to the system) either manipulating or stealing the data is the most dangerous threat to our agency. In an order to combat this, we have greatly strengthened 'user roles' and are rapidly implementing biometrics into our system allowing us the ability to monitor to the individual employee level. We then assessed that a malware, bot, or some type of spy ware intrusion coming into our system via either e-mail or the internet was our second most likely threat. Although these types of attacks continue to grow in terms of sophistication, we used a two pronged defense. First, it was critical to educate and discipline our workforce on suspicious internet and e-mail activity. Secondly, we fielded and integrated into our system several software applications which not only detect but also alert our network operations center if these items have entered our network. Finally, we continue to upgrade our external firewall and

continue to monitor specific internet entry ports and report all suspicious activity to the FBI cyber team.

The future: Our enduring priority remains network security. We have made great progress in encryption of data and are to the point now where even if we were penetrated a hacker would be faced with multiple problems ranging from de-encrypting our data to getting out of our network. Our near term priorities include increasing our bandwidth to handle the increased traffic on our network and working to encrypt our wide area network.

SCDMV Security Infrastructure Prior to DOR Breach

Data Controls:

- Data access is role based
- Access for External Customers requires contracts, DPPA & PIRA's
- SSN data access is SSA Security Design Plan Compliant, has display and entry masked, has restricted DB access, audit table logging for DBA access and gives warning reports to DMV IG & Management
- Credit/Debit Card access restricted to DBA's, CC number are encrypted, access written to Audit Log, settlement file purged biweekly & sent via secure line
- Law Enforcement access controlled by SLED; all other access by SCDMV
- Web Services access via shared secret token
- WiTrans Table records all SCDMV online public & member services transactions
- DB accessed from Web/Services encrypted on Config file
- Reports generated to IG for new Customers, SSN changes and others
- MS Security Health Check by Microsoft

DMZ:

- Internet facing servers: ALIR, CVR, Webtest, Qflow/MVN, FTP with PGP encryp.

- Trustwave – Assists in Payment Card Industry Defined Security Standards (PCI DSS) compliance; Service package includes: external vulnerability scanning service & annual external & internal penetration tests

Remote Data Access Protection:

- VPN (IPSEC) with Radius authentication by Active Directory
- Firewall – Hardware Device: CISCO ASA
- Spam Filter – CISCO Ironport (weekly automatic updates); Scans all Email with quarantine and virus protection; blocks outbound email containing SSN's
- Internet Filter – IPRISM (protection from inside DMV out to Internet)
- CISCO MARS (Monitoring, Analysis and Reporting System) – provides analysis & reports of compiled files (logs) of internet activity
- FBI partnership to analyze attempted network intrusion attempts
- Enterprise Security Authorization is certificate based
- Phoenix domain access controlled by AD 2003 user,password &machine policies
- Operating Systems Software Updates and Patch Management
- End Point Protection – Trend migrated to Sophos

- CACTI SW – monitors & graphs bandwidth utilization
- NTOP SW – monitors data rates & Internet destinations of devices with IP addr.
- What's-Up-Gold – monitors traffic&connectivity (I/O) on key network devices
- Orion Network Mgt. SW – monitors, reports, analyzes devices/systems
- NetTracker – monitor web access, usage, and trends
- All network devices physically secure and protected from public access
- Access to rooms housing network devices policy & secure access controlled All elect. & environ. controls for areas housing network devices are secured & have automatic backup systems in place.

SCDMV Security Infrastructure After DOR Breach through July 2013

- State IG Risk Assessment
- Cisco Firewall upgrade
- Coordinated/Reported intrusion attempts with the FBI
- Implemented USB device policy
- Upgraded IronPort Spam filter
- Upgraded anti-virus software with Sophos deployment
- Tested/implemented process to push security upgrades to PC's/Servers
- DSIT Mandiant monitoring software install
- DSIT Security Information and Event Management install
- GFI LAN manager logging software installed on new network servers
- Mobile Device management install and implementation (Air Watch)
- Evaluated , tested and implemented Orion Network Management software
- Biometric rollout
- Installed remote Internet SW filters on over 200 laptops
- New strong password policy implemented
- Palo Alto Server firewalls installed
- New VPN HW/SW rollout with SecureAuth two factor authentication
- Installed MS SCCM 2012 Systems Center Configuration Manager
- Installed MS SCOM 2012 Systems Center Operations Manager
- Renamed 137 laptops
- Implemented process for required reading for security related information
- SSN Encryption
- Security Awareness training
- Installed Secure FTP Server and process

SCDMV Security Infrastructure August 2013 Forward

- Continue security enhancements identified internally
- Complete DeLoitte risk assessment scheduled for April 7, 2014

- Complete upgrade of network routers and implement encryption for transmissions across the network.
- Continue Trustwave compliance validation services:
    1. Monthly vulnerability scans
    2. Annual external penetration test
    3. Annual internal penetration test
    4. Resolve any Trustwave reported non-compliance issues from the above
- Complete Trustwave PCI compliance questionnaires and resolve any outstanding issues in order to obtain full PCI compliance
- Upgrade the MARS network logging and event reporting system
- Infrastructure upgrades to DMV data network architecture to increase bandwidth to support enhanced security features such as:
    - Real-time facial recognition,
    - Security awareness training,
    - Encryption across WAN,
    - Real-time State-to-State identity validation,
    - Central credential issuance and
    - Security camera installation and monitoring.

Rolf and JR --- GREAT JOB PULLING THIS TOGETHER!!!

Kevin A. Shwedo
Executive Director
South Carolina Department of Motor Vehicles
10311 Wilson Boulevard
Post Office Box 1498
Blythewood, South Carolina 29016

(O) 803-896-8925
(C) 803-609-4218

Your SCDMV -- Each a Role Model; Competent, Committed, Courteous!

"It's a GREAT day in South Carolina!"