From: Taillon, Jeff
To: Godfrey, Rob <RobGodfrey@gov.sc.gov>
Taillon, Jeff <JeffTaillon@gov.sc.gov>
Hall, Taylor <TaylorHall@gov.sc.gov>
churchl@email.sc.edu <churchl@email.sc.edu>
Stirling, Bryan <BryanStirling@gov.sc.gov>
Haltiwanger, Katherine <KatherineHaltiwanger@gov.sc.gov>
LeMoine, Leigh <LeighLeMoine@gov.sc.gov>
Walls, Courtney <CourtneyWalls@gov.sc.gov>
Soura, Christian <ChristianSoura@gov.sc.gov>
Pitts, Ted <TedPitts@gov.sc.gov>
Baker, Josh <JoshBaker@gov.sc.gov>
Bondurant, Kate <KateBondurant@gov.sc.gov>
Walker, Madison <MadisonWalker@gov.sc.gov>
Veldran, Katherine <KatherineVeldran@gov.sc.gov>
Patel, Swati <SwatiPatel@gov.sc.gov>
Schimsa, Rebecca <RebeccaSchimsa@gov.sc.gov>
Date: 11/15/2012 10:59:38 AM
Subject: The State: SC Revenue Department 'believed ... safeguards were in place'

**The State:** SC Revenue Department ‘believed ... safeguards were in place’
http://www.thestate.com/2012/11/15/2520133/sc-revenue-department-believed.html#.UKTsXLRUPfg#storylink=cpy#storylink=cpy
By ANDREW SHAIN

The contractor hired by the S.C. Department of Revenue to provide computer security focused on the agency’s compliance with rules governing the handling of credit-card information, not stopping malicious programs such as those that hackers used to steal the tax records of 4.5 million S.C. consumers and businesses.

The Revenue Department also had its own computer security system that ran periodic scans for viruses and malware that hackers could use.

Neither security effort prevented nor detected the massive theft, conducted using state-approved credentials, until state officials learned of the breach from the Secret Service a month after the data was swiped.
computer crime

“As experts have stated, there is no way to be 100 percent secure. However, at the time of the breach, the department believed appropriate measures and safeguards were in place to protect taxpayer information,” Revenue Department spokeswoman Samantha Cheek said Wednesday.

While many questions remain about how the hacking occurred, Gov. Nikki Haley ordered more computer security Wednesday for the 16 state agencies that are part of her Cabinet.

The agencies will use the Division of State Information Technology’s computer network monitoring services, which can spot unusual uploads or downloads and malicious programs within minutes. The state will assign four employees to provide around-the-clock monitoring of computer systems – such as spotting inappropriate log-ins.

“What I have learned is that these international hackers are not going to do this from 9-to-5,” Haley said. “We need somebody in the office 24 hours a day monitoring those computers.”

Five Cabinet agencies will spend nearly $500,000 for equipment so their computer systems can be part of the Information Technology division’s 24/7 monitoring, the governor’s office said.

South Carolina also will get a program, nicknamed “The Hand” by Washington-based security firm Mandiant, that can shut down computers infected with viruses and malware or uploading large amounts of data. The cost for the $160,000 program will come from the U.S. Department of Homeland Security, Haley said.

Mandiant has a state contract, estimated to reach $500,000, to repair and investigate the hacking of the Revenue Department. The state also is paying for a public relations firm and outside legal advice at a cost expected to top $250,000.

In the past, state agencies have been able to decide on their own computer security measures. The state Information Technology division already works with 54 state agencies – about half the state’s total. Haley said she has encouraged other state agencies that are not under her control to follow her plan.

“This is my way of dealing with my (Hurricane) Hugo,” Haley said.

Before the cyber attack, the Revenue Department had partial state network monitoring but not at the computer struck by hackers. The agency did not use the state Information Technology division’s computer monitoring services because officials thought they were redundant of those being provided by Trustwave, a security contractor the Revenue Department has used since 2005 to ensure the agency could accept credit card payments, Cheek said.

The Revenue Department said Trustwave provides intrusion detection and vulnerability scans. The agency has spent $175,000 during the past three-plus years with the firm.

The department also uses two firewalls, periodic virus scanning, and web and email filtering as part of its security. Social Security numbers and other data were encrypted when in transit but were not encrypted when being stored in servers, where hackers struck, taking the information.

The Revenue Department began encrypting information, and started using state network monitoring and “The Hand” program soon after the state learned about the hacking on Oct. 10.

Haley hopes to release a report on the hacking investigation this week. Officials are unsure when taxpayers will know whose files were taken.

SC data theft help

Consumers: Sign up for one year of free credit monitoring and insurance, and lifetime ID theft-resolution services – protectmyid.com/scdor (use the code “scdor123”) or call (866) 578-5422.

Businesses: Sign up for free monitoring from Dun & Bradstreet Credibility Corp. – dandb.com/sc or (800) 279-9881 – or Experian – smartbusinessreports/southcarolina.

Additional steps

From the SC Department of Consumer Affairs

1. Place an initial fraud alert on your credit report. To place an initial fraud alert on your credit report, you only have to call one of the Credit Reporting Agencies (CRA) and it will notify the other two. This is a FREE service. Once you place the alert, you will receive notice that you can get one free copy of your credit report from each of the Credit Reporting Agencies (CRAs). See No. 3 below for phone numbers.

2. Place a security freeze on your report. You must call each of the CRAs to do this. It is FREE to place, thaw, and lift the freeze for SC Residents. Once you place the freeze, you will receive a PIN number you can use to thaw or lift the freeze. Make sure to keep it in a safe place. You can place the freeze online at the

addresses below or by calling the numbers listed in No. 3:

- freeze.equifax.com
- experian.com/freeze
- freeze.transunion.com

3. The phone numbers are the same to place a fraud alert and to place a security freeze on your credit report:

- Equifax: 800-525-6285
- TransUnion: 800-680-7289
- Experian: 888-397-3742

4. Perform these steps for any Social Security number you think might be affected. The fraud alert and security freeze are linked to your Social Security number, so each person in the household must place it separately.

5. Remember to track your finances. Always review your banking statements as soon as you receive them. Also review your credit report regularly. You are entitled to a free credit report from each one of the three major credit reporting agencies annually. You can obtain your report by visiting annualcreditreport.com or calling (877) 322-8228. Check your statements and credit report for unauthorized purchases/accounts and incorrect information.

6. For more information on protecting against ID Theft, including information on placing a security freeze, visit the SC Department of Consumer Affairs "Identity Theft Resources" webpage.

**Jeff Taillon**
(803) 734-5129|Direct Line
(803) 767-7653|Cell