Universitas Esa Unggul

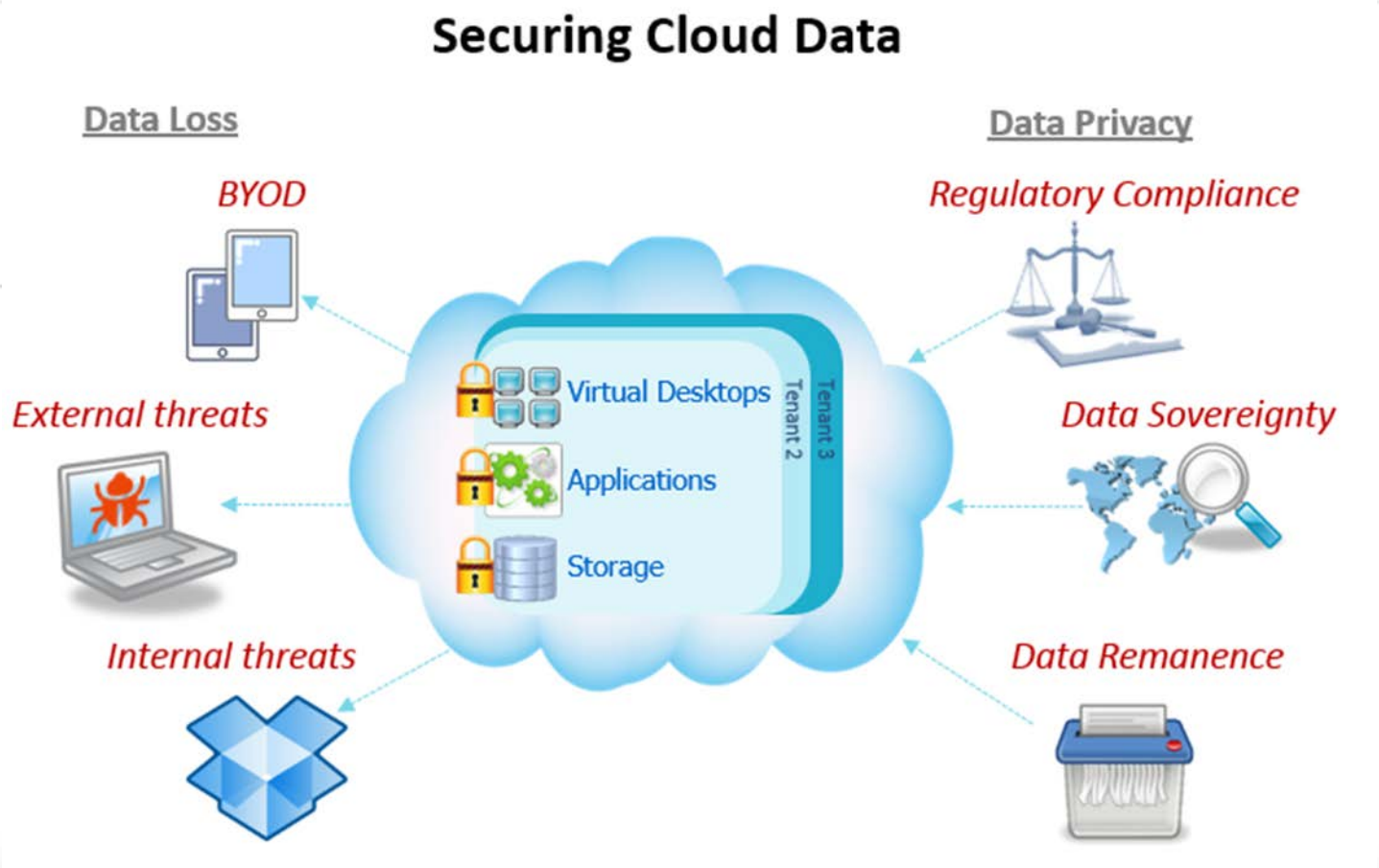
Smart, Creative and Entrepreneurial

www.esaunggul.ac.id

Serangan keamanan pada Data Cloud

Haditya L. Mukri
Prodi RMIK & MIK

Securing your Cloud



Data Lose Scope:

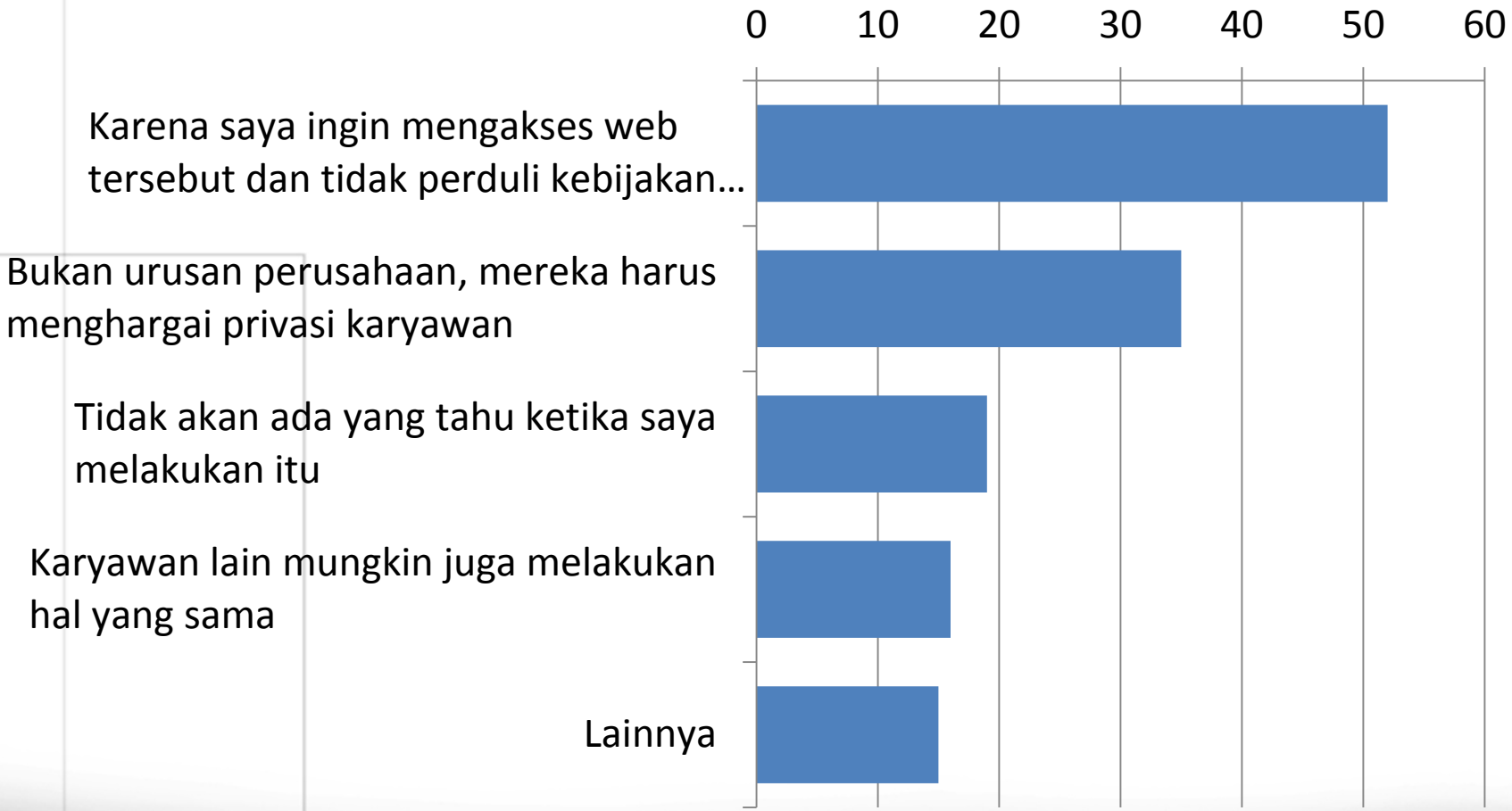
- Pekerja
- Proses
- Lingkungan fisik
- Network and Administration

Sektor Pekerja

Dalam hasil survei yang diadakan oleh cisco terungkap, ketidakpatuhan karyawan seringkali melampaui pentingnya kepatuhan karyawan terhadap kebijakan keamanan data.

Ketika survei tersebut menanyakan mengapa karyawan berbagi informasi perusahaan yang sensitif, misalnya, 44% menjawab bahwa mereka perlu "memunculkan gagasan dari orang lain“. Alasan populer lainnya ialah "Saya perlu curhat," (30%) dan "Saya tidak lihat ada yang salah dengan itu, "(29%).

Alasan karyawan tidak mematuhi Kebijakan keamanan



Sektor Proses

Large office move requires transport of hundreds of hard drives, tapes, CDs and paper records

Outsourced contract requires use of sensitive data for service delivery

Previous archival methods must be refreshed to ensure long term storage of sensitive data

Lingkungan Fisik

Employee copies sensitive data from database to USB for "safekeeping".

USB

Printer

Employee prints sensitive document for review on the road.

Copy & Paste

Employee cuts out sensitive data from working document and uses hotmail to send a copy to his home account.

Network dan administration

- Peer to Peer
- Email
- FTP
- Wi-Fi
- Company Website

Menangkal dan menghindarinya

- Kerangka tata kelola
- Penilaian risiko
- Cybersecurity Training
- Access Management
- Vendor Management

1 Identifying Sensitive Data

- Patient Health Information (PHI)
- Customer Personally Identifiable Information (PII)
- Financial Records
- Proprietary & Competitive Information
- Regulatory Compliance (HIPAA, FINRA, Sarbanes-Oxley)

Identify and prioritize your most valuable data and put in place end-to-end encryption for data in motion and at rest.

2 Considering the Risks

- Email
- Removable Storage Devices
- Web Browsing
- File Sharing Tools
- Mobile Devices
- Network Access
- Cloud Backup

Consider a secure container approach to email and PIM that controls user actions like save, print, forward and cut/copy/paste.

3 Implementation & Deployment

- On-Premise or Cloud management tools
- Governance of multiple device types and user profiles
- Compliance management to enforce policy
- Security safeguards and procedures for lost/stolen devices

Define policy and get employee consent. Make a technology decision on the tools to help govern and maintain policy.

4 Educating Employees

- Sets expectations
- Avoids potential violations
- Promotes proper behavior
- Reinforces awareness
- Deters intentional and malicious breaches

Involve and educate employees so they understand expectations and avoid potential violations.

http://www.notifycorp.com/solutions/data-loss-prevention