

THE CREDIT TIMES



June 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 2

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.

Perform Regular Audits and Vulnerability Scans

You'll need to conduct regular vulnerability scans and penetration tests even if you think nothing in your business has changed recently.

"You don't know if you are secure if you don't test your system," Wright said.

Vulnerability assessments and penetration tests sound similar but are different—and you need to do both. Vulnerability scans assess your systems for weaknesses or malware and are relatively easy and cheap to do, either in-house or through a third party. Wright recommended running these scans quarterly—if not more often.

Penetration tests, on the other hand, are almost always conducted by an independent third-party—an "ethical hacker"—who tries to break into your system and access your data.

If one of these tests reveals an issue, make sure someone on staff is assigned to correct the problem—and follow-up to make sure the system is truly secure.

continued on next page...

In this Issue

- * Taking a Layered Approach - Part 2
- * Birthday Club

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
VP of Business
Development



Congratulations to Audrie Stefanini from TomTom, Inc. & Amanda Jenkins from Sunbelt Rentals, 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.



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



Join our Client Birthday Club!

Send an E-mail to Luz Colon at lcolon@commercialcollection.com to become a member and watch for your gift from CCC on your birthday!

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