Looking for trouble

A proactive approach is best when it comes to protecting customer and corporate data

NICOELNINO / SHUTTERSTOCK.COM

by DAVID P. SCHULZ

When it comes to cybersecurity — as in protecting personal identification data and payment card particulars — retailers want consumers to know they have their backs. The challenges come in determining how to this to tell shoppers, and exactly how much to tell them.

Replaying all the scary things that can happen could be very off-putting and frighten shoppers away from the very merchants trying to educate the public, says Eric Cole, who served on the Commission for Cyber Security during the Obama administration.

Detailing the specific actions a retailer is taking to thwart potential identity thieves could also reveal too much information to the bad guys. "It provides hackers with a road map," says Cole, chief executive of Secure Anchor Consulting and author of the book Online Danger.

Rather than attempting to market cybersecurity efforts to the public, a better approach would be to implement policies and practices that show customers what is being done to protect them. "What I always say is that cybersecurity is not about doing crazy,

> "Security isn't about preventing attacks. It's about minimizing the damage when attacks do happen. And that requires you to actively look for ongoing breaches, even ones you don't know about."
>
> — Eric Cole

complex things," Cole says. "It is doing simple things in a consistent manner."

CONSUMER RESPONSIBILITY

Robust authentication and more and better verification are good starting points. By way of example, Cole says, he does a lot of online shopping, and "Every time I log in on a new device, they notify me and ask if it is really me."

Businesses that have put such precautions in place are doing something right. "You can assume that any retailer that has not yet had a breach has done a good job protecting customer information," he says. "Most individual companies are doing well."

He singles out Amazon.com for its security modeling, noting, "They've done a really good job protecting their information."

Consumers also hold some responsibility for their own security; while individuals swiping their cards had nothing to do with past data breaches, it's important that shoppers realize the role they themselves play.

"This is one point that I've been pushing for a while, and some people get upset with me when I say this," Cole says.

"Cybercrime has a high payoff and a very low risk, so this problem is going to get a lot worse before it gets better. You cannot rely on a third party to protect you."

One way retailers could make this point to their customers is reminding them not to respond to phone calls asking to verify account information or confirm passwords. "Retailers have to tell, and keep telling, their customers that they would never ask for such information over the phone," Cole says.

It also doesn't help retailers when news reports sensationalize data breaches that do occur. When retailers store customer information, many of them use multiple defenses including encryption of the data.

"A point a lot of media are missing when they report breaches is that the encrypted data are stored without [decryption] keys," he says, which makes the data mostly useless to hackers. "The media miss out on this in their stories."

Retailers can also warn consumers to be wary of huge discounts on merchandise, particularly online. "One of the big hacks we've seen recently is that adversaries will buy ads on search engines," Cole notes. Many of these are untrusted sites — shoppers should ask themselves whether an 80 percent discount is worth the risk when more-respected merchants are all offering the same merchandise at much higher prices.

THREAT-HUNTING

In protecting their own data, retailers are also protecting their customers' information. One of the more useful tactics that can be employed is threat-hunting. Retailers should not wait for a breach before they start looking for evidence of cyberattacks.

"Threat-hunting ties into being proactive," Cole says. "Most retailers are reactive. They wait for incidents."

In threat-hunting, retailers should tell themselves something like, "the probability that I'm compromised is 90 percent," and then set out aggressively to look for breaches. "Ideally, it is a continuous process."

Cole says when his firm checks clients' systems for the first time, something is almost always detected or discovered. "Each subsequent threat hunt increases value and benefits," he says.

"Security isn't about preventing attacks. It's about minimizing the damage when attacks do happen. And that requires you to actively look for ongoing breaches, even ones you don't know about."

There are several ways to conduct threat hunts. Check host servers for evidence of compromise; if it's a network, monitor it while looking for anomalies. "Think about how most cyber attackers were caught. They tried to steal too much information," Cole says. "There was unusual network activity and they were slowing down the network."

Looking at the way a network, and its components, is constructed is another part of threat-hunting. "Playing on the theory that there is no such thing as 100 percent secure," he says, "100 percent secure equals zero percent functionality."

This means that "every time you add a function, you have to ask yourself, 'What is the sacrifice in security? Is it worth it? What can I do to recognize exposure?' You have to think like an adversary."

'ASK BETTER QUESTIONS'

A major challenge for IT professionals is getting senior management to understand the importance of security, even though their primary concerns usually involve increasing sales and cutting costs.

"Executives aren't going to understand security, but they can ask better questions," Cole says. One hypothetical: "What are the higher security risks involved with adding a new functionality on the website that could potentially boost sales 15 percent?"

Cole says many lessons have been learned from retail data breaches, which he describes as "a gift that keeps on giving" because of the weaknesses revealed in how organizations approach security.

"The first question that people ask is whether the chief information officer should have been held responsible for the breach," he says. "The bottom line is, when a major event like this occurs, someone needs to be held responsible for the negligence."

"What was surprising is that security was a responsibility of the CIO," Cole says. "The fact that a large organization does not have a separate chief security officer that is a peer with the CIO, is what is most concerning."

Cole's major concern was the dual role of the CIO. "Running the IT infrastructure, typically a role of the CIO, and protecting the information, typically a role of the CSO, are two different roles," he says. STORES

David P. Schulz has been writing for STORES since 1982 and is the author of several non-fiction books.