Iowa Senatorial Delegation Technical Briefing: Equifax

William Stone

The Equifax breach is a primarily a technical issue. Only after the technical details have been investigated can legal culpability be determined.

This brief provides a broad overview of the technical issues at hand; and makes recommendations as to how the Banking Committee may successfully investigate the Equifax breach.

1. Introduction

The Equifax breach is a matter that clearly falls within the purview of the Senate Banking Committee. However, it is first and foremost a technical matter. Only after the technical specifics have been investigated can legal culpability be determined.

To date, the Members of the Senate Banking Committee have not asked the technical questions necessary to reach any determination. They have focused on the matter as a purely legal one.

As a consequence, Equifax has successfully misled the Banking Committee. They have given misleading and/or technically inaccurate testimony. When a question may point toward technical issues, Equifax representatives have successfully deflected in such a way as to appear non-culpable.

The Iowa Senatorial Delegation will find Section *4.2: The FTP Protocol* of particular interest. It details why this this breach was possible; and how Equifax is both incompetent and legally-culpable.

To be specific:

- *This breach occurred because Equifax used an insecure protocol and unencrypted files.*

2. Points Of Failure

Equifax has made the claim that a single individual was responsible for the breach. Allegedly, this individual failed to properly perform their assigned work. While this might appear to be an appropriate answer, it not technically credible.

A competent Information Technology department has controls to prevent such an occurrence. These are outlined below, but Information Technology professionals are always guided by a basic rule:

- There are no single points of failure.

When designing any Information Technology system, points of failure should be first and foremost in any engineer's mind. Particularly with regards to a large business like Equifax, no single point of failure should exist.

There are best-practice business procedures to avoid this. These include:

1. Strict change control procedures.
2. Appropriate security controls and monitoring.
3. Redundant systems.

Lack or failure of any of these will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

Each of the areas outlined in this briefing are designed to eliminate single points of failure. In particular, they are designed to avoid changes that involve human error.

Equifax's claim is that a single individual somehow by-passed all appropriate checks is not technically credible.

For this to be true, any or all of the processes outlined in this briefing were inadequate. In a large company such as Equifax, this could only be the result of poor Information Technology practices.

3. Change Control

In a large company such as Equifax, there must be an appropriate Information Technology Change Control process. This process governs additions or changes to Information Technology systems, particularly business-critical ones, so that changes are never made ad-hoc. This requires a thorough and rigorous Change Control process prior to implementation.

This often causes any change to take several weeks to implement. This is intentional, so as to avoid changes that might have unintended consequences.

3.1. Change Control Procedure

In general, any change to Information Technology systems goes through four phases:

1. Submission to the *Change Control Committee* for consideration.
2. Approval or denial of the change. Denial will typically occur if:
    a. The change would negatively impact other systems.
    b. The change conflicts with another change to a system.
    c. The change isn't appropriately documented.

3. Implementation.
    a. Once approved, the change is assigned an implementation date and time. Depending on business impact, it may be performed after business hours or during a scheduled maintenance window.
    b. In some cases, changes are made by two or more individuals so as to avoid human error.
    c. Once made, the effects of the change are rigorously tested.
        i. If no negative impact is detected, the change is marked successful.
        ii. If there is a negative impact, the change is immediately reverted.

4. Post-implementation review by the Change Control Committee.

Lack or failure of a change procedure will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

3.2. Change Control Committee

In a large company such as Equifax, the change control procedure typically involves a Change Control Committee. This committee is made up of any and all company departments that have a vested interest in Information Technology changes.

This can include almost any department or business unit. A Change Control Committee should at least include:

- Senior company Management
- Any department or business unit that might be impacted by Information Technology changes.
- All Information Technology departments:
    - Management
    - Information Security
    - Applications Development
    - Networking
    - Hardware Systems
        - Mainframe
        - X86 Server
        - Desktop Support

Lack or failure of any or all of these departments to be involved in change control will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

3.3. Recommendations

In this instance, the public availability of the file in question should have been detected by the change control procedure. That it was not suggests that the change control procedure was ineffective.

Banking Committee Members are strongly advised to thoroughly question Equifax regarding its Information Technology change control procedures.

4. Security Controls and Monitoring

A large company such as Equifax must have rigorous security controls. These generally fall into the following categories.

4.1. Information Technology Security Department

A large company such as Equifax must have a dedicated Information Technology Security department. It should staffed by individuals with experience in:

- Intrusion detection
- Vulnerability mitigation
- Disaster recovery
- The Dodd-Frank Wall Street Reform and Consumer Protection Act

These individuals should report to the Chief Security Officer; or a supervisor that reports to the CSO.

It should be noted that Dodd-Frank has proven irrelevant. Its sole impact has been a significant increase in the amount of regulatory activity. Completion of this activity is typically placed under the Information Technology Security department.

As a consequence, many companies' Security departments are overwhelmed with Dodd-Frank compliance tasks. They often have little time to concentrate on other areas of security.

These areas would include:

1. Documenting, implementing, and enforcing Information Technology Security policies.
2. Performing periodic testing of all systems, public or otherwise, for security vulnerabilities.

3. Performing constant monitoring of publicly-available systems for:
    a. Intrusion attempts (successful or not).
    b. Changes made without authorization.
    c. Changes to any publicly-available content. *This would include the vulnerability that caused the breach.*

Lack or failure of security controls will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

4.2. The FTP Protocol

It should be noted that the FTP protocol used for access to the file in question is considered notoriously insecure. It was replaced over fifteen years ago with the far more secure SCP protocol.

In FTP, the file being uploaded or downloaded is sent "in the clear." That means that it is vulnerable to:

1. Interception of usernames and passwords.
2. Interception of data during transfer.

Additionally, the file was not encrypted. A secure implementation would include:

1. SCP in place of FTP.
2. PGP-encryption of the data with at least a 2048-bit key.

Use of the FTP protocol and no file encryption will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

Equifax fell victim to (3) due to incompetent Information Technology Security.

To be clear:

- *This breach occurred because Equifax used an insecure protocol and unencrypted files.*

4.3. Recommendations

In this particular instance, the vulnerability should have been detected by Information Technology Security. That it was not suggests that Information Technology Security was inadequate.

Banking Committee Members are strongly advised to thoroughly question Equifax regarding its Information Technology Security procedures.

In particular, Banking Committee Members should specifically question Equifax's use of FTP without file encryption.

To reiterate:

- *This breach occurred because Equifax used an insecure protocol and unencrypted files.*

5. Redundant Systems

In a large company such as Equifax, there are numerous redundant systems designed to avoid a business-critical failure.

Such redundancies typically include the following.

5.1. Host Redundancy

"Host redundancy" to computer hardware. For example, if one ran a website, one would need to have multiple computers that perform the same task.

In the event of failure, all systems should seamlessly fail-over.

Failure to have host redundancy will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

5.2. Network Redundancy

"Network redundancy" covers numerous areas. In general, they are:

1. Redundant networking equipment.
2. Redundant networking connections, both within the company and where it connects to the Internet.

In the event of failure, all systems should seamlessly fail-over.

Failure to have network redundancy will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

5.3. Applications Redundancy

Programs (Applications) must also be created to operate in a redundant fashion.

In the event of a program failure, it should seamlessly fail-over to a backup application (typically running on another server).

Failure to have applications redundancy will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

5.4. Barriers to Redundancy

In many companies, even large ones such as Equifax, there are often barriers to appropriate redundancy. These typically fall into several areas:

1. Expense
    a. Appropriate redundancy essentially involves duplication of the entire infrastructure. This presents a business with a significant expenditure. In many cases, companies are simply unable (or unwilling) to expend the funds.

2. One-Offs
    a. A “One-Off” describes a situation in which the business made a decision to purchase commercially-available software not intended for business use.
    b. Once that software is implemented, the business then purchase additional software not intended for business usage.
    c. Once dependant on this software, applications are created to connect the software together, often in a fashion neither intended nor supported by the software manufacturer.
    d. “One-Offs” typically accumulate over a period of several years, resulting in:

3. Spiderwebs
    a. A “Spiderweb” occurs when “One-Offs” have been allowed to grow unchecked.
    b. Each individual program (never intended for this use) becomes interconnected to other programs, which are interconnected to other programs.
    c. The result is a “Spiderweb”: a system of connections that is extremely complex and non-intuitive.
    d. On many occasions, “Spiderwebs” are so fragile that any minute change can cause the entire system to collapse.
    e. “Spiderwebs” are present in the vast majority of Information Technology systems. *This includes both the public and private sectors*.

Failure to address barriers to redundancy will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

5.5. Recommendations

The nature of the breach suggests that Equifax's redundant systems may be inadequate.

Banking Committee Members are strongly advised to thoroughly question Equifax regarding its redundant systems.

6. Disaster Recovery

Any company must be prepared for disaster, either natural or man-made, that completely destroys all existing Information Technology systems. In order to prepare for such an instance, a company typically implements the following.

6.1. Disaster Recovery Plan

In the event of a disaster that completely destroys a company's computing systems, there must be a Disaster Recovery Plan in place. This typically includes:

1. Advance rental of computer systems off-site and geographically disparate from the disaster.
2. A written Disaster Recovery Plan that includes any and all instructions necessary to recreate all systems from scratch.

Failure to address Disaster Recovery will result in:

1. Business-critical systems failures.
2. Errors in business-critical data.
3. Security breaches of business-critical systems.

6.2. Disaster Recovery Exercises

While having a written and enforced Disaster Recovery Plan is one step in preparedness, the plan must by tested. This typically includes:

1. Without warning, send a recovery team to the off-site location.

2. Send any and all backup materials in order to restore systems.
3. Provide an SLA (Service Level Agreement) that includes the timeframe that the team has to perform a recovery. In the event of a disaster, this is typically 24 hours.
4. The recovery team then attempts a restoration within the SLA.

Disaster Recovery Exercises should be performed at least annually.

In the event of failure, the results should be analyzed, the Disaster Recovery Plan amended, and then Exercises attempted again.

This should continue until such time as Disaster Recovery Exercises are completed successfully.

Failure to perform successful Disaster Recovery Exercises will result in:

1. Failure of the business in the event of a disaster.
2. Business-critical systems failures.
3. Errors in business-critical data.
4. Security breaches of business-critical systems.

6.3. Recommendations

The nature of the breach suggests that Equifax's Disaster Recovery procedures may be inadequate.

Banking Committee Members are strongly advised to thoroughly question Equifax regarding its Disaster Recovery procedures.

7. Recommendations

It is strongly recommended that:

1. All Members of the Senate Banking Committee be briefed by experienced, private-sector Information Technology and Security professional(s). Such briefing should provide Committee Members with basic questions. Committee Members should be cautioned that:
    a. They will not not understand the Information Technology aspects of the questions.
    b. A significant number of highly-technical follow-up questions will arise.
    c. Follow-up questions cannot be predicted in advance.

2. During hearings, all Banking Committee Members be provided with the following resources:
    a. Experienced, private-sector Information Technology and Security professional(s) immediately available. Such individual(s) will provide appropriate technical follow-up questions to Committee Members.

b. To facilitate this, each Committee Member be provided real-time communications with Information Technology and Security professional(s), who will provide follow-up questions to Committee Members.

8. Summary

The Equifax breach has clear legal implications. However, there are numerous technical issues that must be investigated in order to determine legal culpability. To date, Senate Banking Committee Members have yet to ask such questions.

It is imperative that the Committee ask questions regarding:

- Change control
- Security controls and monitoring
- Redundant Systems

It is equally imperative that Committee Members should be:

1. Briefed by experienced, private-sector Information Technonolgy and Security experts who will provide basic quesions.
2. Advised that basic questions will lead to numerous follow-up questions that cannot be predicted in advance.
3. During Hearings, provided resources allowing real-time communications with experienced, private-sector Information Technology and Security experts who will provide follow-up questions.

9. Author Experience

William Stone III is a retired Information Systems and Security professional of 40 years' experience.

He graduated with a Bachelor's Degree in Computer Science from Northern Illinois University and has worked for companies such as AT&T, Great West Casualty Company, and Chicagoland ISPs. He taught Information Technology at the college level for three years.

Professional certifications include:

- Certified Information Systems Security Professional
- Red Hat Certified Engineer
- Red Hat Certified Administrator
- Certified Cisco Networking Associate