# Comprehensive Data Security Plan

Presented By: Devin Young

CTEC 450 - Dr. Jackson

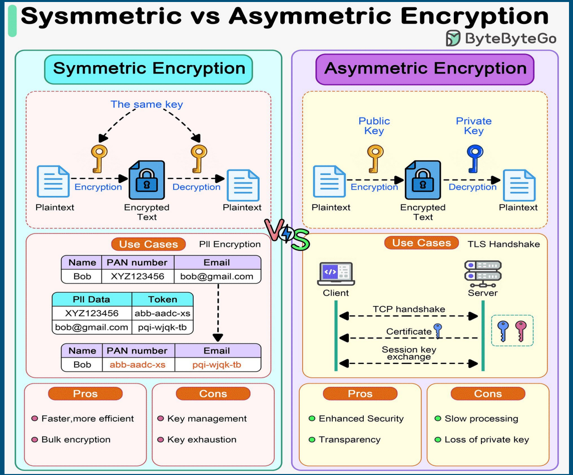
# Key Concepts in Data Security

# Confidentiality, Integrity, & Availability (CIA)

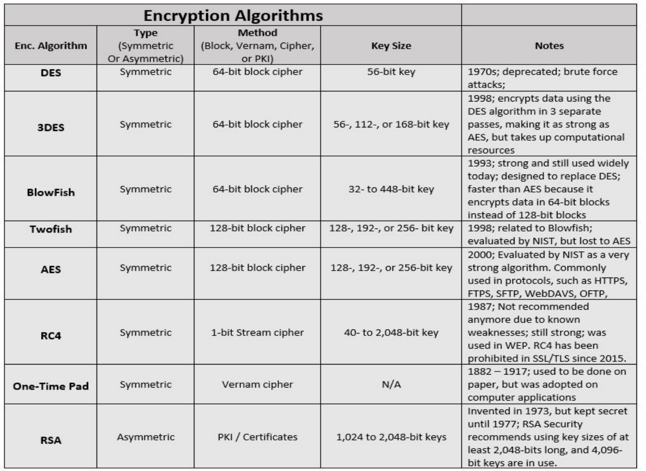
- Confidentiality ensures that only authorized individuals are able to access the company's data
- Integrity makes sure that data is accurate and has not been altered without authorization within a company
- Availability ensures that data is always accessible when it is needed by authorized users

# Encryption Methods

- The goal of encryption is to secure data by turning it into an unreadable format (ciphertext), so that those who are not authorized to access it cannot read it (in plaintext)



(Xu, 2023)



| Encryption Algorithms | | | | |
|---|---|---|---|---|
| Enc. Algorithm | Type (Symmetric Or Asymmetric) | Method (Block, Vernam, Cipher, or PKI) | Key Size | Notes |
| **DES** | Symmetric | 64-bit block cipher | 56-bit key | 1970s; deprecated; brute force attacks; |
| **3DES** | Symmetric | 64-bit block cipher | 56-, 112-, or 168-bit key | 1998; encrypts data using the DES algorithm in 3 separate passes, making it as strong as AES, but takes up computational resources |
| **BlowFish** | Symmetric | 64-bit block cipher | 32- to 448-bit key | 1993; strong and still used widely today; designed to replace DES; faster than AES because it encrypts data in 64-bit blocks instead of 128-bit blocks |
| **Twofish** | Symmetric | 128-bit block cipher | 128-, 192-, or 256- bit key | 1998; related to Blowfish; evaluated by NIST, but lost to AES |
| **AES** | Symmetric | 128-bit block cipher | 128-, 192-, or 256-bit key | 2000; Evaluated by NIST as a very strong algorithm. Commonly used in protocols, such as HTTPS, FTPS, SFTP, WebDAVS, OFTP, |
| **RC4** | Symmetric | 1-bit Stream cipher | 40- to 2,048-bit key | 1987; Not recommended anymore due to known weaknesses; still strong; was used in WEP. RC4 has been prohibited in SSL/TLS since 2015. |
| **One-Time Pad** | Symmetric | Vernam cipher | N/A | 1882 – 1917; used to be done on paper, but was adopted on computer applications |
| **RSA** | Asymmetric | PKI / Certificates | 1,024 to 2,048-bit keys | Invented in 1973, but kept secret until 1977; RSA Security recommends using key sizes of at least 2,048-bits long, and 4,096-bit keys are in use. |

(Thecybersecurityman, 2018)

# Access Control Measures

Methods for restricting access to sensitive data:

- Enforcing strong complex passwords (minimum of 12 characters with a mixture of lowercase letters, uppercase letters, and special characters)
- Multi-factor authentication
- Role-based access control & Time-based access control (can only access resources based on your role and duration of shift)
- Least privilege principle
- Geofencing

(Halstead, 2022)

# Threats and Vulnerabilities (Phishing Attacks)

## Phishing Attacks Explained

Phishing is a cybercrime in which **scammers** try to lure you into giving up your personal information by impersonating a trusted source. Phishers can trick you through:

Text messages

Emails

Phone calls

(Stouffer, 2024)

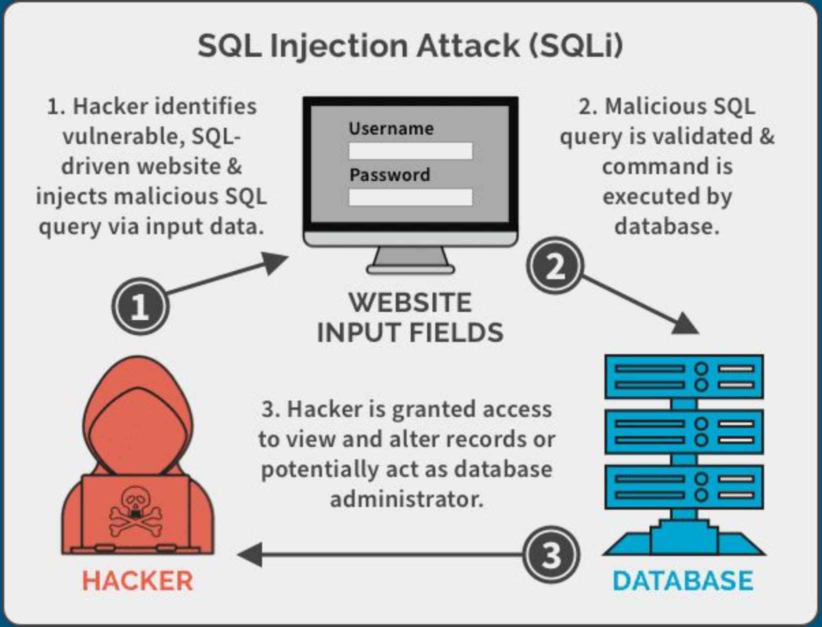
- Attempts to obtain sensitive information by pretending to be a trustworthy entity

# Threats and Vulnerabilities (Malware)

(Graham, 2025)

- Malicious software designed to damage or gain unauthorized access to systems with the intent of extorting victims

# Threats and Vulnerabilities (SQL Injection)



SQL Injection Attack (SQLi)

1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.

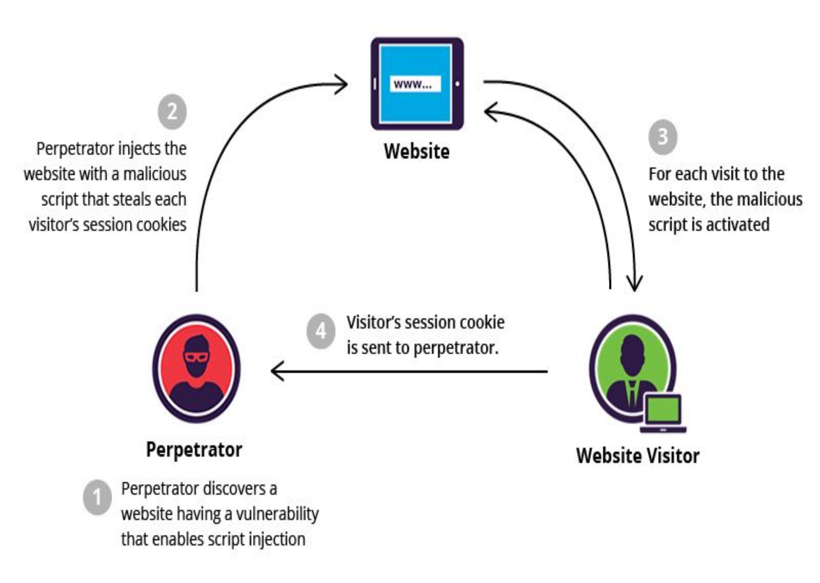
2. Malicious SQL query is validated & command is executed by database.

3. Hacker is granted access to view and alter records or potentially act as database administrator.

(SQL Injection Attacks — Web-based App Security, Part 4 | Spanning, 2019)

- Involves a threat actor inserting malicious SQL code into input fields, allowing unauthorized access to a database

# Threats and Vulnerabilities (Cross Site Scripting)



1 Perpetrator discovers a website having a vulnerability that enables script injection

2 Perpetrator injects the website with a malicious script that steals each visitor's session cookies

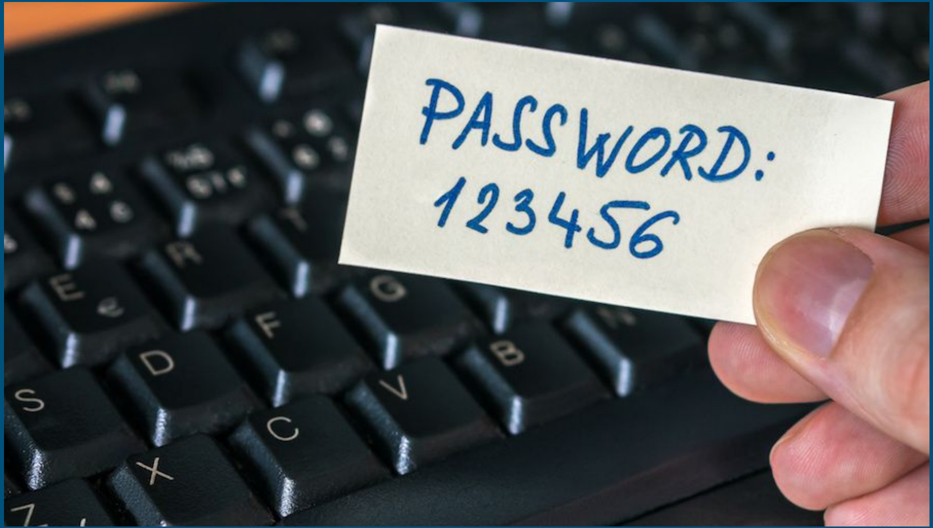
3 For each visit to the website, the malicious script is activated

4 Visitor's session cookie is sent to perpetrator.

(Naer, 2023)

- Consists of malicious scripts being injected into websites to attack users and steal data

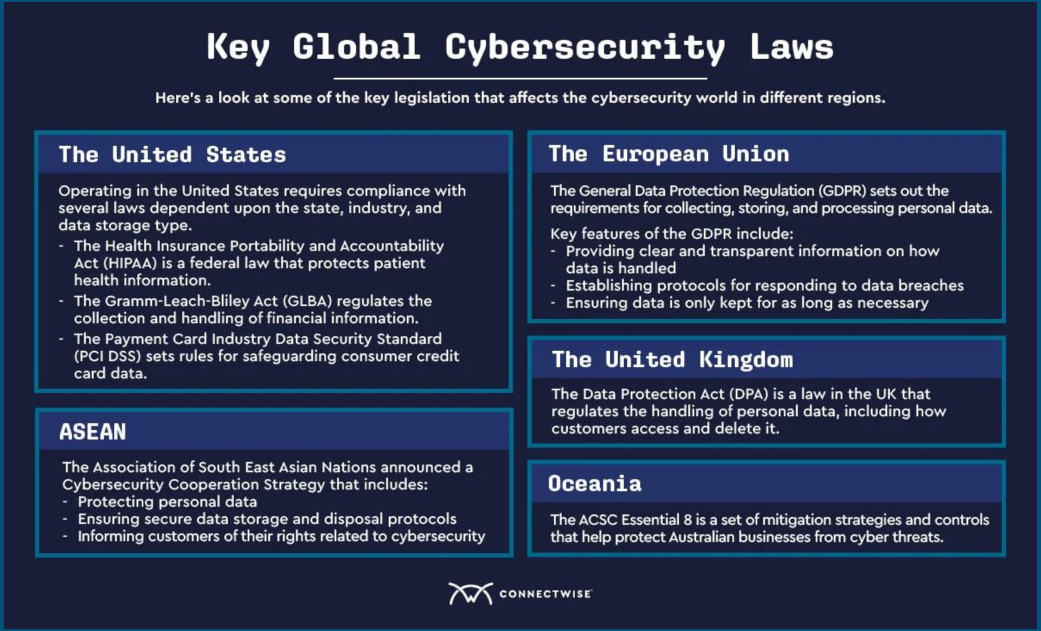
# Threats and Vulnerabilities (Weak Passwords)



Securedatamgt, 2016)

- Consists of malicious scripts being injected into websites to attack users and steal data

# Regulatory Requirements



## Key Global Cybersecurity Laws

Here's a look at some of the key legislation that affects the cybersecurity world in different regions.

### The United States

Operating in the United States requires compliance with several laws dependent upon the state, industry, and data storage type.

- The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that protects patient health information.
- The Gramm-Leach-Bliley Act (GLBA) regulates the collection and handling of financial information.
- The Payment Card Industry Data Security Standard (PCI DSS) sets rules for safeguarding consumer credit card data.

### ASEAN

The Association of South East Asian Nations announced a Cybersecurity Cooperation Strategy that includes:

- Protecting personal data
- Ensuring secure data storage and disposal protocols
- Informing customers of their rights related to cybersecurity

### The European Union

The General Data Protection Regulation (GDPR) sets out the requirements for collecting, storing, and processing personal data.

Key features of the GDPR include:

- Providing clear and transparent information on how data is handled
- Establishing protocols for responding to data breaches
- Ensuring data is only kept for as long as necessary

### The United Kingdom

The Data Protection Act (DPA) is a law in the UK that regulates the handling of personal data, including how customers access and delete it.

### Oceania

The ACSC Essential 8 is a set of mitigation strategies and controls that help protect Australian businesses from cyber threats.

CONNECTWISE

(Chebitko, 2024)

- Government-mandated rules and standards that companies must follow to protect sensitive data

# Common Data Security Risks Organizations Face Today

# Potential Risks (Phishing Attacks)

Risk Description: Attackers can trick users into providing sensitive information

Real World Example:

- “In 2020, U.S. healthcare provider Elara Caring was subjected to a phishing attack that targeted two employees” (8 Devastating Phishing Attack Examples, 2025)
- “With only these two compromised targets, attackers gained access to employee email accounts and compromised the personal information of more than 100,000 elderly patients” (8 Devastating Phishing Attack Examples, 2025)

Possible Consequences:

- Loss of sensitive data, financial loss, and damage to reputation

# Potential Risks (Ransomware Attacks)

Risk Description: Malware that locks or encrypts data and demands ransom for access

Real World Example:

- “In late February, the ALPHV/BlackCat ransomware gang claimed responsibility for hacking Change Healthcare, a subsidiary of UnitedHealth Group. The intruders disrupted operations and stole up to 6TB of data, including personal information, payment details, insurance records, and other sensitive information, which led to a non-verified ransom payment of $22 million (Team, 2024)

  Possible Consequences:

- Data loss, operational downtime, financial penalties

# Potential Risks (Insecure Data Storage)

Risk Description: Storing sensitive data in unprotected systems

Real World Example:

- An unencrypted database with data involving 2.9 billion U.S. citizens was compromised by a cyber criminal group called USDoD (National Public Data Breach Publishes Private Data of 2.9B U.S. Citizens, 2024)

Possible Consequences:

- Data theft, regulatory fines, and a loss of trust from customers

# Mitigation Strategies for Data Security Risks

(Financial Crime Academy, 2025)

# Phishing Mitigation

Technical Solutions

- Implement email-filtering systems and use anti-phishing tools such as Mimecast and Microsoft defender to help protect and block phishing attempts

Policy Measures

- Require employees to train so that they can recognize phishing emails, such as regular phishing simulations

Best Practices

- Mandate the use of multi-factor authentication to reduce the impact of compromised credentials

# Ransomware Mitigation

Technical Solutions

- Perform regular system backups, use of antivirus software, and network segmentation

Policy Measures

- Create an Incident response plan in case of a security breach, and use IDS/IPS, as well as SIEMS for continuous monitoring of network traffic

Best Practices

- Push out regular software updates, and disable macros in email attachments

# Insecure Data Storage Mitigation

Technical Solutions

- Use encryption for data at rest, such as secure cloud storage solutions

Policy Measures

- Implement strong access control policies, such as role-based access control, time-based access controls,  and conduct regular audits of data storage practices

Best Practices

- Lock and monitor physical storage locations, as well as implement the least privilege principle

(Schick, 2015)

# Data Security Plan for “Change Healthcare Inc.”

(Cloud, 2022)

# Risk Assessment

Assets that Need Protection:

- Patient personal & health Information (names, addresses, diagnosis, treatment record, payment data)
- Intellectual property (proprietary data, trade secrets)
- Internal communications and financial Records

Potential Threats to Assets:

- Cybercriminals motivated by financial gain
- Insider misuse of data
- Employee negligence

# Security Controls

Technical Measures

- Firewalls & IDS/IPS to monitor for abnormal network traffic, as well as data encryption using AES-256 for data at rest and in transit
- Endpoint detection and response to monitor for malicious threats

Organizational Measures

- Employee training on data privacy and cybersecurity best practices
- Incident response plan to quickly identify and address security breaches
- Data classification policies to identify protect sensitive patient data

Compliance Measures

- Regular audits and compliance checks to ensure adherence to HIPPA, HITECH, and GDPR
- Secure handling of sensitive data through third-party vendors with strong security protocols

# Incident Response Plan

1. Containment - Isolate affected systems to prevent further data loss or exposure
2. Investigation - Identify the cause of the breach and assess the impact on patient data
3. Communication - Notify affected patients and regulatory bodies within required timeframes
4. Recovery - Restore systems from backups, apply security patches, and ensure full system functionality
5. Documentation - Record the incident for compliance purposes and future improvements

# Compliance and Legal Considerations

HIPPA Compliance:

- “Change Healthcare” must ensure that personal health information is protected through encryption, access controls and regular audits
- Work with third-party vendors to maintain HIPPA compliance

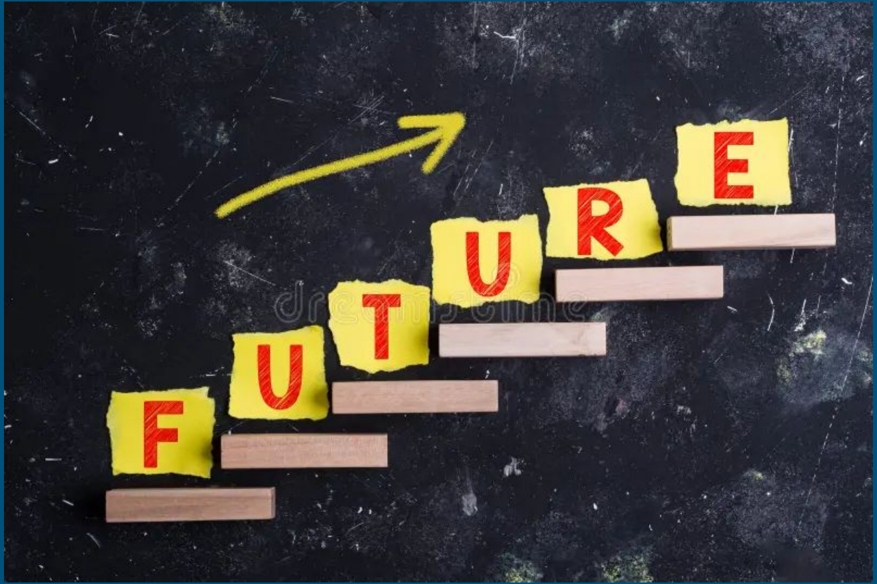
GDPR Compliance:

- Ensure that personal data is processed in compliance with GDPR if dealing with European patients, which includes obtaining patient consent and implementing privacy by design

PCI DSS Compliance

- Ensure any payment card data handled by Change Healthcare is securely stored and transmitted according to PCI DSS standards

# Next Steps



(Future word on steps stock image.  - 131219311, 2018)

# What’s Next?

- Implement the proposed security plan to protect Change Healthcare’s critical assets
- Conduct regular audits and update security measures in response to evolving threats

# Bibliography

Chebitko, R. (2024, February 29). Federal laws relating to cybersecurity. MS.Codes.

https://ms.codes/en-gb/blogs/cybersecurity/federal-laws-relating-to-cybersecurity

Cloud. (2022, November 1). Data security: How to keep data secure in the cloud? Successive Cloud.

https://successive.cloud/keep-data-secure-in-cloud/

8 Devastating Phishing Attack Examples (and Prevention Tips). BlueVoyant. (n.d.).

https://www.bluevoyant.com/knowledge-center/8-devastating-phishing-attack-examples-and-prevention-tips

Financial Crime Academy. (2025, January 24). Risk mitigation techniques you should know. Financial Crime Academy. https://financialcrimeacademy.org/risk-mitigation-techniques/

Future word on steps stock image.  - 131219311. Dreamstime. (2018, November 10).

https://www.dreamstime.com/future-word-steps-yellow-paper-wooden-arrow-black-grunge-background-image131219311

# Bibliography

GeeksforGeeks. (2025, February 23). Difference between symmetric and asymmetric key encryption.

GeeksforGeeks.

https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/

Graham, K. (2025, January 6). Top 7 ransomware attack vectors. Bitsight.

https://www.bitsight.com/blog/top-7-ransomware-attack-vectors-and-how-avoid-becoming-victim

Halstead, J. (2022, December 12). What are access control systems and how do they work?: Blog: Link labs. Link Labs.

https://www.link-labs.com/blog/what-are-access-control-systems-and-how-do-they-work

Naer, S. (2023, December 20). What is XSS | Stored Cross Site Scripting Example | Imperva. Learning Center.

https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/

National Public Data breach publishes private data of 2.9B U.S. citizens. (2024,

August 19). Security Intelligence.

https://securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citizens/

# Bibliography

Schick, S. (2015, August 18). Insecure configuration of MongoDB, other databases could be leaking information. Security Intelligence.

https://securityintelligence.com/news/insecure-configuration-of-mongodb-other-databases-could-be-leaking-information/

Securedatamgt. (2016, March 21). Passwords all employees should avoid - Secure Data MGT. Secure Data MGT.

https://www.securedatamgt.com/passwords-all-employees-should-avoid/

SQL Injection Attacks — Web-based App Security, Part 4 | Spanning. (2019, July 18). Spanning.

https://www.spanning.com/blog/sql-injection-attacks-web-based-application-security-part-4/

Stouffer, C. (2024, December 30). What is phishing? How to spot and avoid it.

https://us.norton.com/blog/online-scams/what-is-phishing

Team, H. (2024, November 6). Understanding the change healthcare breach and its impact on security compliance. Hyperproof.

https://hyperproof.io/resource/understanding-the-change-healthcare-breach/