RESEARCH OF EQIFAX DATA BREACH (2017) & IMPACT

Overview of the Breach

- **Organization Involved:** Equifax, one of the largest credit reporting agencies in the U.S., handling sensitive information for over 820 million consumers.
- **Timeline:**
  - The breach began on May 13, 2017, and continued until July 30, 2017.
  - Equifax publicly disclosed the breach on September 7, 2017.
- **Cause of Breach:** The breach was caused by the Apache Struts vulnerability (CVE-2017-5638), which had been disclosed in March 2017. Despite this, Equifax failed to patch the vulnerability, allowing attackers to gain unauthorized access to their systems.

Impact Analysis

1. **Financial Impact:**
   - Equifax faced a $700 million settlement in 2019, which was part of a resolution with the U.S. Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and 48 states.
   - The breach cost the company approximately $1.4 billion in total, including legal fees, fines, and customer compensation.
2. **Reputational Damage:**
   - The breach severely damaged Equifax's reputation. Following the breach, public trust in the company dropped dramatically.
   - The breach also led to the resignation of key executives, including CEO Richard Smith.
3. **Operational Consequences:**
   - Equifax had to implement significant operational changes, including improving security measures across its platforms.

Lessons Learned

1. **Vulnerabilities Exploited:**
   - The attackers exploited an unpatched vulnerability in Apache Struts, which was a known security flaw with a patch released months before the breach occurred.
2. **Preventive Measures:**
   - Equifax's failure to patch its systems promptly underscores the need for regular vulnerability assessments and patch management processes.
3. **Actions Implemented Post-Breach:**
   - After the breach, Equifax took several steps to enhance its security, including increasing investments in cybersecurity and offering free credit monitoring to affected consumers.

ShieldGuard Inc. Takeaway

Based on the lessons learned from the Equifax breach, ShieldGuard can implement these measures:

1. **Recommendation 1**: Regularly update and patch all critical systems, especially those storing sensitive data.
2. **Recommendation 2:** Develop and test a comprehensive incident response plan for quicker containment of breaches.
3. **Recommendation 3:** Ensure company-wide security awareness and training, ensuring that all employees understand the significance of security protocols.