THALES

Fare collection solutions

Cybersecurity and account based systems

francois.baylot@thalesgroup.com

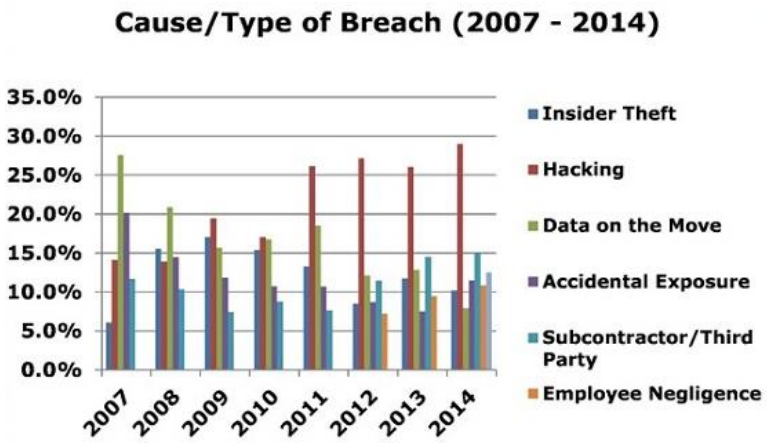
Security breaches – some facts

In a more and more connected world, a proliferation of sophisticated and targeted cyber attacks e.g. against

- Governments,
- Critical infrastructures
- Industrial control system

Consequences of Cyber attacks:

- Financial fraud, disrupted reputation, industrial espionage, etc.



Source: Identity Theft Resource center

Examples of 2015:

- Carbanak, a cyberheist worth 1b$ over 100 banks worldwide
- Kaspersky revealed infiltration of its internal systems

Source: crn.com

Fare collection changes over the last few years

- Technology moved very quickly over the past few years
- Smart mobility raised needs new technological needs
- Public transport industry had to catch up with the new paradigm

Key areas where security is at stake

Fare collection

- Security design national standards (ITSO, Calypso, SDOA…)
- Media and fare intrinsic security

Network/IT

Identity protection & privacy

- Compliance to national privacy rules

Payment standard compliance

- EMV, PCI…

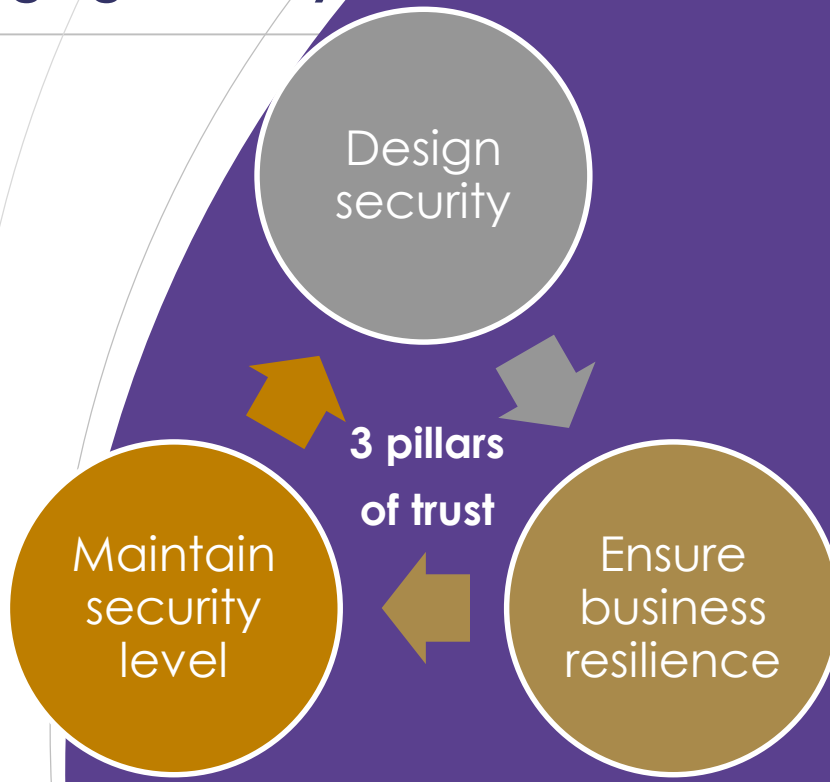
THALES

What are we trying to achieve by managing security?

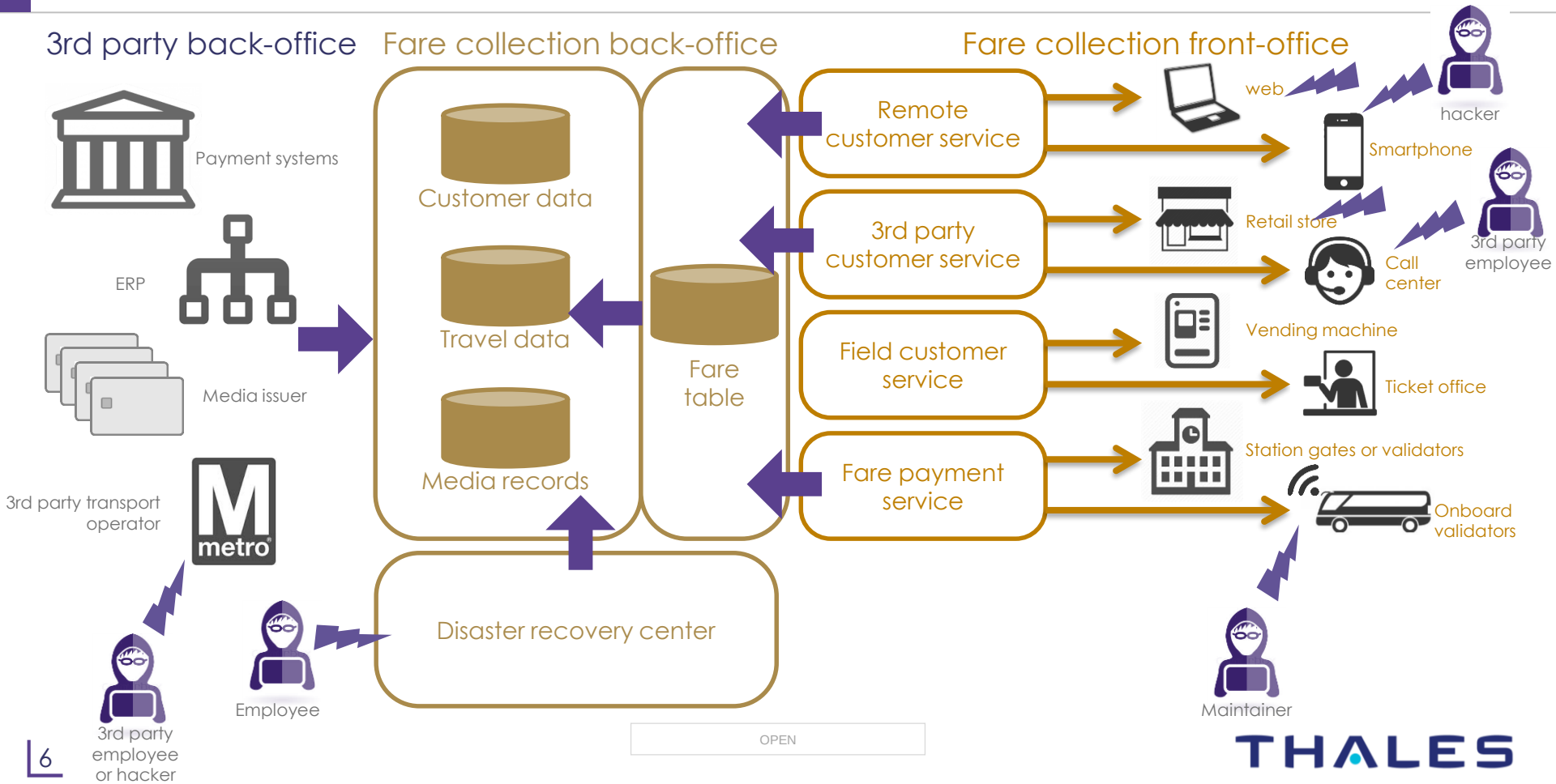
To be evaluated in case of security exposure

- What the financial consequences can be
- How the communication and company image can be damaged
- How the company organization would react
- How resistant is the infrastructure, how fast would it recover
- What level of service it would possible to deliver…

Awareness leads to taking actions and build TRUST



Examples of threat sources in new fare collection solutions



THALES

Typical attack scenario

Initial Intrusion

Target: end-user computer system

- USB key or email attachment
- Known software vulnerability to download .exe
- Remote Desktop control

Intrusion in depth

Target: authentication servers

- Get progressive access to global information system
- Back Door opening

Search for strategic data

Target : application servers & end user terminals

- Keyword based document search
- VIP mailbox scan

Data exfiltrated

- Information gathering
- Massive or discrete data exfiltration

Tips to manage security risks

Tip 1: Standardized security services and processes

Tip 2: Security by design

- For existing solutions, set up basics like:
  - pen testing,
  - reinforced network & IT infrastructure, use probes & logs
  - hardened execution environment,
  - robust identity management…
- For new solutions: software architecture, coding rules, certified building blocks…

Tips to manage security risks

Tip 3: Communication: Cloud to end-point security

- Use appropriately security hardware (HSM) and a security broker for critical credentials (keys, identity management…)

Tip 4: Data storage: encrypt stored privacy-sensitive data

Tip 5: Consider outsourcing security

- ISO 20000/27000 certified « Security-as-a-Service »: 24/7 alert monitoring, incident, problem & crisis management, access control, disaster recovery…

Key take-aways

- **Do not take cyberthreats lightly,**
  - prepare organization, processes and tools accordingly
- **Avoid silos and "CSO-as-a-guru"**
  - integrate smart and affordable security for everyone in your company
- **Mobile, cloud and big data are here and will last**
  - don't refuse them because of security but design security accordingly
- **There are now suitable data/identity protection solutions using encryption**
  - consider them seriously
- **Use external help for design, review, audits…**