Getting Ready – Data Protection Audit

DANIEL GYAMPO

Governance / Risk / Audit / InfoSec / EMBA / ISACA – CGEIT,CRISC,CISA

“Checklist”

- Regulatory requirements
- Data classification
- Data loss prevention
- Network and Data security
- User access management
- Security of mobile devices – access control, remote security, anti-virus
- Data disposal methods

Regulatory requirements

- Country
  - **The Data Protection Act, 2012 (Act 843)** requires every individual or organization that processes personal information to register.
  - **Electronic Transactions Act 772, 2008** - 8(2) Retention of electronic records: The document, record or information shall be kept in electronic form for **at least six years**.
- Industry
  - Financial services – PCI DSS: protection of cardholder data

Data classification

- Data classification is broadly defined as the process of **organizing data by relevant categories** so that it may be **used and protected more efficiently**. The classification process not only makes data easier to **locate and retrieve** – data classification is of particular importance when it comes to **risk management, compliance, and data security**.

Data classification

- **Category 4 [CONFIDENTIAL]:** Highly sensitive corporate and customer data that if disclosed could put the organization at financial or legal risk.
  - Eg: Employee social security numbers, customer credit card numbers, bank account details
- **Category 3 [RESTRICTED]:** Sensitive internal data that if disclosed could negatively affect operations.
  - Eg: Contracts with third-party suppliers, employee reviews
- **Category 2 [OFFICIAL]:** Internal data that is not meant for public disclosure.
  - Eg: Sales contest rules, organizational charts
- **Category 1 [PUBLIC]:** Data that may be freely disclosed with the public.
  - Eg: Contact information, price lists

Data Loss Prevention

- **Data loss prevention** (**DLP**) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what **data** end users can transfer.
  - **Emails and classified documents** – block ability to print/copy/forward emails with classified contents
  - **Mass storage and data transfer devices** – restriction on USB ports and use of mass storage devices
  - **Cloud storage** – restriction on use of cloud storage spaces
  - **Mobile devices** – policy for data / information to reside on company servers and only be accessed by mobile devices

Network and Data Security

- **Network security**
  - Physical and logical
  - Internal and external
  - Firewalls – IPS, IDS
  - Routers and switches – port controls, telnet/ssh, tunneling
  - Network segmentation
- **Data security**
  - encryption of data at rest, in the cloud and in transit
  - anti-virus
  - Protection of physical records/documents

User Access Management

- Rights – create, view, update, delete
- Roles – function within the organization
- Password policy
- Single sign-on solutions
- Regular reviews
- Procedures around joiners and leavers

Security of Mobile Devices

- Access control – password protect / screen lock
- Remote security – delete data, disable device
- Anti-virus – auto updates, protection against malware

Data disposal methods

- Procedure for handling old/obsolete computers and electronic storage devices
- Controlled procedure for deleting and destroying data


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
спасибо
dank je
bedankt
dziękuję
obrigado
sukriya
kop khun krap
go raibh maith agat
merci
terima kasih
grazie
arigalò
dakujem
감사합니다
мерси