Can data breaches be prevented? Congress and companies answer: For now, no.

By Melinda Henneberger, February 5 Washington Post

http://www.washingtonpost.com/business/economy/can-data-breaches-be-prevented-congresss-and-companies-answer-for-now-no/2014/02/05/94d607ae-8e9d-11e3-b46a-5a3d0d2130da_story.html?tid=hpModule_1728cf4a-8a79-11e2-98d9-3012c1cd8d1e

Executives from Target and Neiman Marcus still don't know how they could have better protected their customers from cybercriminals, they said at a congressional hearing Wednesday.

Asked exactly how recent attacks occurred, Target's John Mulligan answered: "We don't understand that today.'' The company is still investigating, said Mulligan, the company's chief financial officer and executive vice president, and "certainly from that there will be learnings."

Michael Kingston, the chief information officer of the Neiman Marcus Group, said, "We've not yet found any evidence of how hackers were able to infiltrate our network.'' The attack was "customized to evade detection'' and occurred "in real time, when the card was swiped" just milliseconds before being encrypted. The breaches prompted several congressional hearings and briefings; last week, Attorney General Eric H. Holder Jr. told the Senate Judiciary Committee that his agency is investigating them.

Wednesday's House hearing, "Can data breaches be prevented?," ran $3^{1}/_{2}$ hours, but the short answer was: No. That's despite the "hundreds of millions" Target spent trying, and the "tens of millions" Neiman's spent.

Again and again, company executives described how sophisticated cyberthieves are: "Very, very, very sophisticated,'' Kingston said. They use malware that deletes itself and cleans up all traces it was ever there.

American consumers, law enforcement officials said, make it pitifully easy for these masterminds. (Psst: They know, for example, that your password is likely to be "password.") The hackers exposed payment card information of some 1.1 million Neiman Marcus customers between July and October of last year, at 77 of 85 Neiman Marcus stores. Target was hit between Nov. 27 and Dec. 8, when the payment card information of 40 million customers and the personal contact information of 70 million more people was exposed. American banks aren't helping, either, by using old-fashioned magnetic-card strips designed in the '70s rather than more secure chip-based cards in use in Europe and much of the rest of the world. Starting next year, Target cards will use chips.

Still, "the notion companies are already doing everything they can is false,'' said Illinois Attorney General Lisa Madigan, who with her counterpart in Connecticut is probing the attacks on Target and Neiman Marcus. Specifically, she said, businesses often fail to encrypt data, or they keep data longer than they have to.

For now, there are no federal standards on cybersecurity or on how customers must be informed in the event of a breach. For years, Madigan said, states have been on the front lines, and “they are panicked and they are angered that companies are not doing more” to protect themselves.

Edith Ramirez, who chairs the Federal Trade Commission, also said, “Congress needs to act” to set federal standards and give the FTC authority to seek civil penalties. Meanwhile, “companies continue to make basic mistakes.”

Rep. Marsha Blackburn (R-Tenn.) accused Ramirez of “saying you want something” in terms of a federal standard without “giving specifics or examples of what people have failed to do,” or expanding on what requiring “reasonableness” would really mean in terms of protecting customers.

A few examples of failures to do that, Ramirez answered, would be the company that does not use strong passwords, encrypt data or update security patches.

Protecting against cyberattacks is “one of the few things Republicans and Democrats agree is a problem,’’ said Rep. Joe Barton (R-Tex.).

But, like lots of Americans, he wasn’t clear on the details of the attacks on Target and Neiman’s, asking executives about what “occurred when criminals came into stores and used credit cards that infected the systems at the point of purchase. I see a lot of blank looks here.”

That’s not how it happened, explained William Noonan, the agent in charge of the criminal investigations division of the Secret Service’s cyber-operations. Instead, “people infiltrated their computer networks and inserted malware code.’’

“Oh, I thought they came with a card,’’ Barton said.

Members of the subcommittee asked whether many cybercriminals were Americans. Those testifying answered that most were “transnational.”

“So, from outside the U.S.?” asked Rep. Billy Long (R-Mo.). Yup.

Rep. John Yarmuth (D-Ky.) asked a good question, wondering why some people who’d never shopped at Target had nevertheless received an e-mail stating that their information might have been compromised. “We very rarely do buy guest information,’’ Mulligan answered.

In other words, we’re all vulnerable. And maybe your new password shouldn’t be “nupassword.”