Deloitte.

From commodity to true value
How to give essence to IT audit today

5th ISACA Athens Chapter Conference

Lajos Antal
DCE Cyber Risk Service Lead Partner

Athens, Greece 2015

IT Auditing in the ‘90s

Pre-Internet era

- Either stand-alone systems or some connectivity, which were not equivalent to what we call “online” today
- All started way before - first known IT-based fraud in 1964 at Equity Funding Corporation of America.
- Collapse of the Barings Bank in 1995 - key characteristics:
  - some level of IT involvement
  - segregation of duties
  - lack of monitoring controls
- The Citibank “hack” in 1994 - 10M USD stolen by Vladimir Levin
- IT Auditing:
  - Auditing General Computer Controls
  - Access control reviews - standard Work Programs
  - “focused” - mostly servers

IT Auditing around Y2000

New approaches

- Pentesting - breaking into systems for fun and for profit
- False sense of security
    - protecting all computers in a network - X vulnerability + pwd crack
    - capturing network traffic in switched LAN
    - default passwords
    - capturing SSL network traffic in clear
- Conflicts: a series of controls operating effectively, lots of controls tests show controls matching best practices, yet the security-level is down.
- Key access controls focus on password controls, whilst successful attacks may not require passwords at all or obtain valid passwords in clear.

IT Auditing around Y2000

Web technologies

- Completely new type of vulnerabilities
  - (lack of) secure development
  - some standard and many unique development issues
- Webapp vulnerabilities
  - Are they scope of an IT audit?
  - Is it enough to check that certain apps/systems have been tested?
  - Scope/quality of testing + vendor selection (accreditation + staff limitation)

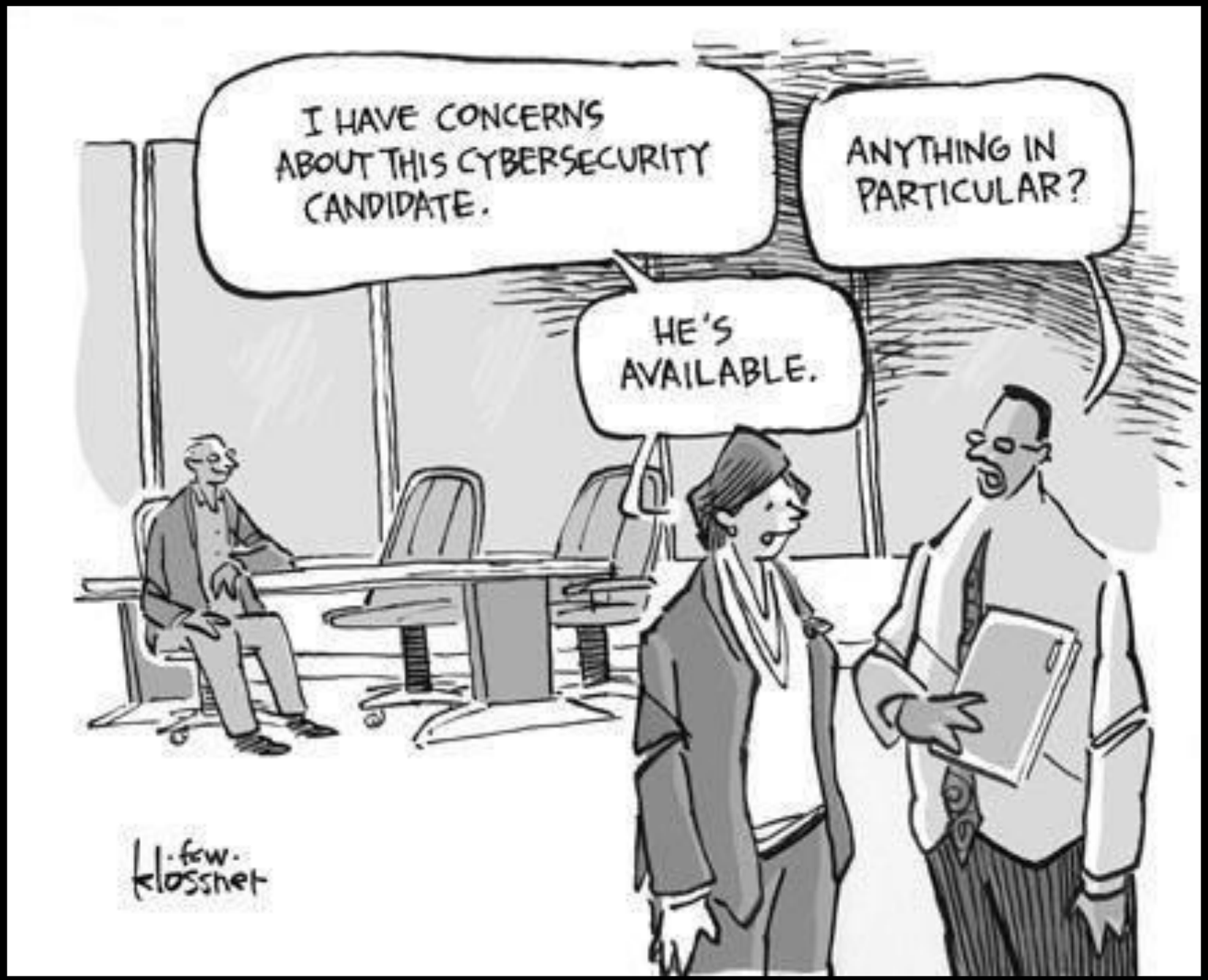
IT Auditing - recent years

The new and the very old technologies

- New technologies
  - Mobile (mainly Android and iOS)
  - Embedded systems
  - Infrastructure/facility protection - entry protections, CCTV, alarms, electricity, cooling
- Legacy systems
  - Mainframe systems
  - z/OS, z/TPS, OS2200 etc.
  - COBOL, PL/I, JES
- The untouched field
  - SCADA
  - Embedded systems

Almost completely out of the radar of IT audits.

Probably the biggest problem in Cyber Security

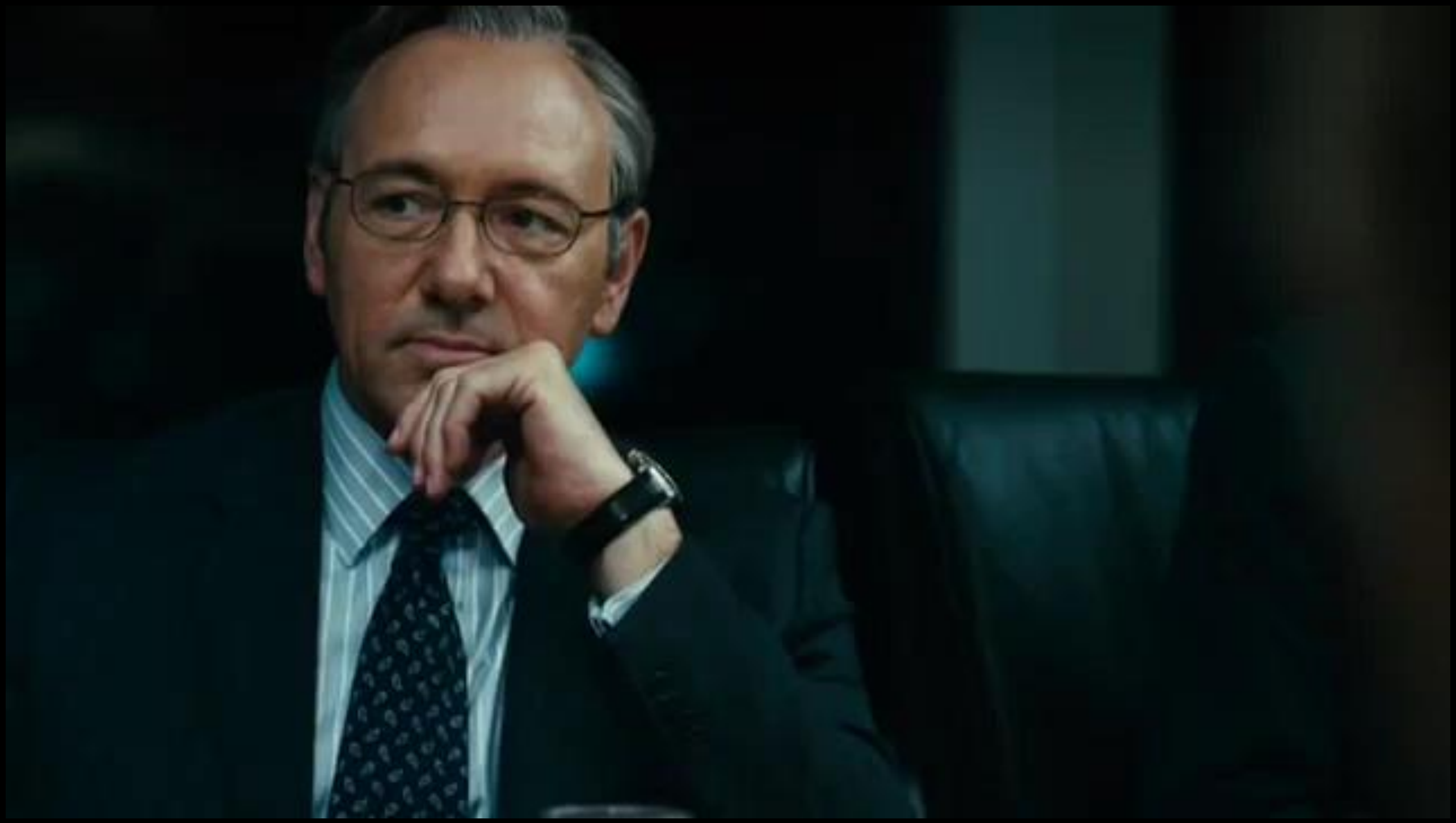


source: jklossner.com

IT Auditing - nowadays

Purpose of IT audits - Risk mitigation

- Recent fraud types
  - spear phishing
  - custom malware
  - insider actions - e.g. kick-back, stealing
  - blackmailing
  - price fixing
  - over-pricing
- Things can also go wrong unintentionally



IT Auditing - nowadays

Purpose of IT audits - Risk mitigation

- Operate with simple questions, e.g.:
  - How does this application authenticate users?
  - What makes the authorisation decision when such transaction is initiated?
- Be sceptical
- Test the quality of works: security tests, UAT
- Verify the acceptance of works performed
- Test ad-hoc - anytime, anywhere
- Exercise
- Be prepared - at some point, someone might fail
- Know your enemy - threat assessment

Deloitte.

Thanks for listening