

EQUIFAX DATA BREACH 2017

By: Arielle Bennett, Adi
Hacker, Bracha Lewittes,
Nicole Mandel, Dassi
Mayerfeld, Meghan Notkin,
Adielle Rosenblum

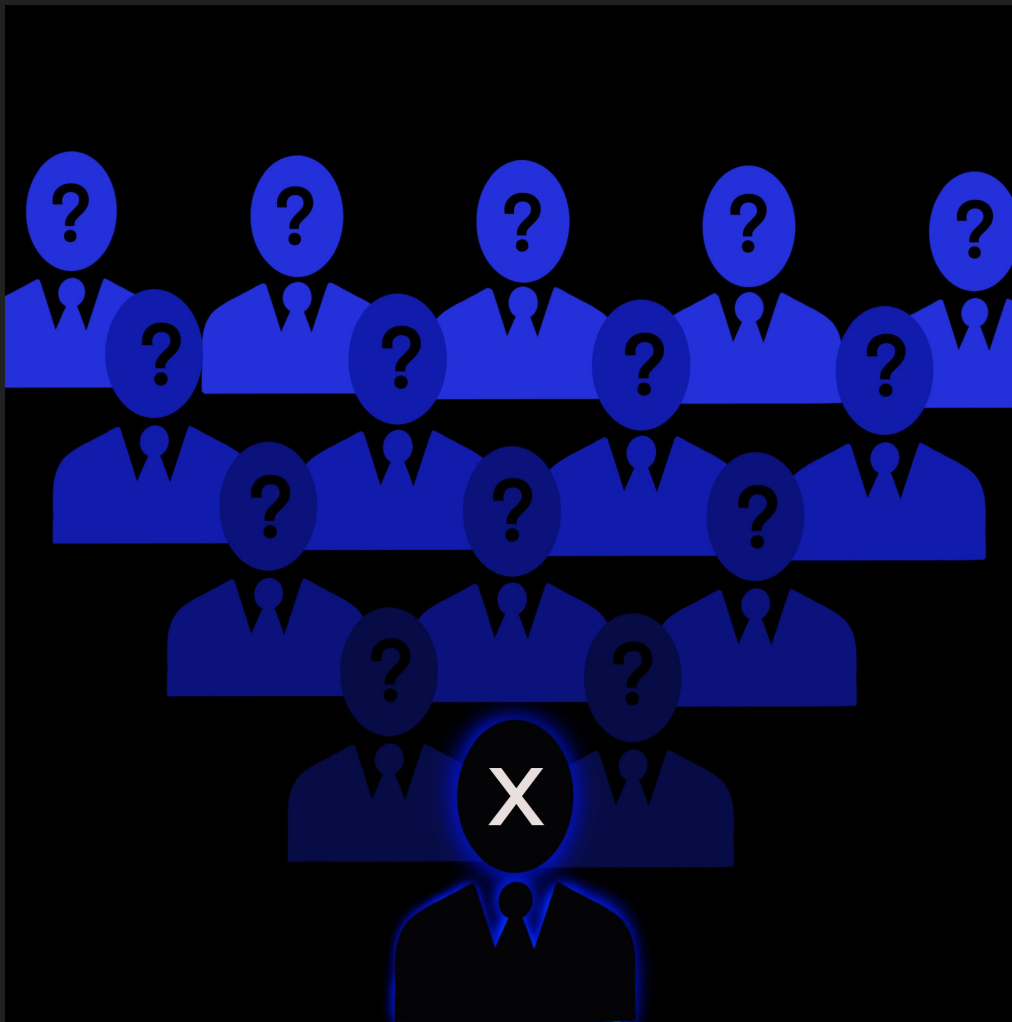


The US CERT Systems informed Equifax about the vulnerability in Apache Struts, but Equifax neglected to fix it immediately following their notification.

The hackers exploited an unpatched Apache Struts vulnerability in the customer service server to gain access to the entire Equifax server network.



STRUTS



Faulty Leadership

When the IT Department informed Senior Management of the breach in late July, Executives were unqualified and ill-prepared to respond. Executives had minimal training in cybersecurity and risk management.

Additionally, top executives sold nearly \$2 million worth of company stock a month before the breach was disclosed to the public, giving rise to accusations of insider trading.

In June 2019, the FBI prosecuted Equifax's CIO Jun Ying for taking advantage of insider knowledge for financial gain.



The hackers got access to the names, addresses, social security numbers, or credit card numbers of 143 million people, many of whom did not even know that Equifax had their information.

ANALYSIS BASED ON THE NIST FRAMEWORK

Identify, Protect, Detect,
Respond, Recover



Protect

Equifax hosted weekly security update meetings, but executives and IT personnel often didn't attend.

Payne, the Senior Vice President and IT-Coordinator, admitted that he was too high up in the company command to oversee communications between IT groups.

Employees later admitted frustration with the ambiguous role of the teams.

The lack of communication proved Equifax unable to protect consumer data in the event of a breach.



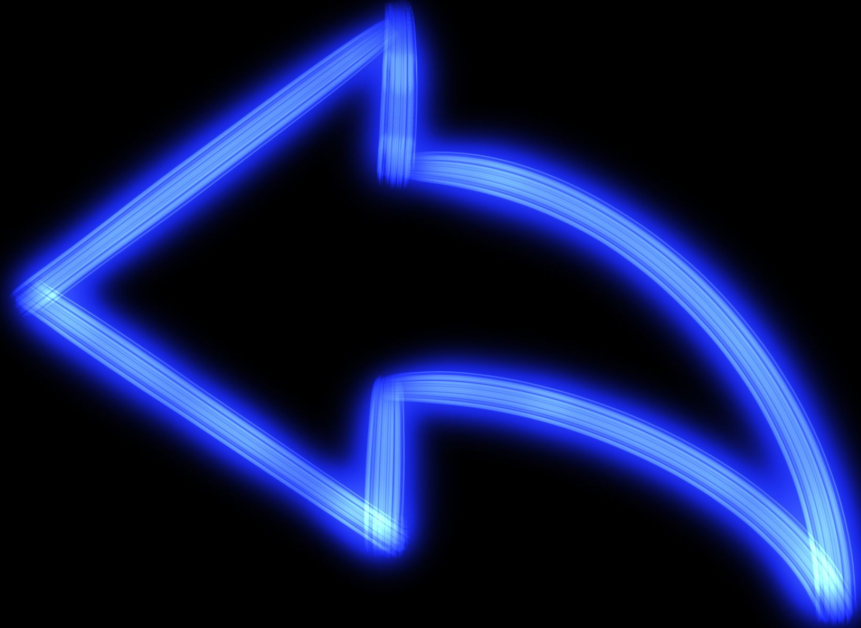
Detect

When Equifax ran a regular security scan, either the system failed to detect the intruders, or Vice President Payne didn't inform the security teams about the breach immediately. The hackers went unnoticed for 76 days, stealing confidential information from 51 different databases.



Respond

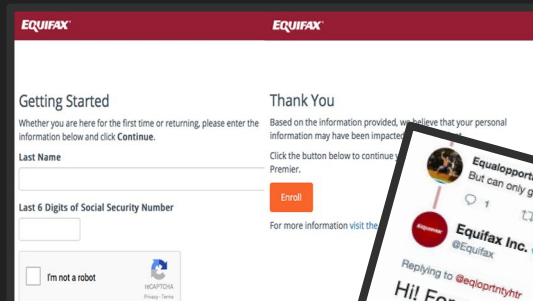
While Equifax employed a response team of 225 personnel, the CEO, Richard Smith, indirectly faulted Payne for not forwarding the warning email about the vulnerability. Payne replied that “if that’s the process the company has to rely on, then that’s a problem.”



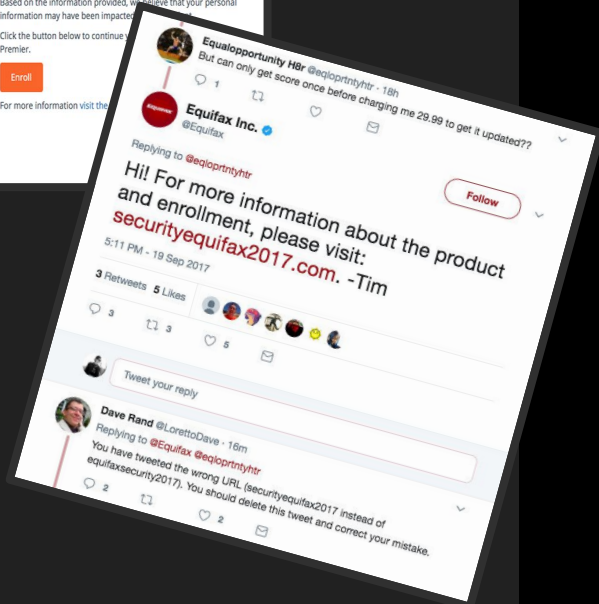
Recover

www.equifaxsecurity2017.com

www.securityequifax2017.com



The image shows two overlapping screenshots of the Equifax website. The top screenshot is the 'Getting Started' page, which asks users to enter their last name and the last six digits of their Social Security Number to continue. It includes an 'Enroll' button and a checkbox for 'I'm not a robot'. The bottom screenshot is the 'Thank You' page, which states that based on the information provided, the user's personal information may have been impacted and provides a link for more information.



Decision-Making Process

Payne and Smith oversaw coordination between the IT group and the Security group, but had too many other more pressing responsibilities. Equifax should've had an employee solely responsible for cybersecurity communications.

Additionally, since Equifax's notification system relied on one person forwarding the warning email, their cybersecurity leadership was bound to fail.

Legal/ Security Chain of Command

CEO Smith



CSO Mauldin



CLO Kelley



Employees

IT Chain of Command

CEO Smith



CIO Webb



Employees

Laws → Equifax

General data
protection
regulation (GDPR)

Federal Fair
Credit Reporting
Act

HIPAA

Data Security and
Breach
Notification Act

California
Consumer Privacy
Act (CCPA)

California Privacy
Rights Act

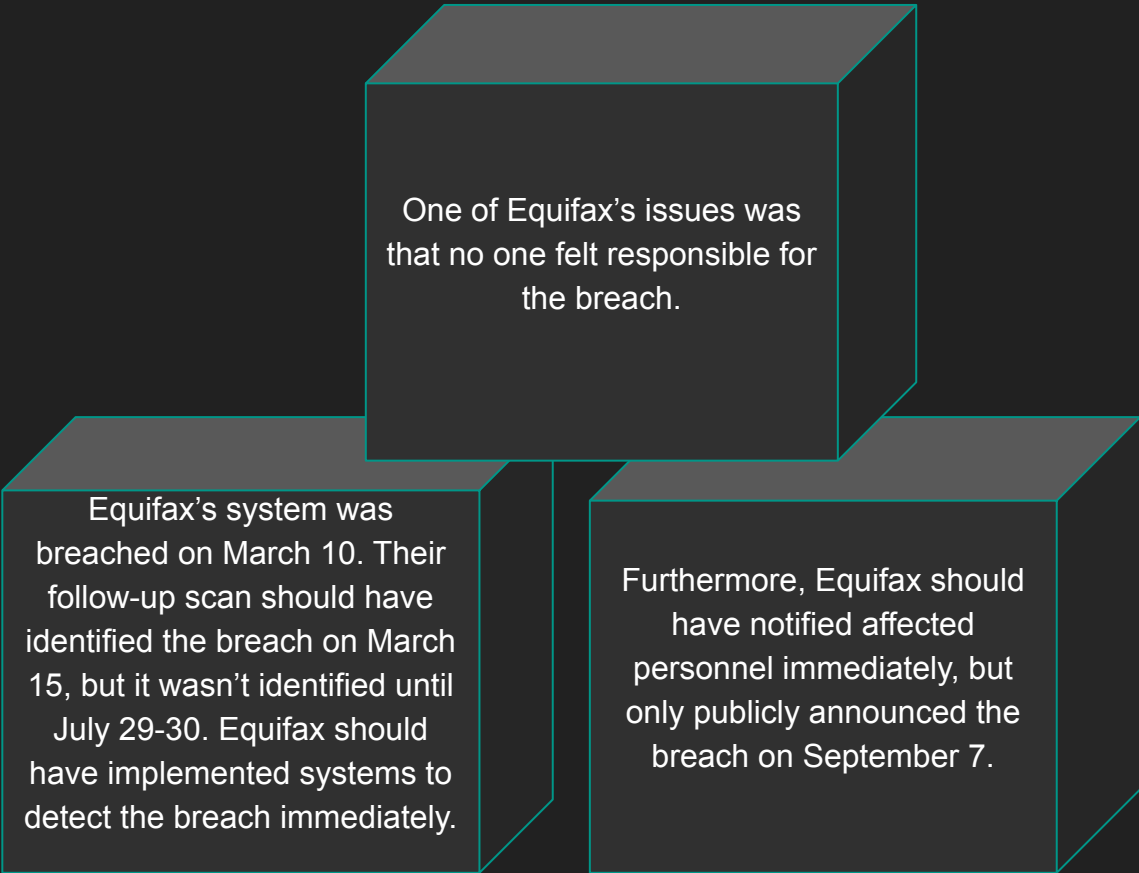
Virginia CDPA

Laws → Hackers

The Computer
Fraud and Abuse
Act (CFAA)

The Stored
Communications
Act (SCA)

Mitigation

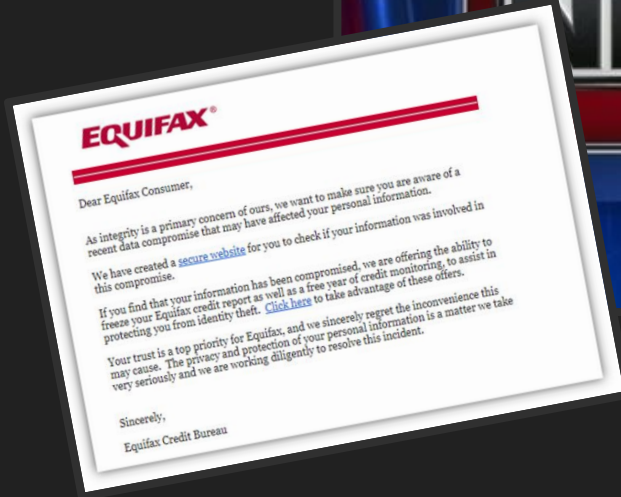


One of Equifax's issues was that no one felt responsible for the breach.

Equifax's system was breached on March 10. Their follow-up scan should have identified the breach on March 15, but it wasn't identified until July 29-30. Equifax should have implemented systems to detect the breach immediately.

Furthermore, Equifax should have notified affected personnel immediately, but only publicly announced the breach on September 7.

PR/Reputation Management Analysis



Recommendations

Recommendation

Implement a cybersecurity strategy and update it quarterly

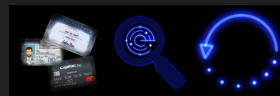
NIST



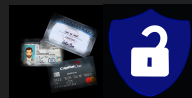
PPT



Penetration Testing



Implement endpoint security services to employee's devices.



Recommendations

Recommendation

NIST

PPT

Enable Multi Factor Authentication



Use Network Microsegmentation



Implement weekly patch updates



Institute mandatory meetings/ detailed briefings for all executives and relevant personnel.



Recommendations

Recommendation

Renew encryption certificates before expiration

NIST



PPT



Backup data



Establish a remote access VPN



Recommendations

Recommendation

Update firewall policies quarterly.

NIST



PPT



Keep encryption keys in a safe place



Install anti-virus software, update it regularly, and have a team responsible for ensuring it's functioning properly



Recommendations

Recommendation

NIST

PPT

Establish monthly communications with the authorities and the public



Provide Fraud Alert System services



Recommend and support victims with applying credit freezes



EQUIFAX DATA BREACH 2017

By: Arielle Bennett, Adi
Hacker, Bracha Lewittes,
Nicole Mandel, Dassi
Mayerfeld, Meghan Notkin,
Adielle Rosenblum

Thank you!