SIGS 6th Cloud Security Forum

Security in the Cloud - The Art of Building on Sand

V. Degtyarev (aka Slava), Head of IT, TradexBank AG

Agenda

- Cloud- Current State
- Choose your battle
- Confidentiality Toolbox
- Integrity Toolbox
- Availability Toolbox
- Deplatforming
- Outlook
- Home Work

Disclaimer

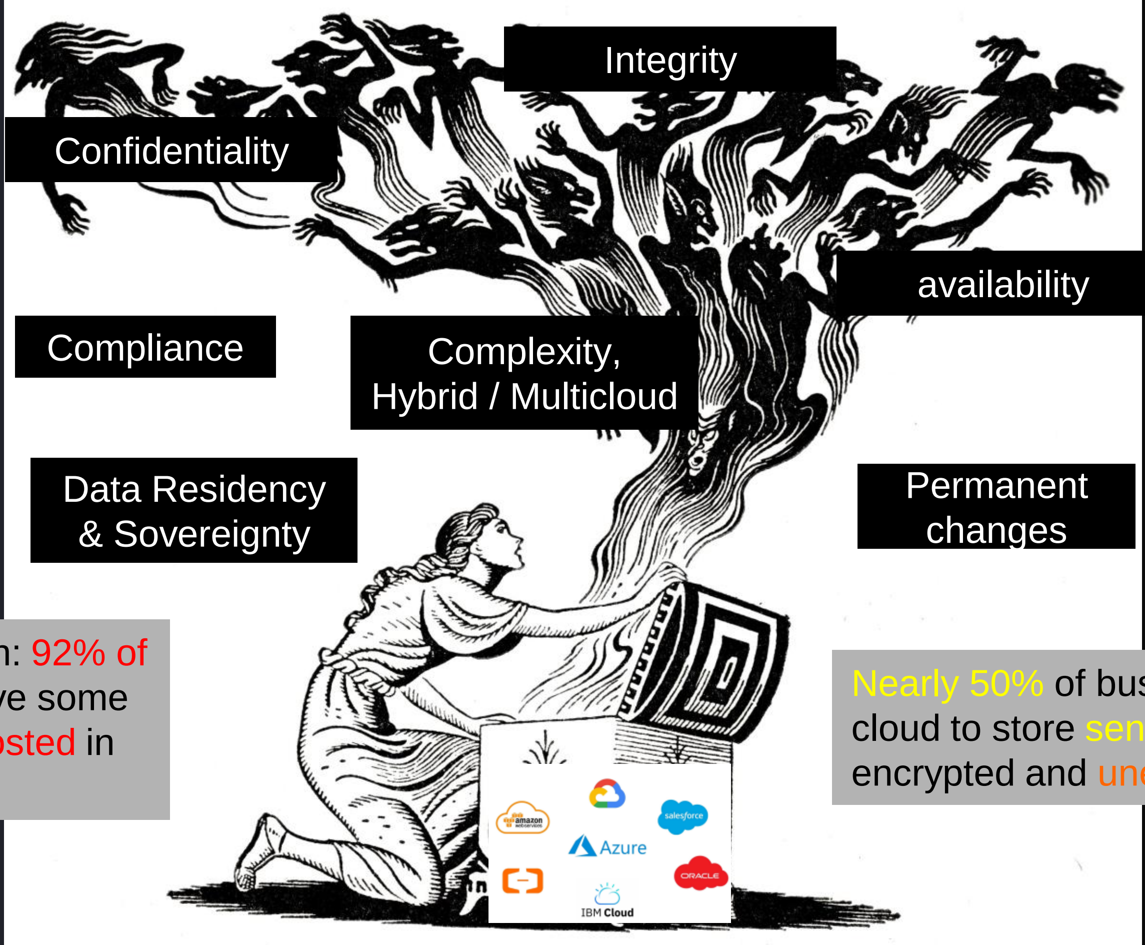
in IT & Security

Everyone Has
An opinion!
Kittens are better than puppies.
I hate spinach!
Pizza tastes better than carrots.
Make Opinion

Any views or opinions represented in this presentation are personal and belong solely to the owner and may not represent SIGS or my employer view's.

This is not a school! I'm not a teacher!

Cloud - Today 2024



Integrity

Confidentiality

availability

Compliance

Complexity,
Hybrid / Multicloud

Data Residency
& Sovereignty

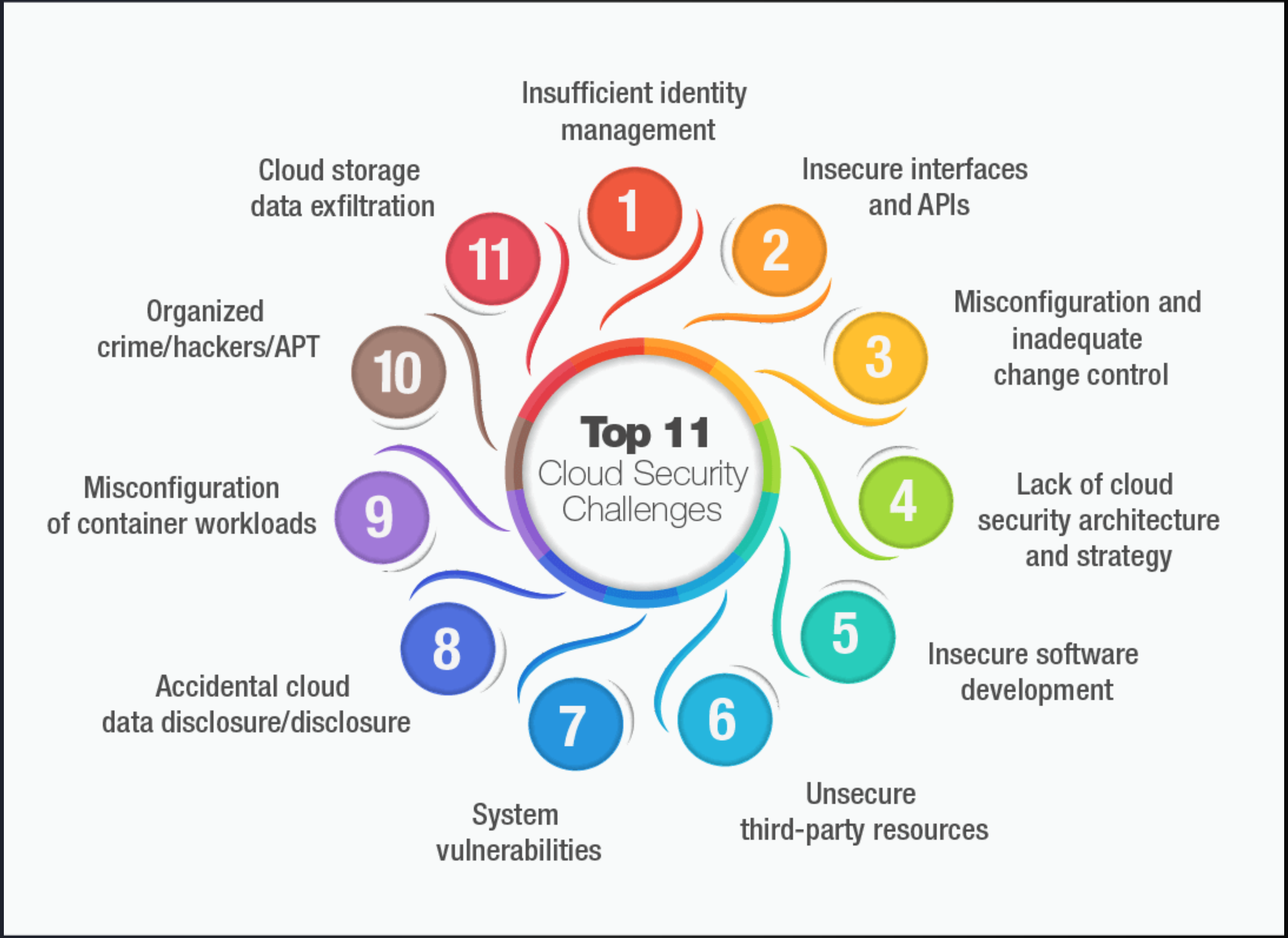
Permanent
changes

Ubiquity of cloud adoption: 92% of organizations already have some of their IT environment hosted in the cloud.

Nearly 50% of businesses use the cloud to store sensitive data; both encrypted and unencrypted.

Check Point Cybertalk: https://www.cybertalk.org/2024/01/24/the-future-of-cloud-security-20-statistics-trends-to-track/

Cloud - Challenges 202x


Top 11
Cloud Security
Challenges
1
Insufficient identity management
2
Insecure interfaces and APIs
3
Misconfiguration and inadequate change control
4
Lack of cloud security architecture and strategy
5
Insecure software development
6
Unsecure third-party resources
7
System vulnerabilities
8
Accidental cloud data disclosure/disclosure
9
Misconfiguration of container workloads
10
Organized crime/hackers/APT
11
Cloud storage data exfiltration

Choose Your Battles - Data

Use FINMA Circular 2023/1 “Operational risks and resilience – banks” as guiding light.
Keep inventory of all IT systems relying on cloud resources from 2 view angles:

“**Critical Data**” these are data that are: *crucial for the successful and sustainable provision of the institution’s services* OR *regulatory purposes.*

Critical data in terms of confidentiality: *“Confidential data is business information, customer or personal data that must be protected from unauthorised access to protect the privacy or security of an individual or organisation”*

Critical data in terms of integrity and availability:

- *Relates to the institution’s ability to operate efficiently and effectively, in some cases to operate at all.*

Critical data are therefore vital for the functioning of the institute (‘mission-critical data’).

- *If this type of data is damaged, destroyed or becomes inaccessible, the institute and its units and staff may no longer be able to perform their duties.*
- *Critical data related to* integrity *and* availability *are to be defined by a risk-based approach*

For people preferring NIST Cybersecurity Framework terminology – IDENTIFY phase

Choose Your Battles - Processes

Use FINMA Circular 2023/1 “Operational risks and resilience – banks” as guiding light.
Keep inventory of all IT systems relying on cloud resources from 2 view angles:

“**Critical processes**” are processes whose significant disruption endanger the provision of critical functions:

- *the activities, processes and services – including the underlying resources necessary for their provision – whose disruption would jeopardise the institution’s continuation or its role on the financial market and thus the proper functioning of the financial markets*
- *systemically important functions*

Every relevant business and organisational area must identify its critical processes and the resources required for these in a business impact analysis (BIA)

Operational resilience refers to the institution’s ability to restore its critical functions in case of a disruption within the tolerance for disruption.

For people preferring NIST Cybersecurity Framework terminology – IDENTIFY phase

Confidentiality – Preventive!

Address the risk at early design phase, use the proper “tools”:

- Delete is one of the best strategy! (consider proper methods)
- Pseudonymization – keep the keys under your control
- Add some “noise”: 99% synthetic or extern data
- Data Masking
- Generalisation
- *Encryption*: Public Key cryptography is your best friend

Integrity – Tight Control!

Trust is good, control is better:

- Data backup: back to premise and Cross – Cloud
- Archiving, immutability, retention
- End of (Day / Week / Month, etc) report of key metrics – out of the cloud!
- Public Key cryptography is your best friend, this time for digital signature
- Consider Blockchain approach
- Data Usage Monitoring + AI for pattern
- Data Quality Checks / Gates between systems

Availability – Plan “Ex”?

Do we have plan for “Abnormal Cloud Exodus”?!

- Early detection: User centric, cross-cloud service monitoring, probes.
- Focus on cross-cloud, well established standards (VMs, Kubernetes, Containers, etc)
- Have your data, artefacts, repo backups ready and accessible
- Keep an eye on DNS
- Know your: source code (cloud dependencies!), Open Sources alternatives for cloud services
- “Table Top” exercise for business for (semi)manual operation during system rebuild
- “Table Top” exercise for IT for system rebuild in alternative cloud or @home

Cloud Crisis – “Deplatformed”

- Geopolitics
- Hackers
- Sanctions
- Censorship
- Competitors
- Rouge employee
- “Voice of society”: for company not being enough "green", "gender", “Pro X / Against Y", etc.
- *Precepted* cloud provider reputation risks
- Broad cloud outage

https://www.gartner.com/smarterwithgartner/can-your-cloud-provider-deplatform-you

QUO VADIS?

- Grow of: Complexity, Uncertainty, Geopolitical tension
- IT personal: shortage * decrees of expertise
- State sponsored actors – increase of vulnerability surface
- Hacktivists
- Cloud offer proliferation
- Supply chain, third-party risks increase
- Increase of cyber-criminal activity
- AI advance, on both defensive AND offensive side
- Man-Made disasters
- Deplatforming cases because of XYZ reasons
- Company “cost optimization” initiatives
- “Cloud Native” apps

Some home work:

- ✓ Get you inventory. You can’t kill them all but at least:
    - ✓ Critical Data
    - ✓ Critical processes
- ✓ Know your cloud dependencies
- ✓ Know your “tools” to address div. risks:
    - ✓ Confidentiality
    - ✓ Integrity
    - ✓ Availability
- ✓ Consider “Deplatfroming Risks”
- ✓ Conduct “Table-Top” exercises