Eliciting Application Security Requirements – Its a Complex Undertaking!

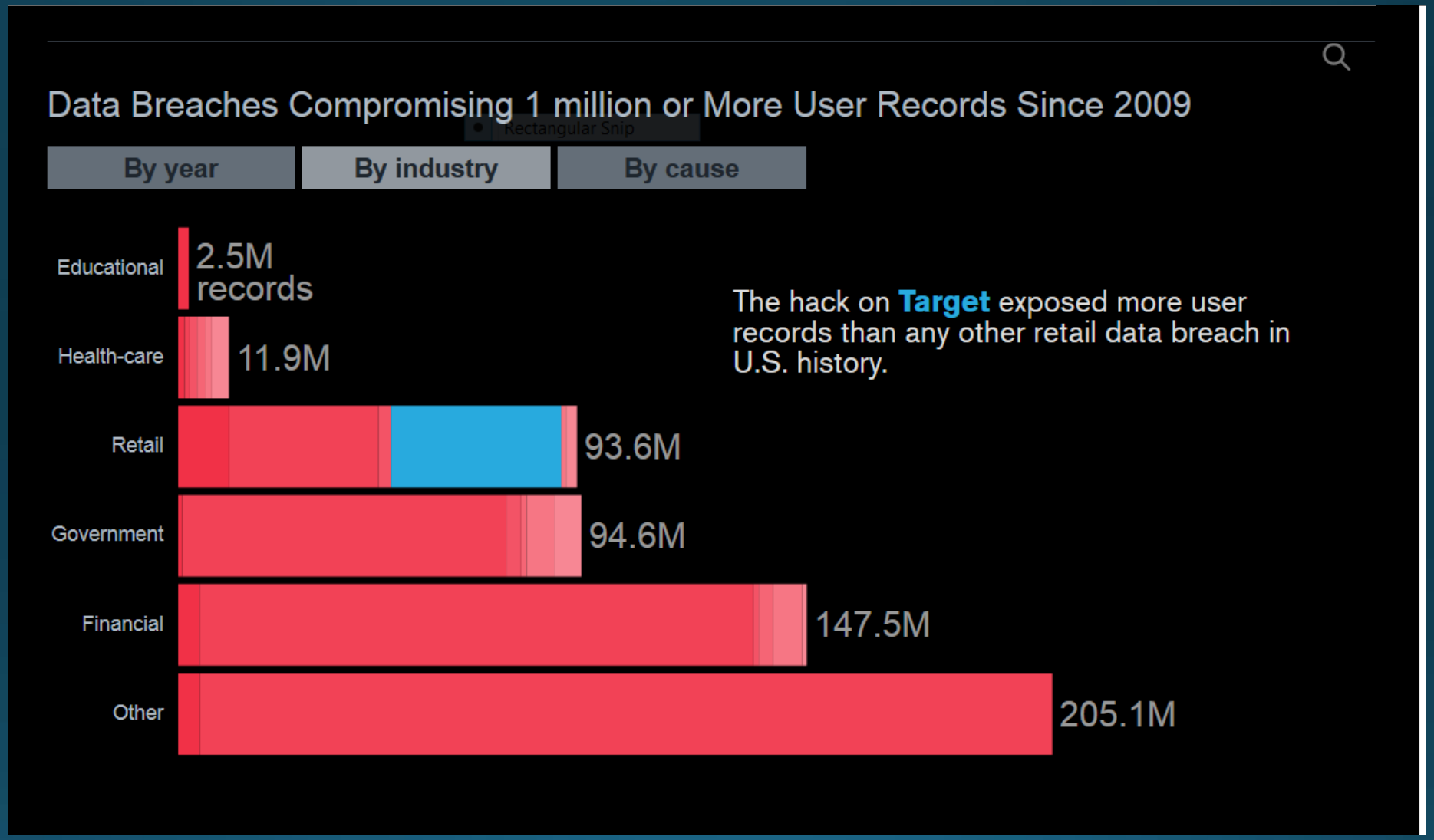
Bhushan Gupta

Gupta Consulting, LLC.
www.bgupta.com

Worst Data Breaches of 21st Century (as of 2016)

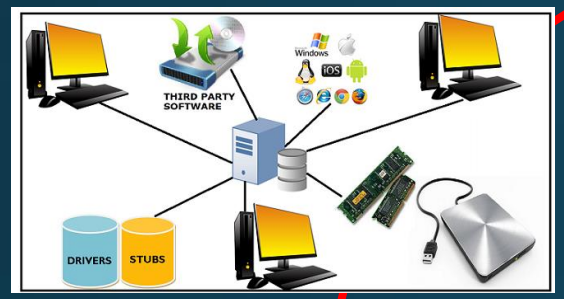
Institution	Impact	Cost	Vulnerability
Hartland Payment systems	134 M Credit Cards Exposed		SQL Injection
TJX Companies Inc.	94 M Credit Cards Exposed		Encryption/Network Break In
Epsilon	Ms Names and Emails	$4B	Undetermined
RSA Security	40 M Employee Records		Spear Phishing
Stuxnet	Intended for Iran's Nuclear Power Program		
Dept. Of Veterans Affairs	26.5 M Records Stolen	$100-500 M	Stolen Laptop and External Hard Drive with the DB
Sony's PlayStation Network	77 M Playstation Network Accounts, 12 M Unencrypted credit card numbers		
ESTsoft	35 M Records (South Koreas)		Malware
Gawker Media	1.3 M Email Address/Passwords, Code		Weak Passwords
Google/Other Silicon Valley Companies			Weakness of Old Version of IE, China Govt.
VeriSign			
Card Systems Solutions	40 M Credit Card Accounts		SQL Trojan - Personal info not encrypted
AOL	20 M Web Inquiries from 650K Users posted publicly on a web site		Released a text file publicly by mistake
Monster.com	1.3 M Job Seekers Confidential information		malicious software program - Ukraine
Fedelity National Info Services	3.2 M Customer Records + credit card, banking, and personal information		Employee sold the data
Target Stores	110 M Credit Card/Contact Information	$162M	
Anthem	78.8 M Personal Information	$100 M ??	
Home Depot	56M Customers Information	$33 M	POS System Malware
Sony Pictures	Employee Information, Data Loss, Unreleased Movies		Malware, Weak Password

Data Breaches By Industry



Source: Privacy Rights Clearinghouse (http://www.bloomberg.com/infographics/2014-05-14/target-data-breach.html)
GRAPHIC: KEITH COLLINS / BLOOMBERG VISUAL DATA

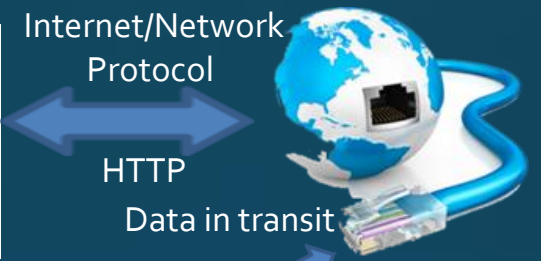
What makes it complex?



Internet/Network Protocol

HTTP

Data in transit

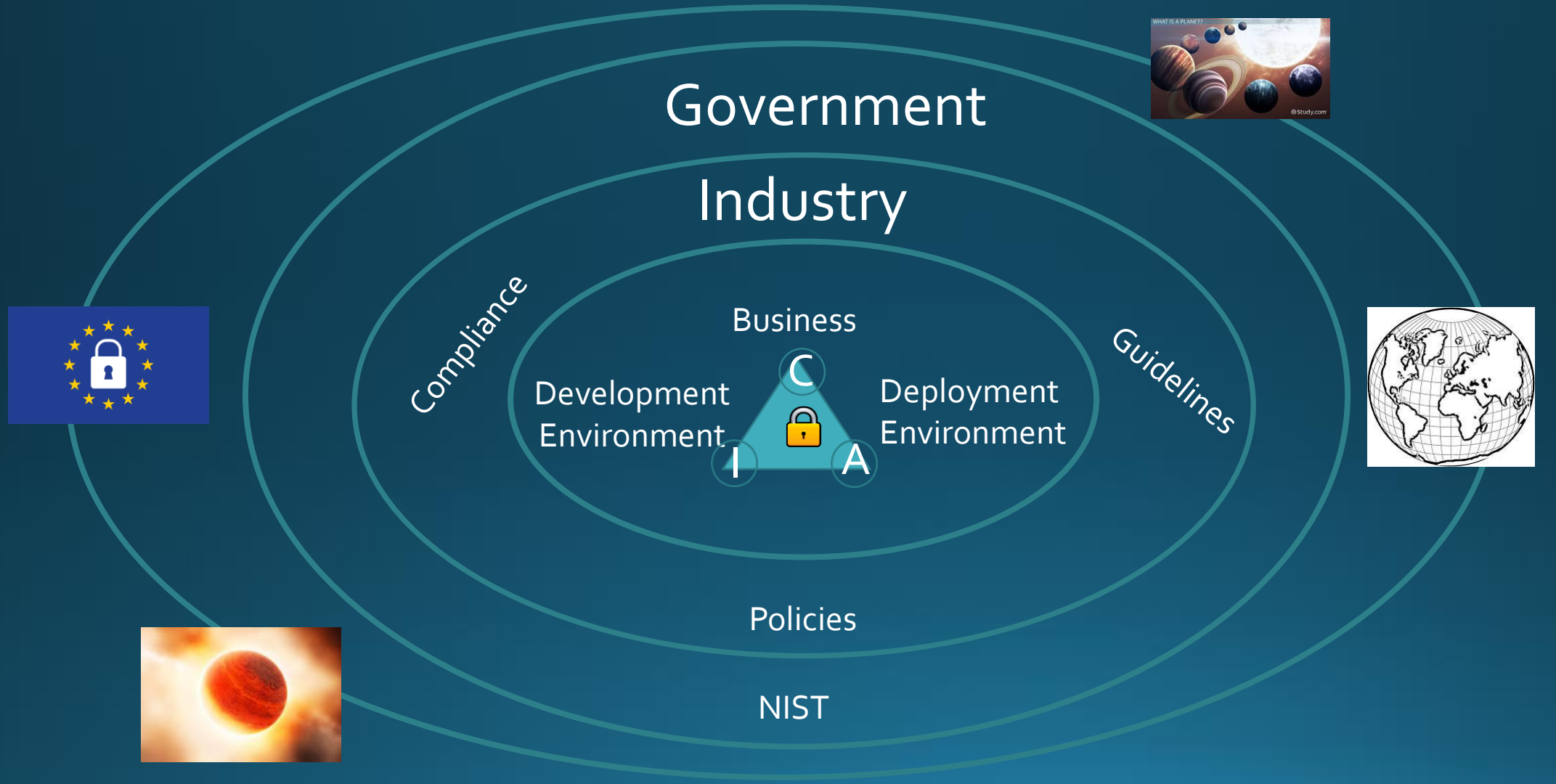


Client browser using client side resources

WEB Server

Backend System (Database Server Applications)

How does complexity manifest itself?



Data Security Requirements

- Confidentiality – Maintaining data privacy (Access Control)
  - Intended malicious access – External or Internal
  - Unintended – someone made a mistake
- Integrity – Authorized Modification of data and system environment
- Availability – Usable during desired hours of service

Not all data is worth protecting!
Protect data while stationary and in motion!

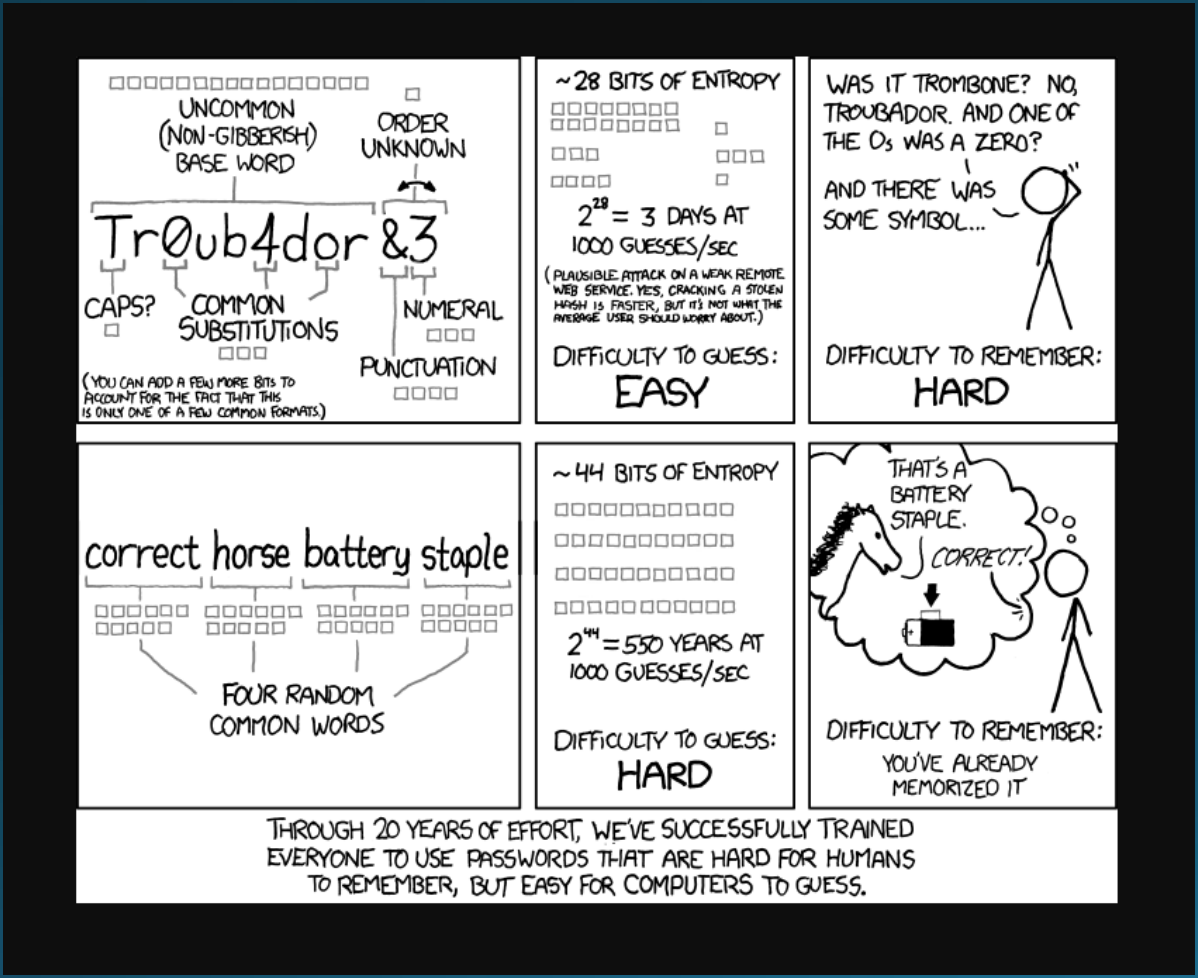
Requirements – Confidentiality: Access Control

- Identification – Tell me Who you are?
  - A simple string of characters non-programmatically generated (my dog's name)
- Authentication – prove to me you are who you say you are
  - Something specific you know (my dog's birthday)
  - Something specific you have (my driver's license, token)
  - A physical characteristic – biometric (my finger or Iris scan)

Requirements – Confidentiality: Access Control

- Authorization
  - Resources you are allowed to access (can not drive over the speed limit like a police officer can)
- Audit - Trail of activities by an entity for future reference

Password over the 20 last 20 years!



https://www.explainxkcd.com/wiki/images/6/6a/password_strength.png

Requirements - Confidentiality

Identification

- Each user have a unique ID that is extremely difficult to guess
- ID should follow a standard convention if needed
- A user ID is not shared with the other users
- ID value is not reflective of position or role
- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) if needed

Requirements - Confidentiality

Authentication (NIST IA Family)

- Character string
  - Complexity/crackability–
    - Difficult to guess (minimal length, required character categories, prohibitive elements – last name, date of birth)
    - Should not require extra efforts to remember to avoid noting it down
- Biometric - Legally allowed human characteristics
  - Iris
  - Retina
  - Finger Prints
  - Palm Scan
  - Hand Configuration

Confidentiality Requirement -

Authentication – you blew it!

- Failure/Recovery Process
  - Number of attempts before Time Out or Locking Out
  - I don't recognize your device - use of security questions for first login attempt from a new device
  - You forgot your password - recovery mechanism – further validation
  - No email distribution of the password

Requirements - Confidentiality

Authentication – some extra leg work!

- Semi logoff or session ending after a period of no activity
- Longevity – password rotation
- Transmission over network
  - Transport Layer Security (encrypted vs. plain text)
- Social Engineering – Shoulder Surfing
  - Option to hiding password as being typed
- Storage – Plain text vs. Cryptographic Hash (a function + Salt)

Requirements - Confidentiality

Authorization

- Policy to control access to objects – database servers
- Processes are also treated as subjects

Data Integrity Requirements

Integrity – Accuracy and validity

Can be threatened by modification of data by unauthorized subjects or by error.

Requirements:

- Integrity maintained while data is at rest or in transit
- Role based access control
- Validation of data both at application and database level
- Any malicious attempts logged with adequate tracking
- Recovery mechanisms are in place in the event the data integrity has been compromised
- Separation of duties to prevent fraud and errors – any function that is subject to abuse

Availability

Availability – Usable during desired hours of service

Requirements:

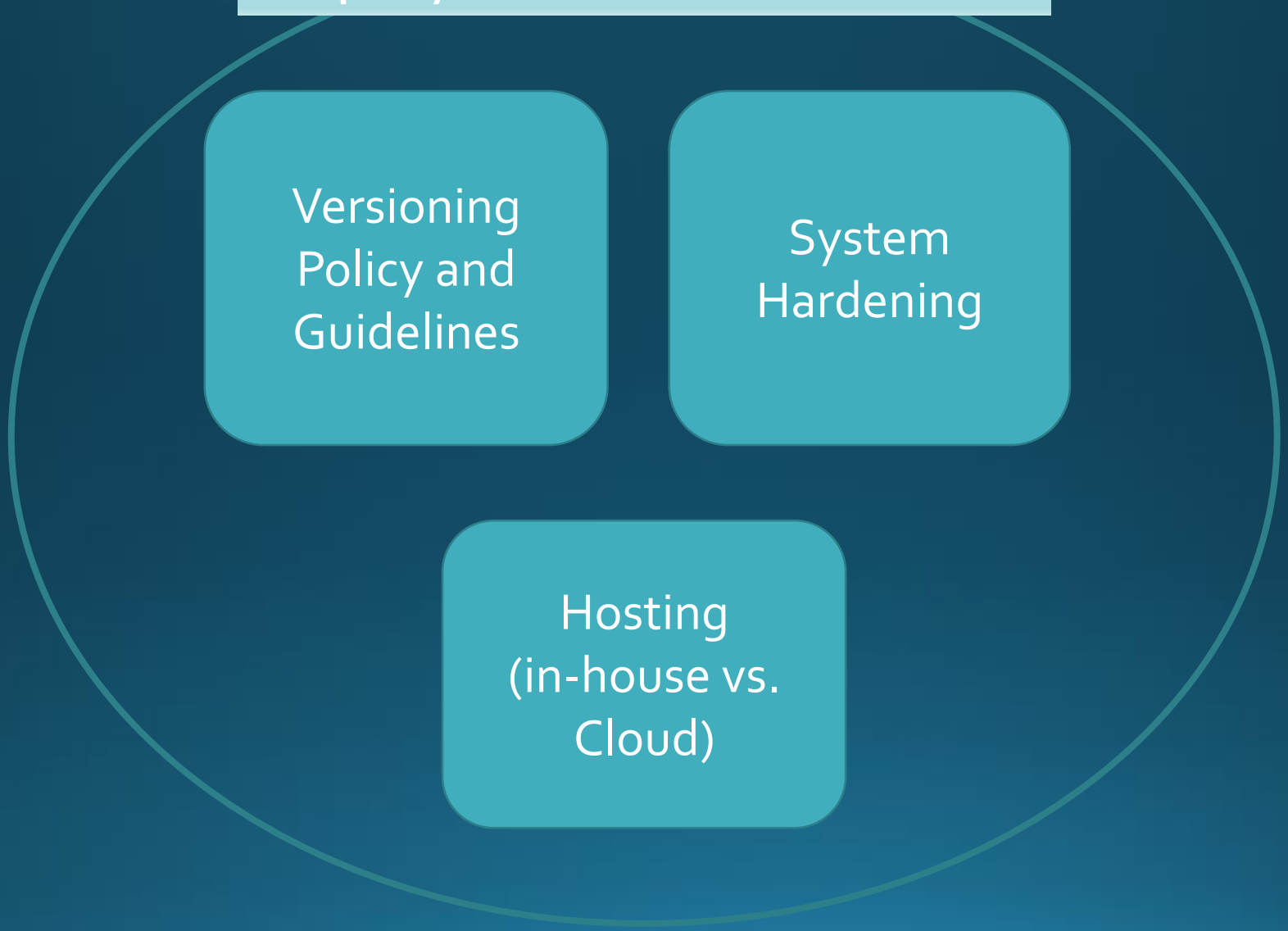
- Available as needed (24x7x365 or as per other criteria)
- Redundancy to reinforce availability

Vulnerability – DDoS attack (Distributed Denial of Service)

How does complexity manifest itself?

Development Environment

Deployment Environment



Security Challenges in Cloud Environment

- Isolation - Weak Access Management
  - Provisioning and de-provisioning of a large number of users
- Insecure APIs to serve clients
- Account Hijacking
- Malicious Insiders
- DOS
- Forensics and Incidence Management

Source: Cloud Security Alliance (cloudsecurityalliance.org)

How does complexity manifest itself?

Industry

Mobile Device Challenges

- Range of Manufactures – hardware, operating system, APIs, configuration
- Broad spectrum of apps on same platform
- Patches and updates – authorized and unauthorized
- Password policy violation
- Theft risk

How does complexity manifest itself?

Government

Industry

Compliance

Business

Development Environment

C

I

A

Deployment Environment

Guidelines

Policies

Standards - NIST

Government

Laws/Regulations:

1974 - Privacy Act – PII
HIPAA – Health Insurance Portability and Accountability Act
COPPA – Children's Online Privacy Protection Act
CAPTCHA

Standards: NIST 800-53 Special Publication - Access Management

Identification
Authentication
Authorization
https://nvd.nist.gov/800-53/

How does complexity manifest itself?

Government

Industry

Compliance

Business

Development Environment

Deployment Environment

Guidelines

C

I

A

Policies

Standards - NIST

International

Laws/Regulations:

May 2018

EU - General Data Protection Regulation (GDPR)

February 2018

Australian Data Breach Law

2017

China Data Protection Regulation (CDPR)

India – Data Protection Bill (Draft)

Highlights of GDPR

- Applies to processing of personal data in EU
- Stiff penalties (4% of annual global turnover or 20M Euros – the larger)
- Consent – Intelligible and easily accessible form with the intent of use of data
- Breech Notification – within 72 hours of being aware of the breech
- Right to Forgotten - Data Erasure
- Privacy by Design

How does complexity manifest itself?

Government

Industry

Compliance

Business

Development Environment

Deployment Environment

Guidelines

C

I

A

Policies

Standards - NIST

What can I do?

- Awareness/Education
- Governance/Policies
- Risk Assessment – not all data is worth protecting
- Secure by Design –
  SQL Injection Avoidance by Prepared Statements
- Development – Secure Software Development Life Cycle
- Deployment and Monitoring
- Online Resources - OWASP

"If you can push security as far as you can toward developers, it's a good thing, because you can catch problems earlier. Dependency graph can shift security very far left."

Liz Rice, Technology Evangelist for Aqua