

The Senate Judiciary Committee on Thursday approved two personal data security bills that would establish federal standards for protecting data and reporting its loss. But security experts say that threats to personal data are evolving faster than our responses to them.

“The crooks are trying to find out how to better impersonate you on the Internet,” said Rick Kam, president of ID Experts, at a recent data security briefing hosted by TechAmerica.

Criminals are aggregating more information about individuals that, though innocuous in itself, could be used for fraud if correlated. They also are tapping new sources and types of data, including electronic medical records. The consequences can be dire, said Dan Steinberg, an associate with Booz-Allen Hamilton. The theft of personal data can create financial problems and interfere with the victim's ability to get health insurance and medical care.

The committee passed S. 139, the Data Breach Notification Act, introduced by Sen. Dianne Feinstein (D-Calif.), by a vote of 14 to 2, and S. 1490, the Personal Data Privacy and Security Act of 2009, introduced by Sen. Patrick J. Leahy (D-Vt.), with a vote of 11 to 5. The Data Breach Notification Act requires agencies and businesses doing interstate business to report any breach of personally identifiable information to the individuals compromised, except in instances when national security or law enforcement activities would be endangered, or if a risk analysis by the Secret Service shows there is little danger from the exposure. It allows civil enforcement by the U.S. and state attorneys general.

Leahy's bill would make theft of personal information liable to federal racketeering charges and prohibit concealment of the breaches, as well as require victim notification. Consumer reporting agencies also would have to be notified for breaches involving more than 5,000 individuals, and the Secret Service if more than 10,000 individuals are involved. It also would establish standards for safeguards to protect the security of sensitive personally identifiable information and impose upon civil penalties on businesses for violating them.

The U.S. Attorney General as well as state attorneys general could bring civil actions for violations. Committee approval does not ensure final passage by the full Senate. The Leahy bill

has been introduced in two previous Congresses and has twice made it out of the committee without being passed on the floor. Data breach notification already is federal policy under directives issued by the Office of Management and Budget (OMB) following the theft of a Veterans Affairs laptop with records on millions of individuals.

Since those OMB mandates, the IRS expanded its privacy activities from a single Privacy Office with seven persons to include an Office for Privacy, Information Protection and Data Security and an Online Fraud Detection and Prevention Office.

The new IRS privacy structure now includes at least 85 people, said Dianne Usry, deputy director for Incident Management in the Privacy, Information Protection and Data Security office. Her office examines breaches and does risk assessments, notifying victims when necessary and helping with credit monitoring, Usry said during the TechAmerica briefing. The office also analyzes breaches for trends and to identify needs for further loss prevention. The IRS has done "a lot of the right things" in notification and analysis, Kam said. "But unfortunately that's where the solution stops."

Organizations need to do a better job of not only protecting data, but of analyzing the resulting fraud so that the source of the misused data can be identified and its use stopped more quickly, he said. And while organizations are focusing on protecting traditional personally identifiable information, such as names, addresses and Social Security numbers, criminals are gathering other types of information as well.

"Crooks are stealing IP addresses, all types of digital attributes about you and your behavior," Kam said.

It is believed this information is being used to help them avoid analytic defenses used in online transactions to spot and avoid fraud. A crook spoofing the appropriate IP address and browser settings can have a better chance of avoiding detection.

"People are becoming more creative, with more strategies for combining information," said Steinberg.

Electronic health records can pose a special set of risks because the information is more personal than financial data, its misuse can be more difficult to spot, and bringing the integrity of records into doubt can threaten health care and coverage, endangering the health and even life of victims, he said. He said that security and privacy concerns have slowed the adoption of electronic health records.

The number of cases of misuse of such data so far is relatively small, but because individuals seldom see their own medical records, breaches probably are underreported. "The problem may be much larger than we know about," he said.

By William Jackson

www.mcpmag.com