Compliance Cops

Healing the Breach: Compliance Cops Strategy for Inject Health's Recovery

Team members : Vijay, Alekhya, Tina and Shashank

CSEC 751 : Information Security, Policy and Law

Date: 06 December 2024

Introduction

ANALYZE

Examine the financial, reputational, and operational consequences of the security breach.

IDENTIFY

Outline the specific regulations and compliance standards that were breached.

FIX

Propose actionable steps to address the violations and ensure future regulatory compliance.

OUR GOAL : ANALYZE, IDENTIFY, FIX

Inject **Health**

Revolutionizing Healthcare: Inject Health is an international consortium of visionary doctors and healthcare professionals dedicated to transforming patient care through innovative alternative medicine. The team includes 35 doctors and registered nurses dedicated to personalized patient care.

INJECT HEALTH HAS STATE-OF-THE-ART FACILITIES IN

- ROCHESTER, NY
- BOSTON, MA
- FRESNO, CA
- PARIS, FRANCE
- VANCOUVER, CANADA

Annual Revenue of approximately **$250 million**

Partnership with **OneSolution LLP** for comprehensive IT Services

The **Russian** Tsunami

Global Impact

20,000

US based organizations **hacked** by Russia

500 million

records exposed of US, EU, and other country citizens

$259

Hackers are **selling** each record with **PII** in the black market

FBI INVESTIGATING POTENTIAL INVOLVEMENT OF CHINA.

Impact on Inject Health

100,000 records

Including personal information, health records, **complete credit card information**, and loan contracts

OneSolution LLP

MFA was **not implemented** for EU residents

Patching of end-user systems **delayed** by 7 months in Fresno, CA due to wildfires

Network passwords did not require complexity due to a **system glitch**

Payroll and HR files were **exfiltrated**

Customer data found on the **dark web**

50,000

records from **US citizens** including states CA,MA,NY

Unencrypted storage of sensitive data

Inadequate employee cybersecurity training

Lack of real-time monitoring and incident detection

Unfolding the **breach**

TIMELINE OF THE BREACH

1 EXPLOITATION OF UNPATCHED SYSTEMS

Delayed Patching in Fresno, CA Office due too wildfires

2 SPEAR PHISHING ATTACK LEADING TO CREDENTIAL COMPROMISE

An employee inadvertently clicked on a malicious link, compromising their login credentials.

3 WEAK PASSWORD POLICIES AND LACK OF MFA

Attackers leveraged stolen credentials to access systems without additional authentication barriers.

4 INADEQUATE VENDOR SECURITY MEASURES

Allowed the attackers to move laterally within the network and access sensitive data stored in the vendor's systems.

5 UNENCRYPTED SENSITIVE DATA STORAGE

Making data easily accessible once the network was breached.

6 LACK OF REAL-TIME MONITORING

Absence of intrusion detection systems delayed the discovery of the breach until unusual activity was noticed 24 hours ago

Regulations **violated**

New York State, USA **Regulation**

REGULATION NAME

NYS Information Security Breach and Notification Act

REGULATION SECTION

NY Gen Bus Law §899-aa

VIOLATION - 1

Inject Health did not notify affected individuals "**in the most expedient time possible**" as required under this law.

IMPACT

- **Civil Penalties**: Potential fines and legal actions by affected individuals for failing to notify in a timely manner.
- **Reputation Damage**: The lack of prompt transparency may lead to mistrust from New York residents.
- **Legal Risks**: Noncompliance could lead to lawsuits or class action claims from affected parties.

REMEDIATION STEPS

- Immediately notify affected individuals in accordance with New York law.
- Develop a comprehensive breach notification protocol to meet New York's legal timelines.
- Enhance internal logging and monitoring to identify breaches more efficiently and minimize delays.
- Provide identity theft protection services to affected New York residents as part of the breach response strategy.

New York State, USA **Regulation**

REGULATION NAME

Stop Hacks and Improve Electronic Data Security (SHIELD) Act

REGULATION SECTION

NY Gen Bus Law §899-bb

VIOLATION - 2

Failure to implement reasonable safeguards. Examples include:

- Administrative safeguards: Lack of regular employee training.
- Technical safeguards: Weak password policies across the organization.

IMPACT

- **Fines**: Civil penalties of up to **$5,000 per violation.**
- **Reputation Damage**: Breach of trust with New York residents could lead to customer loss and reduced credibility.
- **Operational Scrutiny**: Regulators may impose audits or increased compliance requirements.

REMEDIATION STEPS

- Implement a company-wide **password policy** requiring complexity and regular updates.
- Establish an **employee training program** for cybersecurity awareness to mitigate human error risks.
- Conduct a thorough **vendor audit** of OneSolution LLP to ensure compliance with SHIELD Act security requirements.

New York State, USA **Regulation**

REGULATION NAME

New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500)

REGULATION SECTION

- Section 500.2 Cybersecurity Program
- Section 500.9 Risk Assessment
- Section 500.11 Third Party Service Provider Security Policy
- Section 500.12 Multi-Factor Authentication

VIOLATIONS

500.02: No comprehensive cybersecurity program was implemented to protect sensitive data.

500.09: Risk assessments were not conducted to identify and address system vulnerabilities.

VIOLATIONS

500.11: Inject Health failed to ensure OneSolution LLP complied with adequate security measures.

500.12: Lack of MFA left sensitive systems exposed to unauthorized access.

BREACH NOTIFICATION

Under **Section 500.17**, Inject Health must report the breach to **NYDFS within 72 hours** of discovery to avoid non-compliance.

REMEDIATION STEPS

- Implement a comprehensive cybersecurity program to protect sensitive data.
- Conduct regular risk assessments to identify and address vulnerabilities.
- Strengthen third-party oversight to ensure vendors comply with security standards.
- Enforce multi-factor authentication (MFA) for accessing critical systems.

IMPACT

- **Fines**: Penalties up to **$250,000** or **$1,000 per violation per day**.
- **Reputation Damage**: Loss of trust with regulators and customers in New York.
- **Operational Risks**: Increased scrutiny and potential restrictions on operations.

Massachusetts State, USA **Regulation**

REGULATION NAME

Massachusetts Data Breach Notification Law

REGULATION SECTION

MA Gen Law c. 93H Section 3

VIOLATION - 1

Inject Health failed to notify the Massachusetts Attorney General, the Director of Consumer Affairs, and affected residents **without unreasonable delay**, as required by law.

IMPACT

- **Civil Penalties**: The Attorney General may impose penalties of up to **$5,000 per violation** for noncompliance.
- **Consumer Protection Lawsuits**: Affected individuals may pursue civil action, increasing financial and legal exposure.
- **Reputation Damage**: Delayed notification undermines trust among Massachusetts residents and increases public scrutiny.

REMEDIATION STEPS

- Notify the Massachusetts Attorney General's Office and residents immediately upon detecting future breaches.
- Ensure all records containing personal information are encrypted as required by law.
- Implement an employee training program focused on phishing awareness and secure handling of sensitive data.

Massachusetts State, USA **Regulation**

REGULATION NAME

Massachusetts Data Security Regulations

REGULATION SECTION

201 CMR 17.03

VIOLATION - 2

Inject Health failed to implement reasonable security measures:

- Weak password policies and no vendor security audits.
- No employee training on cybersecurity best practices.

IMPACT

- **Civil Penalties**: The Attorney General may impose penalties of up to **$5,000 per violation** for noncompliance.
- **Reputation Damage**: Failure to comply with state regulations can erode trust with Massachusetts residents.
- **Reputation Damage**: Delayed notification undermines trust among Massachusetts residents and increases public scrutiny.

REMEDIATION STEPS

- Implement a comprehensive **password policy** requiring complexity and regular changes.
- Conduct a **vendor audit** to ensure compliance with 201 CMR 17.03.
- Establish a **Written Information Security Program (WISP)** to outline security measures for data protection.
- Provide regular **cybersecurity training** for all employees.

California State, USA **Regulation**

REGULATION NAME

California Breach Notification Law

REGULATION SECTION

California Civil Code §1798.82 – Breach Notification Requirements

VIOLATION - 1

Inject Health failed to notify affected California residents "**immediately following discovery**" of the breach. Notifications must include details of the breach and mitigation steps.

IMPACT

- **Fines**: Penalties for noncompliance can reach **$2,500 per violation**.
- **Reputation Damage**: Delayed notification undermines public trust.
- **Legal Risks**: Civil actions by affected individuals could lead to additional financial liabilities.

REMEDIATION STEPS

- Notify affected California residents immediately and provide free credit monitoring.
- Establish a detailed **Incident Response Plan (IRP)** to ensure timely notifications.
- Assign a **data breach response team** to handle future incidents efficiently.

California State, USA **Regulation**

REGULATION NAME

California Consumer Privacy Act (CCPA)

REGULATION SECTION

§1798.100(e) – Duty to Implement Reasonable Security Practices

VIOLATION - 2

Delayed patching for seven months in California exposed vulnerabilities, violating the requirement for reasonable security measures.

IMPACT

- **Fines**: Up to **$2,500 per violation** or **$7,500 for intentional violations**.
- **Legal Risk**: Residents may file civil lawsuits, increasing financial liabilities.
- **Reputation Damage**: Negligence undermines customer trust in California.

REMEDIATION STEPS

- Enforce a strict **patch management policy** with defined timelines.
- Conduct regular **risk assessments** to identify and address vulnerabilities.
- Improve vendor oversight by implementing compliance audits.

Federal Regulation **HIPAA**

Regulation Name

HIPAA Privacy and Security Rules

Federal Regulation

Health Insurance Portability and Accountability Act

VIOLATION - 1

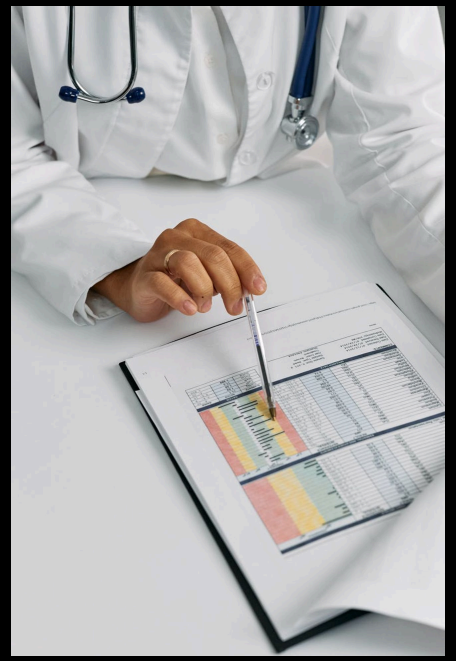
45 CFR §164.312 - Technical Safeguards

- **No Access Control**: Inject Health did not implement **MFA** or enforce **strong password policies**, leaving ePHI vulnerable to unauthorized access.
- **No Audit Control**: Failed to regularly **review system activity logs** to detect unauthorized access or unusual activity.

VIOLATION - 2

45 CFR §164.308(a)(1) – Administrative Safeguards

- **No Risk Analysis**: Inject Health did not conduct a thorough **risk assessment** to identify vulnerabilities to ePHI.
- **No Risk Management**: Failed to implement adequate safeguards, such as **MFA** and **strong password policies**, to mitigate identified risks.
- **No Sanction Policy**: No evidence of enforcement of a **sanction policy** for non-compliance with security protocols.



REMEDIATION STEPS

Implement Technical Safeguards: Stronger password policies and mandatory MFA for all employees with access to PHI.

Conduct Breach Notifications: Notify affected individuals within 60 days as required by HIPAA, as well as HHS and, if necessary, the media.

Training & Awareness: Ensure all employees receive regular training on HIPAA and security best practices.

IMPACT

Fines: HIPAA violations can result in fines ranging from $100 to $50,000 per violation, with an annual cap of $1.5 million for repeat violations.

Civil Lawsuits: Victims of the breach can file lawsuits for violations of their privacy, potentially leading to substantial settlements.

Loss of Business: Violations of HIPAA could damage Inject Health's credibility in the healthcare industry, leading to loss of clients, especially in the medical field.

BREACH NOTIFICATION

45 CFR §164.404 – Notification to Individuals of Breach

Inject Health has not yet violated HIPAA's Breach Notification Rule, but there is a risk of future noncompliance if notification obligations are not fulfilled within the 60-day timeframe.

Federal Regulation **GLBA**

Regulation Name

Gramm-Leach-Bliley Act of 1999

Federal Regulation

Gramm-Leach-Bliley Act of 1999

VIOLATION - 1

16 CFR §314.1 - Safeguard Rule

Developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information is a standard of GLBA. Failure to enforce Exposed loan contracts and credit card information, violating the Safeguards Rule by failing to encrypt sensitive data and implement robust access controls like MFA.

VIOLATION - 2

15 USC §6802 - Privacy Rule

Obligates institutions that handle financial data to notify customers about their data-sharing practices and provide options to opt out of non-essential data sharing. Insufficient transparency about data-sharing practices under the Privacy Rule.

REMEDIATION STEPS

Update customer privacy notices: To detail data collection, sharing practices, and opt-out mechanisms.

Monitor third-party vendors: To ensure compliance with data protection standards

Data Encryption: Encrypt sensitive financial data at rest and in transit.

Access Control: Implement MFA and role-based access controls for all systems handling NPI.

Risk Assessments: Conduct regular risk assessments and security testing to identify vulnerabilities.

IMPACT

Fines: Civil penalties up to $100,000 per violation for the institution.Personal liability for officers and directors up to $10,000 per violation.

Regulatory Enforcement : Actions by the Federal Trade Commission (FTC) or other federal agencies.

Reputational Damage: Loss of customer trust and potential loss of business.

Federal Regulation **Payment Card Industry Data Security Standard (PCI DSS)**

Regulation Name

Payment Card Industry Data Security Standard (PCI DSS)

Regulation Section

Requirement 3: Protect Stored Cardholder Data

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

VIOLATION - 1

Failure to Protect Stored Cardholder Data (Requirement 3)

The complete credit card data was exposed during the breach, indicating that the sensitive information was **not encrypted** or **tokenized** when stored. PCI DSS requires that all stored cardholder data be rendered unreadable through strong encryption or tokenization techniques.

VOILATION - 2

Failure to maintain secure systems (Requirement 6)

Inject Health failed to apply **security patches** in a timely manner, leaving critical systems vulnerable for **seven months**. Regular patching is required to protect against known vulnerabilities and reduce the risk of exploitation by attackers.

VOILATION - 3

Failure to restrict access to card data (Requirement 7)

Inject Health **gave full access to sensitive cardholder data to its third-party vendor, OneSolution LLP**, which may not have needed all the data for its operations. PCI DSS requires that third-party vendors be given **only the minimum necessary access** to data based on their job role or function.

REMEDIATION STEPS

- Achieve PCI DSS Compliance
- Encrypt Cardholder Data
- Implement Access Controls
- Monitor and Test Networks
- Conduct Security Assessments such as vulnerability scans and penetration tests
- Hire a QSA to assess compliance and provide recommendations

IMPACT

Financial Penalties: Fines from payment card brands ranging from $5,000 to $100,000 per month until compliance is achieved.

Increased Transaction Fees: Higher fees imposed by payment processors.

Loss of Merchant Privileges: Risk of losing the ability to process credit card transactions.

Reputational Damage: Loss of customer trust and potential decrease in sales.

Regulations in **France**

GENERAL DATA PROTECTION REGULATION (GDPR)

France follows the General Data Protection Regulation (GDPR), which is enforced by the Commission Nationale de l'Informatique et des Libertés (CNIL). Under GDPR Article 34, organizations are required to report any data breach to the CNIL within 72 hours if it poses a risk to individuals' rights and freedoms. Additionally, affected individuals must be notified without undue delay. The CNIL ensures compliance and can impose penalties for violations of GDPR.

International Regulation **GDPR**

Regulation Name

General Data Protection Regulation

Federal Regulation

General Data Protection Regulation

VIOLATION

Article 32 - Security of Processing

The breach exposed the personal data (PII and health information) of 50,000 EU residents. GDPR mandates that organizations implement appropriate technical and organizational measures to ensure the security of personal data.

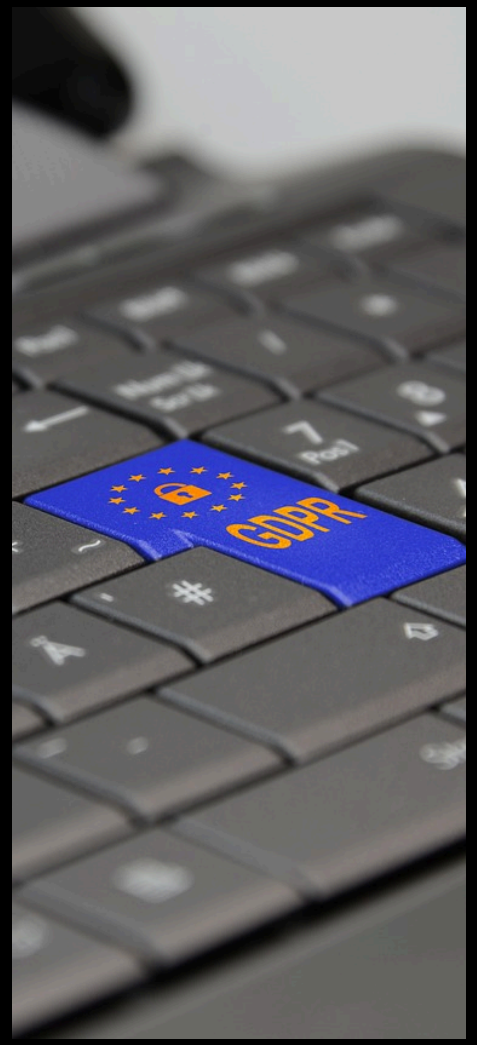
Failure to enforce MFA, delayed patching, and poor password policies are in direct violation of this article.

IMPACT

Fines: Up to €20 million or 4% of global annual turnover, whichever is higher.

Legal Risks: Inject Health may face lawsuits from affected individuals and penalties from EU data protection authorities.

Reputation Damage: Non-compliance can lead to significant loss of trust among EU customers and business partners.



REMEDIATION STEPS

Strengthen Data Security: Implement MFA, enforce strong password policies, and use encryption for sensitive data to align with GDPR security requirements.

Improve Security Practices: Conduct regular security audits, apply timely patches, and ensure vulnerability management to prevent unauthorized access.

BREACH NOTIFICATION

Article 33 – Notification of a Personal Data Breach

Article 34 – Notification to Data Subject

Article 33 requires that the supervisory authority be notified of a data breach within 72 hours of discovery, and Article 34 mandates notifying affected individuals within 30 days. While Inject Health has not yet violated these requirements, it is essential to act quickly. To stay compliant, ensure the breach is reported to the relevant authority within the 72-hour window and affected individuals are notified within 30 days.

Regulations in Canada

REGULATION NAME

Personal Information Protection and Electronic Documents Act (PIPEDA)

REGULATION SECTION

Principle 7 – Safeguards

VIOLATION

Inject Health did not implement sufficient **security measures** to protect sensitive data, such as **credit card information**. Weak passwords, lack of encryption, and failure to patch vulnerabilities led to the breach. This failure to implement reasonable safeguards violates PIPEDA's **Safeguards Principle**.

IMPACT

- **Fines**: **Up to $100,000** for non-compliance with **PIPEDA**.
- **Reputation Damage**: **Loss of customer trust** and negative publicity, especially in Canada where privacy is highly valued.
- **Legal Risk**: **Complaints to the OPC** can result in investigations, penalties, and further legal actions by affected individuals.

REMEDIATION STEPS

- **Encrypt** sensitive data and enforce **strong passwords**.
- **Limit data access** to vendors and ensure they only receive necessary information.
- **Conduct regular audits** to ensure ongoing compliance with **PIPEDA** principles.

BREACH NOTIFICATION

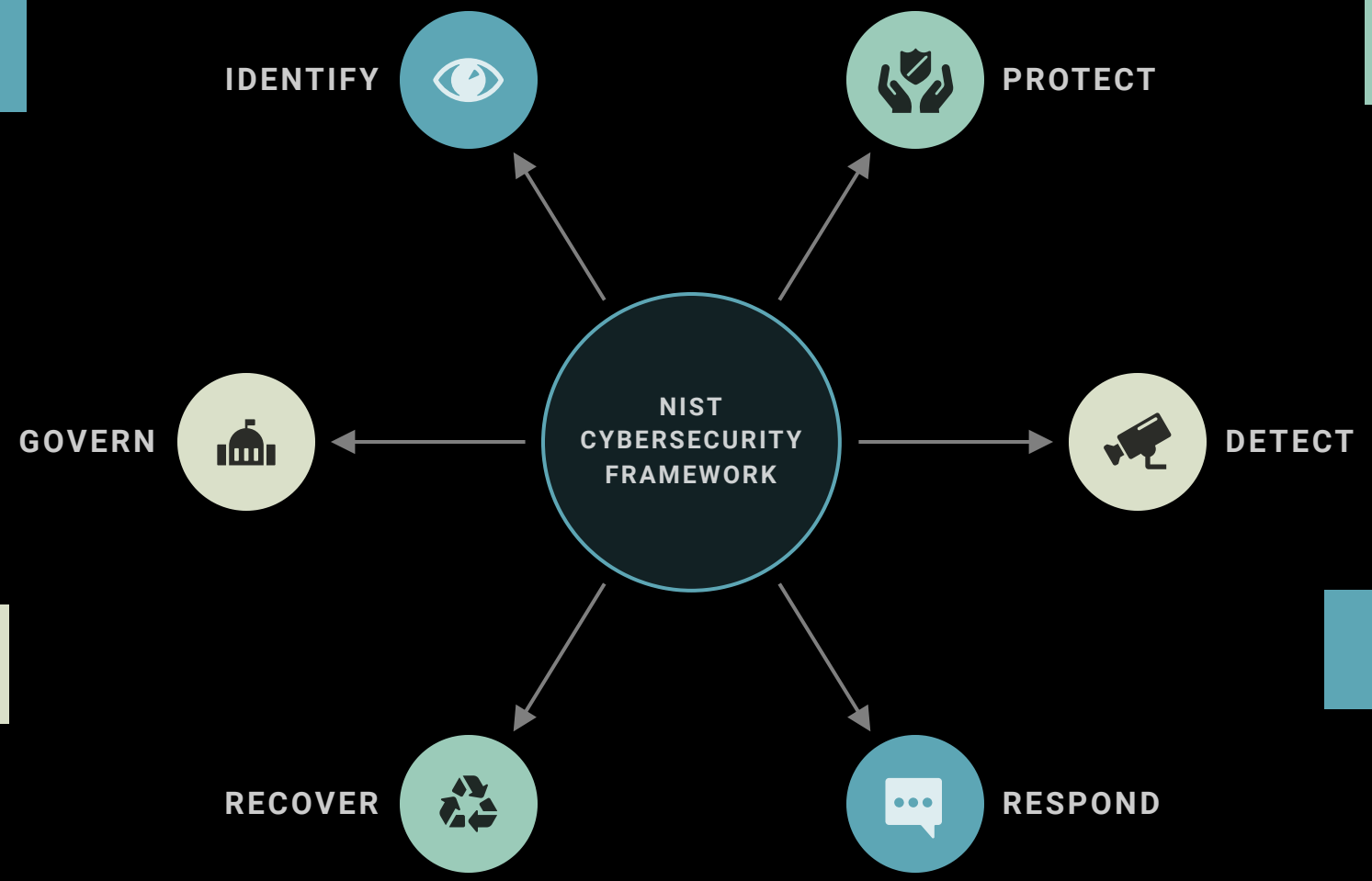
Inject Health must notify affected individuals and the **Privacy Commissioner** of Canada (OPC) **as soon as feasible**. Since the leaked data is now on the **dark web**, it poses a **real risk of significant harm**. The notification should include:

- Details of the breach.
- Affected personal data.
- Steps to protect individuals.
- Actions taken to address the breach.

The Solution **NIST Cybersecurity Framework (CSF) 2.0**

COMPREHENSIVE AND FLEXIBLE

ALIGNS WITH MULTIPLE REGULATIONS



IMPROVES COMMUNICATION

ENHANCING CYBERSECURITY POSTURE

Govern

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

ORGANIZATIONAL CONTEXT - GV.OC

GV.OC-03: Legal, regulatory, and contractual requirements are understood and managed.

Violation: Non-compliance with HIPAA, GDPR, and SHIELD Act.

Implementation: Establish a process to identify and manage all regulatory requirements.

RISK MANAGEMENT STRATEGY - GV.RM

GV.RM-01: Risk management objectives are established and agreed upon by organizational stakeholders.

Violation: Undefined cybersecurity strategy and risk management objectives.

Implementation: Create a risk management strategy that aligns with organizational goals.

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT - GV.SC

GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are defined and communicated.

Violation: Lack of vendor oversight for OneSolution LLP.

Implementation: Define and enforce vendor security expectations.

Identify

The organization's current cybersecurity risks are understood

ASSET MANAGEMENT - ID.AM

ID.AM-03: Representations of authorized network communication and data flows are maintained.

Violation: Unmapped data flows exposing PHI and PII.

Implementation: Map and secure all sensitive data flows.

RISK ASSESSMENT - ID.RA

ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk.

Violation: No risk assessments were performed for seven months.

Implementation: Conduct regular risk assessments to identify high-priority risks.

IMPROVEMENT - ID.IM

ID.IM-02: Cybersecurity practices are updated based on lessons learned and predictive indicators.

Violation: failed to **improve its security posture** after previous incidents or audits, allowing known vulnerabilities to persist.

Implementation: Regularly integrate lessons from breaches and audits into policies and update cybersecurity practices to address evolving threats.

Protect

Safeguards to manage the organization’s cybersecurity risks are used

DATA SECURITY - PR.DS

PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.

Violation: Sensitive data stored unencrypted.

Implementation: Encrypt all sensitive data at rest using industry-standard algorithms.

DATA SECURITY - PR.DS

PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.

Violation: Unprotected data transmission exposing sensitive information.

Implementation: Use secure protocols like TLS for all data transfers.

PLATFORM SECURITY - PR.PS

PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.

Violation: Delayed patching for seven months.

Implementation: Implement a patch management system to ensure timely updates.

AWARENESS AND TRAINING - PR.AT

PR.AT-01: Personnel are provided with cybersecurity awareness and training.

Violation: Employees lacked training, leading to phishing attack success.

Implementation: Conduct regular, role-based training sessions.

Detect

Possible cybersecurity attacks and compromises are found and analyzed

CONTINUOUS MONTORING - DE.CM

DE.CM-01: Networks and network services are monitored for adverse events.

Violation: Lack of real-time monitoring for unauthorized access.

Implementation: Deploy SIEM solutions for continuous network monitoring.

ADVERSE EVENT ANALYSIS - DE.AE

DE.AE-02: Potentially adverse events are analyzed to understand associated activities.

Violation: Delayed breach detection.

Remediation: Implement anomaly detection mechanisms.

Respond

Actions regarding a detected cybersecurity incident are taken

INCIDENT MANAGEMENT - RS.MA

RS.MA-01: The incident response plan is executed once an incident is declared.

Violation: Absence of a formal incident response plan.

Implementation: Develop and maintain an incident response plan.

INCIDENT RESPONSE REPORTING AND COMMUNICATION - RS.CO

RS.CO-02: Internal and external stakeholders are notified of incidents.

Violation: Delayed breach notifications.

Remediation: Create a notification protocol to ensure timely communication.

Recover

Assets and operations affected by a cybersecurity incident are restored

INCIDENT RECOVERY PLAN EXECUTION - RC.RP

RC.RP-01: The recovery portion of the incident response plan is executed.

Violation: No disaster recovery planning.

Implementation: Develop and test a disaster recovery plan.

INCIDENT RECOVERY COMMUNICATION - RC.CO

RC.CO-03: Recovery activities are communicated to stakeholders.

Violation: Inadequate communication during recovery efforts.

Remediation: Share regular updates with stakeholders to maintain trust.

Is it time for a change?

SWOT Analysis

STRENGTHS

S

- Regulatory Awareness
- Recognized Need for Governance
- Commitment to Improvement
- Potential for Policy Alignment with NIST CSF 2.0

WEAKNESSES

W

- Inadequate Governance Structures
- Operational Gaps
- Non-compliance with Regulations
- Lack of Cybersecurity Awareness

OPPORTUNITIES

O

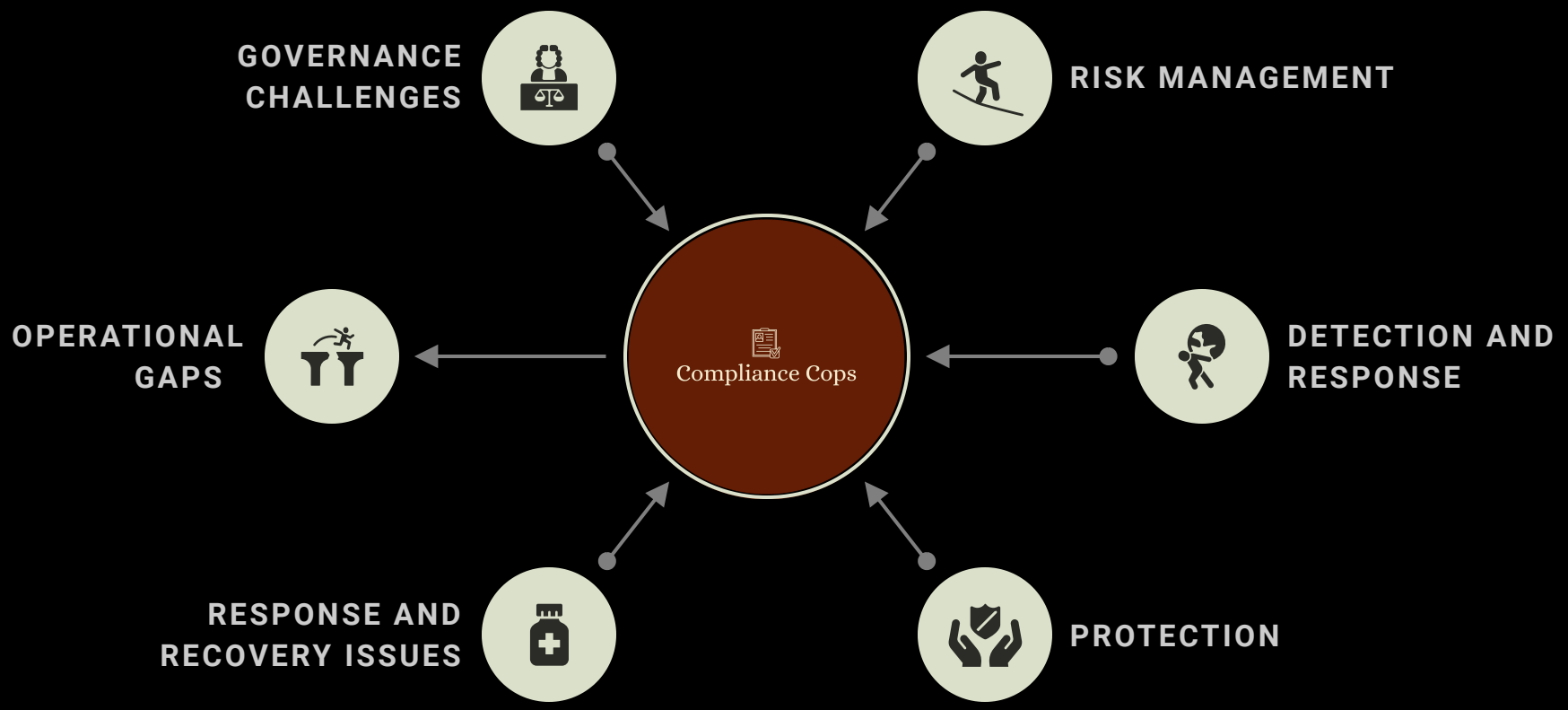
- Leverage NIST CSF 2.0 for Maturity
- Adoption of Advanced Technologies
- Strengthen Vendor Relationships
- Cybersecurity Training and Awareness Programs
- Regulatory Goodwill

THREATS

T

- Regulatory Penalties
- Sophisticated Cyberattacks
- Vendor-Induced Vulnerabilities
- Evolving Threat Landscape
- Stakeholder Expectations

Conclusion



ONE-STOP SOLUTION FOR ALL YOUR PROBLEMS

THANK YOU FOR GIVING US YOUR VALUABLE TIME.

We stay secure together.

PLEASE DON'T HESITATE TO GET IN TOUCH WITH OUR TEAM IF YOU HAVE ANY QUESTIONS OR DOUBTS REGARDING THE PLAN.

Compliance Cops