Data Breach Management Strategies for SMEs to Enterprises

Information Security and Privacy Consultant

Kullatee Boonsiri

Lead Consultant

CERTIFICATES CISA, NIST CYBERSECURITY PROFESSIONAL FOUNDATION, CISSP, IRCA ISMS Lead Auditor, CEH, MCSE, ACSA, *ISO/IEC 27701 Lead Implementer*

EXPERIENCES 18 Years in Information Security and Compliances

PROFICIENCY

- Data Classification
- Information Security Management System (ISMS)
- Privacy Information Management System (PIMS) and Personal Data Privacy Act (PDPA)
- Incident Management and Security Operation
- Cyber Security

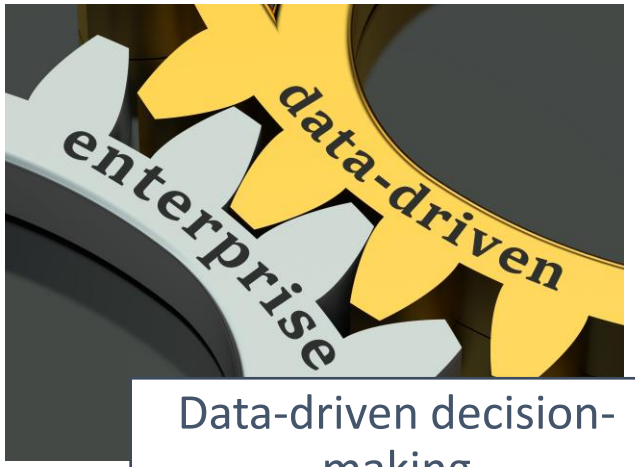
AGENDA

- The importance of data breach management
- Understanding Data Breaches
- Data Breach Management Strategies
- Detecting and Responding to Data Breaches

The importance of data breach management

Factors that amplify the importance of data

Big Data



Data-driven decision-making

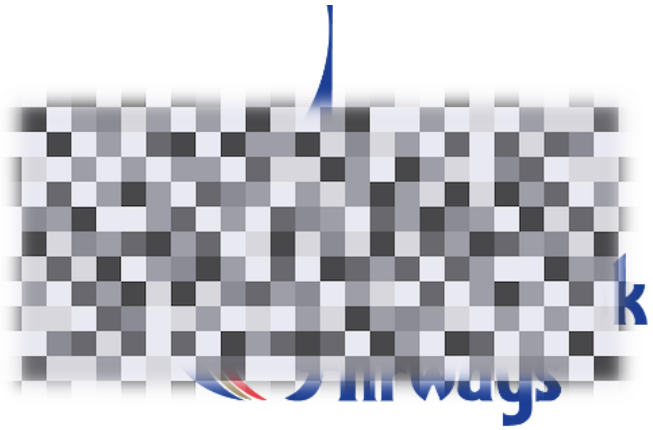
Personalization and Customer Insights

Real-time and Streaming Data

Artificial Intelligence and Machine Learning

Data Privacy and Security

Latest data breach cases



64 – เมื่อวันที่ 23 สิงหาคม 2564 บริษั
ด้านความปลอดภัยทางไซเบอร์ ซึ่งส่งผ
ได้รับอนุญาต

ดังกล่าว บริษัทฯ ร่วมกันกับผู้เชี่ยวชาญ
บคุมเหตุการณ์ที่เกิดขึ้นโดยทันที ในขณ
ความเสียหาย และผู้โดยสารที่ได้รับผลก
งบริษัทฯ ให้มีความเข้มแข็งมากยิ่งขึ้น

บริษัทฯ พบว่าอาจมีข้อมูลส่วนบุคคลที่ถู
สัญชาติ เพศ หมายเลขโทรศัพท์ อีเมล ที่
เดินทาง ข้อมูลบัตรเครดิตบางส่วน และข้
ณ์ที่เกิดขึ้นดังกล่าวไม่มีผลกระทบต่อกา

น์ดังกล่าวไปยังสำนักงานตำรวจแห่งชาติและหน่วยงานที่เกี่ยวข้องแล้ว และเพื่อเป็นการ
แนะนำให้ผู้โดยสารติดต่อไปยังธนาคาร หรือผู้ให้บริการบัตรเครดิต และดำเนินการตามคำ
ว และเปลี่ยนรหัสผ่านที่อาจได้รับผลกระทบโดยเร็วที่สุด

เมื่อเดือน สิงหาคม ปี 2564

สายการบิน**XXXX** แจ้งว่า บริษัทฯ ได้ถูกโจมตีด้านความปลอดภัยทางไซเบอร์

ข้อมูลที่รั่วไหล

ชื่อ-นามสกุลสัญชาติ เพศ หมายเลขโทรศัพท์ อีเมล ที่อยู่ ช่องทางการติดต่อสื่อสาร ข้อมูลหนังสือเดินทาง ประวัติการเดินทาง ข้อมูลบัตรเครดิตบางส่วน และข้อมูลอาหารพิเศษของผู้โดยสาร

Latest data breach cases

ไทยรัฐ ออนไลน์

ข้อมูลผู้ป่วย 11 รพ. ถูกแฮกเผยแพร่ผ่านเว็บ ยังไม่มีเจ้าทุกข์ แจ้งความ

พบข้อมูลผู้ป่วย 11 รพ. กว่าแสนราย ถูกแฮกเผยแพร่ผ่านเว็บไซต์ Raidforums ตำรวจชี้ ยังไม่มีเจ้าทุกข์ แจ้งความ

ผู้สื่อข่าวรายงานว่า มีการโพสต์ข้อมูล อ้างเป็นข้อมูลคนไข้ ซึ่งได้มาจากฐานโรงพยาบาลในประเทศไทยถึง 11 แห่ง (ไม่ระบุชื่อโรงพยาบาล) รวมกว่าแสนรายชื่อหลุดไปอยู่ในเว็บไซต์ Raidforums โดยข้อมูลที่ถูกโพสต์มีทั้ง ชื่อ-สกุล วันเกิด เลขบัตรประชาชน ซึ่งได้เปิดให้บุคคลภายนอกเข้าไปโหลดได้ฟรี ซึ่งอาจสร้างความเสียหายให้บุคคลที่มีชื่อปรากฏ

เกี่ยวกับกรณีนี้ พ.ต.อ.กฤษณะ พัฒน
เปิดเผยว่า พล.อ.ประยุทธ์ จันทร์โอชา
กระทรวงกลาโหม มีความห่วงใยเกี่ย
ความเดือดร้อนให้ประชาชน จึงได้กำ
และดำเนินการป้องกันปราบปรามตา

โดย พล.ต.อ.สุวัฒน์ แจ้งยอดสุข ผู้บัญ
ตามนโยบายรัฐบาล ได้มอบหมายให้
บัญชาการตำรวจแห่งชาติ ในฐานะผู้
ทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) กำกับดูแล และสั่งการให้ทุกภาคส่วน เร่งสร้างการรับรู้ให้กับประชาชน และเร่งทำการสืบสวนปราบปรามจับกุมผู้กระทำความผิดมาดำเนินคดี เพื่อเป็นการจำกัดความ

<u>เมื่อเดือน พฤศจิกายน ปี 2564</u>

มีการแจกข้อมูลที่อ้างว่าหลุดมาจากโรงพยาบาลในประเทศไทย โดยในฐานข้อมูลมีรหัสโรงพยาบาลทั้งหมด **11** แห่ง

<u>ข้อมูลที่รั่วไหล</u>

ชื่อ-นามสกุล วันเกิด เลขบัตรประชาชน ของคนไข้ จำนวนกว่า **1** แสนราย

Latest data breach cases

BUSINESS

CNA cyberattack in March exposed personal information of more than 75,000 people, filings reveal

By Robert Channick
Chicago Tribune • Nov 02, 2021 at 11:38 am

A March cyberattack that shut down systems at Chicago-based insurance giant CNA exposed the personal information of thousands of employees, contractors and policyholders, the company revealed in a Securities and Exchange Commission filing Monday.

More than 75,000 people were affected by the hack, which revealed names, personal identification and Social Security numbers, according to a data breach notification filed with the Maine attorney general's office in July.

"We are not releasing further information beyon
in our recent filings," the company said in an em

CNA discovered the "sophisticated ransomware a
revealing that the hackers accessed company sys

<u>เมื่อเดือน มีนาคม ปี 2564</u>

บริษัท **CNA Financial Corporation** ที่ประเทศสหรัฐอเมริกาถูกโจมตีด้วย **Ransomware** โดย **hacker** ได้เรียกค่าไถ่ข้อมูลเป็นเงินสูงถึง **$40** ล้านดอลล่าสหรัฐอเมริกา

<u>ข้อมูลที่รั่วไหล</u>

ชื่อ-นามสกุล เลขบัตรประชาชน ของพนักงาน คู่ค้า และลูกค้ากว่า **75,000** ราย

Latest data breach cases

<u>เมื่อเดือน มีนาคม ปี 2566</u>

‘9Near – Hactivist’ ประกาศขายข้อมูลส่วนตัวคนไทย 55 ล้านคน พร้อมขายเป็นสกุลเงินบิทคอยน์

<u>ข้อมูลที่รั่วไหล</u>

ชื่อ-นามสกุล ที่อยู่ วันเกิด เลขบัตรประชาชน เบอร์โทรศัพท์ ของประชาชนคนไทยจากหน่วยงานรัฐในประเทศไทย

Potential Consequences and Impact on Businesses

Financial Loss

Reputational Damage

Operational Disruption

Customer and Employee Impact

Legal and Regulatory Consequences

Related compliances and legal requirements

Legal Requirements

Thailand

PDPA
Personal Data Protection Act

Europe

Standards

Information Security Management System
ISO
27001
Certified

800-53
NIST

Related compliances and legal requirements

Personal Data Protection Act B.E. 2562 (2019)
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 37 (1)

- จัดให้มีมาตรการ**รักษาความมั่นคงปลอดภัยที่เหมาะสม** เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

มาตรา 37 (4)

- แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน**เจ็ดสิบสองชั่วโมง**นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิ ทธิ และเสรี ภาพของบุคคล ในกรณี ที่การละเมิ ดมี ความเสี่ยงสูงที่จะมี ผลกระทบต่อสิ ทธิ และเสรี ภาพของบุคคล ให้ แจ้งเหตุ การละเมิ ดให้ เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้ เป็นไปตามหลักเกณฑ์ และวิธีการที่คณะกรรมการ

มาตรา 40 (2)

- จัดให้ มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้ง**แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น**

General Data Protection Regulation (GDPR)

GDPR: IV Section 2.Article 33

- Notification of a personal data breach to the supervisory authority

GDPR: IV Section 2.Article 34

- Notification of a personal data breach to the supervisory authority

Related compliances and legal requirements

ISO/IEC 27001: Information Security Management System (ISMS)

Organizational Controls

- A 5.1 Policies for Information Security
- A 5.2 Information Security Roles and Responsibilities
- A 5.3 Segregation of Duties
- A 5.15 Access Control
- A 5.16 Identity Management
- A 5.17 Authentication Information
- A 5.18 Access Rights

People Controls

- A 6.1 Screening
- A 6.3 Information Security Awareness, Education and Training

Physical Controls

- A 7.5 Protecting Against Physical Environmental Threats
- A 7.6 Working in Secure Areas
- A 7.14 Secure Disposal or Re-Use of Equipment

Technological Controls

- A 8.1 User Endpoint Devices
- A 8.2 Privileged Access Rights
- A 8.5 Secure Authentication
- A 8.7 Protection Against Malware
- A 8.8 Management of Technical Vulnerabilities
- A 8.11 Data Masking
- A 8.12 Data Leakage Prevention
- A 8.13 Information Backup
- A 8.15 Logging
- A 8.16 Monitoring Activities
- A 8.20 Network Security
- A 8.24 Use of Cryptography

NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

Access Control (AC)

- AC-3: Access Enforcement
- AC-4: Information Flow Enforcement
- AC-6: Least Privilege
- AC-16: Security Attributes

Audit and Accountability (AU)

- AU-3: Content of Audit Records
- AU-6: Audit Review, Analysis, and Reporting
- AU-9: Protection of Audit Information

Configuration Management (CM)

- CM-3: Configuration Change Control
- CM-6: Configuration Settings
- CM-8: Information System Component Inventory

Identification and Authentication (IA)

- IA-2: Identification and Authentication (Organizational Users)
- IA-5: Authenticator Management
- IA-8: Identification and Authentication (Non-Organizational Users)

Media Protection (MP)

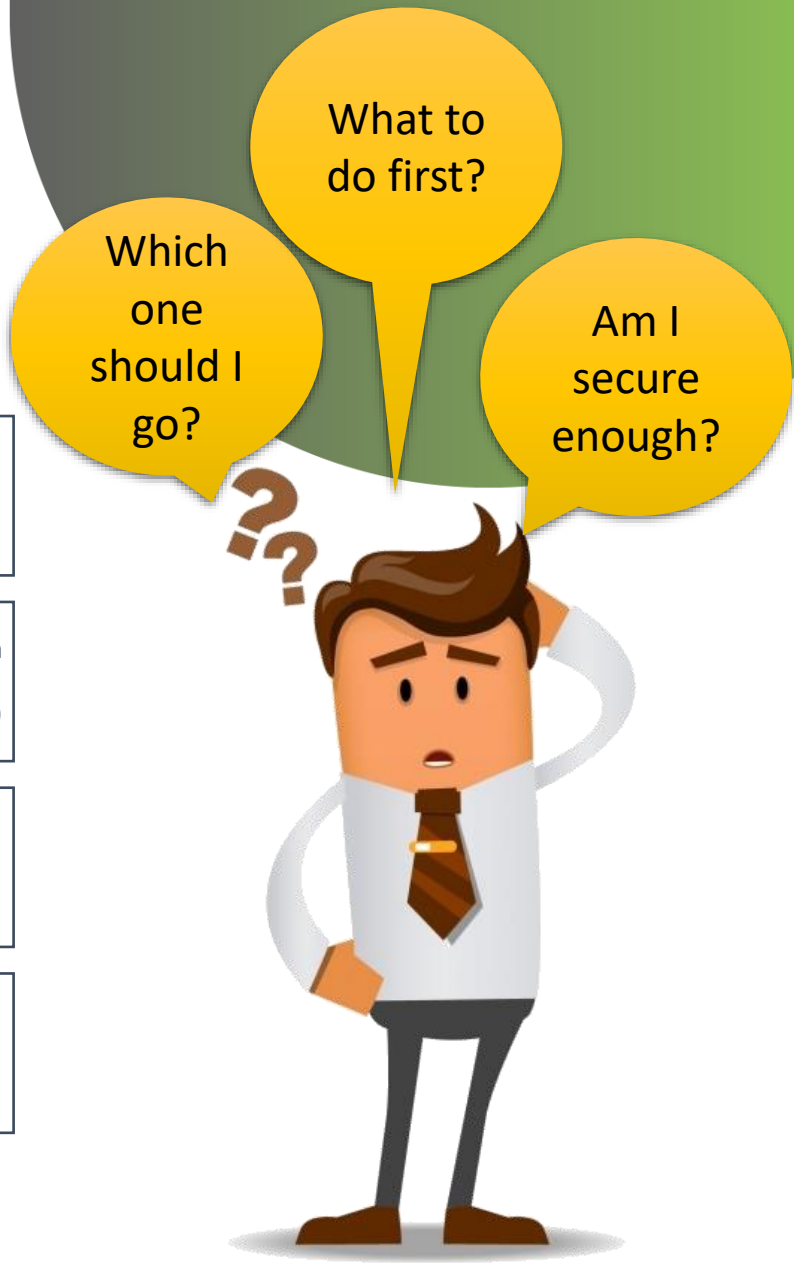
- MP-2: Media Access
- MP-3: Media Marking
- MP-4: Media Storage

System and Communications Protection (SC)

- SC-7: Boundary Protection
- SC-8: Transmission Confidentiality and Integrity
- SC-13: Cryptographic Protection

Data Breach Solutions At A Glance

People	Process	Technology
Encryption	Access controls	Firewalls	Intrusion detection and prevention systems	Two-factor authentication	Data masking
Secure coding practices	Regular security updates and patches	Network segmentation	Secure data backups	Data loss prevention systems	Security information and event management (SIEM)
Security Orchestration, Automation, and Response (SOAR)	User awareness training	Incident response plan	Endpoint Detection and Response (EDR)	User Behavior Analytics (UBA)	File Integrity Monitoring (FIM)
Threat Intelligence Platforms	Security audits and assessments	Security Scanning, Vulnerability Assessment and Penetration Testing	Remote Wiping and Data Erasure	Secure Remote Access and VPNs (Virtual Private Networks)	.....



Demands of SME vs Enterprise

SMEs

VS

Enterprise

Small data footprint, vary depending on the industry and nature of operations.

Data Volume and Complexity

Large volume of data due to scale and operation across multiple departments, locations and business functions.

Limited resources and may rely on smaller-scale data storage and infrastructure solutions such as local servers or cloud-based services.

Data Infrastructure

Sophisticated and scalable data infrastructure including data center, cloud-based solutions, and others

Demands of SME vs Enterprise

SMEs

VS

Enterprise

Require data management solutions that are scalable but also cost-effective and easily adaptable to their evolving business needs

Scalability and Flexibility

Need scalable and flexible data management solutions to accommodate their growing data needs, changing business requirements, and expanding operations

Limited budgets and may need to prioritize their data management activities based on available resources and immediate business needs

Budget and Resources

Large budgets and resources allocated for data management initiatives, including data analytics, infrastructure upgrades, and compliance efforts

Demands of SME vs Enterprise

SMEs

VS

Enterprise

Data management responsibilities may be spread across a smaller team or managed by a single individual

Data Governance

Data governance teams responsible for establishing policies, procedures, and frameworks for data management, privacy, and security

Limited resources and may face challenges in implementing comprehensive security measures, making them potentially more vulnerable to data breaches.

Data Security

Dedicated cybersecurity teams and invest heavily in robust security measures to protect their data against breaches, cyberattacks, and other threats

Demands of SME vs Enterprise

SMEs

VS

Enterprise

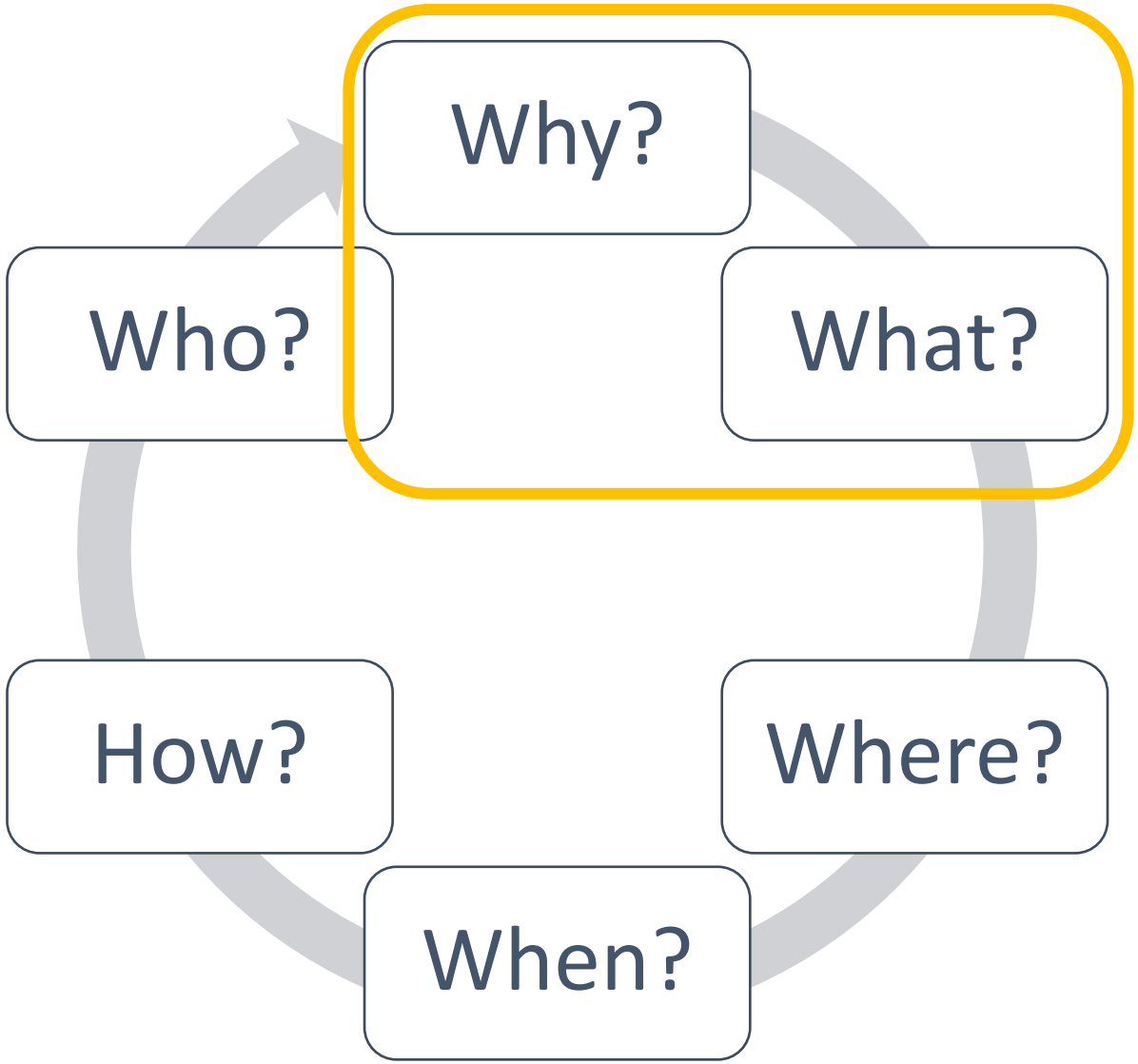
Certain compliance requirements, but the scope and complexity may be relatively smaller, depending on the industry and geographical location

Compliance and Regulations

Broader range of compliance requirements and regulations due to their size, industry, and global operations
e.g. PDPA, GDPR, or industry-specific regulations

Data Breach Management Strategies

6 Questions



Why? and What?

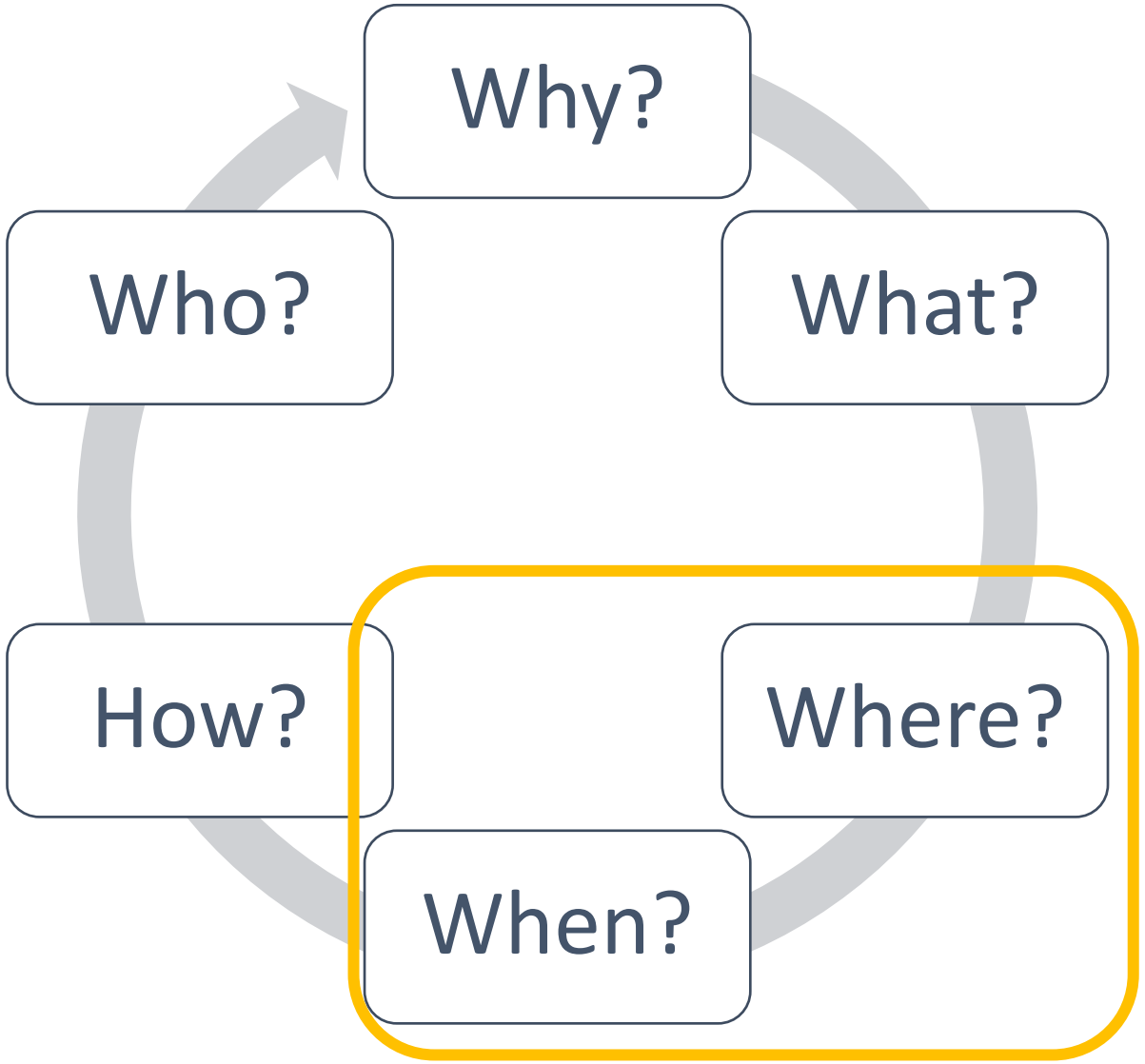
What data should we protect and why?

1. List out all compliances e.g. laws, regulations, policies, standards that the organization have to comply.

2. List out your core data and keep them as data inventory (part of data governance)

3. Classify your data

5 Questions

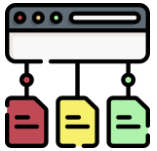


Data Breach Risk Assessment Approach

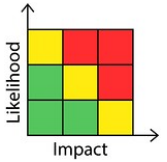
Identify and categorize sensitive data

Identify potential threats and vulnerabilities

Map data flows and systems



Assess likelihood and impact



Determine current controls and safeguards

Conduct a gap analysis

Prioritize and implement risk mitigation measures

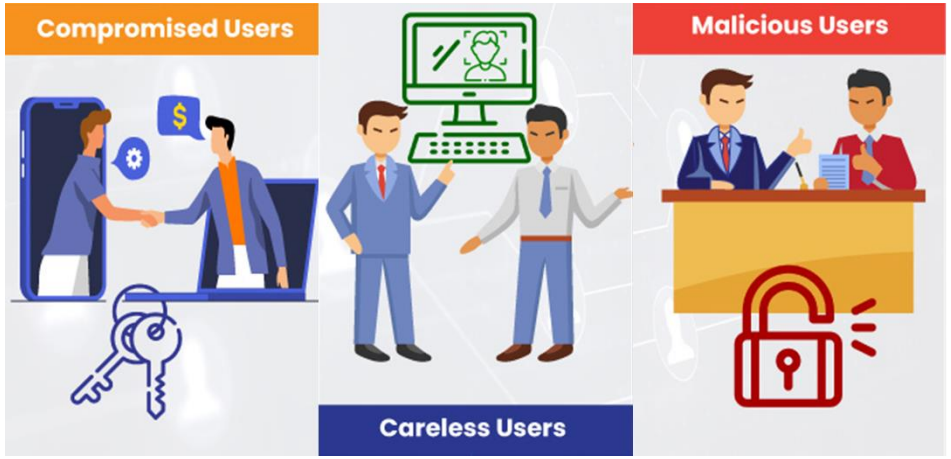
Understanding Data Breaches

Threat Source Types

Hacking and Cyberattacks

- Social Engineering
- Brute Force Attack
- Supply Chain Attack
- Malware
- Exploit Security Vulnerability

Insider Threats



- Compromised Users
- Careless/Negligent Insider
- Malicious Insider

Physical Theft or Loss

- Loss Devices
- Unauthorized Access to Credentials

Channels/ Threat Vectors that can cause data breaches

Data-at-Rest

- File Share Server
- Database
- Hard disk
- Removable Media

Data-in-Motion

- Email
- Web Post
- Network Traffic
- Cloud

Popular techniques that attackers often use to steal your data

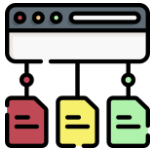
1.  Social Engineering & Spear Phishing
2.  Malware-Injecting Devices
3.  Remote Access Tools
4.  Credential Dumping
5.  Data Exfiltration

Data Breach Risk Assessment Approach

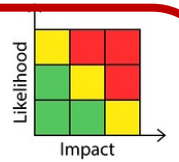
Identify and categorize sensitive data

Identify potential threats and vulnerabilities

Map data flows and systems



Assess likelihood and impact



Determine current controls and safeguards

Conduct a gap analysis

Prioritize and implement risk mitigation measures

Data Breach Risk Assessment Approach

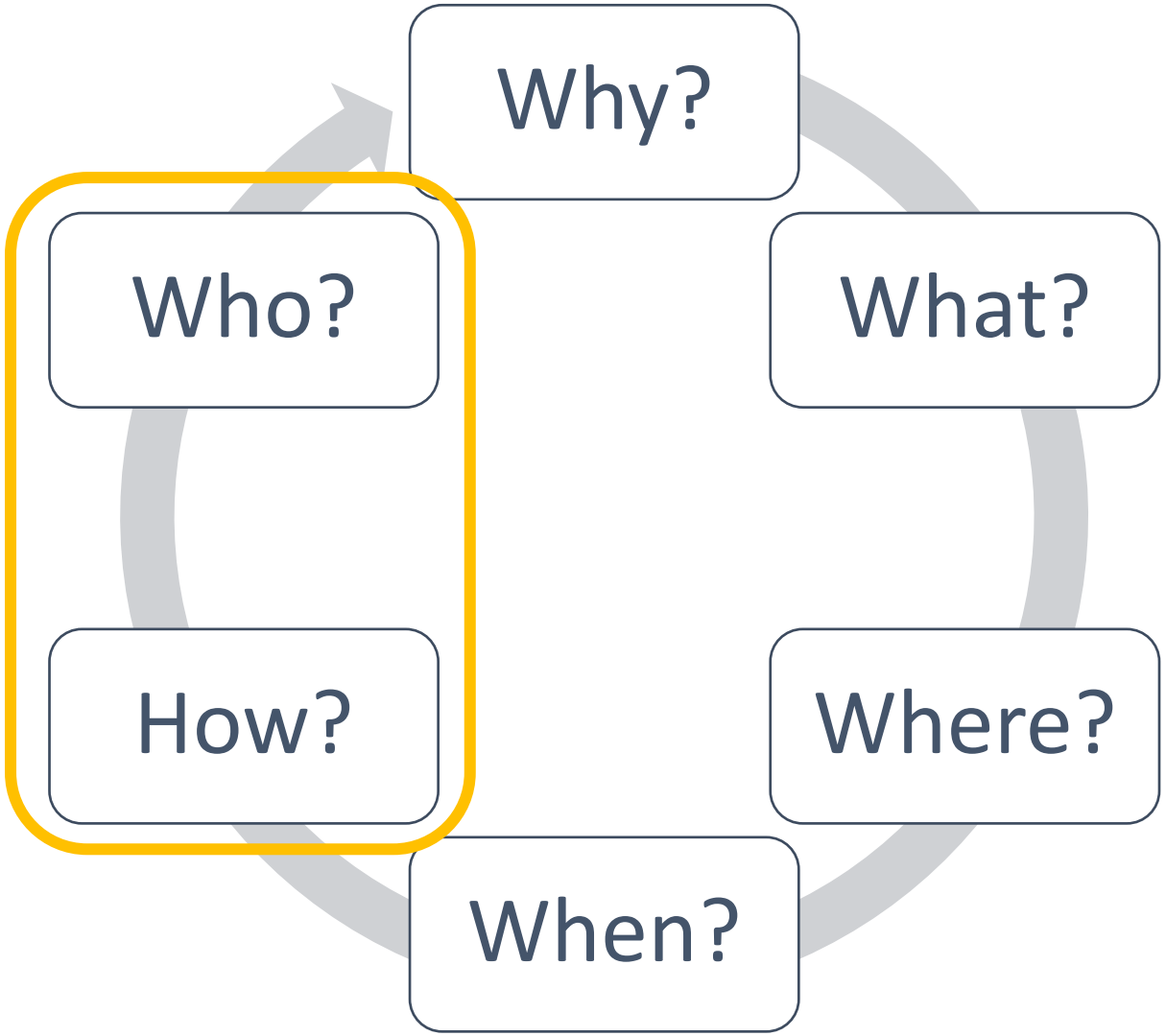
Core Data

- Customer data
- Product data
- HR data
- …

Customer Data

Data Vector			
Email			
CRM App			
CRM Database			
Cloud			

5 Questions



How?

Solutions

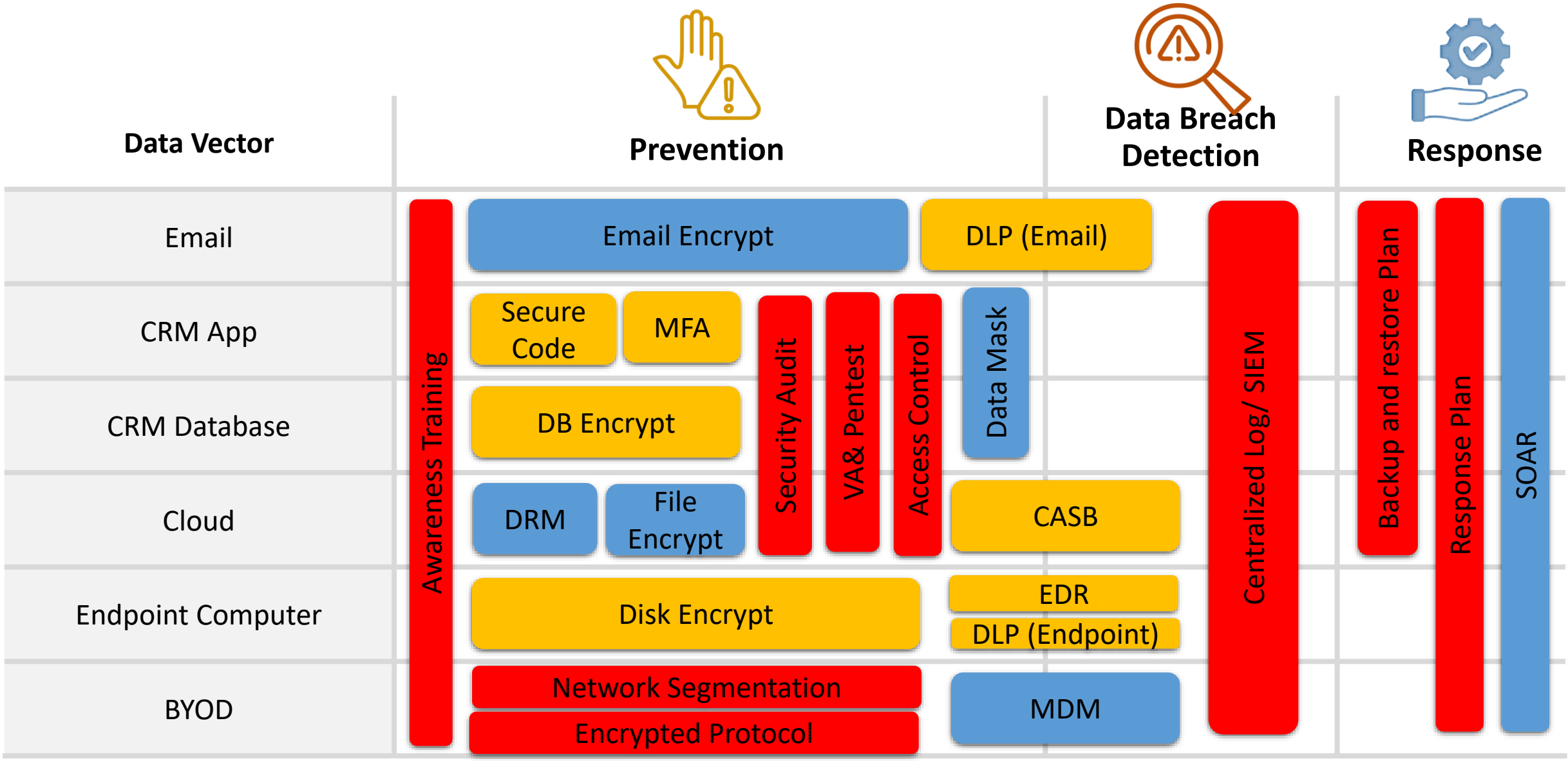
- Encryption
- Data Masking
- DLP
- SIEM
- SOAR
- …

Data Vector	Prevention	Data Breach Detection	Response
Email			
CRM App			
CRM Database			
Cloud			

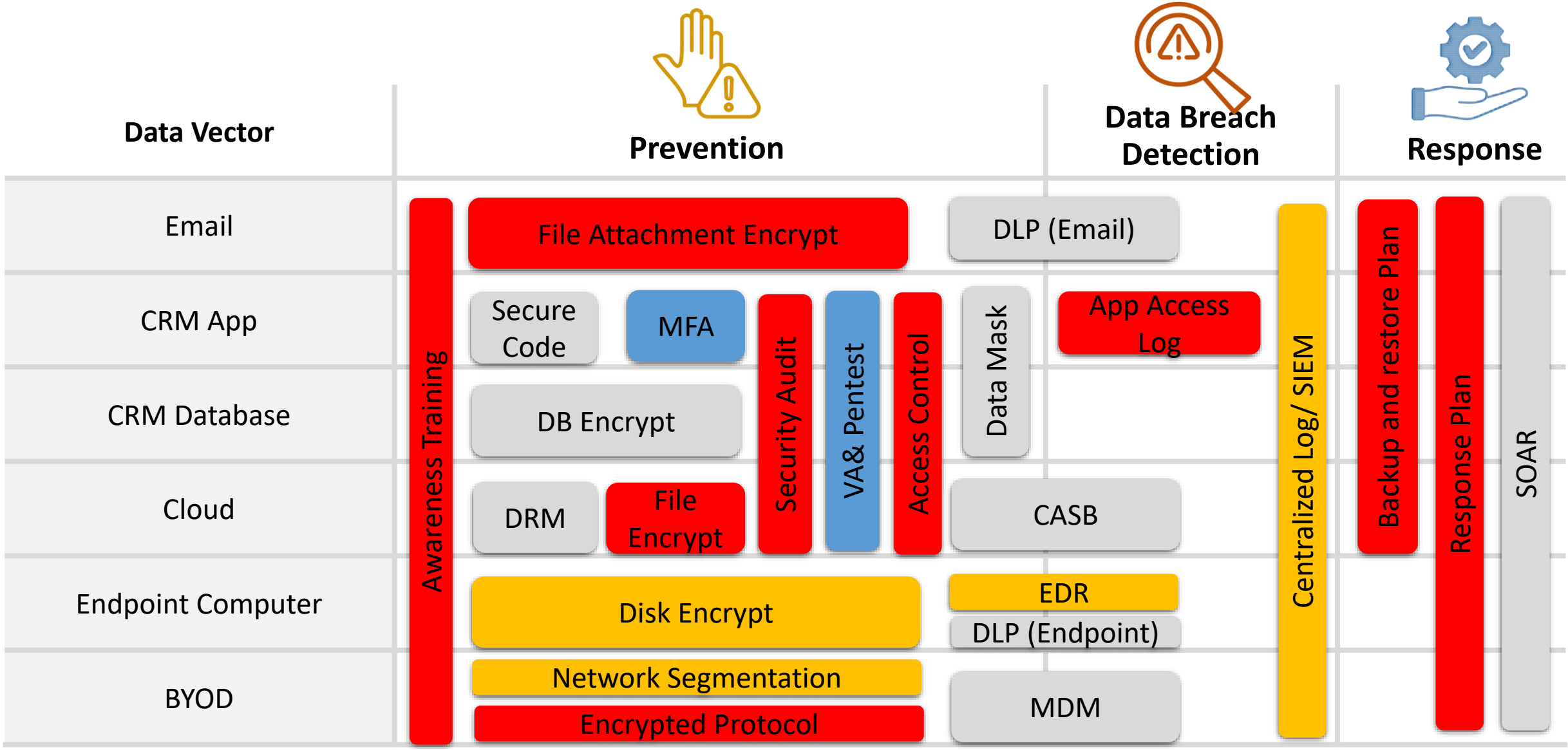
Data Breach Solutions At A Glance

People	Process	Technology
Encryption	Access controls	Firewalls	Intrusion detection and prevention systems	Two-factor authentication	Data masking
Secure coding practices	Regular security updates and patches	Network segmentation	Secure data backups	Data loss prevention systems	Security information and event management (SIEM)
Security Orchestration, Automation, and Response (SOAR)	User awareness training	Incident response plan	Endpoint Detection and Response (EDR)	User Behavior Analytics (UBA)	File Integrity Monitoring (FIM)
Threat Intelligence Platforms	Security audits and assessments	Security Scanning, Vulnerability Assessment and Penetration Testing	Remote Wiping and Data Erasure	Secure Remote Access and VPNs (Virtual Private Networks)	.....

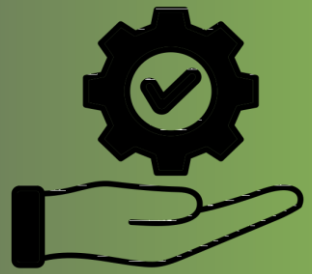
Solution Matrix (Sample for Enterprise)



Solution Matrix (Sample for SME)



Response Plan Stages



IDENTIFY

Notify

Promptly notify the incident response team, IT department, management

Analyze (Impact)

Conduct a preliminary analysis to determine the scope and impact of the data breach.

PROTECT

Containment

Isolate affected systems or networks, shut down compromised accounts, or implement other measures to restrict access.

DETECT

Investigate

Preserve logs, system images, network traffic data, and other relevant evidence for analysis.

RESPOND

Recovery

Implement data backup restoration, system reconfiguration, or other recovery measures.

Eradication

Identify and remove any malicious presence or unauthorized access points within the systems.

RECOVER

Post-Incident

Document the details of the incident, actions taken, and lessons learned throughout the response process.

Lesson Learned Management

Knowledge Base should cover:

Incident Response Plan (Playbook)

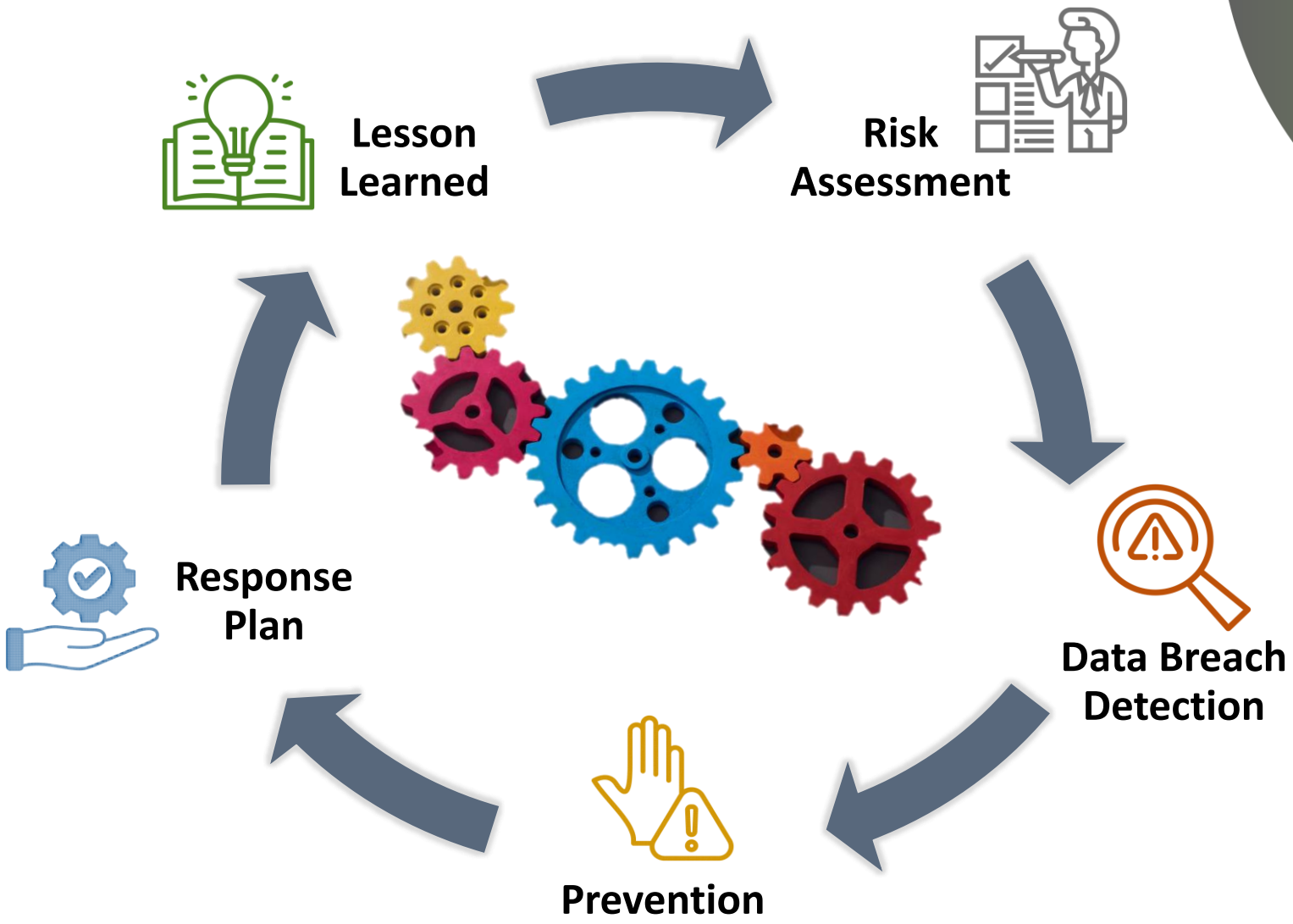
Regulatory and Legal Requirements

Data Breach Impact Assessment

Post-Incident Analysis and Lessons Learned

Resources and References

Summary


Lesson Learned
Risk Assessment
Data Breach Detection
Prevention
Response Plan

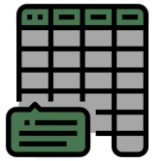
Service Offering

ECM

Enterprise Content Management Using MS Platforms

DATACLASS

Data Classification and Data Loss Prevention (DLP) Consultancy



PRIVACY

Privacy Information Management System (PIMS) / PDPA

CYBER

Cyber Security Risk Management and Cyber Security Act (CSA)

DATA GOVERNANCE

Data Governance (DG)

ISMS

Information Security Management System (ISMS)

Thank You