From: Mayer, Doug
To: Patel, Swati <SwatiPatel@gov.sc.gov>
Pitts, Ted <TedPitts@gov.sc.gov>
Baker, Josh <JoshBaker@gov.sc.gov>
Soura, Christian <ChristianSoura@gov.sc.gov>
Date: 8/8/2013 5:10:37 PM
Subject: DOR Points

This was updated about two weeks ago. Please review it and make any needed edits. I need comments by 12:00 PM tomorrow.

Thanks.

In response to the breach of the South Carolina Department of Revenue's information technology (IT) infrastructure, the State of South Carolina has responded in the following ways:

Cabinet Agencies since the breach

- DOR is now fully encrypted for PII and PCI information and every cabinet agency now has 24/7 monitoring by DSIT.
- Every cabinet agency has looked at their internal structure and determined where information technology best fit (many like LLR and DOR have made the IT director a direct report to the Cabinet Director).
- Every cabinet agency has dedicated additional resources to fortify its system (many have encrypted additional fields, changed login access and the monitoring of that access).
- Every cabinet agency has strengthened controls on which partners have access to their system and to assure that they have appropriate security controls in place (DOR local government example).

State since the breach

- Over 3.8 million letter and email notifications have gone out to affected taxpayers to date.
- DSIT has taken the lead role as the coordinating entity in setting standard policies and procedures for state agencies.
- B&CB hired Delliotte to audit agencies and make recommendations to the state for holistic changes – S. C. patchwork structure is a big part of the problem.
- State is in the process of hiring for the first time a State Chief Information Security Officer.
- Issuing RFP today (July 30, 2013) with the Budget and Control Board to purchase long-term solutions for consumer protections.

Investigation

- Upon notification of a criminal attack via an IT Security breach at the South Carolina Department of Revenue (SCDOR), State and Federal Law Enforcement began an investigation to identify the source and impact of the breach.
- Mandiant, an independent IT firm, was engaged to plug the breach, conduct a forensic investigation,

and determine the causes.

- Outside experts specializing in consumer protection, data breaches, and public notification were hired once law enforcement signed-off on public release.

- Once an internal benchmark set by law enforcement was met in the investigation, State and Federal Law Enforcement cleared SCDOR and the Governor's Office to begin public notification.

- On October 26, 2012, the breach transitioned from a confidential law enforcement investigation to a public notification and protection process.

Public Notification / Consumer Protection

- Public notification began October 26th and has continued since. Initial notifications began through state entities such as the Governor's Office, SCDOR, the Lieutenant Governor's Office, and other agencies with non-state partners such as the Department of Defense, utility companies, AARP, and other associations to hold webinars, conference calls, e-blasts, and print messaging to association members and employees.

- In addition, Governor Haley immediately ordered three actions to help protect taxpayers:

  - Execution of a public notification plan that centered on frequent press events, public-private partnerships to notify consumers, and individual notifications about the breach and identity theft protection measures. This plan was developed during the initial investigation process.

  - Contracted with Experian to provide one year of active credit monitoring and lifetime fraud resolution to all affected taxpayers and one year of active credit monitoring and fraud resolution to all affected minors. With current levels of activations, Governor Haley's contract negotiation with Experian has saved the state over $9,000,000.00.

  - Established a Data Breach Assistance Team comprised of dedicated SCDOR and Governor's office staff with the assistance of the SC Consumer Protection agency to address public information needs and assist individuals with securing identity protection.

- Governor Haley announced free services from both Experian Business and Dun & Bradstreet available to SC businesses affected by the breach that alerts them to potential fraudulent activity.

- Individual notification via letter and email occurred between December 2012 and February 2013.

- On December 5, 2012, SCDOR provided all S.C. banks with information about affected taxpayers so they could notify their customers and put alerts on their bank accounts as needed.

- Governor Haley asked for a time extension for individuals and businesses to sign up for Experian identity protection services from January 31, 2013 to March 31, 2013.

- Dun & Bradstreet extended the deadline for S.C. businesses to sign-up for their services from January 31, 2013 to December 31, 2013.

Immediate Security Improvement

- On October 26, 2012, Governor Haley issued an Executive Order requiring that all state agencies cooperate with the Inspector General on a cabinet-wide evaluation of IT security preparedness.

- On November 1, 2012, Governor Haley held a cabinet meeting mandating that all cabinet agencies engage in public outreach to constituencies to promote public knowledge of the breach.

- On November 14, 2012, Governor Haley issued an Executive Order mandating all cabinet agencies cooperate with the Division of State Information Technology (DSIT) to secure their systems.

- The order mandated 24/7 monitoring and installation of forensic technology and Mandiant equipment. 24/7 monitoring is now complete, and all agencies have participated in monitoring training.

- On November 30, 2012, the IG issued an evaluation report titled “Current Situation & A Way Forward” based on agency self-assessments and security initiatives agencies had undertaken in the first month following the public announcement of the breach. Agencies continue to implement security recommendations received from Mandiant and the IG.

- After implementation of IG and Mandiant-recommended security patches, agencies have prioritized their security needs by threat and risk and implemented improvements as time and resources allow.

Long-term Security Implementation

- In March 2013, the Budget and Control Board engaged an external evaluator, Deloitte & Touche, to conduct a rolling evaluation of state agency IT systems, including cabinet and non-cabinet agencies. The three initial agencies selected are a representative sample of health, law enforcement, and administrative agencies.
- This process will continue over the next several years as Deloitte reviews more agencies and provides further system-wide recommendations, as the General Assembly provides financial resources to execute those recommendations, and as agencies move from implementation to active management of more secure systems.

- Governor Haley remains resolute in her position that the answer to long-term security and sustainability of South Carolina’s IT infrastructure will only be achieved through centralized IT management and procurement.

Douglass V. Mayer
Communications Director
Direct: 803-734-3146
Cell: 803-360-3285
dougmayer@gov.sc.gov