$575Million Equifax Settlement Illustrates Business Security Basics

Posted At : August 27, 2019 9:21 AM | Posted By : Admin
Related Categories: Your Business, Security

We recommend and help implement security for every one of Computing Center's clients. While totally baffling given what Equifax's business is, they apparently didn't do many of the basics. A bit of a long read, but there are many lessons to be learned here. No time to wade through the entire article...checkout the last section - what you and every business should be doing is listed there.

Patch your software. Segment your network. Monitor for intruders. According to tech experts, those are security basics for businesses of any size. But when you're industry giant Equifax – a company in possession of staggering amounts of highly confidential information about more than 200 million Americans – it's almost unthinkable not to implement those fundamental protections. **An FTC, CFPB, and State AG settlement of at least $575 million** illustrates the injury to consumers when companies ignore reasonably foreseeable (and preventable) threats to sensitive data. Read on for security tips for your business and what consumers can do to get compensation for their losses and sign up for free credit monitoring.

The Equifax data breach has been in the headlines, but what happened behind the scenes? According to the complaint, in March 2017, US-CERT – Homeland Security's cyber experts – alerted Equifax and other companies about a critical security vulnerability in open-source software used to build Java web applications. The alert warned anyone using a vulnerable version of the software to update it immediately to a free patched version. It didn't take long before the press reported that hackers had already started to exploit the vulnerability.

Equifax's security team got the US-CERT alert on March 9, 2017, and sent it to more than 400 employees with instructions that the staffers responsible for the affected software should patch it within 48 hours, as required by the company's Patch Management Policy. Within a week, Equifax performed a scan intended to search for vulnerable forms of the software remaining on its network. But the scan Equifax conducted wasn't up to the task, which ultimately proved devastating to consumers. According to the complaint, the company used an improperly configured automatic scanner that failed to detect that the vulnerable software was alive and well on a part of the company's Automated Consumer Interview System (ACIS). The lawsuit alleges that Equifax didn't detect the "open sesame" vulnerability in its system for months.

How sensitive was the data stored on the ACIS portal? If it's been a while since you've made that hands-on-face shriek from "Home Alone," now may be the time because it was the portal where Equifax collected information about consumer disputes, including documentation uploaded by consumers. In addition, Equifax used that platform for consumer credit freezes, fraud alerts, and even requests for a free annual credit report. Thus, millions of consumers interacted with the ACIS portal every year.
The complaint outlines the specifics, but suffice it to say that for infocrooks looking for Social Security numbers, dates of birth, credit card numbers, expiration dates, and the like, the data on ACIS was Grade A primo stuff.

Compounding the injury to consumers was the fact that ACIS was originally built in the 1980s and even in-house Equifax documents referred to it as "archaic" and "antiquated technology." What's more, the complaint alleges that when Equifax sent that email to more than 400 of its employees warning them about the need for the patch, the company didn't alert the staff member responsible for the part of ACIS with the vulnerability.

Equifax failed to discover the unpatched vulnerability for more than four months. In late July 2017, the company's security team spotted suspicious traffic on the ACIS portal. They blocked it, but identified

additional questionable traffic the next day. That's when Equifax took the platform offline and hired a forensic consultant who determined that hackers had already exploited the vulnerability. But it gets worse. The consultant figured out that once inside the ACIS system, attackers were able to gain access to other parts of the network and rummage through dozens of unrelated databases also containing highly confidential information. In addition, they accessed a storage space connected to the ACIS databases that included administrative credentials stored in plain text, which they used to grab even more sensitive data. According to Equifax's forensic analysis, attackers were able to steal (among other things) approximately 147 million names and dates of birth, 145 million Social Security numbers, and 209,000 credit and debit card numbers and expiration dates.

The complaint alleges that a number of Equifax's actions – and failures to act – led to violations of the FTC Act and the Gramm-Leach-Bliley Safeguards Rule, which requires financial institutions to implement and maintain a comprehensive information security program. For example:

- **Equifax didn't check to make sure employees followed through on the patching process;**
- **Equifax failed to detect that a patch was needed because the company used an automated scan that wasn't properly configured to check all the places that could be using the vulnerable software;**
- **Equifax failed to segment its network to limit how much sensitive data an attacker could steal;**
- **Equifax stored admin credentials and passwords in unprotected plain-text files;**
- **Equifax failed to update security certificates that had expired 10 months earlier; and**
- **Equifax didn't detect intrusions on "legacy" systems like ACIS.**

The complaint cites those as factors that contributed to a breach of consumers' personal information of massive proportions.

The settlement requires Equifax to pay at least $300 million to a fund that will provide affected consumers with credit monitoring services, compensate people who bought credit or identity monitoring services from Equifax, and reimburse consumers for out-of-pocket expenses incurred as a result of the 2017 data breach. Equifax will add up to $125 million more to the fund if the initial payment isn't enough to compensate consumers for their losses. Equifax also will pay $175 million to 48 states, the District of Columbia and Puerto Rico, and a $100 million civil penalty to the CFPB. (The FTC doesn't have legal authority to get civil penalties in a case like this.)

Financial remedies are only part of the settlement. Under the order, Equifax must implement a comprehensive information security program requiring – among other things – that:

- Equifax must conduct annual assessments of internal and external security risks, implement safeguards to address them, and test the effectiveness of those safeguards;
- Equifax must assure that service providers with access to personal information stored by Equifax also implement appropriate security programs; and
- Equifax must get annual certifications from Equifax's Board of Directors saying, in effect, "Yes, I attest that the company is complying with the order's requirement of an appropriate information security program."

The Equifax settlement is a study in how basic security missteps can have staggering consequences. Here are some tips other companies can take from the case – and we didn't have to look far for advice. The quotes are all from the FTC's brochure, **Start with Security**.

"Update and patch third-party software." Companies should treat a security warning from US-CERT with the utmost seriousness. Equifax's 48-hour Patch Management Policy may have looked good on paper, but paper can't patch a critical software vulnerability. Of course, you should tell your IT team to implement appropriate patches and fixes. But you also need a belt-and-suspenders system to make sure your company follows through effectively.

"Ensure proper configuration." There's nothing inherently wrong with using an automated vulnerability scan, but if it's not set up to know where to look, it's just another collection of zeros and ones. The complaint alleges that Equifax compounded the problem by not maintaining an accurate

inventory of what systems ran what software – a fundamental practice that would have made it easier to find the vulnerability in the ACIS platform.

"Monitor activity on your network." Who's coming in and what's going out? That's what an effective intrusion detection tool asks when it senses unauthorized activity. An effective system of intrusion detection could have helped Equifax detect the vulnerability sooner, thereby reducing the number of affected consumers.

"Segment your network." The idea behind ships' watertight compartments is that even if one portion of the structure sustains damage, the entire vessel won't go under. Segmenting your network – storing sensitive data in separate secure places on your system – can have a similar mitigating effect. Even if an attacker sneaks into one part of your system, an appropriately segmented network can help prevent a data oops from turning into a full-fledged OMG.

The FTC has more **security advice** for businesses. Are you a consumer affected by the Equifax breach? Visit **ftc.gov/equifax** for information about how to apply for compensation.