Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Data Breach Report Calls For Race To Catch Up With Hackers

By **Allison Grande**

Law360, New York (April 26, 2016, 11:44 PM ET) -- Businesses are largely failing to keep up with hackers, who can turn employee missteps into damaging breaches in mere days, according to a report released Tuesday by Verizon Enterprise Solutions, highlighting the need for companies and their counsel to focus on enhancements to training and mitigation protocols in order to slow down the attackers.

According to Verizon's 2016 data breach investigations report, it took hackers minutes or less to compromise systems in 93 percent of the 2,260 breaches that Verizon analyzed, and the infiltrators were able to extract the data from the system within days in more than 98 percent of the incidents.

By contrast, the targets of these breaches didn't find out they'd been breached for weeks or more in 83 percent of the cases, with the notification coming from law enforcement or some other external source the majority of the time, the report said.

"Until you change the dynamics of cybercrime, we're not going to see any significant changes in the tactics, techniques and procedures used by hackers," said Gabriel Bassett, a senior information security data scientist with the Verizon Enterprise Solutions team that prepared the report. "Right now, hackers have a good opening move, and if the person they are playing against doesn't know what's going on, they're going to win every time."

In order to help reverse the trend, businesses would be wise to focus less on reacting to incidents and more on taking proactive steps to cut down detection time and make it harder for hackers to gain entry in the first place, according to experts.

"There's no question that today we have to do whatever we can to set roadblocks to make it slower for hackers," said Jeffer Mangels Butler & Mitchell LLP partner Robert E. Braun. "But on the other hand, simply reacting to the threats is how we got into this situation."

One area that would be useful for companies to focus on is how they train their employees to spot and report suspicious emails and activity. This is especially true in light of the Verizon report's findings that the most popular way for hackers to gain access to a system is by tricking employees to open or click on phishing emails that plant malware on their systems.

"We need to build security into people in addition to building security into our machines," Braun said.

The cost of human error goes far beyond phishing schemes, according to the report.

While “miscellaneous errors” — which are characterized as any unintentional action or mistake that compromises security and results in the loss of assets — led the pack when it came to the root causes of intrusions, insider misuse and physical theft and misuse weren’t far behind. The three factors outpaced actions taken by hackers, such as injecting malware into systems or overwhelming systems with malicious traffic, to steal corporate data, the report said.

“Of many breach trends detailed in Verizon’s latest report, the continued increase in attacks that are due to employee negligence clearly stands out,” said Michael Bruemmer, vice president of Experian Data Breach Resolution. “Be it from the use of weak passwords, which were involved in over 63 percent of breaches, or the steady increase in successful phishing attacks leading to the loss of information, it’s clear more needs to be done to address the human aspects of security.”

To help address the vulnerability, experts recommend that companies invest more time and resources in employee training, with a specific focus on helping them identify malicious emails and finding ways to reward them for following security procedures and reporting suspicious activity.

“The way to slow the hackers down is to not let them in, and the way to do that is to have adequately trained people,” Braun said.

The findings that hacking and malware are the two most popular vectors for breaches also underlines the need for strong technical safeguards to complement their training procedures, according to attorneys.

“I would suggest the need for organizations to undertake proactive security assessments through forensic companies, at the direction of counsel, to identify potential weaknesses and determine whether they are already compromised,” said Al Saikali, co-chair of Shook Hardy & Bacon LLP's data security and privacy group.

Companies should also look at the threats to their systems that go beyond what was identified by the Verizon report, including the recent spate of spyware attacks that render data unavailable or unreliable, attorneys noted.

“It’s one thing to steal credit card information to sell it on the black market — that causes a lot of harm in and of itself. It is an entirely different situation to cripple an organization and prevent it from earning revenue or conducting operations,” said Pillsbury Winthrop Shaw Pittman LLP partner Brian Finch. “As that trend grows, so does the possibility of economic harm exponentially greater to attack victims.”

Taking steps to shore up physical security and employee awareness of potential attacks are vital to raising the barriers to entry for potential bad actors, which can help not only bridge the gap between infiltration and detection but also thwart some attacks by frustrating hackers.

“They’re just like any business; they’re going to go where there’s the best return on their investment,” Braun said.

The Verizon report backs up these sentiments. According to the report, more than three-quarters of attacks were motivated by financial gain, with espionage a distant second.

“Although much time is spent discussing potentially devastating state-sponsored and terrorist threats,

financially motivated hackers still dominate the threat," said Edward McNicholas, co-leader of the privacy, data security and information law practice at Sidley Austin LLP.

Further driving hackers' ambitions is the increasingly robust market for the fruit of their efforts.

According to the report, even though the market value for some payment card data is falling, the data game is still profitable, and hackers are finding themselves having to steal more — or more lucrative — data, such as protected health information and intellectual property.

But as scary as this escalation may sound, Bassett offered a reminder that hackers are humans, too.

"It's important for companies to remember that they're not playing against superhuman commando teams," Bassett said. "These are normal people that can be stopped."

--Editing by Mark Lebetkin and Kat Laskowski.
