From: Taillon, Jeff
To: Godfrey, Rob <RobGodfrey@gov.sc.gov>
Stirling, Bryan <BryanStirling@gov.sc.gov>
Taillon, Jeff <JeffTaillon@gov.sc.gov>
Date: 11/21/2012 10:23:48 AM
Subject: The State: Haley admits state failed to protect its residents

The State: Haley admits state failed to protect its residents
Tally of victims rises again; agency director Etter resigns
http://www.thestate.com/2012/11/21/2527941/haley-admits-state-failed-to-protect.html#storylink=cpy
By ANDREW SHAIN

Columbia, SC — As more South Carolinians learned that hackers hold their tax return data, Gov. Nikki Haley admitted Tuesday that the state did not do enough to protect their sensitive financial information and accepted the resignation of the agency director in the middle of the controversy.

"Could South Carolina have done a better job? Absolutely, or we would not be standing here," said Haley, who had insisted in the first days after revealing the cyber attack that nothing could have prevented the breach.

Hackers possess Social Security and other data belonging to 5.7 million people – 3.8 million taxpayers and their 1.9 million dependents, Haley said. The number of businesses affected has risen slightly to nearly 700,000. All of the stolen tax data dating back to 1998 was unencrypted.
haley-hacking

The theft at the S.C. Department of Revenue is the largest known hacking at a state agency nationwide, according to the San Diego-based Privacy Rights Clearinghouse, which has been collecting breach data since 2005.

Hackers took tax information only of people who filed returns electronically, Haley said. Taxpayers whose information was stolen will receive notification soon by letter or email, she said.

Thieves also have bank account information belonging to 3.3 million S.C. taxpayers, Haley said. The S.C. Banking Association has asked banks to step up surveillance for fraudulent activity and share news of attempts to drain accounts, said Fred Green, the group's president.

Hackers duped a revenue department employee to click on a link in an Aug. 13 email, according to a report from Mandiant, a Washington computer forensics firm hired by the state to investigate the incident. The link appeared to trigger a program to steal the employee's username and password. The crooks uploaded files on Sept. 13 and 14 after accessing the system eight times and stealing passwords of three other employees during the previous month, Mandiant said. The hackers used a virtual backdoor on Oct. 17, a week after the Secret Service alerted the state about the breach.

After saying soon after the attack that no one in state government should be blamed, the governor accepted the resignation of revenue department director Jim Etter. He will leave at the end of the year.

"Jim and I both agreed that we probably needed a new set of eyes on the Department of Revenue – one that looked at data in terms of securing it," Haley said.

Etter, who had no comment Tuesday, will be replaced by Bill Blume, director of the S.C. Public Employee Benefit Authority.

Still, Haley said the breach was not Etter's fault.

The governor, a frequent critic of federal policies, pointed to IRS rules that do not require encrypting taxpayer data in servers as part of the “cocktail for an attack.” IRS rules require encryption while transmitting data.

Haley sent a letter to the IRS asking the federal agency and all states to encrypt taxpayer data in servers. She called the IRS’s cyber-security standards outdated, a departure from when she said encrypting data was not an industry standard soon after revealing the breach on Oct. 26. The state is encrypting all data at the revenue department.

The IRS said in a statement Tuesday that it uses “a variety of safeguards – including encryption,” though the agency did not say if data in its servers are encrypted. The IRS said it is reviewing Haley’s letter.

Haley also blamed the breach on the revenue department not using a double-password to log-in and a computer system from the 1970s.

Some lawmakers said problems lie within state policy. S.C. Rep. Dwight Loftis, R-Greenville, said allowing state agencies to run their own technology operations creates turf wars that increased the likelihood of a massive breach.

“We’re just in the 19th century in technology in this state,” said Loftis, who has introduced bills to put all state agency computer work under one umbrella.

Haley said she will ask lawmakers to develop an emergency cyber-attack plan like the one the state uses for hurricanes. The plan would include unannounced tests of computer systems at state agencies.

“The Legislature and I can no longer allow us to have archaic data, archaic equipment and archaic systems that don’t protect the most sensitive of information for people of our state,” Haley said.

More than 843,000 people have enrolled to receive a free year of credit-report monitoring from Experian that is costing the state $12 million, the governor said.

But the crooks can use Social Security numbers, usually sold on the black market for $10 to $20 each, for years, identity theft experts said. Even information belonging to children can be used to give employers a valid number for a job or open credit-card accounts. Parents will have to monitor their children’s credit reports as well as their own.

“The Social Security number is the key to everything,” said Nikki Junker of the San Diego-based Identity Theft Resource Center.

What’s new

- S.C. Department of Revenue director Jim Etter resigned, effective at the end of the year.

- The state revealed how many dependents’ numbers were stolen – 1.9 million – and how many bank accounts numbers were taken – 3.3 million.

- Only those who filed tax returns electronically had their data stolen. People affected will get a letter or email soon.

TIMELINE

Over two months, hackers managed to gain access to the S.C. Department of Revenue computers and steal state tax data belonging to 6.4 million consumers and businesses. Mandiant, a Washington computer forensics firm hired by the state to investigate the incident, offered details Tuesday of how the hacking unfolded:

Aug. 13: Hackers send emails to several department employees with a link that contained malware. One employee clicks on the link unleashing a program that likely steals that person’s username and password.

Aug. 27 and 29, Sept. 1-4 and Sept. 11: Hackers log into the department remotely and introduce more programs to help in their theft. They try to steal all the department passwords but use those from three additional employees, including some who have wide access to the computer system. The hackers install a backdoor and perform reconnaissance into department servers and the system that handles credit-card payments.

Sept. 12: Hackers copy and create 23 database backup files and leave them in a directory.

Sept. 13-14: The databases are compressed into 14 smaller files and moved onto Internet. A 15th compressed file has an encrypted version of the department's data encryption key. The hackers delete the copies left on department computers.

Oct. 17: A week after the Secret Service informs the state about the breach, investigators find the backdoor when the hackers check their connection to a department server.

Oct. 19-20: The security holes are closed. Investigators report no sign that the hackers have tried to pry into the system since.

By the numbers

4

S.C. Department of Revenue employee accounts used in the hacking

4

Internet addresses the hackers used

12

Times between Aug. 27 and Oct. 17 that the department computer system was accessed

33

Pieces of malicious software and utilities used

44

Revenue department systems attacked

74.7

Gigabytes of data 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