SHADOW IT: PRIVACY AND RECORD MANAGER CONCERNS

Linda Rush

February 22, 2019

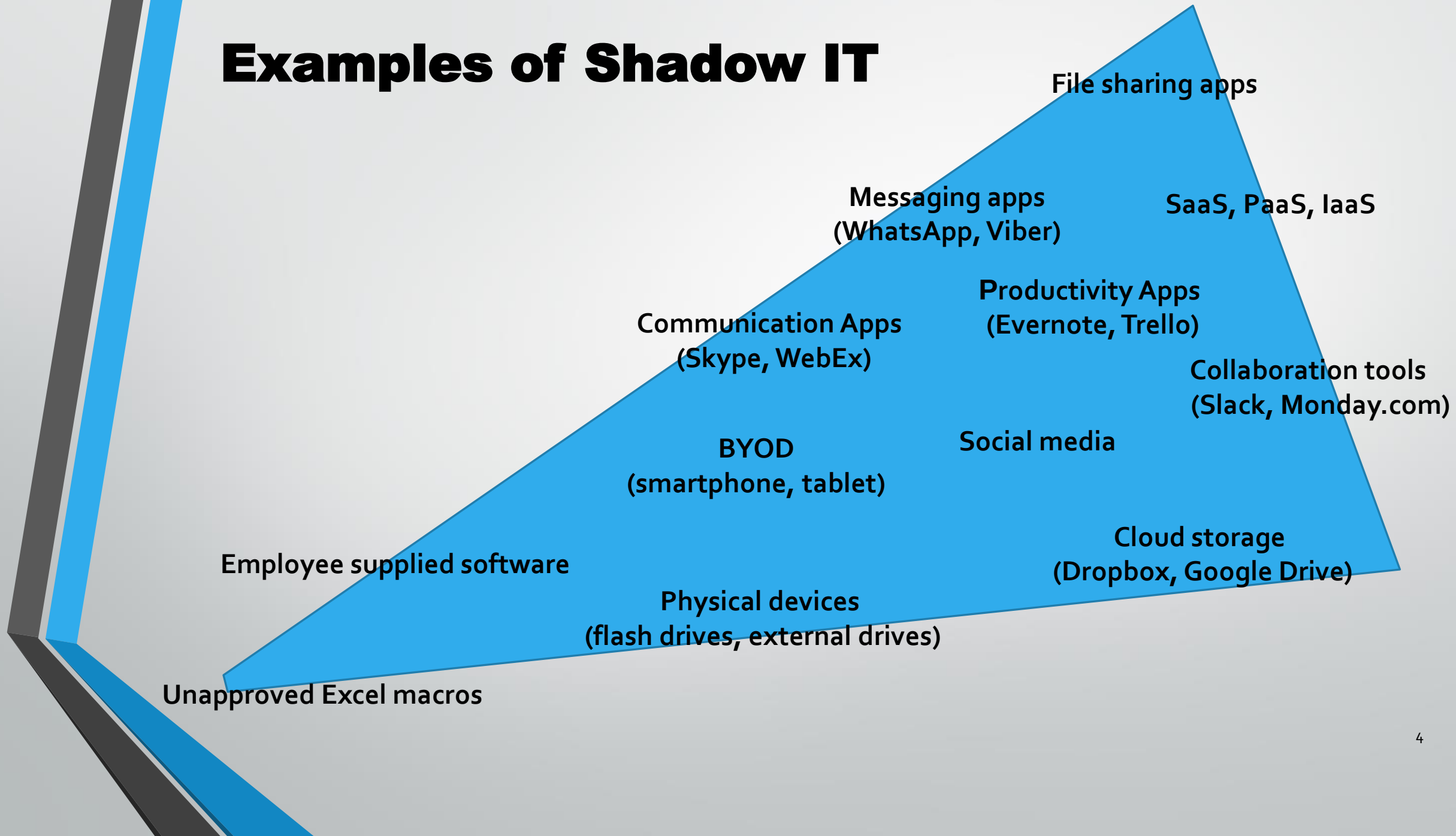
Disclaimer

The statements and opinions made during this presentation are those of the presenter only and do not necessarily reflect the official policy or position of any organization, employer or company.

What is Shadow IT?

- **IT systems and solutions built, used and/or managed without explicit organizational (IT) approval (or proper licensing)**
- **Can be used on corporate devices/systems or cloud**
- **Any resource or applications**

Examples of Shadow IT



DOES YOUR COMPANY HAVE SHADOW IT?

Shadow IT comprises **50%** or more of IT spending (Everest Group)

Shadow IT **30%** to **40%** of IT spending in large enterprises (Gartner)

CIOs underestimate number of cloud shadow IT by a factor of **15** to **22** (Cisco)

By 2020 **1/3** of successful attacks experienced by companies will be on shadow IT resources (Gartner)

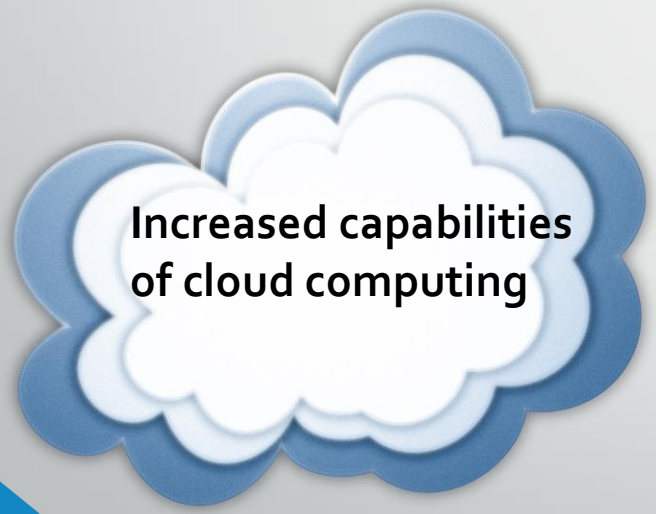
83% of organizations don't know the number of Shadow IT apps in use by their staff (Cloud Security Alliance)

18.1 % of files uploaded to cloud-based file-sharing and collaboration services contain sensitive data (McAfee)

Why do employees use Shadow IT?

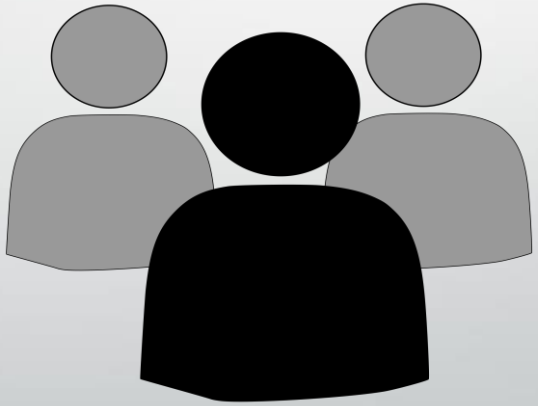
Company IT solutions seen as not efficient or cost-effective

Tech savvy employees (using applications/devices for personal use)



Increased capabilities of cloud computing

Common Practice



Industry-specific/cross industry SaaS

Opportunities for Company

- Business more competitive
- Employee engagement with technology can lead to productivity
- Less need for employee training and management
- Relieve IT dept from supporting physical infrastructure
- Lead to innovations in business process/operations
- Cost savings
- Business-critical processes developed – efficient and effective operations

Risks to Company

Security/Privacy

- Data breaches
- Introduction of viruses, malware, etc.
- Use of unauthorized/unsecured devices
- Insufficient security controls (i.e. encryption, access)
- Duplication of systems
  Loss of respect for IT organization

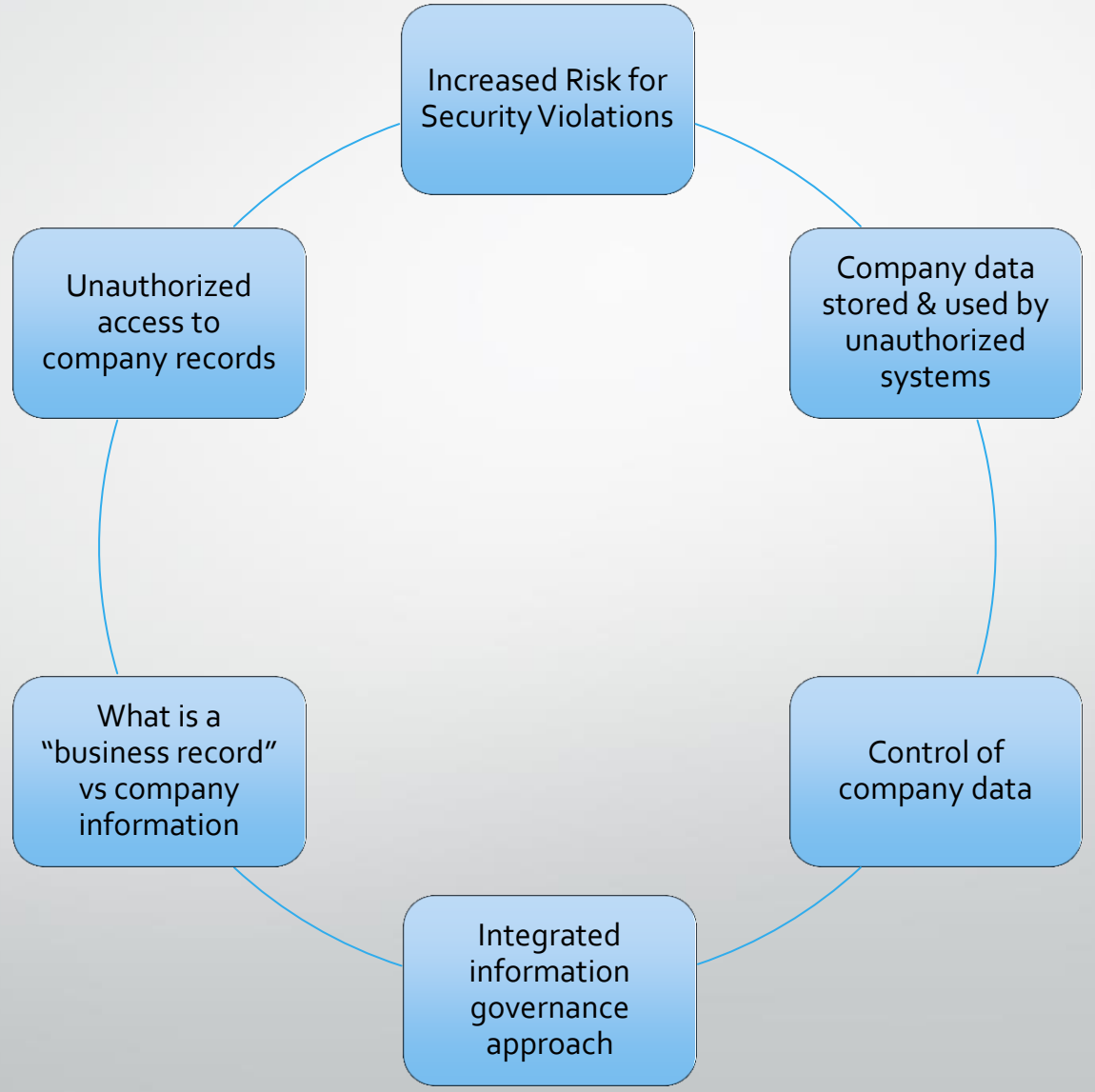
Corporate/Record Management

- Loss of control of data
- Company records/information leaving
- Duplication of records data
- Regulatory audit
- Lack of integration/consistency among corporate users
- Loss of access to records/information (IT blocks)

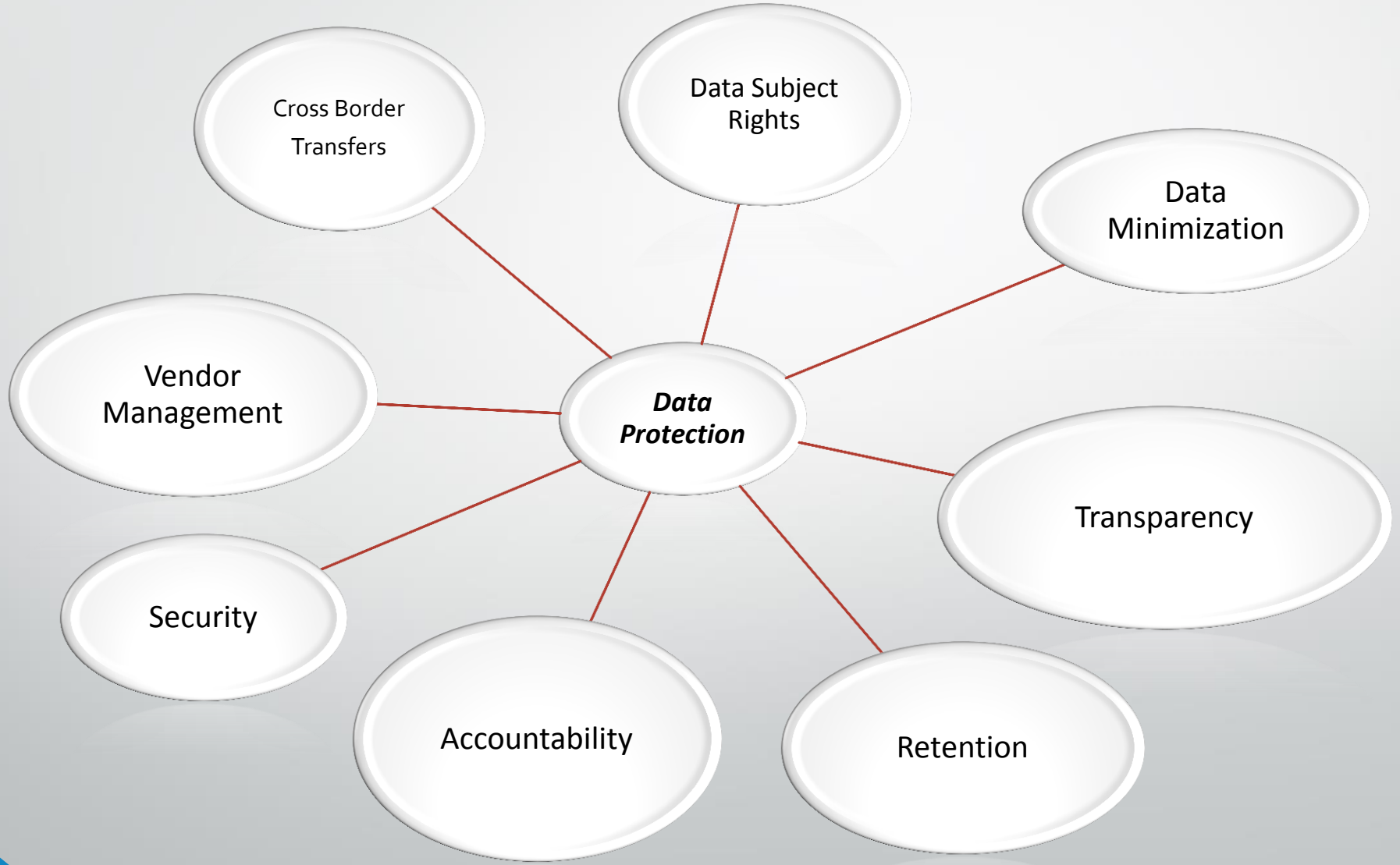
Third Party Rights

- License compliance
  no license/improper use
- Intellection Property violations
  infringement/combination
- Customer audit

As a records manager, why should you care?



Privacy Concerns



What should your company do?

DISCOVER/IDENTIFY

MANAGE/GOVERN

Notable Breaches in 2018

vtech

LifeLock

amazon

FedEx

Atrium Health

ORBITZ

VOVOX

UNDER ARMOUR

AIR CANADA

Panera BREAD

POLAR

TCM Bank

G+

QUESTIONS?

Linda Rush

Linda.rush@techdata.com