THE WALL STREET JOURNAL.
WSJ.com

January 12, 2016, 10:57 AM ET

Cybersecurity Startup QuadMetrics Calculates Odds a Company Will be Breached

ByRachael King

From left: Mingyan Liu, QuadMetrics chief science officer; Wesley Huffstutter, CEO; Manish Karir, chief technology officer.

QuadMetrics Inc.

QuadMetrics Inc. says it can predict with greater than 90% accuracy the likelihood that a company will be breached within the next year.

While one customer says the young company’s technology is still maturing, its prediction efforts represent an emerging capability in the fight against cybercrime. QuadMetrics says that chief information security officers are using its product as their primary risk management tool, but admit that it is one tool of many that customers have in their arsenal to fight cybercrime.

Most cybersecurity tools focus on detecting a breach that has already happened, but few, if any, can predict the probability that a specific company will suffer a breach over the following three to 12 months, according to Stewart V. Nelson, senior risk advisor at Kapnick Insurance Group, where he specializes in cybersecurity insurance. The general inability to forecast cyber risk has made it difficult for companies to benchmark their relative risk to their peers, he said. It's also made it difficult for insurance companies to develop actuarial data to calculate premiums for cyber breach insurance and to determine the relative risk profile of the companies they insure. His company, an early customer, has been using the QuadMetrics service since May.

Some companies such as BitSight Technologies and SecurityScorecard do evaluate the security posture of companies and assign security risk ratings but they don't predict the probability of a breach, said Jon Oltsik, senior principal analyst at the IT research firm Enterprise Strategy Group, where he covers cybersecurity.

QuadMetrics' cloud service determines the probability of a breach at a particular company by collecting from its network more than 250 different data points, such as the misconfiguration of servers and routers or whether spam can be seen exiting the network. The technology doesn't require inside access and instead observes all such characteristics from the outside of the company's network. That profile is then compared against predictive risk models. QuadMetrics looks for cybersecurity characteristics that share similarities with organizations that have historically reported incidents.

CEO Wesley Huffstutter likens the process to driving by a person's home and looking at it from the street. "We can notice that the windows are open, the doors are ajar or you only have one lock instead of two or your garage door is open," he told CIO Journal. Other indicators, such as un-mowed grass, chipping paint or a shutter hanging from one hinge can round out the picture. "These aren't necessarily security issues but it goes to the fact that this may be a human element of whether you're paying attention or not to what's going on in your property," he added.

Built on research conducted at the University of Michigan in partnership with the Department of Homeland Security, QuadMetrics has been in business for about a year, said Mr. Huffstutter. So far the company has a variety of customers including universities, insurance companies and some Fortune 500 companies. The DHS has given a grant to the University of Michigan to research a global network reputation system. Dr. Mingyan Liu, QuadMetrics' chief science officer, is also the principal investigator on that project.

"There are other people out there that do things similar to this but there's nobody to my knowledge that will tell you that you've got a 60% chance of being breached," said Kapnick Insurance Group's Mr. Nelson. Today, for example, a company applying for cyberliability insurance will typically fill out an application of 50 to 75 questions about their security posture, he said. Those questions ask about the company's firewalls, whether they've done any penetration testing, whether there's a dedicated chief information security officer and other questions about data security hygiene. But they largely rely on self-reporting and it's very difficult for insurance companies to measure relative risk independently.

In order to assess the probability of a breach, researchers at the University of Michigan and QuadMetrics looked at hundreds of companies that had been breached and determined what their networks looked like just before the breach. From this information, researchers built cyber risk models. The researchers used several sources including the VERIS Community Database, the collection maintained by the Verizon RISK Team and used in the Verizon annual data breach investigations report, to gather data about previous incidents. The company then used machine -earning techniques to develop predictive models of data breaches and cybersecurity incidents.

Michael Donald Bailey, a professor at the University of Illinois at Urbana-Champaign, previously worked with two QuadMetrics executives Manish Karir and Dr. Liu at the University of Michigan. In one scientific paper which he co-wrote, they used the models and gathered data about networks to predict the contents of the Verizon Data Breach Report for the following year and got a 90% accuracy rate, he told CIO Journal. “It’s important to note that we don’t predict the exact time in which a breach will happen,” he said. Rather, a risk score is generated for each corporate network examined and the most risky networks are more likely to be the ones that are experiencing data breaches, he added.

A main challenge involves acquiring high-quality incident data. While machine-learning techniques have the power to make accurate incident forecasts, the data collection is lagging by comparison, the authors said in a research paper.

Through research, QuadMetrics has identified some main symptoms of network mismanagement that are the most important when predicting a breach. Metrics that measure mismanagement or the human element in cybersecurity are some of the most predictive features in QuadMetrics’ machine learning models, according to Mr. Huffstutter.

Of those symptoms, a good predictor of an upcoming breach occurs when a website’s security credentials, known as certificates, are invalid. When a user communicates with a website whose address starts with “https,” the communication is known to be encrypted. Before starting the encrypted communication, the website will present the browser with a certificate to identify itself. This lets the browser know that the site is actually the site it claims to be. When the user gets a warning from the browser, it could mean that a criminal is trying to spoof the site in order to get financial or other data from the user.

Other problematic symptoms include corporate domain name system servers that are left open, allowing outsiders to use them to launch denial of service attacks against other companies, said Mr. Huffstutter. A third sign of misconfiguration is when certain settings on corporate email servers are left open and can be enlisted by people on the outside to send spam to other people.

An assessment of whether malicious activity is coming from a specific corporate network also is added into the cyber risk profile of a company. Suspicious activity is matched to many different external data sets that keep track of spam, malicious software, phishing and other schemes.

Fidelis Cybersecurity, which responds to data breaches, is starting to use QuadMetrics with its clients. Ryan Vela, regional director at Fidelis Cybersecurity, said he has worked in the industry for 15 years, previously at General Dynamics . Mr. Vela went to Ann Arbor to meet with QuadMetrics and said he got chills during the meeting. “They were identifying organizations that had a high probability of being breached and there were organizations that I knew had been breached but they were not public,” he said, adding that due to non-disclosure agreements, he couldn’t tell QuadMetrics that the company was right.

The risk prediction level that QuadMetrics’ service generates is not yet good enough yet to take to the board of directors risk subcommittee, Mr. Vela said. “What it is good for is to start a discussion that organizations are having right now [about cybersecurity] in their risk departments.”

Mr. Huffstutter said that since this type of forecasting has never been done before, the company has faced questions about its accuracy. Still, he said that the research underpinning the product is sound and has been peer-reviewed. In fact, he said that some companies are using this service as their primary risk management tool.

Write to rachael.king@wsj.com