Navigating the Security Maze

Arshad Noor, CTO, StrongAuth, Inc.

Professional Strategies – S22

Course Objectives

- Brief History
- Root Causes
- Problem Scope
- Solution Architecture
  - Flowchart
- Summary

Brief History

First internet-scale “attack”

- November 2, 1988
- “Morris Worm”
- Estimated 6,000 computers infected
  - 10% of the internet
- No PII was compromised

Source: wikipedia.org

California's Senate Bill 1386

- July 1, 2003
- 2002 attack on Teale Data Center, CA
- PII compromised for 6 weeks for:
  - Every CA government employee
  - Every elected official
- 200K (State Controller's site)
- 1.7M (CalPERS)

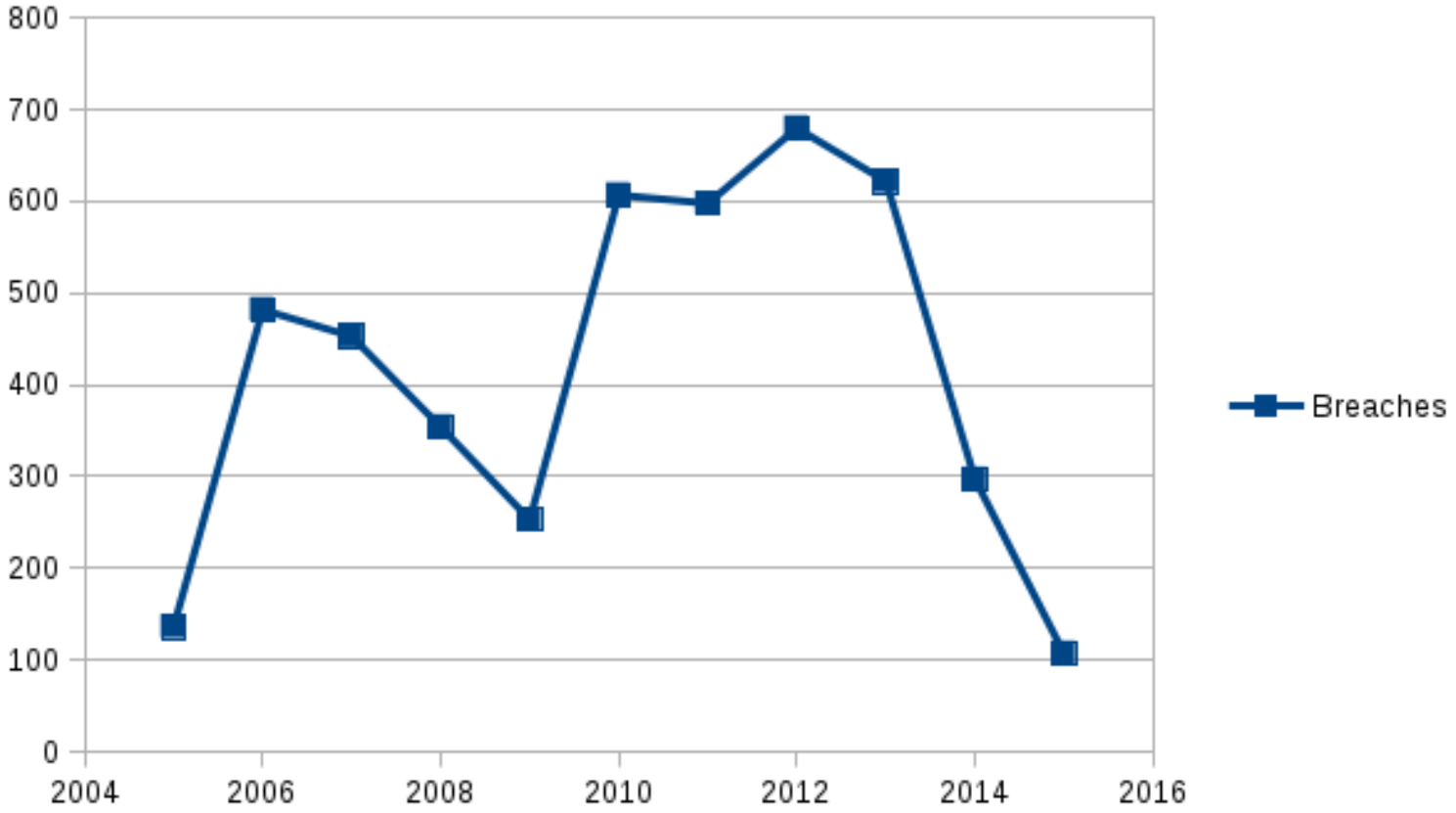
Source: Various

Today

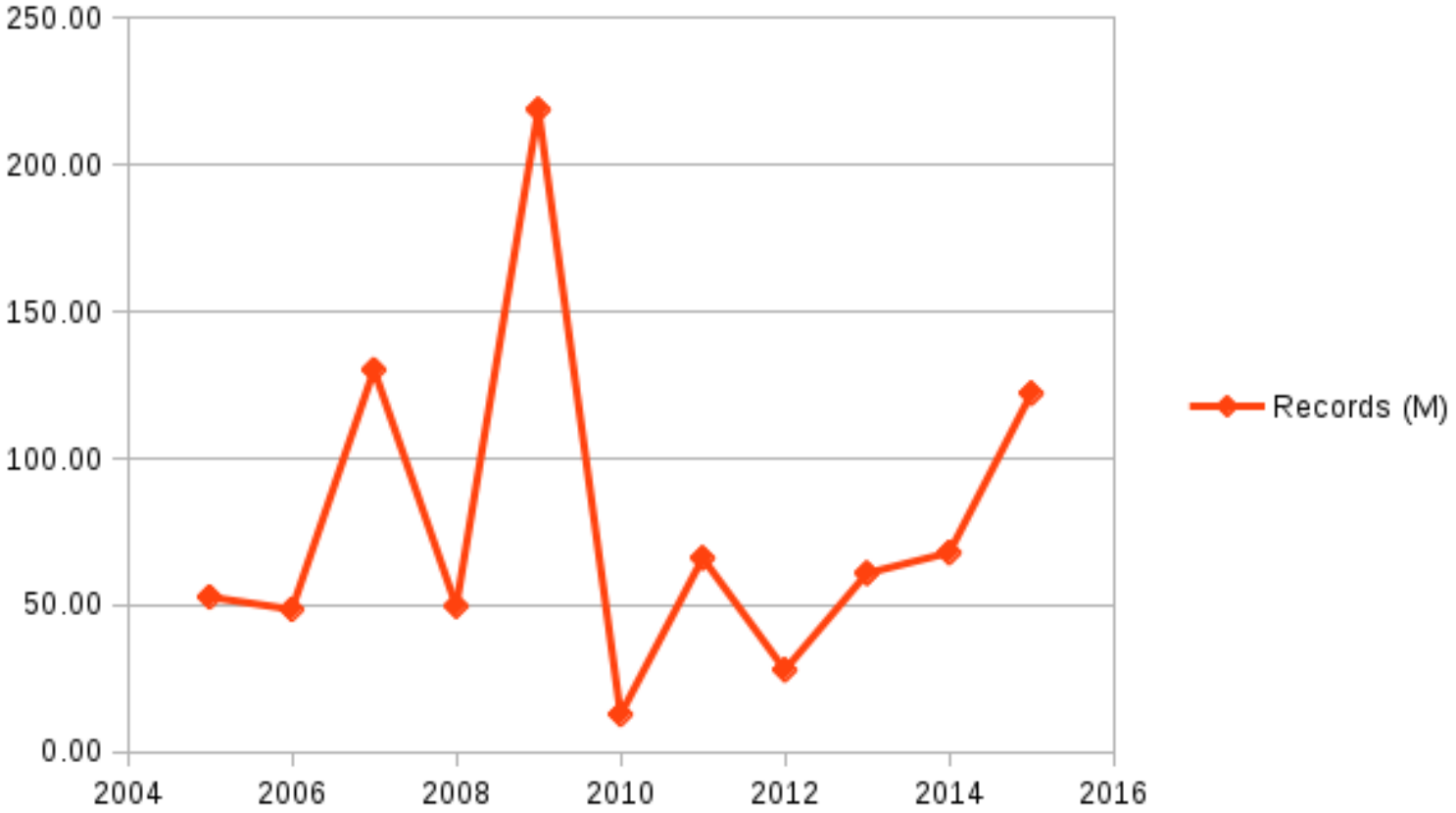
- September 2015
- 4,603 public breaches since 2005
- 868,403,517 records breached
  - Anthem's 80M record breach not even in *Top 10*
- Office of Personnel Management/Target

Source: privacyrights.org

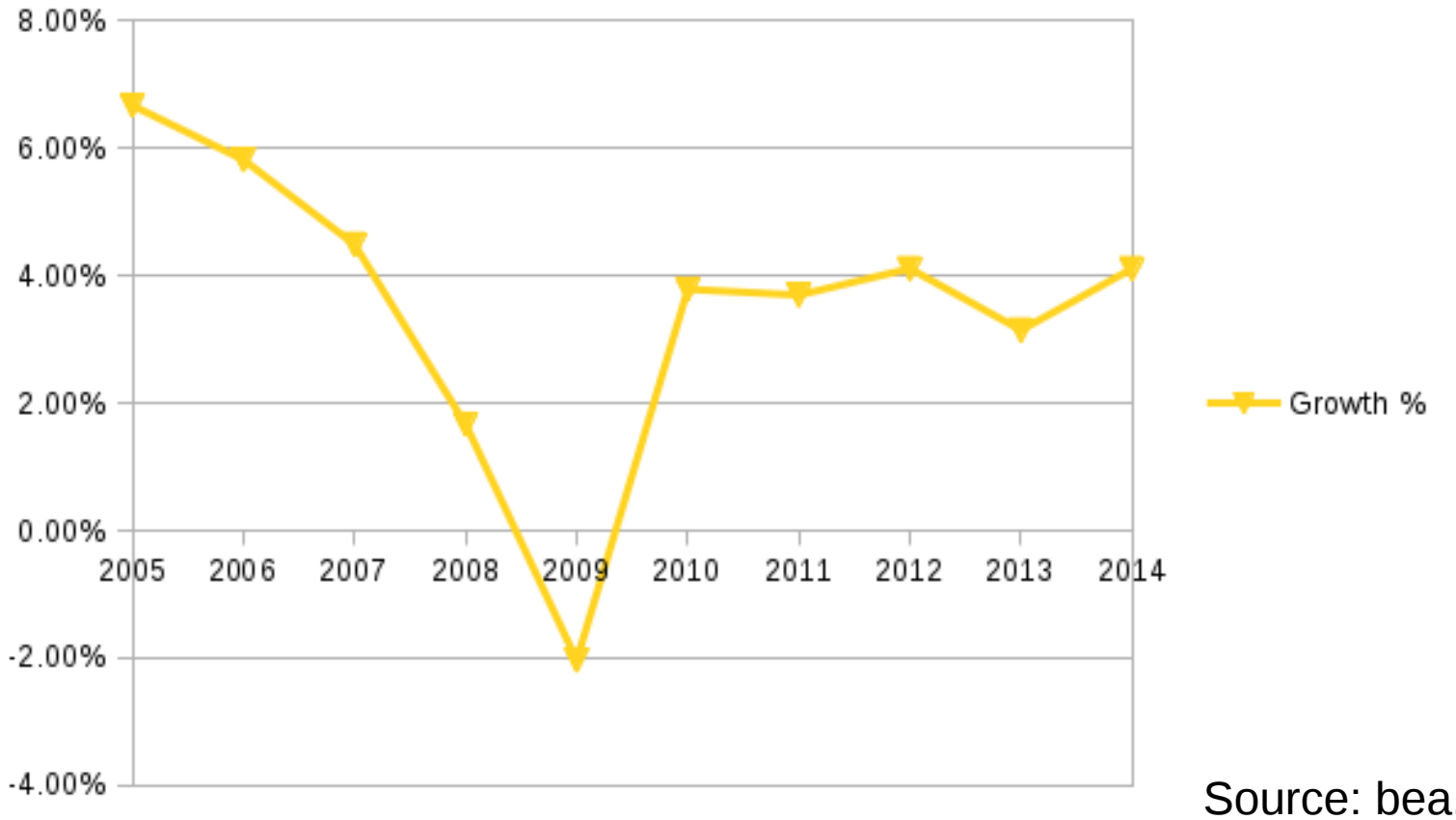
Breaches since 2005



Records breached since 2005



US GDP Growth %

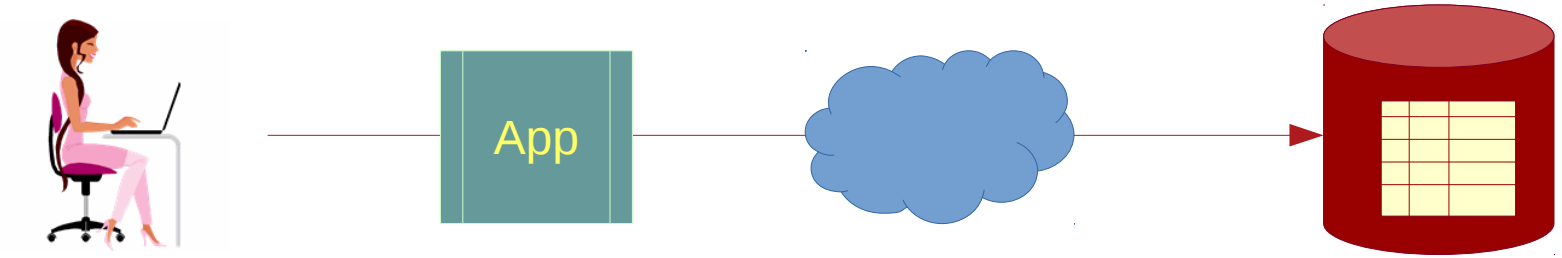


Source: bea.gov

Root Causes

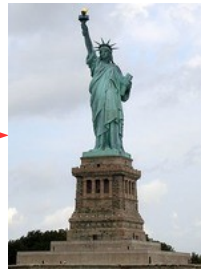

ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

Big Picture



User Application Network Data

An analogy - NHTSA



User + Application

Network

Destination

NHTSA Stats

	1996	2013	%
Registered Vehicles (Millions)	192	269	40.10%
Resident Population (Millions)	260	316	21.54%
Vehicle Miles Traveled (BILLIONS)	2358	2988	26.72%
Deaths	40716	32719	-19.64%
	2009	2015	
Budget (Millions)	820	830	1.22%
Deaths	33883	32719	-3.44%

NHTSA Focus

- Federal Motor Vehicle Safety Standards
  - Brakes, tires, lighting, …
  - Safety belts, airbags, energy-absorbing steering columns, crumple-zones, child safety seats, motorcycle helmets, …
- Vehicle recalls
- Driver Licensing and Education
- Speed enforcement

IT Security Focus

- Application Standards
  - OWASP Top 10, …
- Password policies, Patching, OTP, SSL/TLS, …
- Application and Network Audits
- Programmer and User Education
- Malware detection, IDS, IPS, Pen-Testing, Security incident event-reporting, …

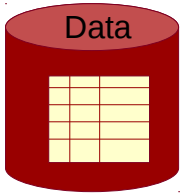
But something is still missing…

- While publicly-announced breaches are going down,
- Breached data continues to rise

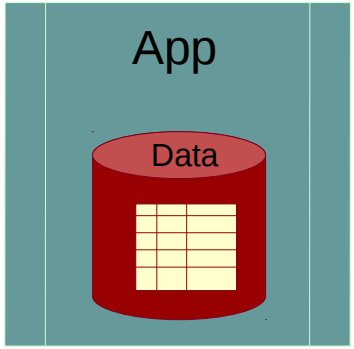
- So, where's the disconnect?

Problem Scope

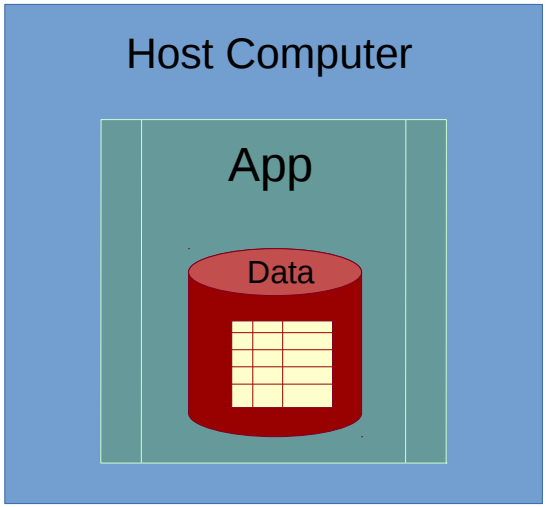
At the core…



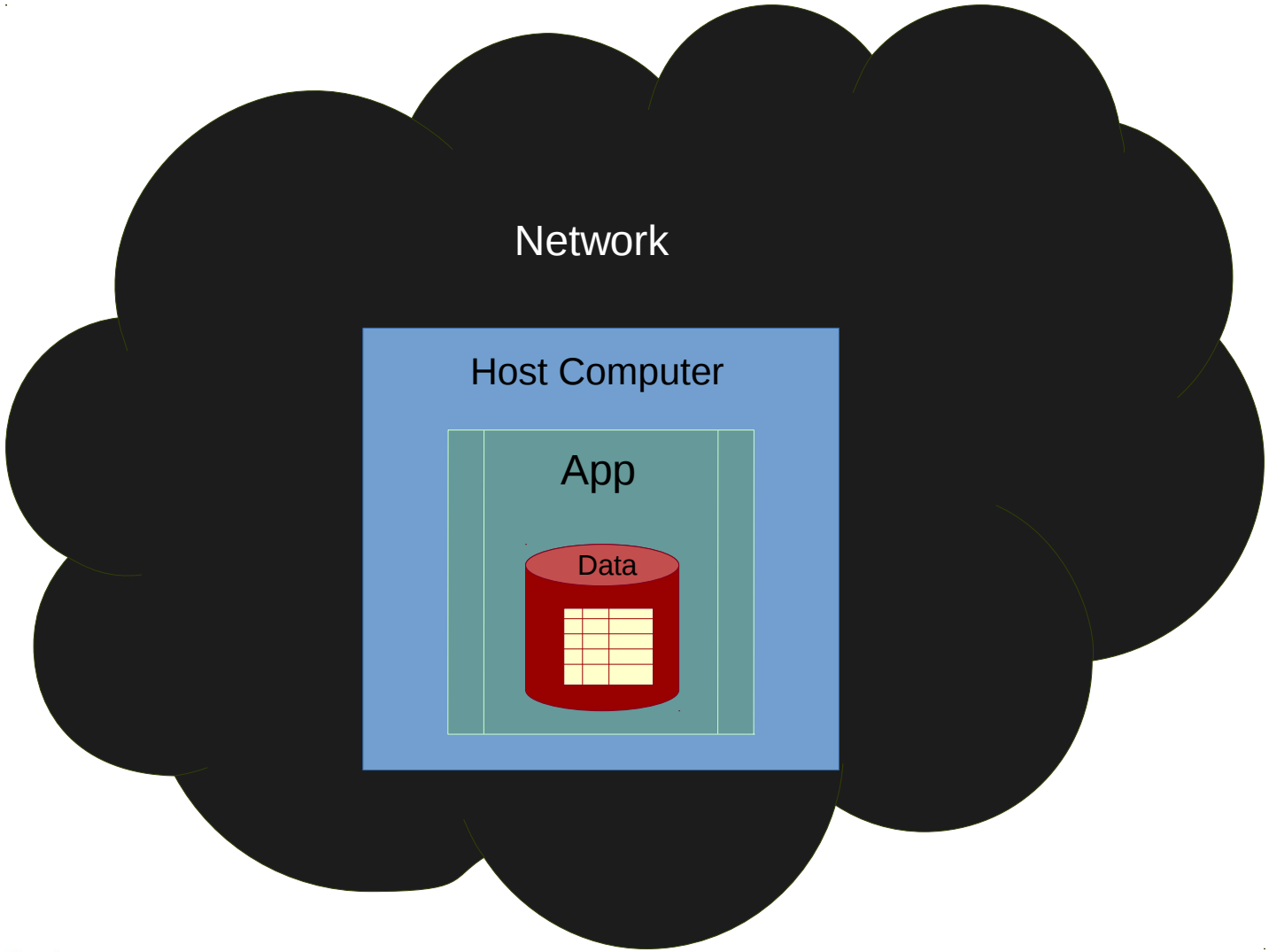
Used by…



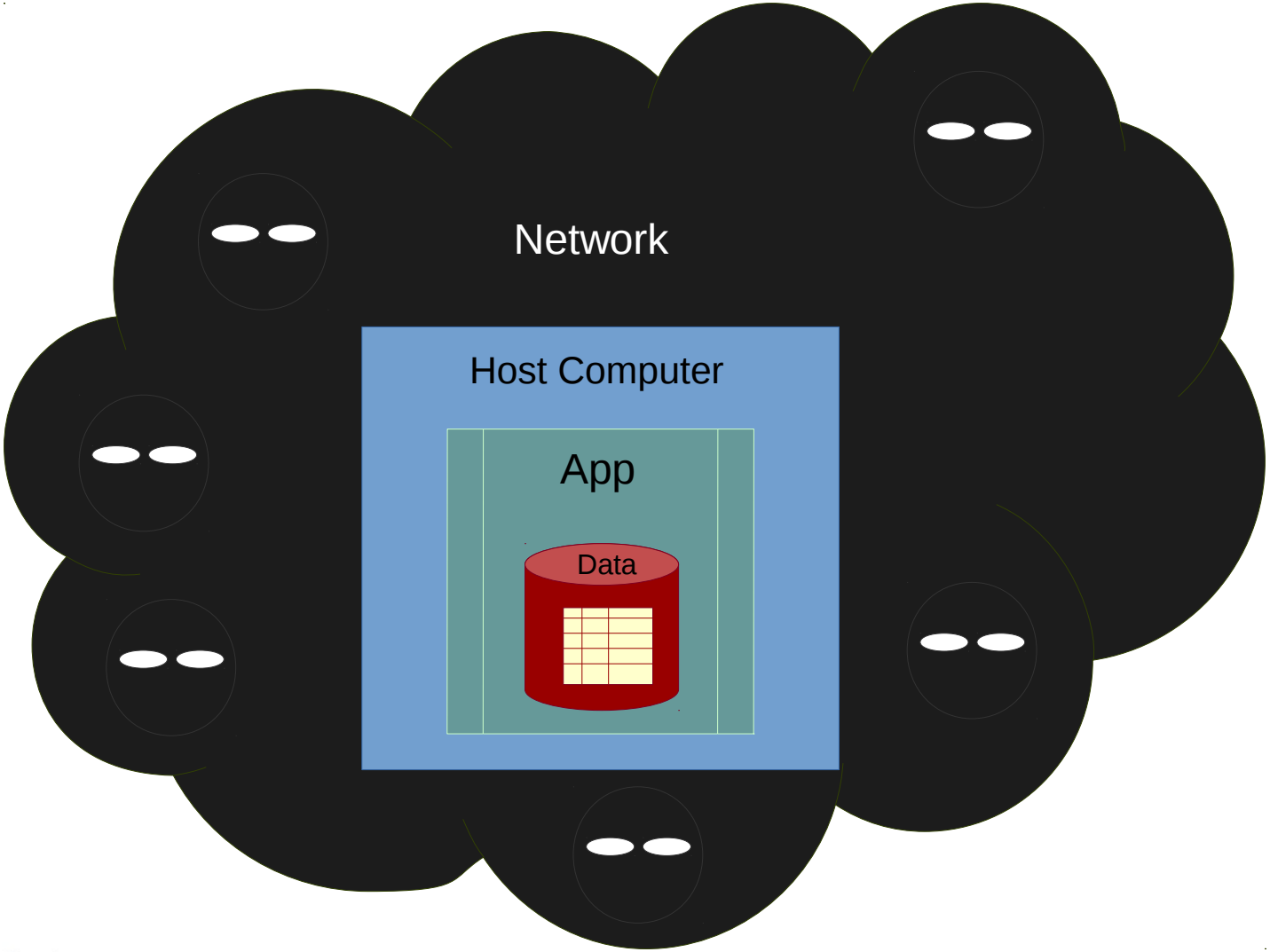
Within a…



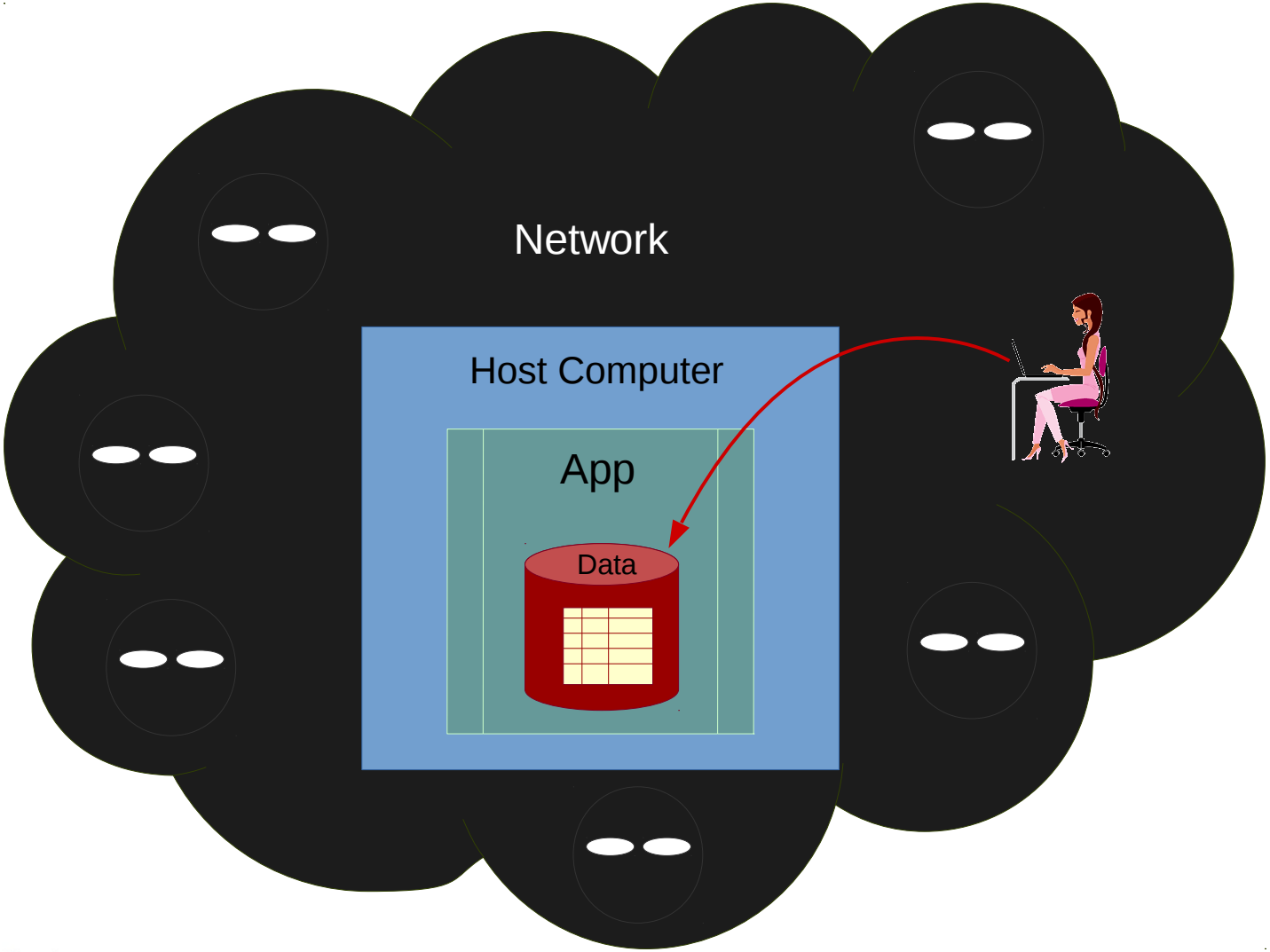
On your…



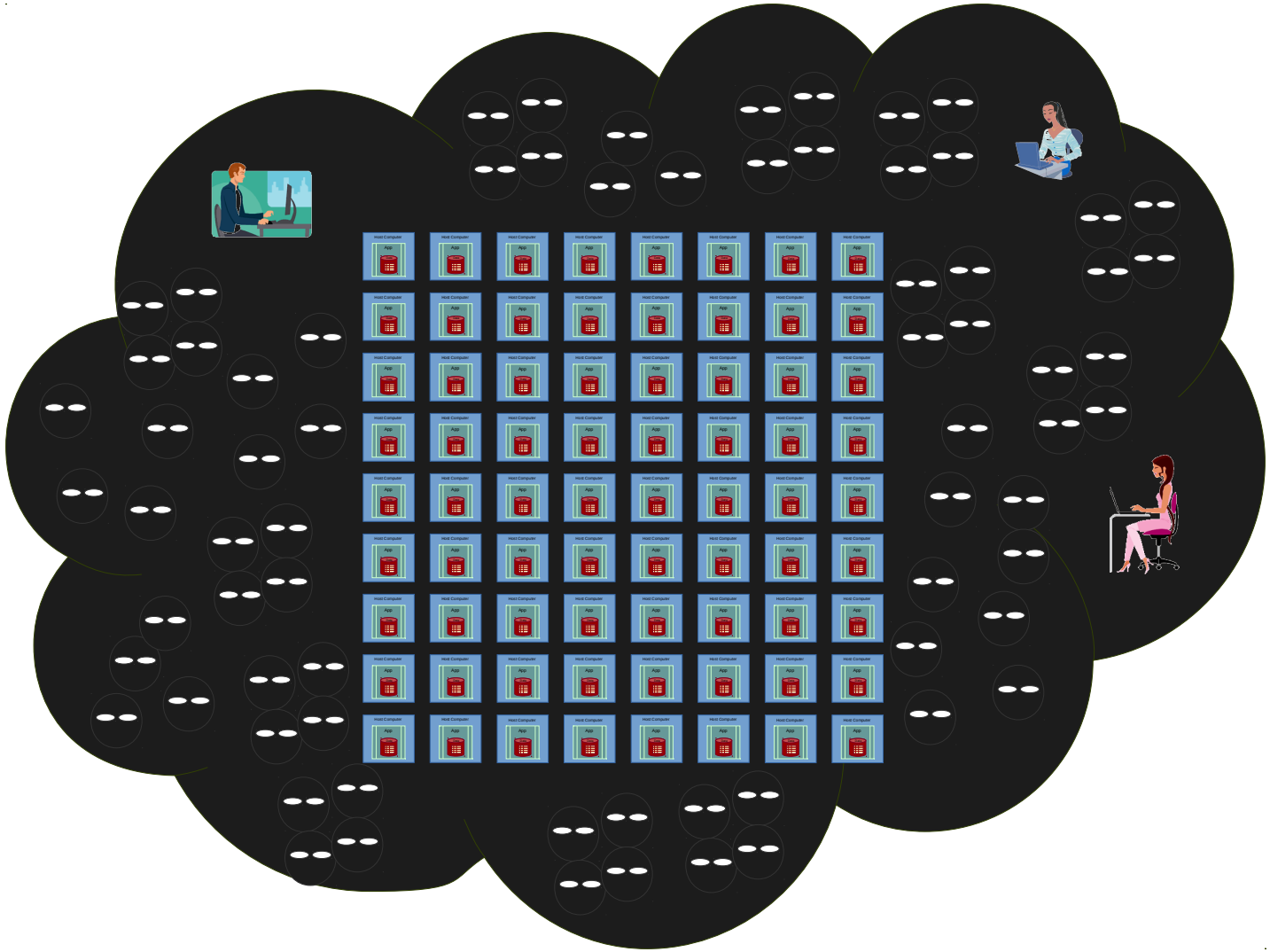
What you cannot predict…



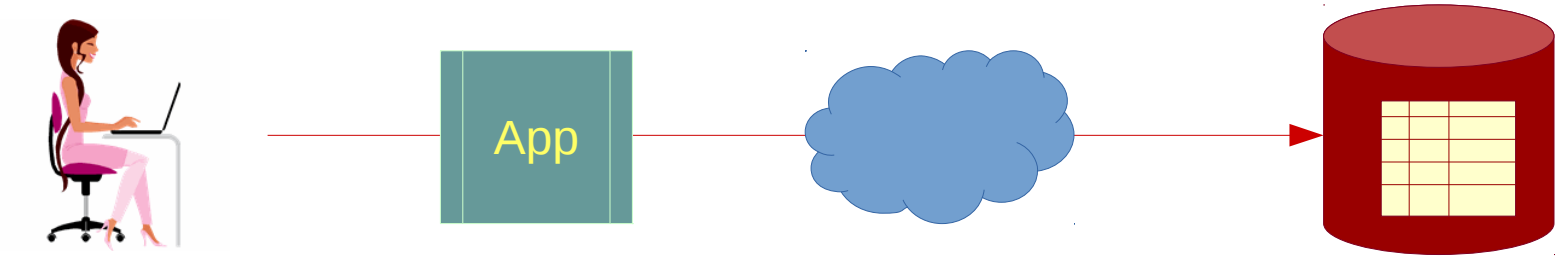
What you need to enable…



On this scale…



So, what do you do?



User Application Network Data

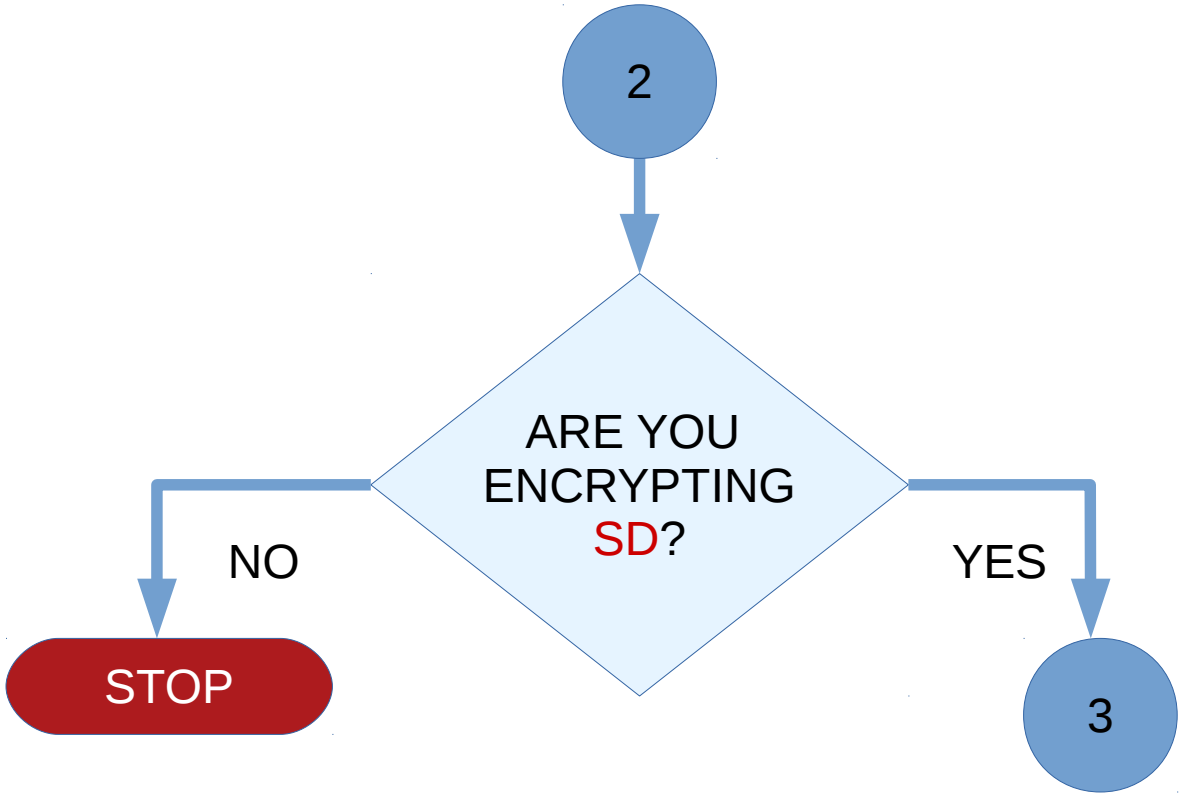
Solution Architecture

“Its the data, stupid!”

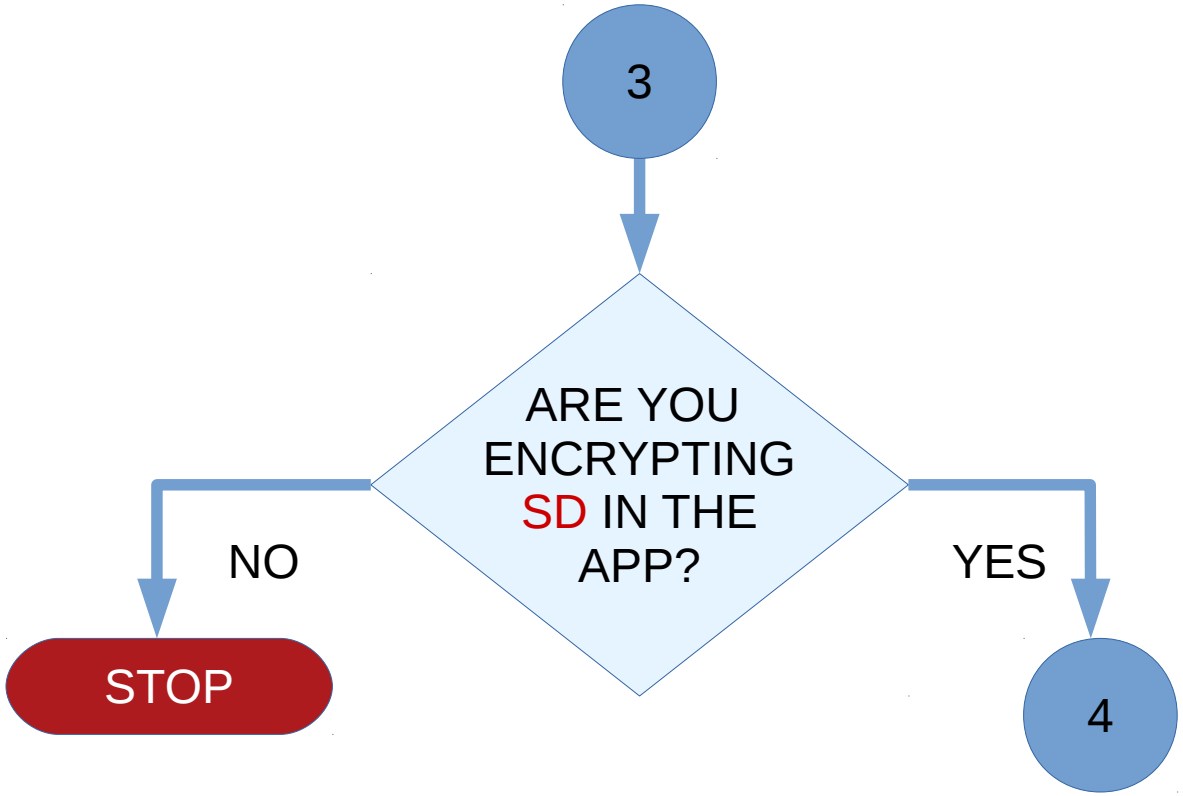
- What are the attackers after?
- What are we protecting?
- What percentage of the IT Security budget goes to:
  - Protecting data?
  - Protecting the host?
  - Protecting the network?
  - Ensuring the right user sees the data?

Data Security Flowchart - 1

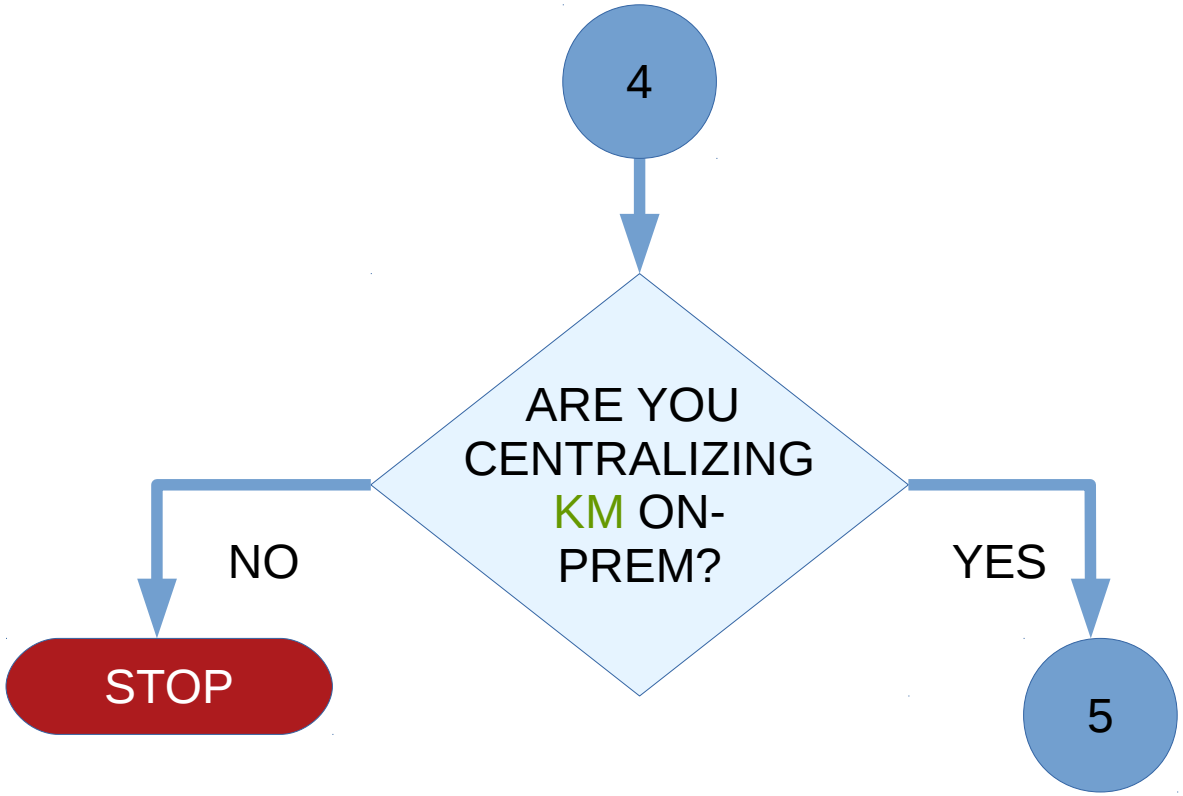
Data Security Flowchart - 2



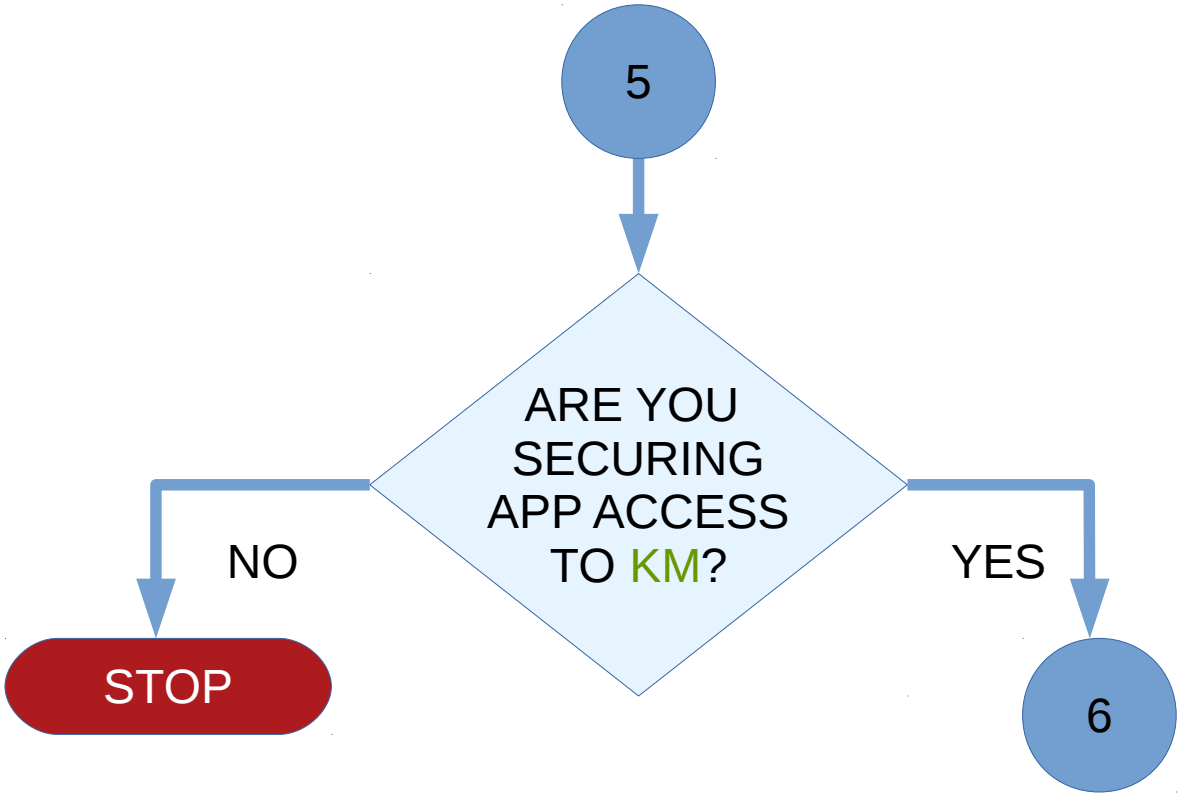
Data Security Flowchart - 3



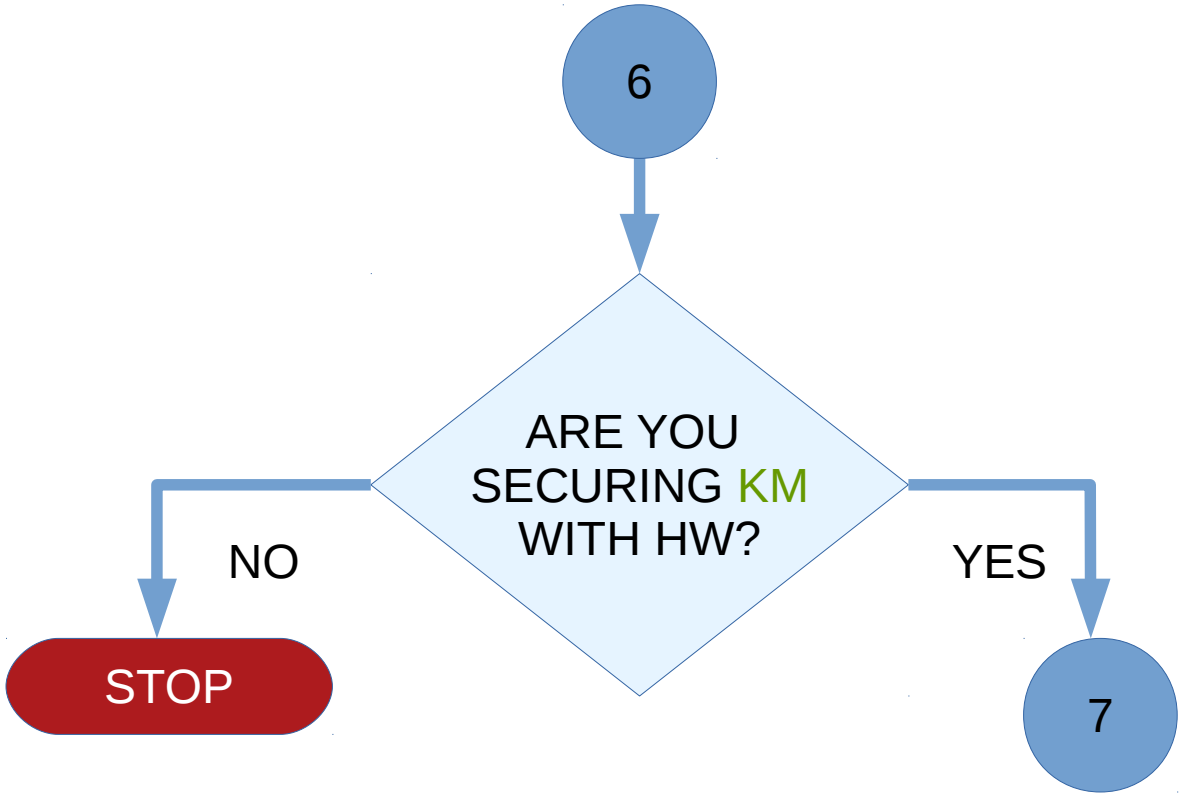
Data Security Flowchart - 4



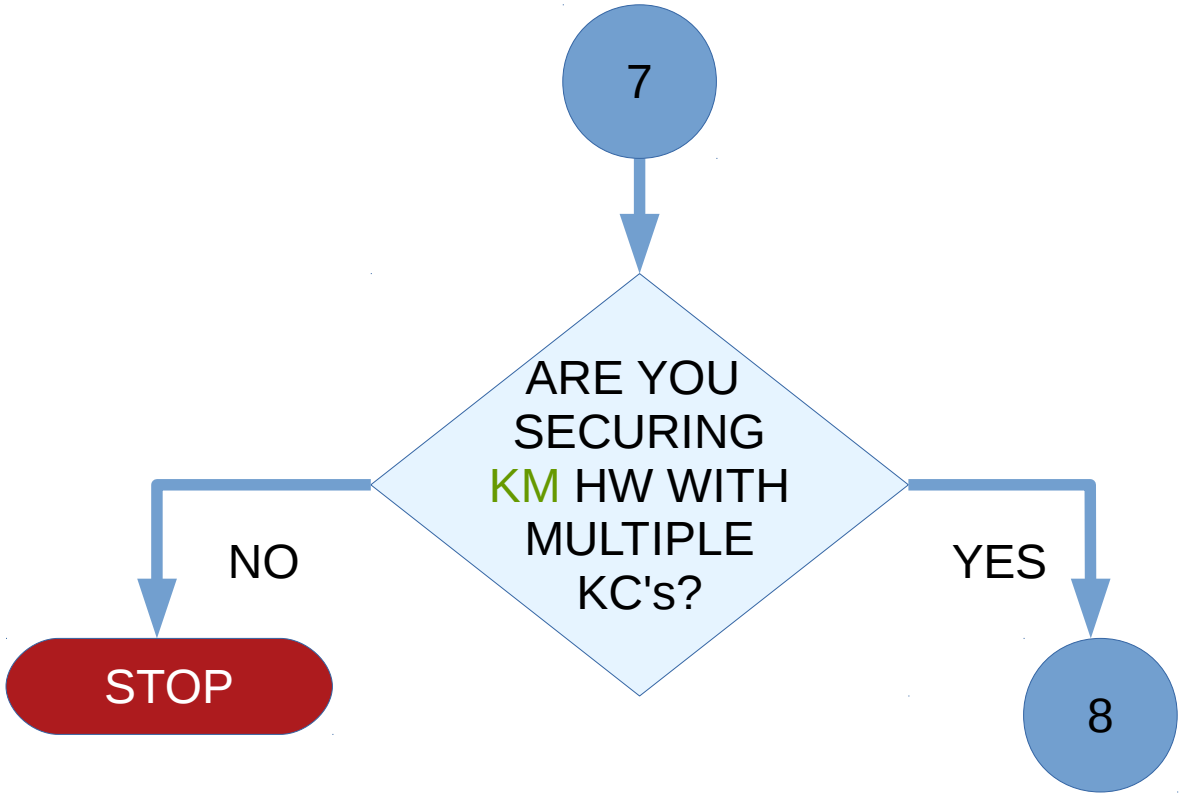
Data Security Flowchart - 5



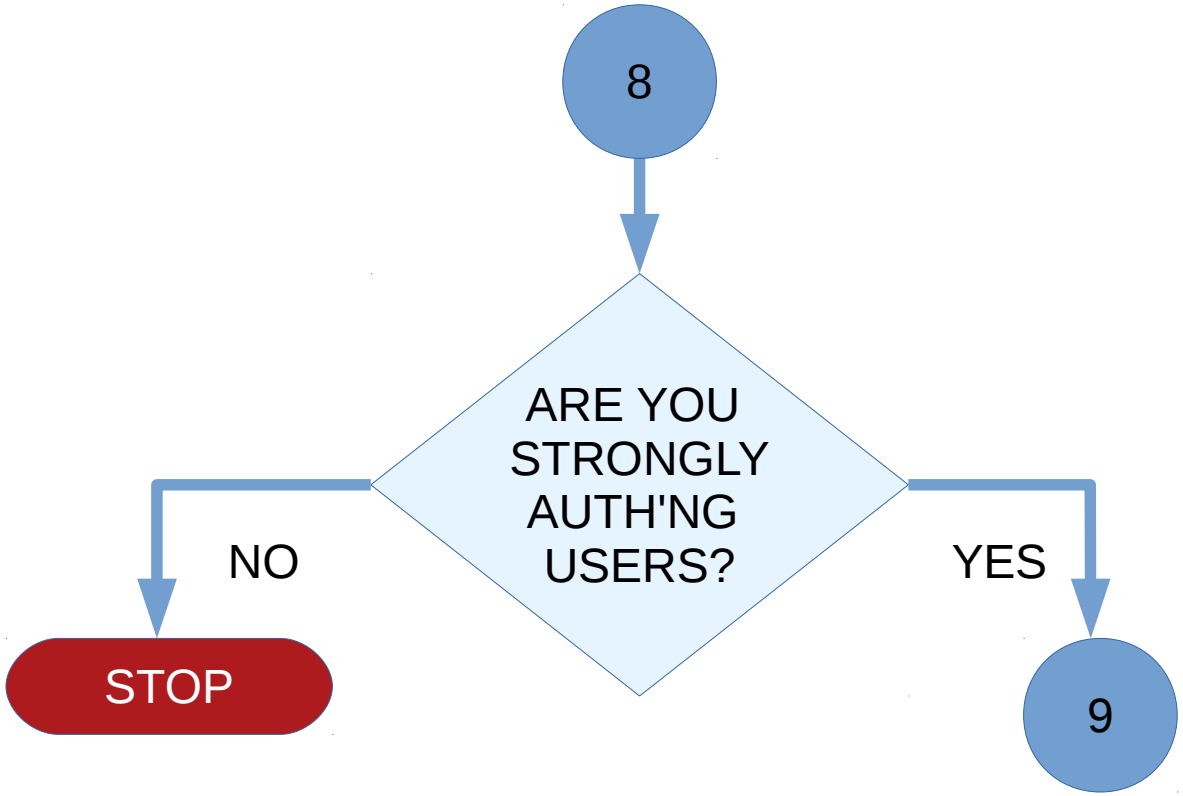
Data Security Flowchart - 6



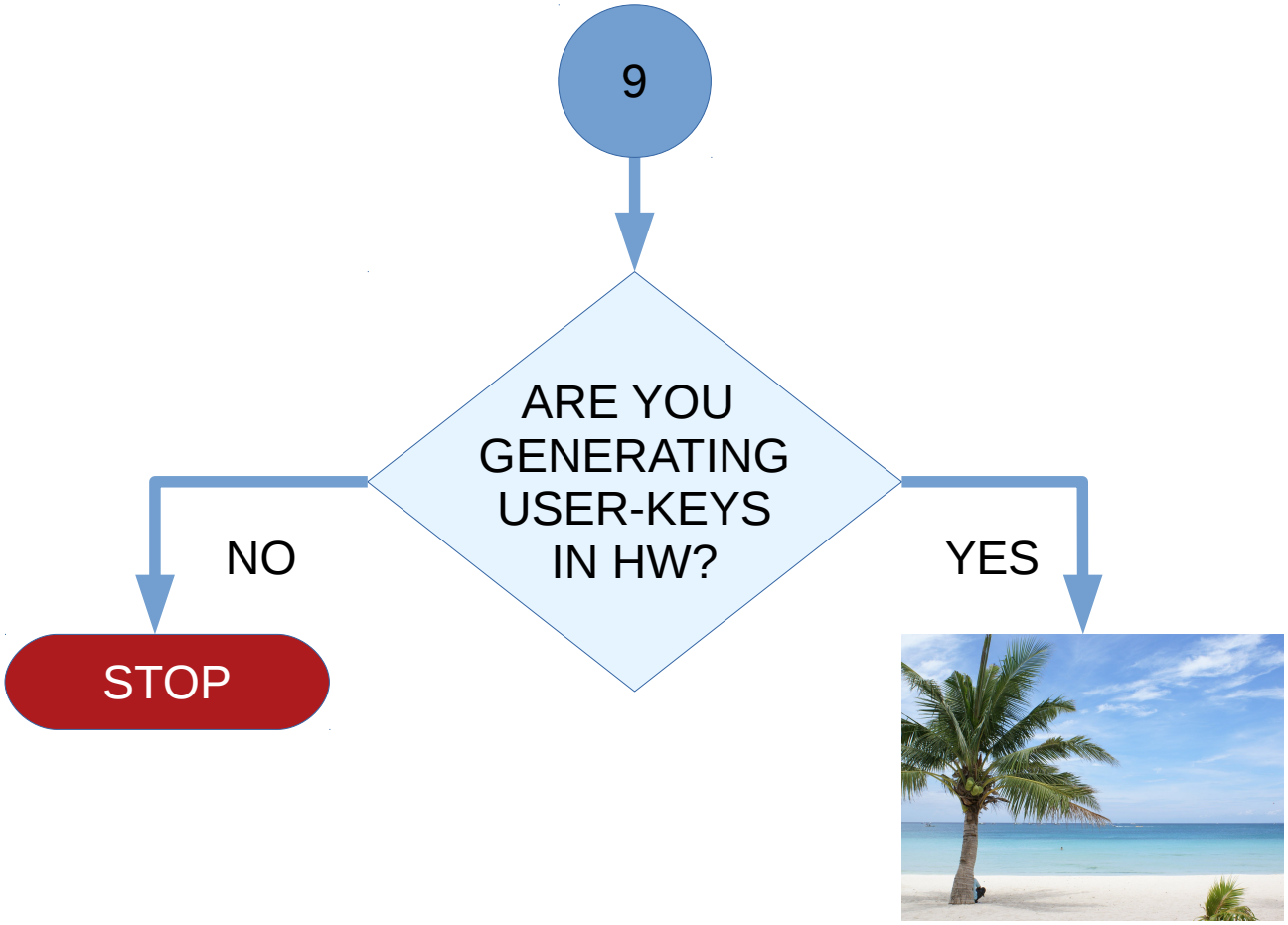
Data Security Flowchart - 7



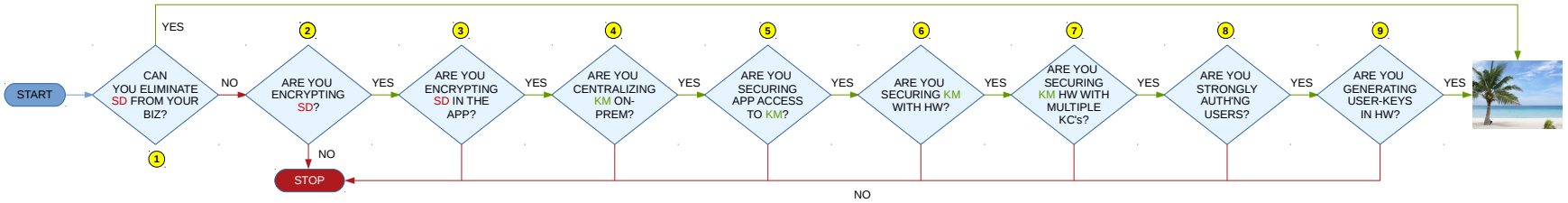
Data Security Flowchart - 8



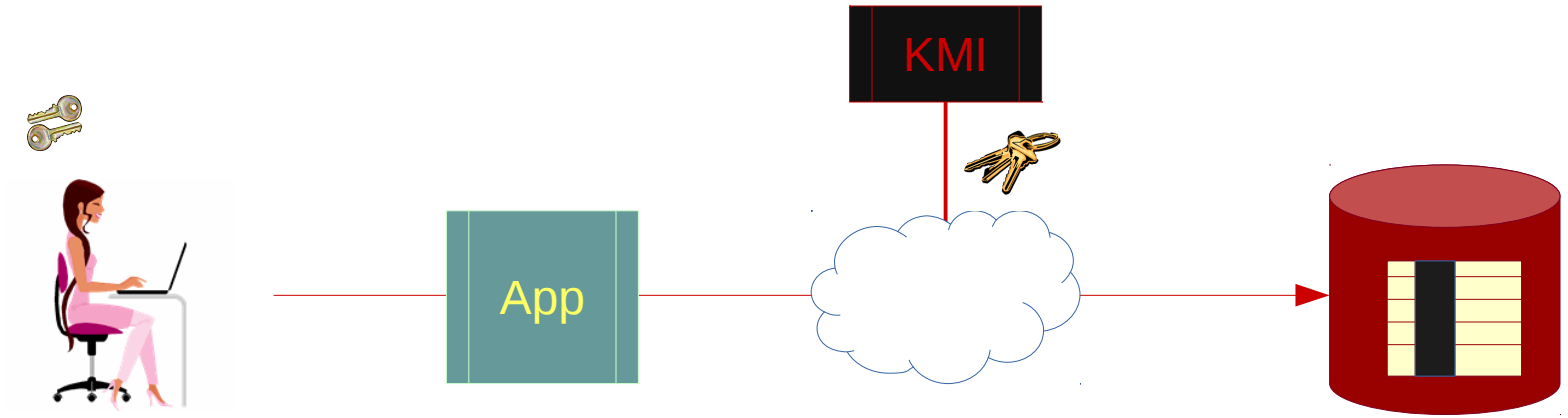
Data Security Flowchart - 9



Data Security Flowchart - 10



Back to fundamentals



User Application Network Data

Summary

- If you're NOT encrypting sensitive data…. you're toast!
- If you're NOT encrypting sensitive data in the authorized application…. you're toast!
- If you're NOT centralizing encryption keys, on-premises…. you're toast!
- If you're NOT securing application service credentials to key-management…. you're toast!

Summary

- If you're NOT using a cryptographic hardware module for your key-management…. you're toast!
- If you're NOT using multiple Key Custodians to secure cryptographic hardware…. you're toast!
- If you're NOT using asymmetric-key based strong-authentication for users…. you're toast!
- If you're NOT generating/storing asymmetric keys in hardware devices…. you're toast!

Summary

- Enable strong-authentication now!
  - $5 FIDO tokens available on eBay now
  - Free and open-source FIDO servers available now
- Enterprise-scale, open-source encryption tools available now
- Free and open-source secure cloud-computing architecture available now
- So, what are you waiting for?

Thank You!

"If you're focused on protecting the network, you've already taken your eye off the ball!"

Arshad Noor
StrongAuth, Inc.
arshad.noor@strongauth.com
(408) 331-2000
www.strongauth.com