How Organisations and Their Employees can Ensure Data and Device Security

Proper data and device security is essential for maintaining confidentiality, integrity, and availability of data, protecting the organisation's reputation, and ensuring trust among customers and partners. It is an ongoing process that requires continuous efforts and vigilance to adapt to evolving cyber threats and ensure the highest level of data and device protection. Proper implementation of data and device security policy allows organisations to protect their information assets from cybercriminal activities and guard against insider threats and human errors.

The purpose of this advisory is to provide organisations with a list of non-exhaustive recommendations on how to mitigate risks and safeguard their information assets. In the same vein, this advisory provides organisations with guidelines and best practices for ensuring data and device security, with a focus on the following key areas:

- Data Handling
- Data Classification
- Secure File Sharing
- Physical Security

Data Handling

Data handling refers to the process of managing and manipulating data throughout its lifecycle. It involves various activities related to the collection, storage, processing, transmission, protection, retention, sharing, and governance of data. Data handling encompasses the proper management of data, in the aspects of data encryption, data access controls, data retention and data backup and recovery, to ensure its integrity, security and usability. Effective data handling practices are essential for maintaining data quality, facilitating decision-making, and ensuring the confidentiality and integrity of sensitive information.

Data Encryption

Data encryption is key in ensuring the confidentiality, integrity, and security of sensitive information. All sensitive data, both in transit and at rest, should be encrypted using strong encryption algorithms. Organisations should employ industry-standard encryption protocols to protect data from unauthorised access and ensure data confidentiality. The following is a general guide on how to implement data encryption.

i. Identify Data to Encrypt

Begin by identifying data that requires encryption, both at rest and in transit. This may include Personally Identifiable Information (PII), financial data, health records, intellectual property, or any other sensitive data that needs protection.

ii. Choose Encryption Algorithms and Methods

Choose strong encryption algorithms that are widely recognised and deemed to be secure according to industry standards and decide on the type of encryption to be used. Common ways that encryption can be applied to data include:

- *Data at Rest Encryption:* Encrypt data stored in databases, files, or storage devices.
- *Data in Transit Encryption:* Encrypt data transmitted over networks or communication channels.
- *End-to-End Encryption:* Encrypt data on the sender's end and keep it encrypted until it reaches the intended recipient.

Common methods of data encryption include:

- *Symmetric Encryption:* Encrypt plaintext and decrypt ciphertext using a single secret key only. Both the sender and receiver have private access to the key, which can only be used by authorised recipients. This is also known as private key cryptography, and some common algorithms include:
  - Advanced Encryption Standard (AES)
  - Data Encryption Standard (DES)
  - Triple DES (TDES)
  - Twofish
- *Asymmetric Encryption:* Encrypt and decrypt data using two keys (a public key and a private key). This is also known as public key cryptography, and some common algorithms include:
  - Rivest Shamir Adleman (RSA)
  - Elliptic Curve Cryptography (ECC)

iii. Encrypt Data Properly

Encrypt the identified sensitive data using the chosen encryption tools and algorithms. Ensure that data is encrypted before storage or transmission and decrypted only when necessary. One cryptographic technique that allows computations to be performed on encrypted data without the need to decrypt the data first is homomorphic encryption. This enhances data privacy and security as data remains in its encrypted form while computations are carried out. This is particularly useful in scenarios where data needs to be processed by third parties.

iv. Monitor and Audit

Implement monitoring and auditing mechanisms to track data encryption processes and detect any anomalies or unauthorised access attempts. Examples include behavioural analysis tools that can detect abnormal data access patterns, such as unexpected spikes in decryption requests, and User and Entity Behaviour Analytics (UEBA) solutions that can help identify unusual user behaviour related to data encryption and access.

v. Conduct Regular Training

Provide training to employees on best data encryption practices and how to use encryption tools correctly. Regular updates to the curriculum and practical exercises can help to ensure employees understand, keep up-to-date and adhere to data security and privacy policies.

vi. Review and Update Regularly

Regularly review and update encryption measures to adapt to emerging threats and security best practices.

Data Access Controls

Data access controls are crucial for maintaining the security and confidentiality of sensitive information within an organisation. Implementing data access controls involves defining and enforcing measures to regulate access to sensitive information and ensure that only authorised users can view, modify, or interact with specific data. The following are general measures to take for data access controls implementation.

i. Require User Authentication

Require strong user authentication mechanisms, such as passwords, multi-factor authentication (MFA), or biometrics, to verify users' identities before granting access to data. Enable user access logs or any other relevant logs to track data access and monitor for any suspicious activities such as mass file data downloads.

ii. Implement the Principle of Least Privilege and Access Control Lists (ACLs)

Apply the principle of least privilege, which grants users the minimum level of access required to perform their job functions. Avoid granting unnecessary permissions that could lead to data exposure. Use ACLs to specify access permissions for individual users or groups at the file or database level. This allows for more granular control over data access.

iii. Conduct Regular Training

Train employees on data access policies and security best practices. Raise awareness about the importance of data protection and the potential consequences of data breaches.

iv. Review and Audit Regularly

Regularly review access privileges to ensure they are up-to-date and aligned with job roles. Monitor user activity and access logs to detect and investigate any suspicious access attempts. Conduct regular audits and security assessments to evaluate the effectiveness of data access controls and identify areas for improvement.

Data Retention

Data retention policies are essential for managing and disposing of data in a way that aligns with legal requirements, security needs and business objectives. Organisations should implement policies and regularly review and update them based on the industry, regulatory environment and data types. The following are some general guidelines that can be taken as part of the organisation's data retention policies.

i. Data Inventory

Maintain an inventory with appropriate retention periods of all data assets, including their location, owner and retention requirements, and regularly update the inventory to reflect changes in data holdings. This can help to ensure that data retention policies align with local, national and international standards.

ii. Data Disposal

Determine who is authorised to approve data disposal and implement access controls to prevent unauthorised data deletion. Establish secure methods for data disposal, such as shredding physical documents or securely erasing electronic media. Keep records of data destruction activities, including dates, methods used, and responsible personnel. This can help to maintain documentation as evidence of compliance.

iii. Data Transfer and Deletion during Employee Transitions

Implement procedures for transferring or deleting data associated with employees who leave the organisation. This also helps to ensure that departing employees do not retain unauthorised access to data.

iv. Monitoring and Enforcement

Implement monitoring mechanisms, such as audit trails and logs to record data access, modification and deletion activities. This ensures compliance with data retention policies.

Data Backup and Recovery

Data backup and recovery are essential components of a comprehensive data management strategy. Organisations should regularly back up critical data to secure storage locations and maintain reliable backup procedures to ensure data availability and facilitate timely recovery in the event of data loss, system failures, or security incidents. The following are some measures that can be taken as part of the organisation's data backup and recovery process.

i. Back Up Data Regularly and Secure Offsite Storage

Implement a regular and comprehensive data backup schedule and store backup data in a separate, secure location, preferably offsite or in the cloud and is disconnected from the organisation's network. This prevents the backup data from being affected by a cyber incident that affects the primary data stored in the organisation's network.

ii. Utilise Multiple Backup Copies

Keep multiple backup copies of critical data to ensure redundancy. Use different backup media, such as tapes, external hard drives, or cloud storage to minimise the risk of data loss due to hardware failures or cyber-attacks.

iii. Establish Data Recovery Points

Set recovery points to specific time intervals based on the needs of your organisation. This allows you to restore data to a known clean state before the cyber incident occurred.

iv. Monitor Backup Processes

Continuously monitor backup processes to identify any anomalies or failures. Automated alerts can help detect potential issues early and enable prompt action.

v. Document and Review

Document all data backup and recovery processes, including the technical details and configurations. Regularly review and update these procedures to adapt to changes in your organisation's infrastructure and cyber threat landscape.

By implementing encryption, access controls and having backup, organisations can establish a more comprehensive security strategy to create a more robust data protection system.

Data Classification

Data classification is the process of categorising data based on its sensitivity, value, importance, and other relevant characteristics. It is an important aspect of data security in an organisation as it helps organisations manage and protect their data more effectively by assigning different levels of security control, access restrictions and handling procedures based on the classification. With proper data classification strategy in place, an organisation can better safeguard sensitive information, ensure compliance with regulations and optimise data handling processes. The following are some ways that an organisation can adopt to put data classification measures in place.

i. Implement a Data Classification Framework, and Classify Data Assets

Define a clear and comprehensive framework for classification that aligns with the organisation's regulatory requirements and industry best practices. The framework should include various categories and labels that show the sensitivity and confidentiality of the information. Common classification levels include public, internal, confidential, and highly confidential. Define the criteria for each data category including the sensitivity level and access control levels. Identify and categorise the types of data, their sensitivity levels and the systems or databases that store them. Educate and train employees on the framework to ensure that data classification is practised accurately and consistently.

ii. Identify the Level of Data Ownership Between the Stakeholders

Understand the roles of the different stakeholders in the organisation and the data that they require access to. Practise the principle of least privilege and limit the users' access rights to only what they strictly require for their jobs. As such, entry level employees should not have access to data that are classified as highly sensitive within the organisation. Employees should be accountable for classifying, protecting, and managing data that is only within their scope of work.

iii. Conduct Audits and Assessments

Perform an assessment of the organisation's current data assets, including file systems and databases. Assess the data to evaluate its value, sensitivity, and confidentiality. This assessment will help in the process of designing the data classification framework for the organisation. Conduct regular audits on the organisation's data to ensure that the data remain properly classified.

iv. Review and Improve the Framework

As the organisation matures, it is crucial to update the data classification framework regularly. Conduct periodic reviews to re-evaluate the different data classification categories and policies.

When there is proper data classification being put in place, the organisation can have better data protection, regulatory compliance, and operational efficiency. With evolving business needs and changing data landscape, it is crucial to update data classification framework regularly.

Secure File Sharing

Secure file sharing refers to the process of sharing files or documents with others in a way that ensures the confidentiality, integrity, and availability of the shared information. It involves using encryption, access controls, and other security measures to protect the files during transit and while stored on the recipient's end. Secure file sharing is essential for preventing unauthorised access to sensitive information and maintaining data privacy.

To make sure that files are only accessible to the intended recipients, it is important to share files securely and privately. Big cloud storage providers, like Google Drive or Dropbox, encrypt files in transit or at rest in their servers, but shared files are not end-to-end encrypted, and the provider still holds the encryption key. If the provider suffers a data breach, the threat actor may also steal the keys to shared files, which will be detrimental to the organisation. The following are some guidelines that an organisation can look out for to share files securely:

i. Use End-to-End Encryption

With end-to-end encryption, users hold the encryption keys to the files, so they can be sure that users and their organisations are the only ones who can access them. Implement end-to-end encryption to ensure that files are encrypted on the sender's device and remain encrypted until they are decrypted on the recipient's device.

ii. Use Strong Passwords

Use strong passwords that are relatively long, typically containing 12 or more characters, and include a mix of uppercase letters, lowercase letters, numbers and special characters. To help users remember their passwords, organisations may encourage them to use passphrases by putting together a sentence or combination of words based on a memory unique to them. Passphrases are more secure than typical passwords as they are generally longer and require significantly more time for cybercriminals to crack It is essential to have unique passwords for different files to enhance security.

iii. Password-Protect Files

Protect both file-sharing links and the files shared with passwords to prevent any unintended audience from accessing them. Share the passwords separately from the links and files to enhance security.

iv. Turn On Two-Factor Authentication (2FA)

Require users to go through an additional authentication step, such as a One-Time Password or biometric verification, before accessing shared files.

v. Set Time Limits for Sharing Files

Set an expiration date and time for the file-sharing link to work, after which, the link will be made inaccessible. This ensures that files are accessible only for the required period and reduces the risk of unauthorised access after the sharing period ends.

vi. Implement Access Control Measures and Monitor File Access

Make use of application control to create rules to accept file transfers only for groups with specific user IP addresses while blocking the other IP addresses. Also, regularly monitor file access and review logs to detect any suspicious activities or unauthorised attempts.

vii. Use Secured Transmission

Public Wi-Fi networks are often insecure, so it is important to use a Virtual Private Network (VPN) to encrypt your traffic if you are using a public wi-fi network for this purpose. When sharing files with servers or remote locations, use Secure File Transfer Protocol (SFTP) or other secure file transfer protocols to protect data during transit.

viii. Conduct Regular Trainings

Conduct training for employees to educate them on the sensitivities of different types of data and the risks associated with the mishandling of information, as well as on the best practices of secure file sharing.

By employing secure file sharing measures, and with employees each doing their due diligence, the organisation can ensure that data will not be lost in transit to malicious threat actors who might use them for nefarious activities.

Physical Security

Physical security refers to the measures and safeguards put in place to protect physical assets, facilities, and resources from unauthorised access, theft, damage or harm. It involves a range of strategies and practices designed to secure physical locations, equipment, and personnel. Ensuring physical security of devices is essential for safeguarding sensitive information and protecting an organisation from potential security breaches. The following are some guidelines that an organisation can follow to ensure physical security.

i. Implement an Asset Management Checklist

Conduct an inventory check on all devices within the organisation, including desktops, laptops, tablets, servers and other electronic devices. Create an asset management checklist to track the ownership and status of each device. This would help the organisation better manage their devices and employee's accountability.

ii. Implement Access Control Measures

Implement strong access control measures for physical access to inventory. Use biometrics for authentication and install video surveillance system to prevent unauthorised entry and track access. Limit the access to inventory only to employees who require such access.

iii. Conduct Regular Trainings

Conduct training for employees to educate them on the importance of physical security. Remind employees on best practices such as not leaving devices unattended, locking devices when they are left unattended and procedures for reporting missing devices. In addition, enforce the use of strong passwords and full disk encryption to ensure that even when the devices are stolen, data stored in the device remain protected.

By following the abovementioned guidelines, the organisation can ensure a strong physical security for their devices. Having proper measures for physical security can help mitigate risk, protect and build awareness among the employees.

In conclusion, effective data and device security is not only a necessity but also a strategic asset for any organisation. By safeguarding sensitive information and building trust with stakeholders, proper data security measures provide the foundation to build a safe and secure environment in this digital age.

References:

https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html

https://www.rudderstack.com/learn/data-security/data-access-control/

https://www.techtarget.com/searchdatabackup/tip/Ten-ways-you-can-make-your-data-backups-more-secure

https://www.ibm.com/topics/data-security

https://www.nccoe.nist.gov/sites/default/files/legacy-files/data-classification-project-description-draft.pdf