Lesson Plan: Equifax Breach

Assignment

Listening assignment: Listen to the “Equifax Breach” episode of the “How Hacks Happen” podcast.
Length: 70 minutes
Where to listen: On most popular podcast platforms, search for “How Hacks Happen”. You may also listen at https://howhackshappen.net/episodes

Reading assignment: The bulk of the research for this podcast comes from two government reports:

- U.S. House of Representatives Committee on Oversight and Government Reform: The Equifax Data Breach
- United States Government Accountability Office Report to Congressional Requesters (GAO report)

These reports are lengthy and, in some places, hard to digest. If you wish to give a reasonable reading assignment to augment the podcast, I recommend pages 10-16 of the GAO report. The GAO report is generally a pretty easy read, and will give students a bird’s-eye view overview of the Equifax breach.

There are additional resources listed on the podcast page. On the website, click the podcast listing to expand and show the resources.

Discussion Questions

Q. What were some of the mistakes the Equifax cybersecurity team made that allowed the hack to happen? What could you do, if you were in a similar role, to prevent these mistakes?

> You can find a list of possibilities for discussion under the last question in the Quiz/Assignment Questions section.

Q. Discuss the importance of a Patch Plan. Find references to patch plans online, and discuss what they entail and how they’re implemented. What is “Patch Tuesday”?

Q. The hackers apparently found out about the Apache Struts vulnerability by reading about the patch in a public place. Is there a better way to publicize patches? Where is the balance between “public’s right to know” and hackers’ ability to find out the same information?

Q. How is it possible that the company’s internal scan found no instances of the Apache Struts framework running on any system in the network, but the hackers were able to find it?

Q. Why should you never leave a piece of equipment at the default settings, or without at least looking at all the default settings to see if they’re right for your organization?

Q. How do you think the Equifax breach will affect US citizens in the years to come? How great is the risk of identity theft and other fraud, from the hackers?

Q. Why do you suppose the hackers were interested in the stolen information, if not for identity theft?

Q. Do you think Consumer Reporting Agencies should be held to a higher standard of cybersecurity than other types of organizations? Why?

Q. Do you think Equifax acted responsibly after the breach was discovered? If not, what should they have done differently?

Q. Suppose there's a legacy system in your network. It runs on Windows XP, and know you need to upgrade it. However, it's running software that the Accounting department claims is critical to their work, and there's no version of the software that runs on the latest OS. The Accounting department most definitely doesn't want to change things, as it would disrupt their operations. What would you do to get the update to happen?

Food for discussion: Here are a few options for approaches to the problem.

- Force the update (the fastest way, but you'll have angry staff on your hands).
- Educate them to get their agreement and help them find a modern solution (but this might take a while, and in the meantime the system is vulnerable).
- Get management involved to help force the issue (might cause friction).
- Figure out a way to have an air gap between Accounting and the internet.
- Leave it as is, and the joke will be on them when they get hacked.

Quiz/Assignment Questions

These questions can be posed as essay questions for quiz or assignment, or as multiple-choice questions. For multiple choice, the correct answer is indicated by a checkmark (✓) and some suggested wrong answers are indicated with (x).

Q. What is the primary security problem caused by using a legacy operating system that the manufacturer no longer supports?

- ✓ Security vulnerabilities are no longer patched by manufacturer's updates, leaving the system open to attacks.
- x The OS can never be updated to the latest version, so the software running on the system can never be updated.
- x Newer technology personnel won't know how to update the system, so they can't perform security measures on it.
- x Employees who won't learn new software are also the ones most prone to phishing attacks.

Q. How did the Equifax hackers mostly likely learn about the Apache Struts vulnerability?

- ✓ Through a public patch notice from Apache
- x From a hacking playbook purchased from a dark web marketplace
- x By studying Edward Snowden's leak of NSA exploits
- x By attending a specialist "hacking school" sponsored by the Chinese military

Q. What is a "patch" in cybersecurity?

- ✓ A software update that addresses security vulnerabilities and fixes bugs.
- x A list of vulnerabilities published by a software company to warn software users about potential issues.
- x A piece of tape pasted over a laptop camera to prevent spying.
- x A USB thumb drive that, when inserted during software use, prevents hacks from occurring.

Q. When should you apply a software company-issued patch to a system?

- ✓ As soon as is reasonably possible, preferably within a few days.
- x When the system is down for other kinds of maintenance, like updating the graphics on the home page.
- x Doesn't matter. Patches are more "nice-to-have" than necessary.
- x Never. Patches often contain viruses that can compromise the system.

Q. In cybersecurity, what is an “inventory”?

- ✓ A list of all hardware and software in the network, and their locations and versions.
- x A list of all patches applied to date, and the dates they were received and applied.
- x A list of all cybersecurity-related regulations that pertain to the company, and the company’s current status with regard to compliance.
- x An encrypted list of all the databases in the system, their locations on the network, and their root-level logins and passwords.

Q. How did the hackers use the ACIS portal to gain access to the Equifax network?

- ✓ Through an upload button on the website, they uploaded files that contained shells, which executed commands.
- x They used SQL injection to cause the login field to execute commands to the database.
- x They used Equifax’s publicly available API to send bogus commands to the database.
- x A clever phishing email caused an Equifax employee to give the hackers an administrator’s login and password.

Q. How is it that the hackers were able to transfer large quantities of data from the Equifax network without arousing suspicion? (essay question only)

- ✓ The hackers used an expired digital certificate to encrypt the data, then exfiltrated it in small pieces so as not to trigger any suspicion. This was possible because the router could not do its usual job of decrypting, inspecting, and re-encrypting traffic because it was configured to only recognize encryption from current certificates. Also, the router was configured to ignore encrypted traffic that it could not recognize, so the router let the data pass through. This configuration was the result of leaving router settings at their default values.

Q. What were the factors that contributed to the hackers being able transfer large quantities of data from the Equifax network without arousing suspicion? (multiple choice version) (multiple answers)

- ✓ Router left at default settings
- ✓ Router configured to ignore encrypted traffic that it didn’t recognize, and allow it through
- ✓ Router not able to decrypt and inspect data encrypted with expired keys
- ✓ Expired digital certificates left hanging around on the system
- x Router inspected traffic coming in, but not going out
- x Router configured to allow files of 1TB or more to pass through uninspected
- x A hacker posed as an employee and took over the admin’s workstation
- x No security guard at the front desk
- x A hacker posed as an employee and copied the data to a thumb drive, and walked out
- x A hacker posed as an employee and walked out the door with a hard disk
- x The Chinese military has developed highly sophisticated exfiltration software

Q. According to the podcast, what are some of the errors and oversights that allowed the Equifax breach to happen? (multiple answers)

- ✓ Didn’t implement a critical patch immediately
- ✓ Lack of inventory
- ✓ Expired digital certificates lying around
- ✓ Router left at default settings
- ✓ Databases not segmented
- ✓ Passwords stored in plaintext
- ✓ Social security number used as index for relations in database
- ✓ Scan of network failed to discover servers running Apache Struts framework
- ✓ Incomplete email list used to inform all security personnel of the vulnerability
- x Password on sticky note
- x Visitor to Equifax office was able to plant a thumb drive with malware
- x Administrator posted password on a hacker’s forum
- x System became vulnerable during power outage
- x Passwords not changed after employee terminated
- x Used password “password123” on critical systems
- x SQL commands to databases not limited to specific queries
- x Security personnel ignored direct instructions to update systems