SyberGRC: Insider Risk

Name of Presenter

Agenda

- Insider Risk | Introduction
- Access to Data or Permissions to Data
- Archival and Deletion according to company policies
- Third Party Risk Regulations
- CIS Data Discovery Controls
- NIST Data Discovery Controls

Insider Risk:

- Insider Risk Definition:
  - 'Insider Risk occurs when any data exposure (regardless of perceived data value or user intent) jeopardizes the well-being of an organization and its employees, customers or partners.' Insider Risk's focus is on an organization's data problems rather than its people problems
    - *Ref: CERT insider threat center*

- Legal Risk:
  - Complying to Data Archival and retrieval policies

Types of Insider Risk

Sabotage: The insider uses their legitimate access to damage or destroy company system or Data

Fraud: The theft, modification or destruction of data by an insider for the purpose of deception

Intellectual property Theft

Espionage

Data Breach Facts

According to Verizon 22% of the data breaches happens from Insiders.

34% of businesses around the globe are affected by insider threat yearly.

- 66% of organizations consider malicious insider attacks or accidental breaches more likely than external attacks.
- Overt the last 2 years the number of insider incidents has increased by 47%
- *By techjury.com*

34% of businesses around the globe are affected by insider threat yearly.

More Insider Risk Facts:

Employees use company's email to exfiltrate company's sensitive data	25%	Cyber attacks are attributed to Insider Threats	60%
Data Breaches are caused by insiders	30%	Insider threat incidents are caused due to negligence	63%
Global businesses are affected by insider threat annually	34%	Unintentional insider threat attacks are caused by phishing attacks	67%
Increases in insider threat incidents over last 2 yrs.	47%	Org. failed to determine the actual damage of an insider attack	85%
Organizations believe that they are vulnerable to insider attacks	50%	IT Professional considers insider threats as a cultural issue	86%
Employees involve in an insider threat had a history of IT Security violation	51%	Insider threats succeed an adverse work event as termination or demotion	92%
Org. considers privilege users as a greatest insider threat risk	55%	IT leaders Insider threat as a major security concern	97%
Employees leaving an org. takes sensitive company data with them	59%	Cost of Insider threats for organizations in 2020	$2.7 9 M

More Insider Risk Facts

Average number of days to identify a data breach

197

Average nos. of days to contain an incident

77

Average amount spend by a large enterprise on insider threat in 2019

17.82M

Internal breaches occur in US daily

2500

Managing Insider Risk

Knowing your internal Data

- Structured and unstructured data

Knowing your inventory on unstructured data

Access Control on Internal Data

Probability of insider risk or Fraud

- Insider privilege and Misuse stats *(Ref: CIS Community Defense Model 2.0)*

Controlling Insider Risk: CIS community Defense Model & NIST

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST 800-53 Controls
3	3.1	Data	Identify	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	PR.IP-6
3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	ID.AM-5
3	3.6	Data	Identify	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	
3	3.7	Data	Identify	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	ID.AM-5
3	3.7	Data	Identify	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	ID.RA-5
3	3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	PR.AC-4

How iDPS maps to NIST & CIS controls

Title	NIST 800-53 Controls
Establish and Maintain a Data Management Process	PR.IP-6
Establish and Maintain a Data Inventory	ID.AM-5
Configure Data Access Control Lists	PR.AC-4

iDPS Feature
Complete Data Governance/Information Risk Solution
Complete Data Scanning and Reporting with iDPS
Provide visibility of permission on structured and unstructured Data

Take Away

- Insider Risk remains the BIGGEST threat to the organization

  Ref: https://www.cisecurity.org/white-papers/cis-community-defense-model-2-0/

  - CIS and NIST offer frame works to manage Risk/Threats
  - iDPS is developed on such frameworks to manage Risks/Threats


Q
&
A

What’s next??

- ???