LESSONS LEARNED FROM ANOTHER BIG BREACH

An interview with Josh Shaul, VP, Web Security Products

Q&A

Let's start with some background on the problem of consumer data breaches.

Josh: It's an enormous problem. We've seen more than a billion records stolen so far this year, which is not unprecedented. In the large attacks that make the news, for example at major retailers, hackers most often steal usernames and passwords. The ultimate purpose is to make money, most often by fraudulently purchasing goods that can be sold on the black market. And the potential fraud isn't limited to the breached company — it extends across other online businesses.

Here's how it plays out: Hackers don't steal actual passwords. They get cryptographic, or hashed, versions of them — represented as a bunch of 1s and 0s. They can't work backwards to determine the real password, but the hashing algorithms organizations use to protect their passwords are well known. So they can guess at passwords (and at what additional info may have been added to the password before hashing it) and then run them through the same algorithm, and sometimes they get a match — the same bunch of 1s and 0s.

Next, they take advantage of the fact that most of us reuse usernames or passwords — or slight variations on them — across accounts. The attackers start with massive

numbers of usernames and passwords. They go from website to website, stealthily and in a distributed way, with the intention of validating the credentials. They go to a major retailer site and find a dozen accounts that work there, then to a banking site and find the accounts that work there. Then to an e-commerce site, and so on.

These validated credentials are valuable. The actual fraudsters, usually different people, buy the credentials and access the accounts to make money. In the cases most damaging to individuals, the fraudsters access not just retail accounts, but online banking or personal email accounts. The email accounts can be the keys to the kingdom because, for example, online passwords to various accounts can typically be reset via email.

In short, this is a big problem because attackers and fraudsters are smart, devious, organized, and automated. Large data breaches are their raw material.

What's different about the Equifax breach?

Josh: The data stolen in the Equifax breach can feed the process I've just described, but that's just the start of the problem. Deep personal information was stolen — not just usernames and passwords, but names and addresses and birth dates and, most importantly, social security numbers. With that level of information, fraudsters can go directly to trying to sign up for new accounts — a new bank account, a new loan,

a new payday lending service, as well as new accounts for purchasing goods and services. There's potential for a wave of identity theft like we've never seen.

The most analogous major breach was probably that of the Office of Personnel Management a few years ago. Deep personal information on 21.5 million federal employees and contractors was stolen. Interestingly, we don't know much about the extent of identity theft that ensued. You don't see statistics about it because it's the type of thing compromised organizations aren't compelled to publish. But a lot of the affected individuals probably signed up for credit monitoring services, including Equifax, to reduce their risks. Now many have come full circle and seen their data stolen again.

What are the implications for enterprises?

Josh: All organizations that serve consumers online want to protect those customers and avoid being party, however unwittingly, to fraudulent transactions. Those transactions have direct costs in terms of stolen goods, services, and money, plus administrative costs to unwind the damage and restore customer accounts. The financial exposure is enormous.

In the wake of the Equifax breach, enterprises face a new level of security concerns specifically around identity theft. How do you protect your business and its customers when their personal information is no longer private? And when the data points you've been using to validate customer identities are known to criminals?

The fraudsters can write software that attempts to open millions of new accounts across thousands of different businesses. If only a small percentage succeed, they're still taking in lots of money. They may also try to open or change accounts the old-fashioned way, by phoning a company's call center and providing all the right information. That's a harder problem to solve and requires more authentication, but it's also a much more expensive proposition for the attackers. Still, where the payout seems high enough, they will go to the trouble of putting authentic-sounding people on the phone. How many customer support people are attuned to the small signs that they may be talking with a fraudster — or have even been asked to think about that?

CEOs and CIOs in organizations providing Internet-based services that can touch people's finances really need to be thinking hard about how they can make sure that the data that was leaked isn't being used to turn their organizations into vehicles for identity theft by originating loans, providing benefits or tax refunds, or making sales to people who shouldn't get those things.

What should enterprises do to protect themselves and their customers?

Josh: Since the Equifax breach, any online consumer-facing company has got to be more wary of new accounts and account and password changes, even those initiated

by people over the phone. Additional authentication steps may be in order, and smart consumers will recognize them more as precaution than inconvenience.

Most enterprises should get better at recognizing when they are under attack by hackers trying to guess usernames and passwords. Even at small scale, you can notice them if you know what you're looking for. They should also get better at distinguishing humans from robots. Is the login failure a human mistyping or bot guessing? Is the entity signing up for a new account online a real person or a bot with someone's stolen information?

If it is a bot, is it behaving correctly? Some bots you want on your website. For example, customers use Mint or Yodlee as their financial information aggregators, and give those services permission to access their accounts. And if the bot is not behaving properly, can you quickly show it the door or lead it into a maze where it gets confused and your security staff can diagnose what it's up to?

More fundamentally, many enterprises need an extra layer of security wrapping their online environments. This wrapper doesn't need to know what all your assets are. It does need to be thorough in watching who is coming to your address and in recognizing the latest threats.

This isn't the part of the story that's been talked about the most, but it's extremely important. Equifax said publicly that they had found a vulnerability in their systems. They thought they'd patched all of the systems with the vulnerability, but they missed one. That was all it took. The attackers eventually found and exploited it.

The lesson is that, even when you're being diligent, identifying systems that are vulnerable and remediating them as quickly as possible, you still may miss something. There's still potential for error. There may be vulnerable systems on your network that aren't in your inventory — that you don't even know about. And patching isn't instantaneous — it may take minutes or take days to roll out the software. Attackers are alert to the latest vulnerabilities and may get in while you're still patching.

In all those cases, a second layer of security provides additional assurance that, if you missed something, you've still got some protection. Equifax thought they'd fixed the problem and were wrong.

What other kinds of organizations are likely targets of customer data theft attacks?

Josh: First of all, no organization is immune to cyberattack, so everyone doing business online and storing customer data is vulnerable. The cybercriminals would like to go where there's lots of potentially valuable data. That means the other credit bureaus, the major credit card companies, and now companies like LifeLock, the identity theft protection company that has been advertising extensively and adding customers in the wake of recent breaches. Equifax was breached, but one would hope that these organizations have "military-grade" security in place.

Cybercriminals, like the proverbial bank robber, would also like to go where the money is, but major financial services institutions invest heavily to maintain that military-grade security. They're protecting their assets, operations, and high-value corporate and individual customers. Regular retail customers benefit from the level of security in place.

More vulnerable are companies like large retailers that have lots of consumer data but not the profit margins and funding — or perhaps not yet the motivation — to layer on the protection that they could. There's a mismatch between the value of data to protect and the security they can afford. These organizations should be re-evaluating their security postures and strategies in light of the Equifax breach and the amount of data about their customers that is already compromised.

On the government side, the IRS is probably the biggest target. They have everybody's information, and they have pretty much every bit of information that a fraudster could ask for. They have really robust security, of course, both for protecting data and for detecting identity theft. But they haven't been perfect. Agencies that disperse benefits, like Medicare, seem to be better at protecting data than preventing fraud, but their challenge is complicated by the fact that fraudulent claims take so many forms.

An industry in a difficult position is healthcare. Provider organizations and exchanges have an enormous amount of people's personal information on top of the clinical information in their electronic health records. They're under great pressure from HIPAA to protect patients' personal data. But they also have a fundamental tension

between clinical and other expenditures. Physicians and provider organizations are focused on patient outcomes — it's how they're wired. So they prefer to spend on clinical technology rather than on information or security technology. I had an interesting conversation with the CIO of a major medical center, who said, "My biggest worry is that somebody comes to my hospital sick, leaves healthy, but is worse off for having come here because of what happened to their data."

You've talked about cybercrime as though it's a business.

Josh: That's exactly what it is, and it's big business with different business models. Some cybercrime, including many state-sponsored attacks, amounts to industrial espionage. The attackers want to steal technical data, trade secrets, or other proprietary information of corporations and government agencies. Very different attacks aim to disrupt business operations by taking down servers, networks, and websites. Those are often the work of "hactivists" or disgruntled users.

The cybercrime we're discussing today, which starts with stealing data about large numbers of individual consumers, is likely all about making money. The harm to the business operations and reputations of compromised corporations is a byproduct. This version of the cybercrime business has its own markets and supply chain:

- Hackers find and exploit vulnerabilities in corporate systems to steal and sell vast amounts of data about individuals.

- Middlemen buy the data wholesale and put people and software to work testing and validating consumer credentials, or rounding out the data needed for identity theft. They're essentially culling and adding value to the data.

- Specialized fraudsters buy that validated data and monetize it through various channels of retail theft, financial fraud, or government benefits and tax fraud.

The supply chain is supported by a whole ecosystem, including software developers making tools of the trade and a workforce of hackers for hire. There are services to turn stolen data into money, to turn stolen goods into money, and to conceal hacking activity. And this ecosystem has a currency of choice in bitcoin.

Also note that cybercrime is a 24/7 business. The hackers are constantly at work, but at two tempos. They are targeting specific enterprises and trying to exploit newly discovered vulnerabilities before they can be patched. Hackers are spearfishermen looking for big fish. But they are also constantly working in the background, casting a wide net and waiting patiently for whatever fish come to the surface, including old vulnerabilities incompletely patched.

This may be the most important point for CEOs, CIOs, CSOs, and business executives in general in the aftermath of the Equifax breach: Know your enemy. You're not dealing with isolated hackers, but with well-organized and resourced cybercriminals. They are in the business of defrauding individuals and the organizations that serve them. And theirs is a growth industry. Do not underestimate their capability, resourcefulness, or imagination around where, when, and how to steal valuable data.

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.
