The South Carolina Data Breach and the Failure to Encrypt

By Sharon D. Nelson, Esq. and John W. Simek

It is nothing short of astonishing that more than 75% of South Carolina's residents had their social security, credit card numbers and other personally identifiable information breached. News of the breach came in October, though it actually began in August. Who uncovered the breach? Usually it is the FBI, but this time it was the Secret Service that notified S.C. on October 10th.

How did the breach happen? Someone, as yet unknown, stole legitimate credentials from one of the 250 state employees with access to the South Carolina Department of Revenue (DOR) database.

Why was the attack so easy? Because (pulling our hair out here) the data was not encrypted. While this was horrific enough, the statements by S.C. governor Vikki Haley may have been more alarming. With 3.6 million of her citizens affected, Haley was in full defensive posture, saying that encryption was "complicated and cumbersome technology." Perhaps using an actual car key instead of pushing a button to start your car is cumbersome too? It just isn't that hard Governor.

No wonder we teach a seminar entitled "Encryption Made Simple." The fallacy that encryption is rocket science apparently will keep our data in danger of being purloined.

Haley leaked other dirty secrets when she said "The industry standard is that most Social Security numbers are not encrypted. A lot of banks don't encrypt. A lot of those (government) agencies you might think encrypt Social Security numbers actually don't . . . It's not just that this was a DOR situation, but an industry situation."

Well Governor Haley, you may have overstated the truth in your zeal to defend the indefensible. Today, encryption is fairly routine in any environment governed by the PCI-DSS (Payment Card Industry – Data Security Standard). While the governor may have been correct about state governments, it is hard to conceive of a bank not using encryption. And of course no specific examples were offered.

It wasn't just citizens that were impacted – businesses had their data breached as well. The attackers wasted no time in making use of their ill-gotten gains – not only for identity theft purposes but also state-sponsored attacks against manufacturers, the defense industry and other government agencies.

Why are we not getting the critical need for encryption? It certainly isn't because the need for encryption isn't clear. Even before the S.C. data breach, the Privacy Rights Clearinghouse identified 18 data breaches in October involving the compromise of tens of thousands of Social Security numbers.

One spot on comment came from industry expert Adrian Lane, the CTO of Securosis. He said, succinctly and accurately: "In most cases, encryption or other forms of obfuscation (masking, tokenization) can be done transparently to business operations and at a reasonable cost. It need not be complicated – but you have to actually invest some time and money to get it done, and that's how most states fail."

No doubt you will be shocked to learn that Governor Haley has said S.C. is now considering encryption as an option. Why is it that this always happens when all the horses have left the barn? Now we want to shut the door. Sigh. The state has agreed to pay for a year of real-time credit monitoring for anyone who signs up. It has also provided $1 million in insurance to pay for data breach investigations.

Governor Haley, who seems to suffer from chronic foot-in-mouth syndrome, has said, "This is a situation where a sophisticated, intelligent criminal got into a database and it's unbelievably creative how they did it." Really? Stealing credentials is not exactly unheard of. And leaving data wholly unprotected from access due to stolen credentials is reprehensible in the extreme. This incident wasn't just predictable – it was inevitable. Leaving data unprotected is an engraved invitation to criminals and state-sponsored hackers.

It is time for all governments and private sector entities to recognize that encryption's time has come in spades. Failure to encrypt personally identifiable data is almost certainly going to be deemed by the courts as per se gross negligence in the near future – and under some laws, now.

The authors are the President and Vice President of Sensei Enterprises, Inc., an information technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)