Battling the forces of darkness: Cybersecurity firm CEO talks Equifax, more

October 4 2017, by Ethan Baron, The Mercury News

For millions of Americans, the cybersecurity problem plaguing U.S. businesses just hit home in about the worst way possible. The failure of one business, Equifax, to keep its data secure will lead to a decades-long threat to the finances of more than half the nation's adults.

Major companies such as Equifax are under constant bombardment by hackers seeking everything from customers' credit card numbers to company secrets. Attackers may be freelance profit seekers, contractors, organized criminals or nation states.

Increasingly, attackers and defenders are focusing on the weakest link in virtually any company, the digitally connected worker. Joe Schmo's cubicle has become the new battleground in a war that sees the criminals and spies furiously innovating to stay one step ahead of people like Gary Steele. He's CEO of Proofpoint, a Sunnyvale cybersecurity company whose researchers helped stop the world-wide "WannaCry" ransomware attack in May. The $4 billion public company counts among its customers almost half of the Fortune 100, all five top U.S. banks, six of the world's top 10 retailers and seven of the top 10 technology firms.

The Mercury News spoke with Steele about the threats facing individuals and companies, and what we can expect the future to hold for personal and business data - including what was taken from Equifax. His comments have been edited for length and clarity.

Q: What does the Equifax hack say about security of Americans'

personal data?

A: The Equifax breach has broad impact on many Americans today, exposing their personal data to hackers. It also speaks to the fact that every company in America is vulnerable and we still have a long way to go to improve the overall security posture across corporate America.

Q: What are the hindrances to an improved security posture?

A: The bad actors continue to operate broadly. Their trade craft and capabilities continue to improve and corporate America has to continue to invest in cybersecurity. Frankly, we've seen a faster rate of innovation from the bad actors than we have from corporate America keeping up a security posture. It's investment, it's getting the right people in place that can help drive an appropriate security posture, and its vigilance, you've got to stay on it every day.

Q: With names, Social Security numbers, dates of birth and addresses stolen from Equifax - all that's necessary to fake an identity or loot a bank account - are we all under threat for life?

A: There's definitely a large population that is at risk and vulnerable. What's required is close monitoring for a long period. This will likely be used for many years to come. So it's incumbent upon all individuals who were impacted by the Equifax hack to closely monitor their credit over a long period. This won't go away - people need to be thinking in terms of decades not just in terms of a few years.

Q: Is it likely that stolen Equifax data will get sold around on the dark web?

A: It really comes down to who that actor was. But it's highly likely that it ends up on the dark web for sale.

Q: What can we expect next from this dangerous cybersecurity threat environment?

A: We will continue to see high-profile breaches, for example the notice about Deloitte (reports in September revealed a major hack of the accounting giant) was another significant breach in a very short period of time. We should be ready for significant breaches throughout corporate America.

Q: How does Proofpoint prevent phishing attacks from being successful?

A: We have a set of techniques including machine learning that enables us to very quickly identify these kinds of attacks and make sure they don't get delivered. These attacks have gotten much more sophisticated and they're truly socially engineered in that the email that is sent has lots of information and context (to fool the recipient into thinking it's from a legitimate source). The best way to protect that employee is frankly not having them see it at all.

Q: Where is our personal data most vulnerable?

A: Your personal data is spread across many different organizations. Retailers you do business with. Banks. Credit-reporting agencies. Your doctor. Your insurance company. Many, many organizations have personal and private data that needs to be well protected.

Q: What measures should a person take to protect all that data?

A: Use two-factor authentication with all your bank accounts and financial accounts. Use credit reporting to understand whether there's any bad actor that's already gotten to your data. Think hard with who you do business with and how you interact on the web - think about who you're providing your personal information to. We see malicious mobile

apps, which may look like it's coming from your favorite bank but they might not actually be the publisher of that app. It's not uncommon for bad actors to post malicious links on social accounts, or place malicious content there.

—-

Name: Gary Steele

Title: CEO, Proofpoint cybersecurity

Education: BS in computer science, Washington State University, 1984

Age: 55

Family: Married, no children

Home town: Naches, Wash.

City of residence: Hillsborough, Calif.

Five things about Gary Steele:

1. Part of the founding team at Proofpoint 15 years ago

2. Grew up in a small farm town of 650 people

3. Avid runner

4. Collector of contemporary art

5. Worked at a golf course through high school and college