Security Incident Response for Inject Health

Kompliance Krew

- *Shriram*
- *Julie Dzeze*
- *Mohammed Adnan*
- *Sidharth Krishna*

Presented to: Inject Health CEO and Board of Directors
CSEC 751.01 – Fall 2024
Information Security, Policy and Law
Date: 12/04/2024

Introduction

Reason for this presentation: It details about the recent cyber attack on Inject Health named “Russian Tsunami”, which caused massive data breach affecting both clients and employee records.

Why does it matter?

It is a threat which opened a gate for bigger risk and even a privacy dilemma for clients.

It highly affected the reputation of the company and the employee trust it carries along with clients.

The data has lot of potential which can mutate in different level and can affect the clients.

The possibility of selling the stolen records on dark web is highly possible and a serious threat.

It can highly affect the company legally for not safeguarding the assets through proper regulations and policies.

This breach is part of the attack and chance of being in the attack life cycle is high.

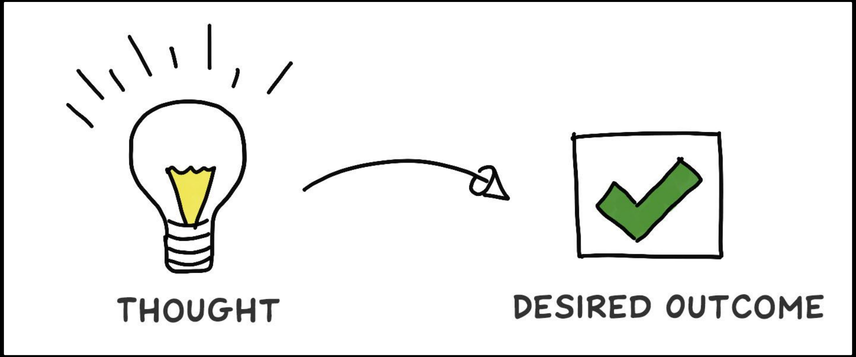
Overview

Our Comprehensive overview or just a table of contents as follows:

- Background of Inject Health and it’s assets (Inventory).
- Summary of the breach especially the technical vulnerabilities.
- How breach happened? Based on current information we have.
- Complete analysis of regulatory violations.
- Compliance requirements across jurisdiction.
- Recommended solution and controls from security frameworks.
- How we can prevent this in future.

Expected Outcome

- Clear analysis and understanding of security gaps and regulatory requirements.
- Next steps for applying the regulatory frameworks.
- Understanding of regulatory frameworks on different regions.
- Protecting the assets of the “Inject Health”.



Background: Inject Health

- International group of doctors, offering alternative health services to its patients. Services include:
  - Specialized Lab Testing
    - Gut Health
    - DNA based testing
  - Mental Health & Wellbeing
  - Metabolism and Heart Health
  - Non-Invasive Plastic Surgery
- Provides patient loans
- Has doctors and nurses in New York, Massachusetts, California, France, and Canada
- Annual revenue is $250 million
- Impacted by the “Russian Tsunami” where Russia successfully hacked and exposed 500,000,000 patient records containing patient PHI
  - Inject Health’s customer database was hacked, resulting in 100,000 compromised patient records
- Database vendor is OneSolution LLP

Russian Tsunami - Summary

- Russia, with suspected chinese involvement, hacks 20,000 US organizations exposing 500 million records (est 120 billion at 259$/record.), US and EU citizens among them.
- North East companies like CODA, Inject Health, and Placebo Pharmaceuticals lost patient records.
- Local educational institutions lost students and employee records, records leaked in social media and their websites defaced.
- MegarCorp Alternative Inc., employee personal data found in online games.
- Terminus Education and MegaCorp Alternative under scrutiny by CA state for selling customer information without authorization.

Russian Tsunami - Inject Health

- Approximately 100,000 records (50,000 from US, rest from EU) compromised, and found on dark web (not yet made public)
- Information includes ePHI, loan contracts, credit card information, payment records, payroll, and HR files.
- Hacked 24 hrs ago and authorities not yet notified.
- OneSolution (vendor for IT services) failures:
  - No MFA for EU
  - Patching in CA delayed 7 months
  - Simple network password due to glitch

Likely Causes of the Breach

Insufficient Security Controls and Weak Vendor Management

- Lack of Comprehensive Security Framework
- Failure to adopt robust security practices for internal systems and third-party vendor relationships are root cause.
- Critical security measures are missing making it easier for attackers to exploit vulnerabilities.

Main idea: OneSolution LLP, the IT vendor was not sufficiently monitored. This oversight transformed as a security gap, which ultimately contributed to the breach.

Supporting Vulnerabilities

1. Lack of Multi-Factor Authentication (MFA)

   Misconfigurations on MFA for accessing the critical records includes sensitive data like EU customer records created a easy point for attackers. It lead to compromised credentials.

2. Not updating the system (Delayed Patching of Known vulnerabilities)

   Failure to not apply proper patching and updating the system highly contributed to breach. Attacker took advantage of the vulnerabilities for example tls 1.0 or log4j or sql injection (not using tokens) etc.

3. Weak Password Policies

   Brute force attack can reveal the weak passwords and reused credentials is one of the root cause for lateral movement across the network and resources.

Additional Details to Consider

1. **Logging and Monitoring**

   Having a proper SIEM solutions for monitoring logs and handling system generated resources is crucial. Especially having XDR solutions and playbooks reduce the chance of breach.

   Lack of Proper Incident Response.

2. **Insecure data transmission**

   Transmission of data between Inject health and OneSolution LLP without proper encryption give a way for spoofing and tampering attacks like Man in the middle. Chance of exploiting and stealing the data in transit.

Boston - MA

Massachusetts Data Privacy Law (Massachusetts General Laws Chapter 93H and 201 CMR 17.00)

Sections Violated:

- Section 17.03: Security Standards
- Section 17.04: Computer System Security Requirements
- Section 17.05: Compliance deadline

Specific Violations:

- Exposure of patient health information for Boston-based customers(might be part of 50,000 US records)
- Potential compromise of personal and financial data of Massachusetts residents (might be part of 100,000 employee records)
- Failure to implement adequate cybersecurity measures to protect sensitive information (Lack of robust password complexity requirements due to a system glitch)

How to Address Regulation Violation

- Establish and enforce complex password requirements(fix the glitch!)
- Deploy multi-factor authentication across all systems (if not already implemented for US)
- Conduct a thorough security audit and patch all systems promptly(if fresno was not the only office to be patched, also must be done at annually as per 17.03)
- Create and maintain detailed documentation of security measures(for future uses.)
- Develop a robust incident response plan(taking into account all the recent changes)
- Educate employees on proper use of the computer security system and the importance of personal information security. (training)
- Ensure Vendor is compliant with all standards.
- Following a specific controls like CIS (Center for Internet Security Critical Security Controls) will help strengthening overall cybersecurity posture by prioritizing critical security actions and having good practices.

Boston - MA

Sections Violated:

- Section 93H-2: Duty to Safeguard Personal Information
- Section 93H-3: Notification Requirements

Specific Violations:

- Failure to immediately notify affected individuals about the data breach
- Not reporting the breach to appropriate state authorities within the mandated time frame
- Compromise of 50,000 US citizen records, including Massachusetts residents

Specific Actions Needed

- Send notice to all affected Massachusetts residents with all the requirements(right to police report, a security freeze at no charge, etc)
- Establish a dedicated support mechanism for impacted customers.
- Prepare a detailed report for the Massachusetts Authorities.
- Conduct regular HIPAA and state law compliance audits.

Boston - MA

Additional Regulations Violated: HIPAA

Privacy Rule (45 CFR 164.400-414)

- **Violation**: Exposed sensitive health information (ePHI), violating patient privacy protections.
- **Solution**: Encrypt ePHI and apply strict access controls to safeguard patient data.

Security Rule (45 CFR 164.308, 164.312)

- **Violation**: Lack of administrative, technical, and physical safeguards, such as delayed patching and weak passwords.
- **Solution**: Deploy technical safeguards like Multi-Factor Authentication (MFA) and timely software updates.

Vancouver, Canada: Regulations Violated

- Regulation violation: **PIPEDA (Personal Information Protection and Electronic Documents Act)**
- Overview: PIPEDA is a Canadian federal law that governs how private-sector organizations handle personal information in the course of commercial activities. It aims to balance individuals' privacy rights with organizations' need to collect, use, and disclose personal data.
  - Does not apply to Quebec, Alberta, and British Columbia

Vancouver, Canada: Regulations Violated

- OneSolution LLP failed to follow:
    - **PIPEDA Principle 7 – Safeguards**
        - Principle states that business “**must protect personal information against loss or theft as well as unauthorized access, disclosure, copying use or modification. Level of security should be based on sensitivity of the information**”
        - **How the violation occurred**: Passwords to the network did not require complexity due to a glitch in the system i.e. weak password requirements
    - **PIPEDA Principle 4 – Limiting Collection**
        - “Organizations must collect only what is necessary for their operations and ensure appropriate data retention policies.”
            - Inject Health collected and stored highly sensitive data (e.g., health information, payment records, loan contracts, and payroll data)

Vancouver, Canada: Regulations Violated

- OneSolution LLP failed to follow:
  - **Breach notification requirement**
    - Under PIPEDA's breach notification requirements, organizations **must** report breaches involving a "real risk of significant harm" to individuals to:
      - The Office of the Privacy Commissioner of Canada (OPC).
      - Affected individuals as soon as possible.
    - Inject Health has **not** notified authorities or individuals 24 hours after discovering the breach, violating this requirement.
  - **PIPEDA Principle 1 – Accountability**
    - Organizations are responsible for ensuring that third-party vendors (e.g., OneSolution LLP) comply with privacy requirements.
      - The breach originated from their vendor, and poor oversight of vendor practices, including delayed patching and insecure passwords, reflects non-compliance.

Vancouver, Canada: Violation Solution

- To address the situation, Inject Health must:
  1. **Immediately** notify affected individuals and Canadian authorities (OPC).
  2. **Enhance** security measures, including enforcing MFA, strengthening passwords, and expediting patches.
  3. **Audit and improve** vendor management practices to ensure compliance.

Rochester, New York: Regulations Violated

New York State Data Protection and Privacy Regulations

1. Regulation: NY SHIELD Act (Stop Hacks and Improve Electronic Data Security Act). Effective Date: March 21, 2020
2. Overview: This act considered important data protection requirements for the business handling private information of New York residents. It needs good administrative, technical and physical safeguards for protecting the data.
3. Sections Violated: Following sections are violated by the OneSolution LLP.

- Reasonable Safeguards (General Business Law 899-bb): Inject health and it's vendor didn't implement basic MFA and timely patching caused the violation.
- Data Breach Notification (General Business Law 899-aa): Inject health failed to notify the affected NY residents with 24 hours of breach.

Rochester, New York: HIPAA Compliance and Breach Impact in NY

1. Regulation: Health Insurance Portability and Accountability Act (HIPAA).
2. Overview: HIPAA handles Protected health Information (PHI) by covered entities and businesses. If a breach is happened it must be reported to Department of Health Services (HHS) and affected individuals.
3. Identification of Violations: Lack of encryption for sensitive information, unauthorized access due to MFA, Complicating HIPAA by not protecting Credit card information according to PCI DSS standards.
4. Sections Violated: Privacy Rule and Security Rule has been violated.
   - Privacy Rule (45 CFR 164.400-414): PHI has been compromised and leaked.
   - Security Rule (45 CFR 164.308, 164.312): Missing basic requirements and it''s safeguards like Administrative, physical and technical safeguards.

Paris, France: Regulations Violated

GDPR: Article 32 – Security of Processing

- **Violation**: Sensitive personal data was compromised due to the lack of robust security measures like Multi-Factor Authentication (MFA).
- **Solution**: Enforce MFA for all access points, ensure strong password policies, and implement continuous security monitoring.

GDPR: Article 33 – Breach Notification

- **Violation**: Breach not reported to EU authorities or impacted individuals within the required 72-hour timeframe.
- **Solution**: Establish a clear Incident Response Plan to meet GDPR’s notification deadlines.

Paris, France

GDPR: Article 28 – Processor Responsibilities

- **Violation**: Poor oversight of IT vendor OneSolution LLP, leading to delayed patching and weak security practices.
- **Solution**: Regular vendor audits and enforcement of GDPR-compliant security standards.

Recommended Actions

1. **Conduct Compliance Audits**: Perform a detailed GDPR compliance check across European operations.
2. **Strengthen Data Protection**: Encrypt all sensitive data, including patient records, during transmission and at rest.
3. **Vendor Management**: Establish clear contracts and monitoring mechanisms to ensure third-party compliance.

Fresno, California - Regulations Violated

CCPA: Section 1798.100 – Data Transparency

- **Violation**: Insufficient disclosure of data collection and sharing practices with customers.
- **Solution**: Update privacy notices to align with CCPA guidelines and clearly outline data usage policies.

CCPA: Section 1798.150 – Breach Notification

- **Violation**: Notification delays left residents unaware of the breach, increasing risk exposure.
- **Solution**: Create a protocol for timely notifications and communication with affected individuals.

California Data Breach Notification Law (Section 1798.82)

- **Violation**: Failure to notify authorities and individuals about the breach within a reasonable time frame.
- **Solution**: Develop an emergency response plan to ensure rapid notifications during future breaches.

Fresno, California

Additional Regulations Violated: HIPAA

Privacy Rule (45 CFR 164.400-414)

- **Violation**: Protected Health Information (PHI) was exposed, violating patient privacy.
- **Solution**: Encrypt PHI and restrict access through robust access controls (e.g., MFA).

Security Rule (45 CFR 164.308, 164.312)

- **Violation**: Missing administrative, physical, and technical safeguards, such as lack of encryption and delayed patching.
- **Solution**: Implement security measures like timely patching, end-to-end encryption, and employee cybersecurity training.

Fresno, California

Recommended Actions

1. **Streamline Patching**: Implement remote contingency measures to expedite patching during emergencies like wildfires.
2. **Enhance Training**: Educate staff on CCPA and California-specific privacy regulations to avoid future violations.
3. **Deploy Encryption**: Protect sensitive data in storage and transit with advanced encryption techniques.

Framework Selected - NIST Cybersecurity Framework (CSF)

Identify Function (ID)

- Address vendor management risks with OneSolution LLP
- Conduct comprehensive asset inventory and risk assessment
- Develop a clear understanding of organizational cybersecurity risks

Protect Function (PR)

- *Identity Management and Access Control (PR.AC)*
- Implement Multi-Factor Authentication (MFA) for all users, especially EU residents
- Establish strong password policies
- Create robust access control mechanisms

Data Security (PR.DS)

- Protect sensitive customer and employee data
- Implement encryption for stored and transmitted data
- Establish data protection procedures

NIST CSF

Information Protection Processes and Procedures (PR.IP)

- Develop and maintain configuration management processes
- Create a systematic patch management strategy
- Establish baseline security configurations for systems

Detect Function (DE)

- *Security Continuous Monitoring (DE.CM)*
- Implement continuous monitoring of systems
- Use intrusion detection systems
- Monitor for unauthorized access and potential breaches

Respond Function (RS)

- *Response Planning (RS.RP)*
- Develop an incident response plan
- Create clear communication protocols for breach notification
- Establish procedures for containment and mitigation

NIST CSF

Recover Function (RC)

- *Recovery Planning (RC.RP)*
- Develop comprehensive disaster recovery plans
- Create backup and restoration procedures
- Establish communication strategies for stakeholders during recovery

Key vulnerabilities addressed:

- Lack of MFA
- Delayed system patching
- Weak password requirements
- Potential vendor-related security risks
- Access Control and Security Monitoring
- Response and Recovery Planning

THANK YOU!