

Shadow IT - Reasons, Risks and Remediation

Hannes Lubich

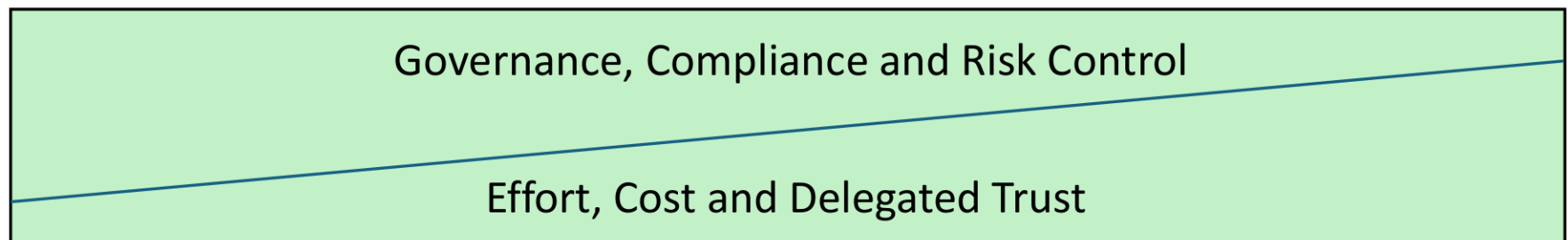
IT Dinosaur in Residence

lubich@acm.org

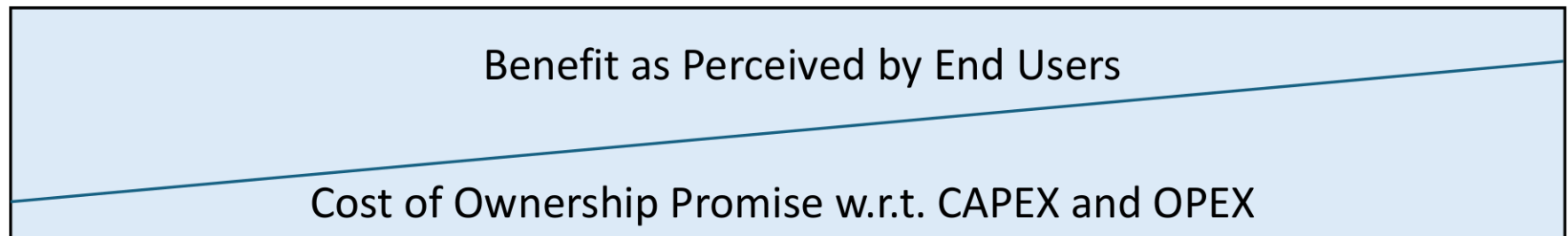


Types of «Hidden» IT

Shadow IT Physically Hidden IT Non-Local IT Supply Chain IT

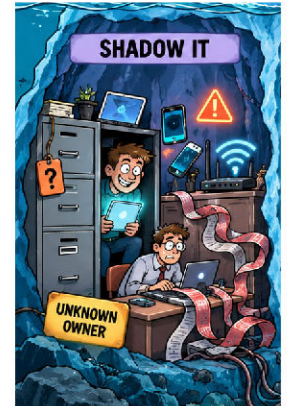


but also:



«Shadow» IT

Hardware / software utilized by end users without knowledge or consent of IT organisation / employer (or because BYOD is misinterpreted / misunderstood)



Reason:

- Users consider the «official» corporate IT environment and associated processes as insufficient or difficult to use, compared to their preferences and past experience.

Risk:

- Unmanaged and unpatched IT systems and services:
 - data loss
 - intrusion etc.
- Undocumented connections
- Bypassed access restrictions
- Insufficient governance and compliance
- License / terms-of-use violations and associated cost

Remediation:

- User awareness (for those who listen 😊)
- Limitation of access and privileges
- Systematic search for forensic evidence
- Active search for hardware artefacts or installed software

Physically Hidden/Invisible IT

IT hardware / devices that don't look «like IT» or are an embedded part of a larger IT system, such as storage arrays, medical equipment etc.



Reason:

- Many complex, but formally «analogue» devices become networked and require locally embedded computing, storage and networking capabilities

Risk:

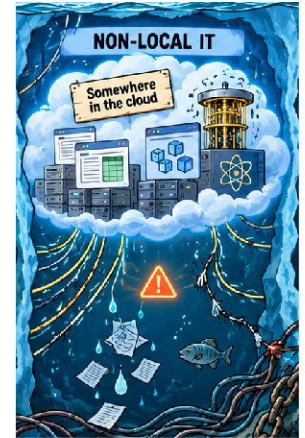
- Unknown IT sub-systems that are fully integrated into the local IT environment but can not or may not be updated (no access or loss of certification)
- Direct supplier access

Remediation:

- Central procurement with risk remediation as part of the process
- Up-to-date inventory
- Ring-fenced installations with limited privileges
- Controlled supplier access and logging

Non-local IT

Cloud-based «aaS» environments or virtual machines / desktops (e.g. to access entire application suites or services such as AI frameworks or quantum computers)



Reason:

- Out-tasking of IT-based tasks (SaaS Sprawl) because use is forbidden, or local procurement and operation considered infeasible or costly
- Insufficient internal resources

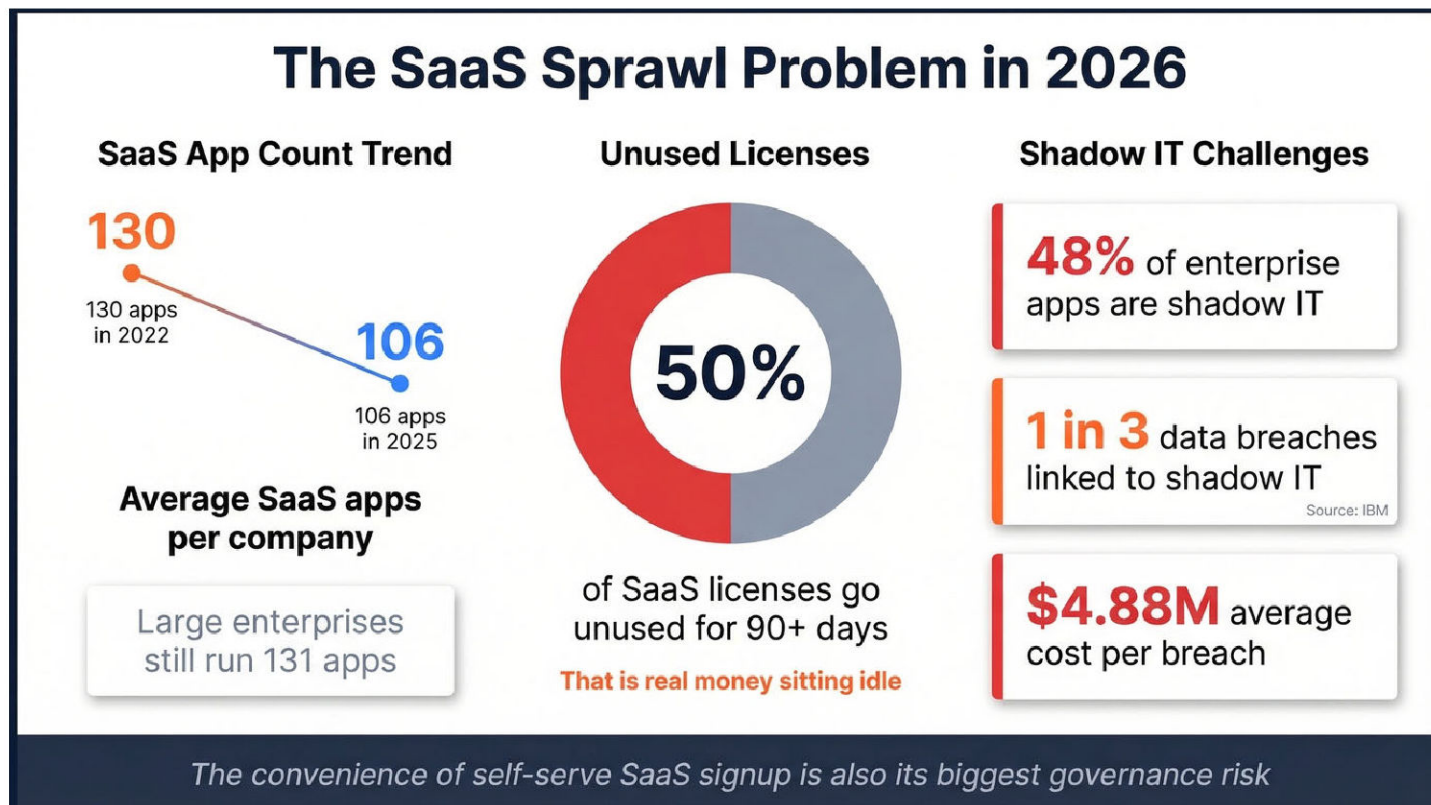
Risk:

- Data compromise
- Availability / BCM dependencies
- Difficult to audit and control beyond contract clauses and self-declarations
- Additional security requirements?

Remediation:

- Proper due diligence and risk assessment
- Allowed suppliers
- Additional internal rules and processes
- On-going monitoring of use and safeguards
- Proper supply chain management

SaaS Sprawl has Increased because of AI-aaS



Source: <https://prospero.io/s/what-is-b2b-saas>

Supply Chain IT

Entire, complex IT environments run by external suppliers and their sub-entities whose existence and operation is vital to a customer's business / core processes



Reason:

- Use of externalized services that in turn use complex and potentially (sub)-distributed IT environments to outsource complete processes for cost / efficiency reasons

Risk:

- Deterioration of governance and control along the supply chain
- Uncertainty w.r.t responsibility
- Substantial dependency risk for own core processes

Remediation:

- Proper due diligence and risk assessment, including SBOM
- Supply chain management and information about subsequent suppliers
- Redundancy planning and proven exit / transition strategy

«Insecure IT» Can Hide in Many Places

User
Suppliers
Integrators
(Sub)-Contractors
Ops. & Maintenance
User Interfaces / Config.
Applications Local / Cloud
Inventories and Databases
Operating Systems / Middleware
Source Code / Compilers / Interpr.
Periphery & Devices at End Points
Microcode, BIOS / UEFI & Firmware
System Hardware, Memory, CPU/GPU

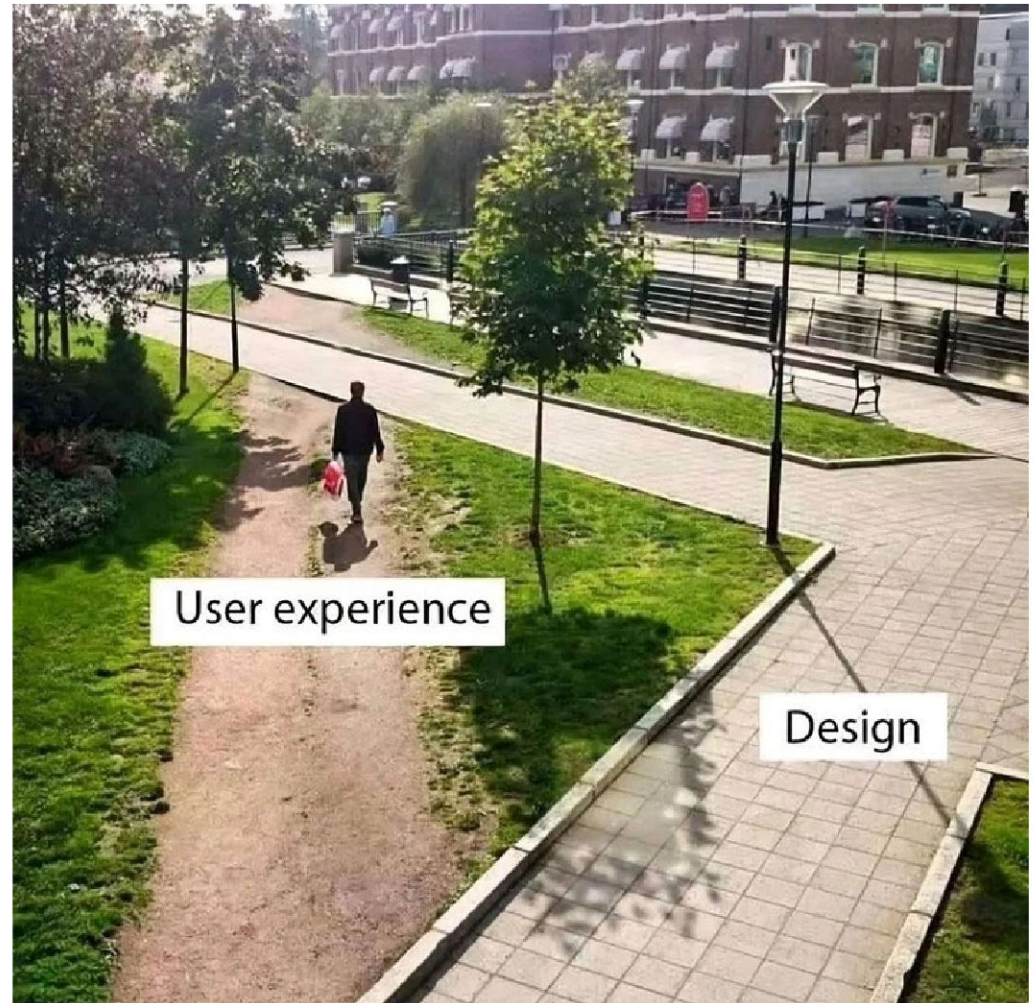


Complexity and Speed become Major Issues



Lessons Learned #1:

Never Underestimate
the Creativity of Users



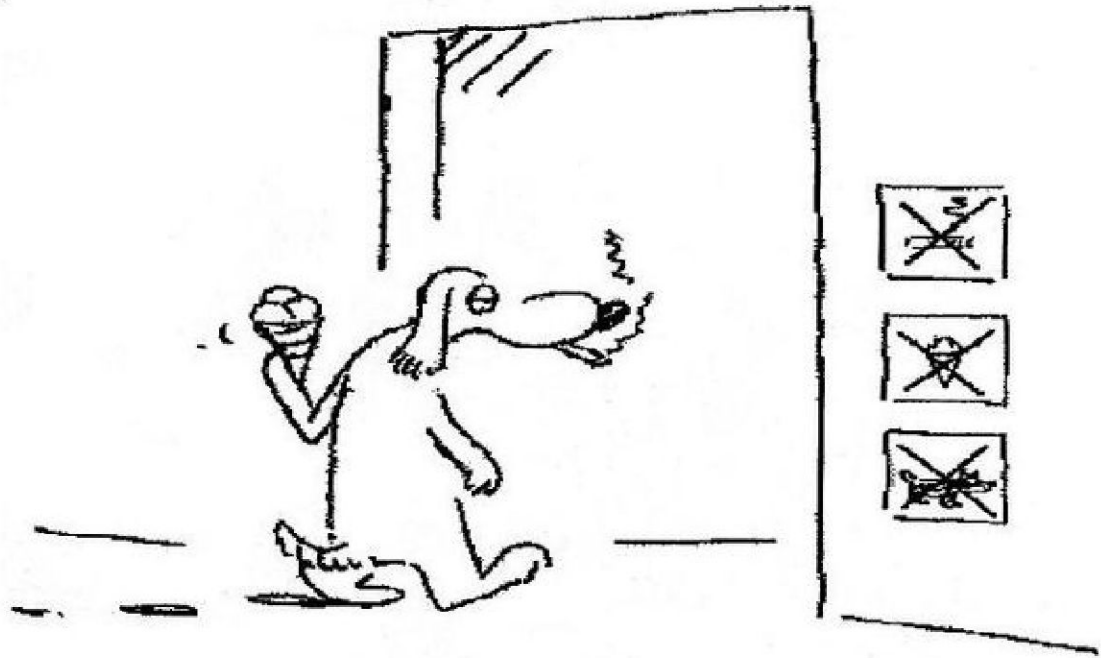
Lessons Learned #2:

Never Overestimate
the Discipline of
Administrators and
Power Users



Lessons Learned #3:

Never Rely Only on
the Effectiveness of
Trainings or Regulation



Lessons Learned #4:

Never use the sentence
«Look, I told you so» in
a security incident
management meeting,
even if you did tell them



Conclusion

- The problem will not go away
- Complexity & speed increase further
- Resources will remain limited
- Misuse increases dramatically
- Regulatory requirements increase

- Automated Detection
- «Near time» Response
- Evidence
- Realistic «Plan B»
- Rethink Trust (zero?)

