THE CREDIT TIMES

CCO of New York
Serving the Credit Industry's Professionals

March 2018

A Publication of The Commercial Collection Corp. of NY, Inc.

Taking a Layered Approach

What the Equifax breach can teach you about shoring up your company's data security.

By Anne Rosso May, editor of Collector magazine

Special Contributor to Scope

Part 1

The massive data security breach Equifax suffered early last summer compromised the personal information of 145.5 million consumers - 60 percent of the adult U.S. population. The negative effects of this event will likely last for decades, and since announcing the breach in September, the backlash against Equifax has piled up: its CEO stepped down and was called to testify before Congress, dozens of lawsuits have been filed against the company and it's being investigated by multiple state attorneys general as well as the federal government.

Equifax had a responsibility to protect consumers' personally identifying information, and it failed. But a consumer reporting agency is a big target and that's likely why hackers pounced…right?

Unfortunately, no. A five-seat collection agency in Smalltown, U.S.A., is just as vulnerable as a giant financial services firm - maybe even more so because small businesses often don't believe they are even on hackers' radars. But in 2016, hackers breached half of U.S. small businesses, according to a Ponemon Institute survey.

It's time to double-down on your data security. Here are five lessons you can learn from the Equifax breach and tips to help you boost your own security efforts.

Assign Someone to Keep Up With (and Implement!) Patches

The Equifax breach happened in part because a system patch for a known vulnerability wasn't applied. You may wonder, "If Equifax's 225-person security team couldn't get this done, what chance do I have?"

Actually, this is one of the easier tasks on your security to-do list. First, draft a policy that dictates who will keep track of the software products you use, and make sure that person is alerted to any related patches or security announcements.

Michael Wright, chief security officer for TECH Lock, said he recommends his clients sign up to receive security notices from the U.S. Computer Emergency Readiness Team, which works in conjunction with the Department of Homeland Security.

"In their bulletins they let people know when these types of vulnerabilities appear," Wright said. "They give you the criticality and tell you if there is a patch available."

Next, decide who will be responsible for applying these fixes and within what timeframe. Equifax's policy dictated that patches should be applied within 48 hours of notification - a noble goal, if followed.

Sarah Morris, managing editor at KirkpatrickPrice, suggested agencies apply the updates as soon as it is practical, ideally within 30 days of being notified.

"Most of the time attackers will go after a known vulnerability, usually resulting from a patch that was released that people failed to update," she said. "That is probably the number one takeaway from the Equifax breach and other major breaches."

continued on next page...

In this Issue

Management Team

Robert Ingold
Chief Executive Officer

Joseph Grieco
President

Judith Mattioli
Sr. Vice President

Patricia Stelter
VP-Controller

John Chotkowski
VP of General Collections

Darlene Evans
VP of Operations

Bryan Rafferty
VP of Legal & Marketing

Frank Vecchio
VP of Collections

Valerie Ingold
VP of Outsourcing

Chad Haynie
Director of Business Development

Congratulations to Cathleen DesRoche from Caleres & Rachel Hancock from Morningstar Inc. on winning an Echo Dot in our drawing.

Make sure to enter this month's drawing by using your Special Placement form. For every claim you place you will be entered for a chance to win one of two Echo Dots.

Certified By CLLA
Endorsed By IACC

con't

And don't just drop this responsibility in your IT director's lap and walk away; someone on the executive level should be knowledgeable about cybersecurity too. Admittedly, this can be a tall order for a small business.

"If you are a small agency with 45 collectors, you might have one server and your IT guy is your nephew who comes in part time," Wright acknowledged. "In a case like that, you're not going to have the option to even have a chief security officer because you won't be able to afford it."

The solution? Hire a data security professional to come in regularly - once a year, or even once every other year - to assess your security and update you on any potential threats.

Put Some Thought Into Your Passwords

Internationally, Equifax also had other problems this year. A third-party security firm found that one of Equifax's employee portals in Argentina used the same basic username and password -"admin"- which made it simple for hackers to gain access to the data.

While this misstep was not related to the U.S. breach, it does underscore the importance of secure passwords. A recent Verizon report found that 81 percent of hacking-related breaches were the result of stolen or weak passwords.

In addition to "admin," here are a few other easily crackable but unfortunately common passwords to avoid:

- 123456
- password
- login
- welcome

Use a unique password for each piece of software in the company and make it as strong as possible: use numbers, capital letters and special characters.

Make sure employees are not writing passwords on sticky notes and posting them at their desks. Password management applications can help you keep track of everything.

Implement Layered Security Controls

Equifax's former CEO Richard Smith told Congress that its breach was the result of "both human error and technology failures." Not only did Equifax's security team fail to implement a critical software patch, but its information security scans also failed to identify any systems that were compromised by the vulnerability.

This illustrates the importance of having layered security controls, which Morris said is something organizations of any size can tackle on their own. The idea is to put several different obstacles in front of potential hackers, including firewalls, anti-virus software, multifactor authentication and intrusion detection, and follow it up with regular monitoring.

Don't forget about data encryption - even though Equifax did when its consumer dispute portal was compromised. In an October congressional hearing, Smith said that while Equifax protects much of its data through encryption, the information in the compromised portal was in plaintext.

While encryption won't stop hackers from breaking in, it can render any data they steal useless.

But the most important layer of information security in your business might be your employees. You need to create a culture of compliance and security to help ensure the "human error" Equifax suffered doesn't happen to you.

Train everyone on data security - why it's important, what they need to do - and follow-up regularly to drive the message home. Employees are often the weakest link in the data security chain, so limit their access to critical systems and software unless necessary, set up guidelines for internet use and teach them how to spot social engineering and phishing scams.

Additional content of this article will be continued in the next edition of The Credit Times

For more information on any of CCC's services...
3rd Party Collections
Business Process Outsourcing (BPO)
Mechanic's Liens
UCC Filings
Credit Reports
Please contact Chad Haynie at 1-800-873-5212 or E-mail chaynie@commercialcollection.com

The Commercial Collection Corp. of NY, Inc.
PH: 800-873-5212 / Fax: 800-873-5211
www.commercialcollection.com