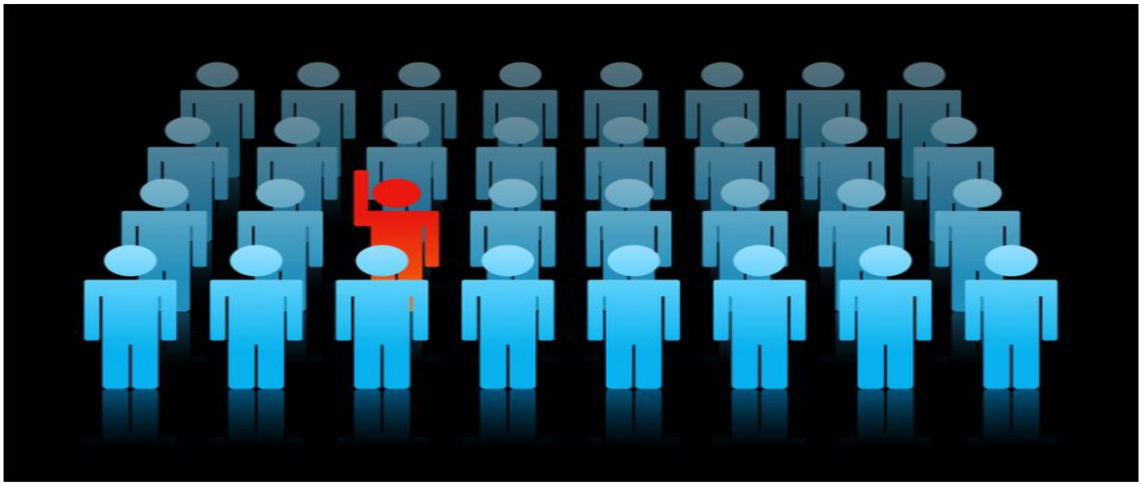
PREVENTING DATA EXFILTRATION – INSIDER THREATS



Data exfiltration is the unauthorized copying, transfer, or retrieval of data from a computing device. It can be accidental or malicious activity that occurs in two main ways: outsider attacks and insider threats (from within the organization). Both are major risks. Organizations with sensitive or confidential data are particularly at risk of these types of attacks.

Data exfiltration from outside an organization can occur when an attacker infiltrates the organization's network to steal data or sensitive information, such as personally identifiable information (PII) or protected health information (PHI). This can be a result of cybercriminals directly breaching devices or networks or injecting malware onto a device, such as a computer, smartphone or a USB drive that is connected to the organization's network.

Insider threats are one of the top causes of data exfiltration. Insider threats can involve malicious insiders (i.e., employees or contractors) stealing their own organization's data and selling sensitive information to competitors, cybercriminals, or nation-states. According to Proofpoint, which provides software as a service and products for email security and data loss prevention, two out of three insider threat incidents are accidental, and most of these are via email.

Accidental data loss from an insider threat could prove equally costly to an organization. **Careless employee behaviors can result in sensitive data falling into the hands of bad actors.** For example, an employee can exfiltrate data by sending it out through email, losing the company's computing device or storage device, or by loading company data onto a personal external storage device, such as a USB drive or external hard drive.

June 2022 https://it.nc.gov/media/3105/download?attachment
Rev 02/2023

The following tips can help organizations minimize the risk of data exfiltration:

- **Implement multi-factor authentication**: MFA adds a layer of protection to user credentials that makes it less likely that passwords will be compromised, and sensitive data will be breached.

- **Implement data loss prevention:** Data loss prevention is used to detect data-use policy violations and to prevent data loss. It involves data discovery and classification to find, categorize and understand sensitive data and then prevent such data from leaving an organization's network/devices.

- **Identify and redact sensitive data:** Not all data carries the same level of risk for exfiltration. Identifying systems on which sensitive data resides and ensuring that it is properly secured helps prevent exfiltration. Where sensitive data is not needed, it should not be stored.

- **Block unauthorized communication channels:** Some strands of malware use external communication channels to exfiltrate data, which can be blocked.

- **Educate users:** Ensure employees can detect the signs of a cyberattack and that they know not open malicious attachments or click links in unsolicited emails. Organizations should also educate employees about company policies about data sharing as best practices for keeping data secure.

HOW TO REPORT INSIDER THREATS:

Security incidents, for example, suspicious events (e.g., insider threat), software errors or weaknesses, system vulnerabilities associated with security incidents (e.g., Ransomware), **and lost or stolen State computer equipment, shall be reported immediately to the agency management.**

June 2022 https://it.nc.gov/media/3105/download?attachment
Rev 02/2023

a. All suspected security incidents or security breaches are reported to your supervisor and CSS Security immediately. Also, the IRS Office of Safeguards must be notified immediately, but no later than twenty-four (24) hours after identification.

i. To report an incident, you will complete the NCDHHS Privacy and Security Office-Incident Reporting Form at https://security.ncdhhs.gov.

ii. Organizations shall notify consumers in the event of a security breach resulting in the unauthorized release of unencrypted or un-redacted records or data containing personal information with corresponding names. Note: The acquisition of encrypted data is only a breach if a confidential process or key needed to unlock the data is also breached, or if the data is encrypted by an unauthorized or malicious process, such as ransomware.

b. Information recorded about information technology security breaches shall cover the following at a minimum:

i. Identify the current level of impact on agency functions or services (Functional Impact).

ii. Identify the type of information lost, compromised, or corrupted (Information Impact).

iii. Estimate the scope of time and resources needed to recover from the incident (Recoverability).

iv. Identify when the activity was first detected and when corrective actions were implemented.

v. Identify the number of systems, records, and users impacted.

vi. Identify the network location of the observed activity.

vii. Identify point of contact information for additional follow-up.

viii. Identify the attack vector(s) that led to the incident.

ix. The method of breach detection and incident response actions

x. Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident.

xi. Provide any mitigation activities undertaken in response to the incident.

June 2022 https://it.nc.gov/media/3105/download?attachment
Rev 02/2023