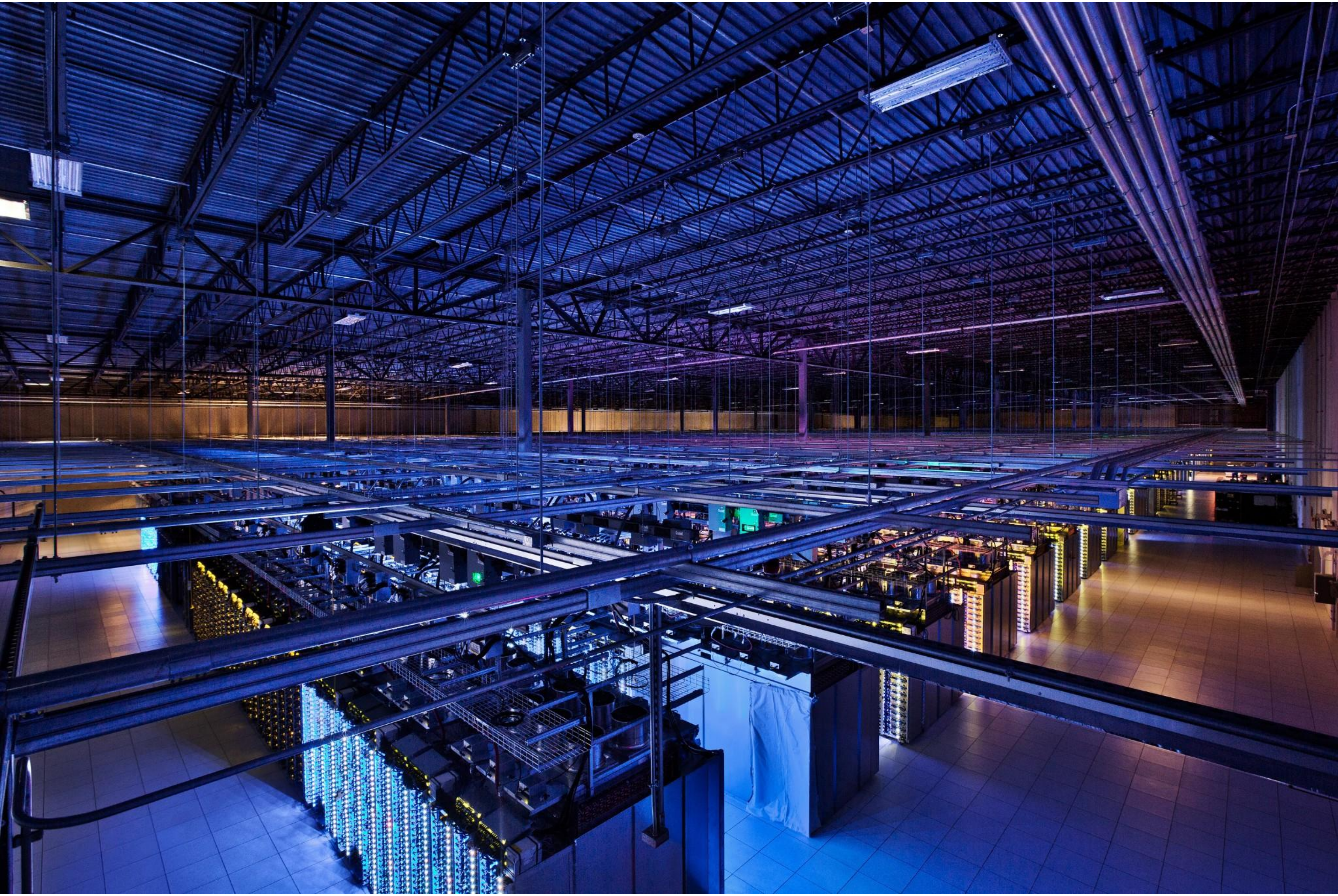
SaTC 2012 wishlist

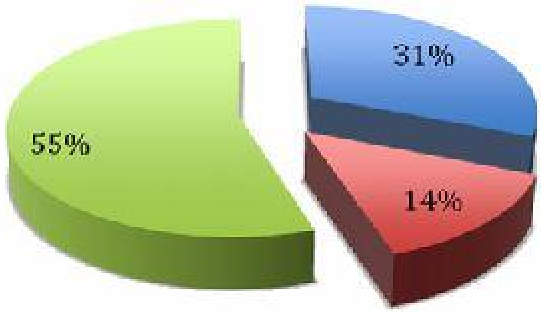
Eric Grosse   ehg@google.com



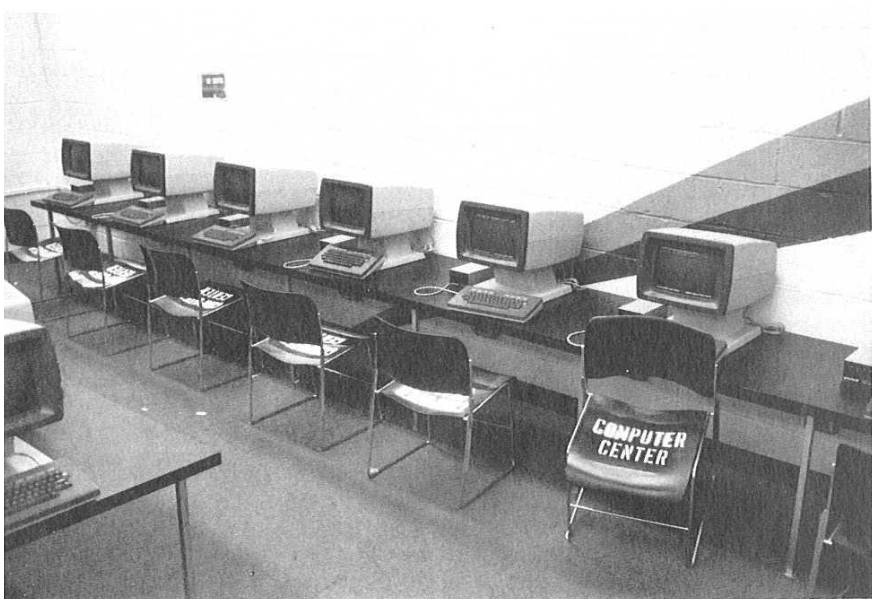
What keeps me awake at night:

1. **malware**, mostly on client machines
2. user, employee, machine, and service **authentication**
3. network **intercept**, such as RootCA compromise
4. product **vulnerabilities**, such as XSS or misconfiguration
5. **espionage**

Zeus and AV



trend: dumb terminal to dedicated device



device-centric auth

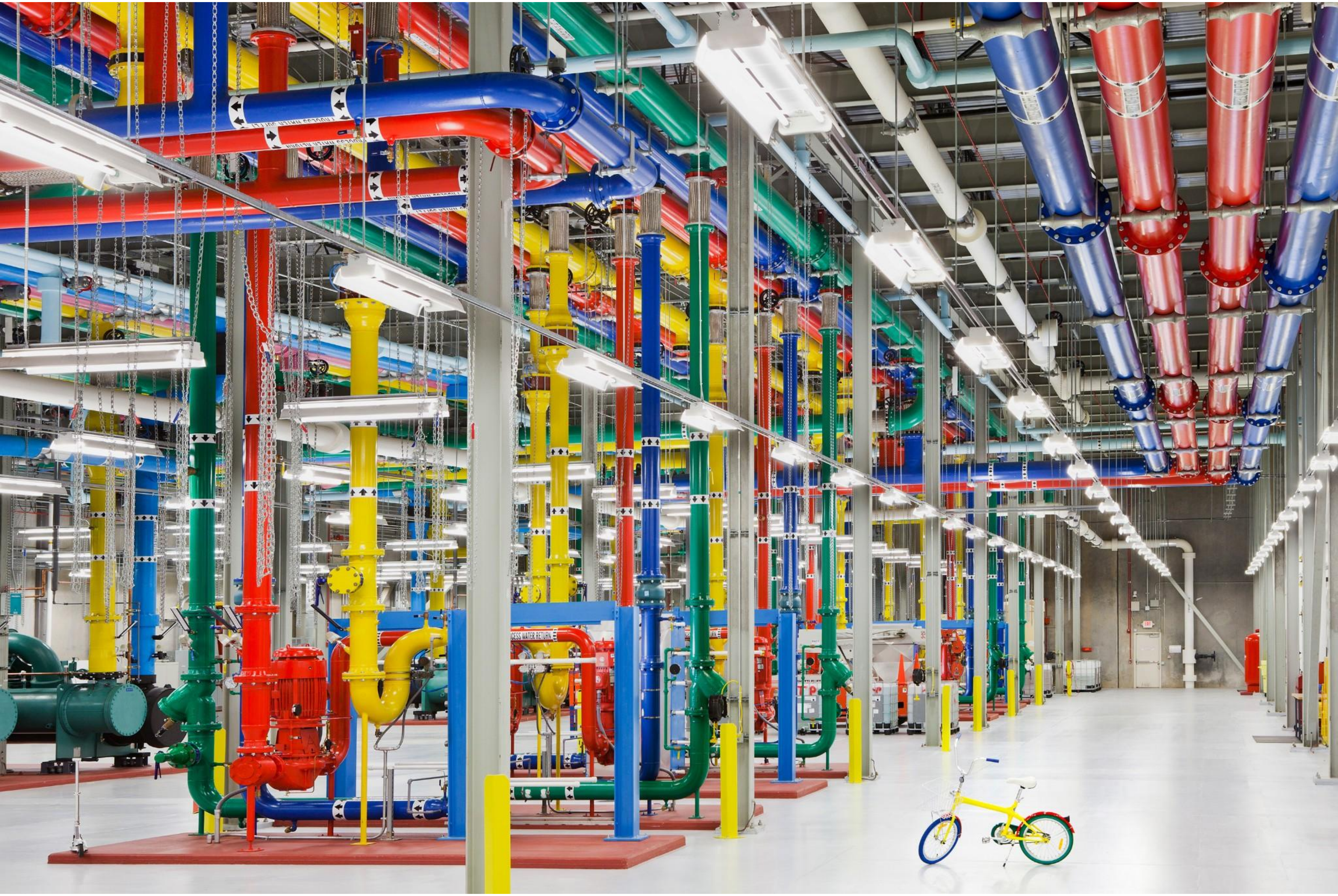
- client device holds strongly asserted identity (public key crypto)
- "blessed" by owner at acquisition, from existing devices
- device has long-term account access, for update/ring/...
- revoke quickly and selectively when lost, or abuse detected

- protect physically and by operating system
- shared devices(1): system-isolated accounts
- shared devices(2): family machine with scoped delegation

- supplement with high-value transaction confirmation

hardened systems; app isolation

beyond OS: fuzzing, web app vuln, SQLi, ...


CESS WATER RETURN

recovery after attack

undo

but expect root escalation, distant network

biggest concern: theft of user data

modification not *yet* an observed threat

how to adjust derived data?

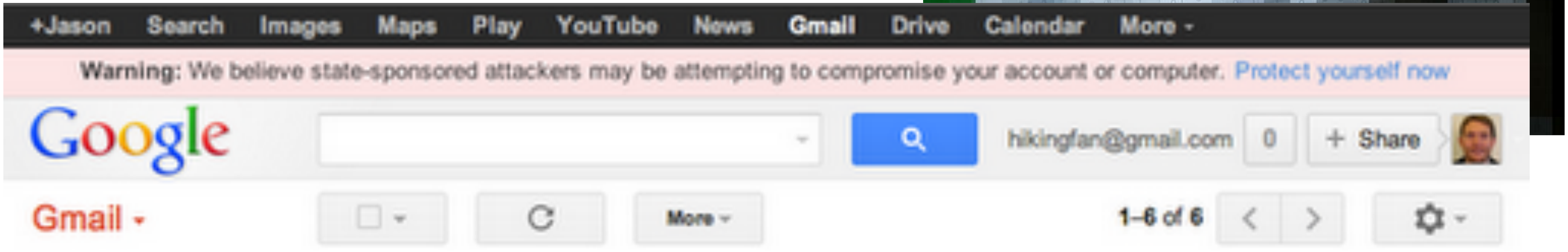
how to assist, not replace, self-help?

2.0TB
2.0TB
Seagate
LSI

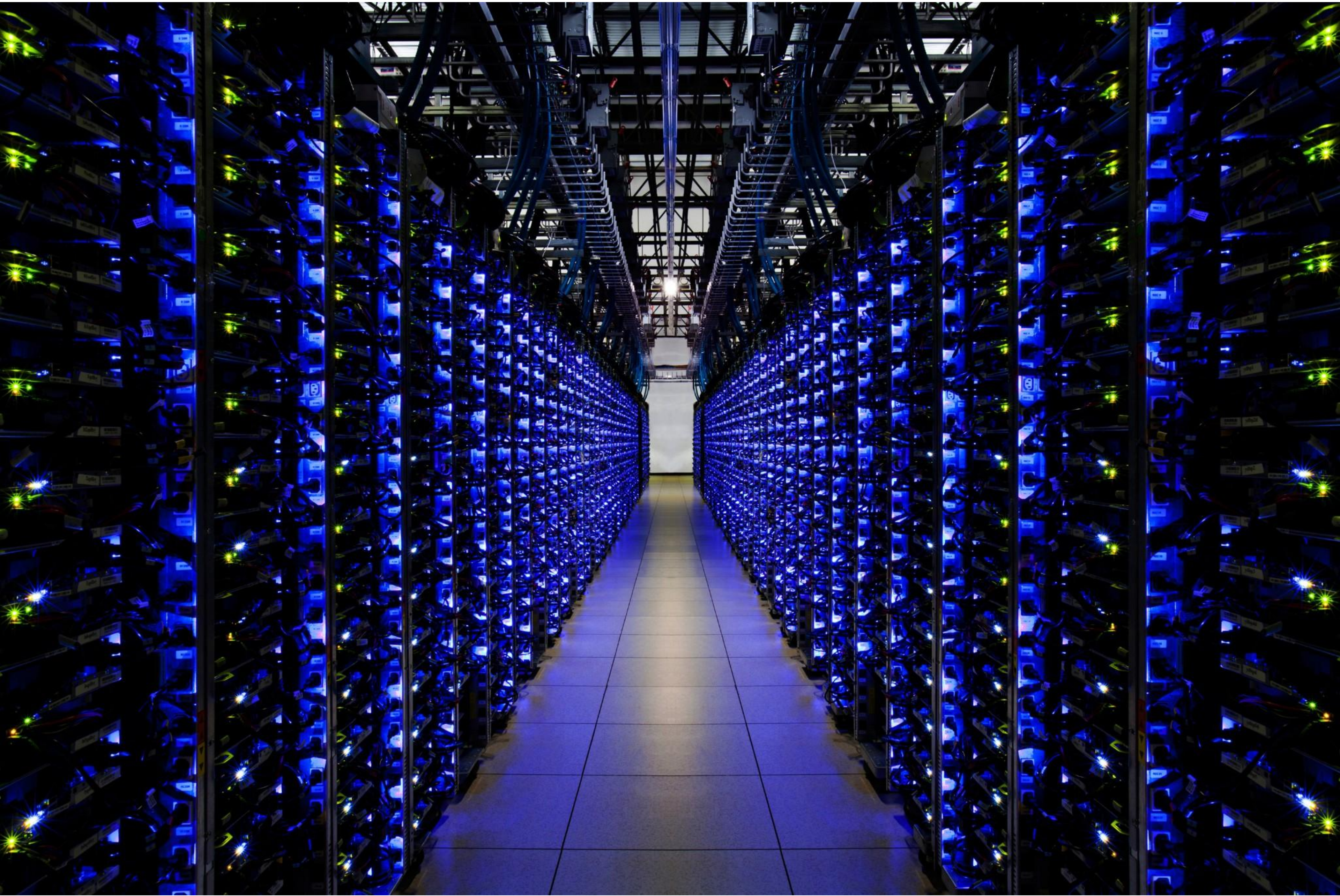
social engineering, malware

password reuse - Fallows
pw hash - LinkedIn, Bloggtoppen
account recovery - Palin, Honan

need: stronger mental models,
tested on real users



Warning: We believe state-sponsored attackers may be attempting to compromise your account or computer. Protect yourself now



www.google.com/about/datacenters/gallery