Security Case Study and Report

Equifax Data Breach (2017): Lessons for Better Security

MIT xPRO

Presented by:
Subhadra Mahanta

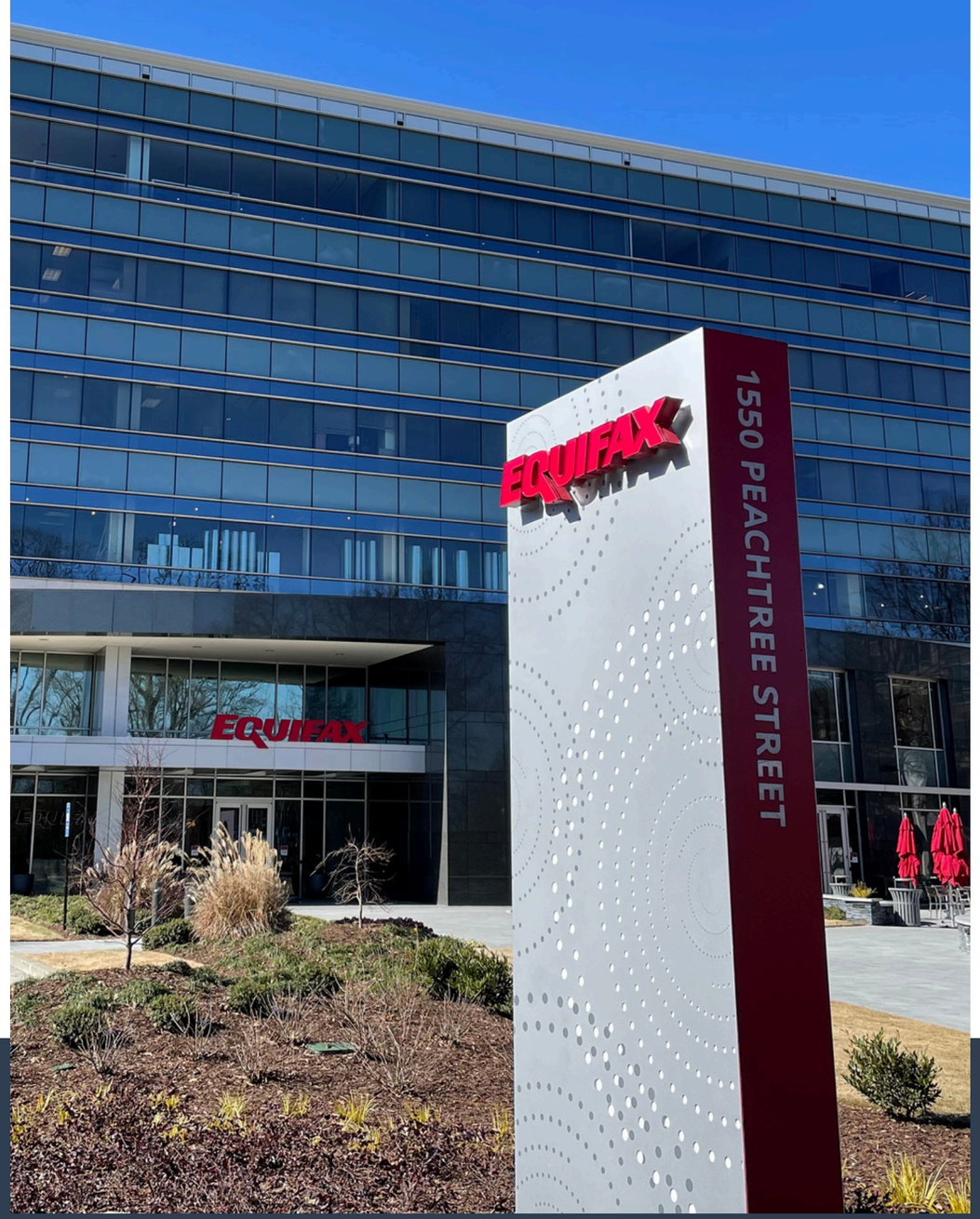
Date Presented:
24 April 2025

MIT xPRO

Agenda

Presentation Breakdown:

- All About The Breach
- Improved Handling Strategy
- Conclusion



Breach Overview

The 2017 Equifax breach exposed data of 147 million Americans due to a missed Apache Struts patch. Hackers accessed Social Security numbers, birth dates, and more. It revealed major cybersecurity failures and sparked widespread concern over data privacy and corporate responsibility.

Breach Overview

Key Events:

- Mar 6, 2017: CVE-2017-5638 (Apache Struts 2) publicly disclosed.
- Equifax failed to patch.
- May–July 2017: Attackers exploited the flaw, deployed web shells.
- July 29: Breach discovered.
- Sept 7: Publicly disclosed.

Impact:

- Affected 147.9M US, 15.2M UK, 19K Canada citizens.
- 209K credit card numbers stolen.

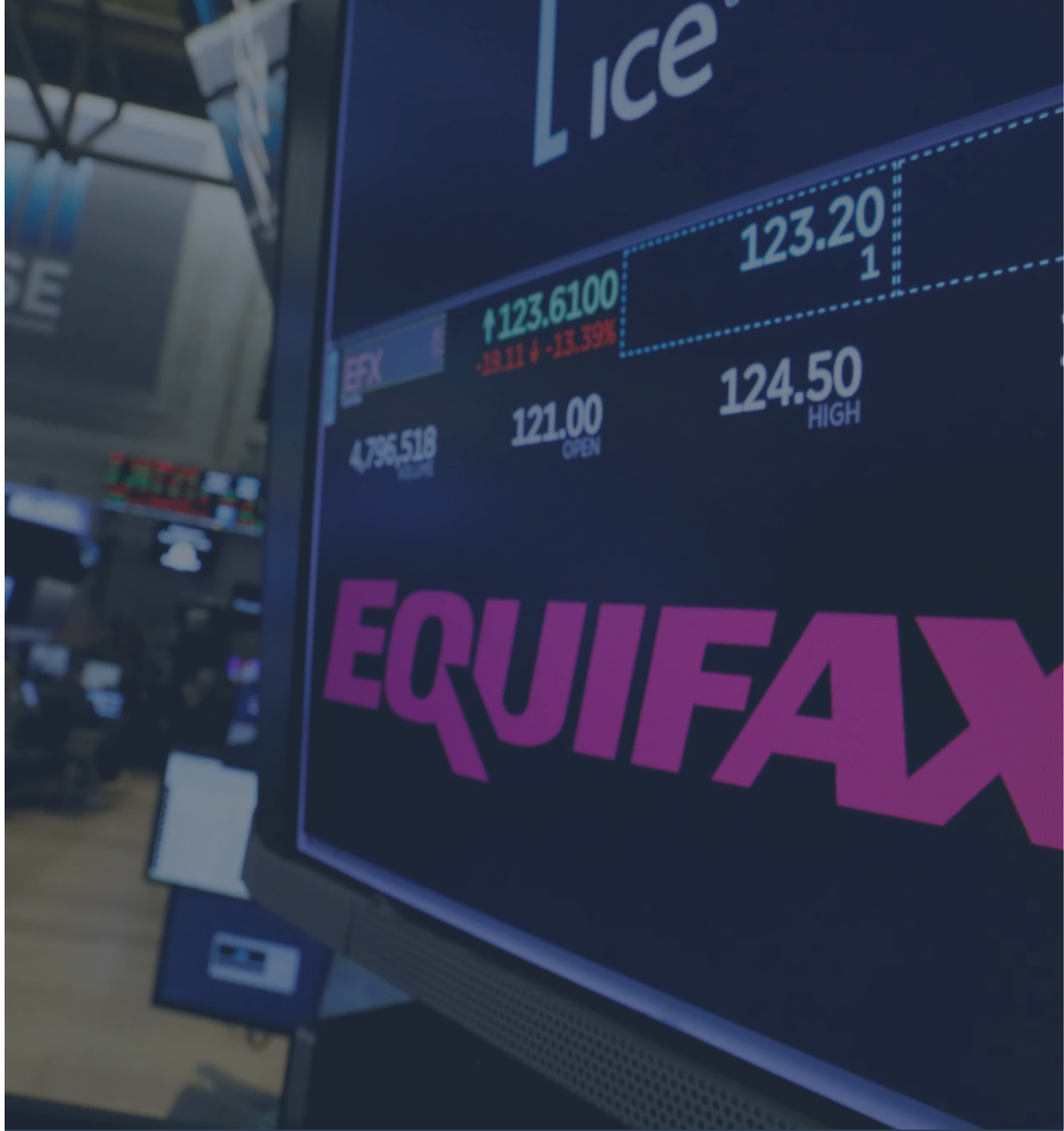
Breach Timeline

March 6	May 12	July 29	September 7	Post-Breach
CVE published, along with fix. Apache Struts vulnerability (CVE-2017-5638) publicly disclosed, along with an available patch to fix the issue.	Exploitation begins Attackers begin exploiting the unpatched vulnerability to access Equifax's systems undetected.	Detection Equifax detects suspicious network activity and identifies unauthorized access to sensitive data.	Public disclosure Equifax publicly announces the breach, triggering massive public and governmental backlash.	Resignations, lawsuits, settlement Executives resigned, multiple lawsuits were filed, and a $700 million+ settlement was reached with regulators and victims.

Scope of the Breach

Equifax breach exposed unencrypted PII of 147M.
Leading to major resignations, lawsuits, $700M+ in settlements, and stock crash.

- 44% of US population affected
- Unencrypted PII including SSNs, DoB, addresses
- $700M+ in settlements
- Stock price dropped by 13%
- 30+ lawsuits filed
- CEO, CIO, CSO resigned



Organizational Failures

Systemic Security Negligence Across Key IT Domains

not just a tech failure, but a cascade of ignored warnings, weak controls, and organizational complacency

- **Patch Management**: No follow-up on critical patches
- **Asset Management**: Poor visibility and accountability
- **IAM:** Weak credentials, no MFA
- **Monitoring**: Expired certs, failed detection
- **Network**: Flat architecture, no segmentation
- **Disclosure**: Delay in public and internal communication

Root Cause Analysis

Immediate Weakness:

Unpatched Apache Struts vulnerability exploited via HTTP headers.

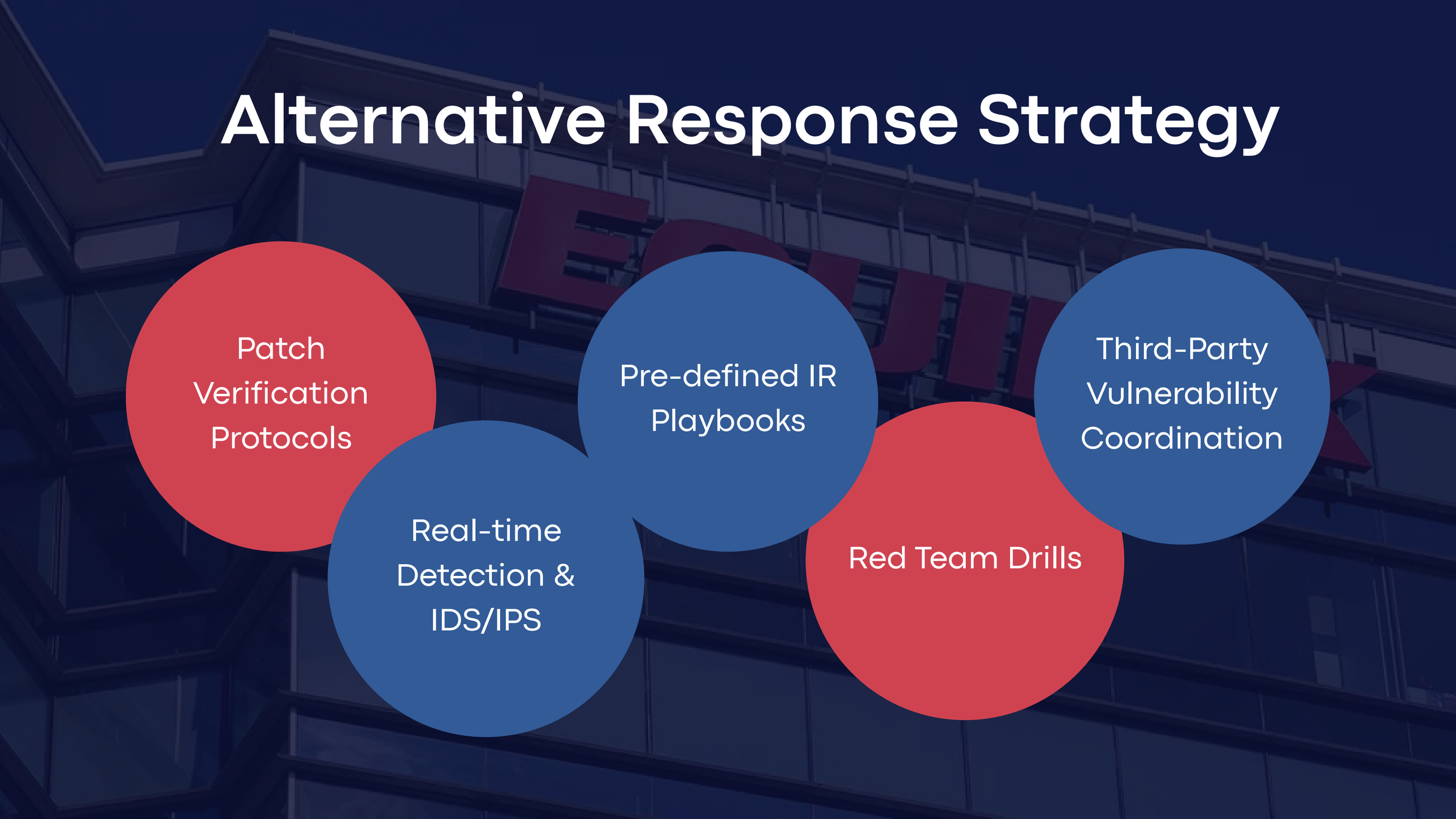
Systemic Failures:

- **Flat network with no segmentation**
- **Weak encryption or plaintext PII**
- **Excessive privileges, no IAM enforcement**

Incident Response Failures

!	!!	!!!	!!!!	!!!!!
8-week delay in public disclosure	Web shell credentials remained active	Poor internal and public communication	Forensics missed backup abuse	Executives delayed action

Alternative Response Strategy



Preventive Measures

Implement NIST Cybersecurity Framework

Deploy Zero Trust Architecture

Use Software Bill of Materials (SBOM)

Full Encryption (At Rest & In Transit)

AI-based Anomaly Detection

Regular Security Audits

Employee Training & Accountability

Lessons Learned

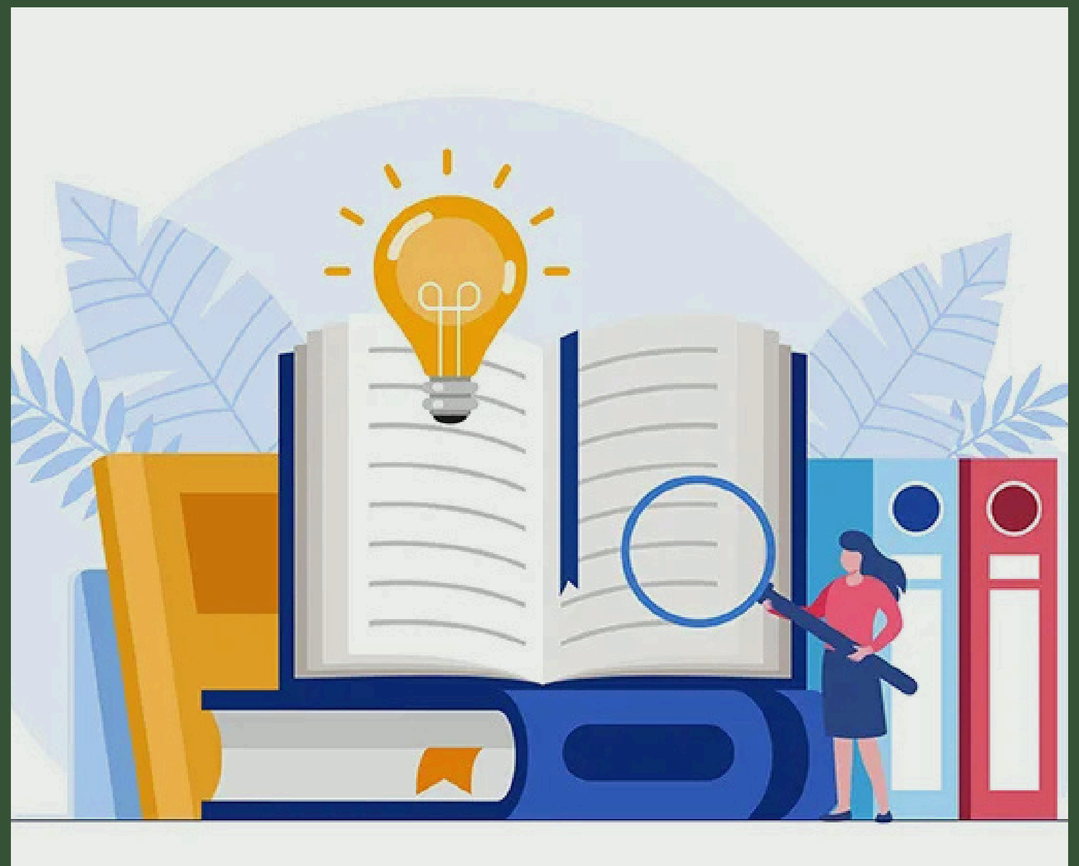
- Assign CVE ownership with deadlines
- Embed security in development lifecycle
- Zero Trust: Verify everything
- Run drills and respond mid-incident
- Transparency reduces fines and restores trust

Final Thoughts

Real security is accountability!

Real security isn't just firewalls and patches—it's accountability at every level. The Equifax breach showed that when no one owns risk, everyone pays. Strong policies mean nothing without responsible action. Security fails when accountability fades; it thrives when every individual treats protection as their personal duty.

References



https://en.wikipedia.org/wiki/2017_Equifax_data_breach#:~:text=On%20September%2026%20Equifax%20announced,Paulino%20do%20Rego%20Barros%20Jr.

https://sevenpillarsinstitute.org/case-study-equifax-data-breach/#:~:text=On%20July%2029th%2C%20Equifax%20renewed,collect%20American%20data%20(Fruhlinger).

https://www.youtube.com/watch?v=_6Qbslgpw8U&t=206s

https://www.youtube.com/watch?v=g6sb6LhO0U4

https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html

https://www.secureworld.io/industry-news/equifax-breach-social-media

https://www.cnbc.com/2018/03/14/former-equifax-executive-charged-with-insider-trading-ahead-of-data-breach.html

https://www.secureworld.io/industry-news/equifax-post-breach-why-the-ceo-survived-just-19-days https://www.secureworld.io/industry-news/day-by-day-timeline-of-equifax-breach

https://www.youtube.com/watch?v=bh1gzJFVFLc