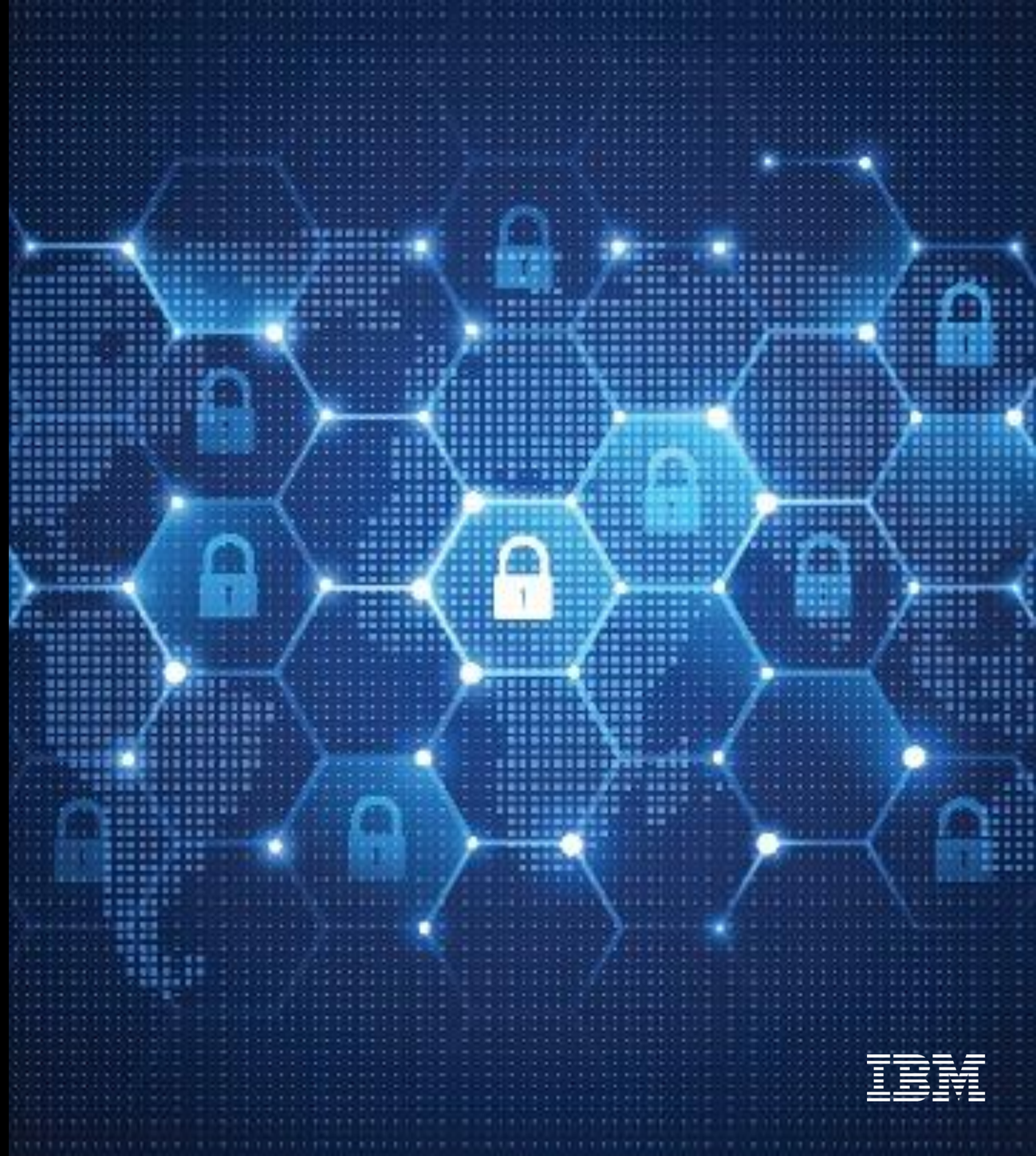
Case Study

Ransomware

Equifax



Attack Category:
Ransomware

Description:
Ransomware is malicious software that encrypts or locks a victim's files or system, demanding payment to restore access. Types include:
- Crypto Ransomware: Encrypts files.
- Locker Ransomware: Locks the system.
- Leakware/Doxware: Threatens to release sensitive data.

Statistic:
In 2022, 64% of organizations faced ransomware attacks, with the average ransom payment at $570,000. The total global cost of ransomware attacks exceeded $20 billion.

Sources:
- Sophos 2022 Threat Report

- X-Force Threat Intelligence Index 2023

Company Description and Breach Summary

Company: Equifax

Description:
Equifax is a major U.S. credit reporting agency providing credit-related services.

Breach Summary:In 2017, Equifax suffered a data breach due to an unpatched Apache Struts vulnerability. This exposed personal information of 147 million people, including Social Security numbers and birth dates. The breach was discovered in July 2017 and publicly announced in September 2017.

Sources:
- Equifax Data Breach Overview

- FTC Equifax Breach Information

Timeline

1. **March 7, 2017:** Apache Struts vulnerability (CVE-2017-5638) disclosed, which Equifax failed to patch.
2. **May 13, 2017:** Attackers exploit the unpatched vulnerability to gain access to Equifax's systems.
3. **July 29, 2017:** Equifax detects suspicious activity and begins its investigation into the breach.
4. **August 2, 2017:** Equifax confirms the breach and starts assessing the extent of the data compromised.
5. **September 7, 2017:** Equifax publicly announces the data breach, disclosing that personal information of 147 million people was affected.
6. **September 15, 2017:** Equifax offers free credit monitoring and identity theft protection services to those impacted by the breach.

Vulnerabilities

Equifax’s breach resulted from unpatched software, poor patch management, inadequate network segmentation, and weak incident response.

Vulnerability 1

Unpatched Software

- **Issue:** Failure to apply a critical Apache Struts patch.
- **Impact:** Allowed unauthorized access.

Vulnerability 2

Poor Patch Management

- **Issue:** Delays in applying security updates.
- **Impact:** Systems remained vulnerable.

Vulnerability 3

Inadequate Network Segmentation

- **Issue:** Lack of separation between network areas.
- **Impact:** Attackers accessed sensitive data.

Vulnerability 4

Weak Incident Detection and Response

- **Issue:** Slow breach detection and response.
- **Impact:** Increased data exposure.

Costs and Prevention

Costs

- 1. $700 million: Settlements with affected parties.
- 2. Over $1 billion: Cost for credit monitoring services.
- 3. Significant Loss: Consumer trust.
- 4. Stock Price Drop: Negative impact on market value.

Prevention

1. Regular Software Updates: Ensure timely patching of vulnerabilities.

2. Network Segmentation: Separate sensitive data from other areas.

3. Incident Response Plan: Develop and test a response strategy.

4. Employee Training: Regularly train staff on cybersecurity practices.