the FORECASTER

Cybersecurity Experts Urge Diligence at Portland Conference

By William Hall | May 14, 2013

From a Maine nonprofit group's leak of confidential data in February, to the May 9 discovery that a worldwide gang of criminals stole $45 million by hacking into a database of prepaid debit cards, information security problems are a widespread concern these days.

A group of national experts is in Portland this week to discuss ways of dealing with cybercrime and other information-technology risks.

The 11th annual Excellence in Governance, Risk Management and Compliance Conference runs through Thursday at the Portland Regency Hotel. The meeting is expected to draw about 80 people from banking, insurance, health-care and other industries.

The conference is sponsored by NMI LLC of Kennebunkport, which was founded in 1990 as one of the first information security companies in the world, according to its website.

Dan Mitchell, a lawyer specializing in information security issues at the Bernstein Shur law firm, said there's good reason to be concerned.

While it's hard to quantify the incidence of cybercrime, he said, "my sense is that it's increasing. Any industry that handles electronic data for customers, not just credit cards, is at risk today."

Consumers and businesses exchange confidential information not only when people make purchases on the Web or use an ATM, but when data is shared routinely via text messaging, smartphone applications, GPS location services, social media and in many other forms and using many types of devices.

Security problems range from accidental leaks, to attempts to take over or vandalize corporate databases, to sophisticated cyberthefts such as the "massive, 21st-century bank heist" announced last week by the U.S. attorney for Brooklyn, N.Y.

In Portland, The Works Bakery on Temple Street was the target in January of a malware attack designed to gather personal information as customers swiped their credit or debit cards. Federal authorities advised customers to contact their banks immediately if they suspected their data had been compromised.

The problem with such warnings is that the damage is already done – while hackers or criminals have already moved on to another group of unsuspecting data users.

"We move so much information electronically that there are myriad ways it can be accessed," Mitchell said. "And there are a lot of different targets. Criminals look for 'soft' targets."

Denise Butler, a New Hampshire consultant speaking at the conference, said, "Web applications and mobile apps are acting more and more like PC apps. With devices being able to do more, there is much more opportunity for hackers."

Some victims aren't the target of crime, but merely of human error or technology glitches.

In Brunswick, nonprofit People Plus displayed a portion of its membership database – including names, donation amounts and home addresses – on its website for at least two weeks.

The posting was discovered by a reporter for The Forecaster, and was corrected within an hour after the group was notified.

And in Cumberland, the town recently was forced to change security procedures after the names and Social Security numbers of nearly 300 employees somehow ended up on the town website.

Despite incidents like these, there are steps consumers and businesses can take to protect themselves against the risk of a data breach.

Butler said users of smartphones and other mobile devices should make sure they're equipped with strong anti-virus programs and other protective software, just as home computers usually are. Passwords should only be sent in an encrypted form.

She also said people should frequently monitor their credit history and other records to look for fraudulent financial activity and identify theft.

Consumers may even want to get their credit and debit cards reissued regularly, to reduce the chance that thieves will get access to the accounts.

"I have my cards reissued every six months," Butler said. "I just feel more comfortable that way."

Businesses can take steps to prevent information security problems, even without large technology staffs, both Butler and Mitchell said.

For example, Mitchell said a small business might conduct its online transactions on a single, well-protected computer terminal rather than multiple machines – each of which could become a hacker's target.

And just as consumers should monitor the use of their financial accounts, businesses should monitor the use of their websites, according to Butler.

"There are lots of applications that track traffic, and businesses really need to know what's going on and ask themselves, 'Is this behavior unusual for the site?'" she said. "It's easy today to put up a site, but it's hard to protect it."

Dan Mitchell is a shareholder and member of Bernstein Shur's Business Law Practice Group and Data Security Team. He can be reached at 207 228-7202 or dmitchell@bernsteinshur.com.