Data Protection and Management

Evolution of Data Protection Solutions

Learning Outcome

At the end of this lecture you should able to;

- Explain the evolution of data protection
- Describe solutions for evolving data protection trend
- Identify key data protection management activities

Data Protection

- Data become imperative assets of modern society
- It has evolved from procedural function into an essential component
- Privacy rights continuously evolve, ragulators are facing challenges to identify best practices because
  - new business models
  - technologies,
  - Big Data
  - Analytics
  - AI and profiling

Data Protection Vs. Data privacy

- Data protection is about securing data from unauthorized access
- Data privacy is about authorized access (personal information)
- Data protection is a technical issue
- Data privacy is a legal matters pertaining to personal information
- Data protection may not comply with every stipulated compliance standard
- Data privacy involves legal implications associated with privacy laws

Factors affecting the evolution of Data Protection

- **Regulatory Compliance:** Specifing how organizations should protect Personally Identifiable Information (PII), and other sensitive information.
- **Intellectual Property:** Data protection solutions should be capable of identifying and safeguarding crucial knowledge properties.
- **Data visibility:** should safeguard sensitive data (must aware the existence, the detail about data and the usage)

Quick Review

- Explain the differences between Data Protection and Data Privacy
- Explain the factors that affect data protection

Reasons for Data Protection in Modern Organizations

- Technology evolve very fast
- IoT devices become common
- Malicious attacks, accidental data leakage, BYOD (Bring your own device)
- Weak in a small sectors on a disk drive or weakness or failure of an entire data center
- New regulation needed to protect data

Solution – Best-in-Class Practice

Is to implement a solution that provides smart, resource-centric (i.e. people and dynamic data-centric) refined data protection regulation with cost-effective and fast recovery

Types of Essential Data to be Protected

- Data that is in use – day-to day data or information that exist in the users’ fixed devices need to be protected from leakages (e.g. copying to other portable devices or media
- Data that is in motion: Data that is in action through wired or wireless (in the form of download or upload). The processes need to be protected.
- Data at rest: Data that in in the repository such as backup or archive. The usages need to be tracked and audited.

- Provide reasons for data protection
- Explain the different types of essential data to be protected

Data Protection Strategy

- Create data protection policy compliance with SOX (Sarbanes & Oxley) and PCI (Payment Card Industry) rules
- Establish DLP strategy to identify which data need to be protected.
- Steps to Data protection straregy

Steps to Data protection straregy

- Identify critical and sensitive data
  - – Establish a list of controlled and confidential data
    - Away to identify e.g. data which uses high security to secure such as biometrics.
- Define policy
  - – Each policy must provide with a distinct set of rules
    - E.g. identity card number and bank account number or PIN
  - – If the policy did not cover certain data then create a special rules and processes with regular expression

Continue….

Steps to Data protection straregy

- Establish flow of information
  - Prepare questionnaires
  - Find the starting point of the data and how and where it is flowing.
  - Identify the person who responsible for that data

DLP implementation

- First, Establish list of organozation’s crucial and critical data
- Acquire DLP product which necessary for the organization
- Investigate and analyse the DLP product they buy is able to support the organization’s DLP requirements.
- Start the DLP implementation from small base and gradually increase the base. In this ay we can able to protect from costly damages.
- Identify and update risk profile regularly and document of any DLP insidents

Quick Review

- Explain in detail a strategy for data protection

Why Data Protection need to Evolve

- Increased Cyberthreats
- Predominant of 5G
- Lack of Cybersecurity Professionals
- Enhanced Digital Transformation

Increased Cyberthreats

- Global cybercrime damage predicted to hit $10.5 trillion annually by 2025. [Cybercrime Megazine]
    - damage and destruction of data,
    - stolen money,
    - lost productivity,
    - theft of intellectual property,
    - theft of personal and financial data,
    - embezzlement,
    - fraud,
    - post-attack disruption to the normal course of business,
    - forensic investigation,
    - restoration and deletion of hacked data and
    - systems, and reputational harm.

Predominant of 5G

- Propagation of Internet of Things (IoT) which build with lack of security
- Cyberattacks such as malicious actors uses technology such AI and machine learning to attack faster
- Business competition - technology providers will skip critical steps that ensure these devices are secure

Lack of Cybersecurity Professionals

- Everyone is struggl ing for the same talent.
- An critical shortage of advanced cybersecurity skills. (difficult to find an experienced threat hunter, incident responder, or cloud security architect)
- With digital transformation, IoT, and “smart” infrastructure, the cybersecurity skills shortage should be seen as an existential threat,

Enhanced Digital Transformation

- For example, when a data is the cloud, visibility will be diminished. These will cause the world
    - No real-world view of exactly how their data is protected
    - no regulators will know their own responsibilities from legislative perspective

Quick Review

- Why data protection need to develop gradually

How Data Protection will Change in the future

- Machine learning will play a important role in data protection
  - It will be used to investigate the critical and crucial data to deploy and modify data protection algorithms and approaches.
  - Then regulators can learn from the data and make improvements before a new threat.
- Artificial intelligence will be used both increase data vioation and protect against them
  - AI makes malware faster more adaptable, and harder to detect
  - Progression in AI-powered cybersecurity - such as biometric authentication, cybernetics security policy deployment, and IoB (Internet of Behavior) - more instrumentation of AI technology

How Data Protection will Change in the future

- Distant workers will prompt increased security. E.g. work from home (WFH) workers
  - New data protection policies
  - Improved access management
  - Data protection awareness training
  - Increased data protection funding
- More countries will legislate data protection laws
- Organizations will employ profession data protection workers

References

Cybercrime Megazine - Top 6 Cybersecurity Predictions And Statistics For 2021 to 2025 (cybersecurityventures.com)

Q & A

Next Topic

Data Protection and Availability Solutions

- Explain the evolution of data protection
- Describe solutions for evolving data protection trend
- Identify key data protection management activities