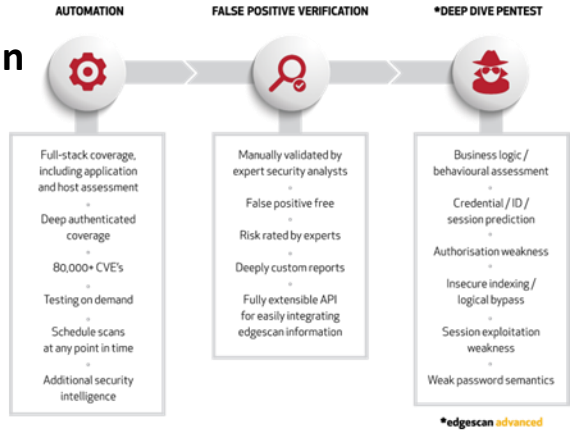
Introduction to Application Security

Eoin Keary

CTO BCC Risk Advisory / edgescan

www.bccriskadvisory.com
www.edgescan.com



Where are we going?

Web Security and HTTP Basics	What is Web Application Security?
	HTTP GET/POST
	HTTP Security Response Headers
	Sensitive data in transit
	stuff
	More stuff

Today's State: "Our Website Is Safe"

We Have Firewalls and IPS in Place

Port 80 & 443 are open for the right reasons

We Audit It Once a Quarter with Pen Testers

Applications are constantly changing

We Outsource

We Use Network Vulnerability Scanners

Neglect the security of the software on the network/web server

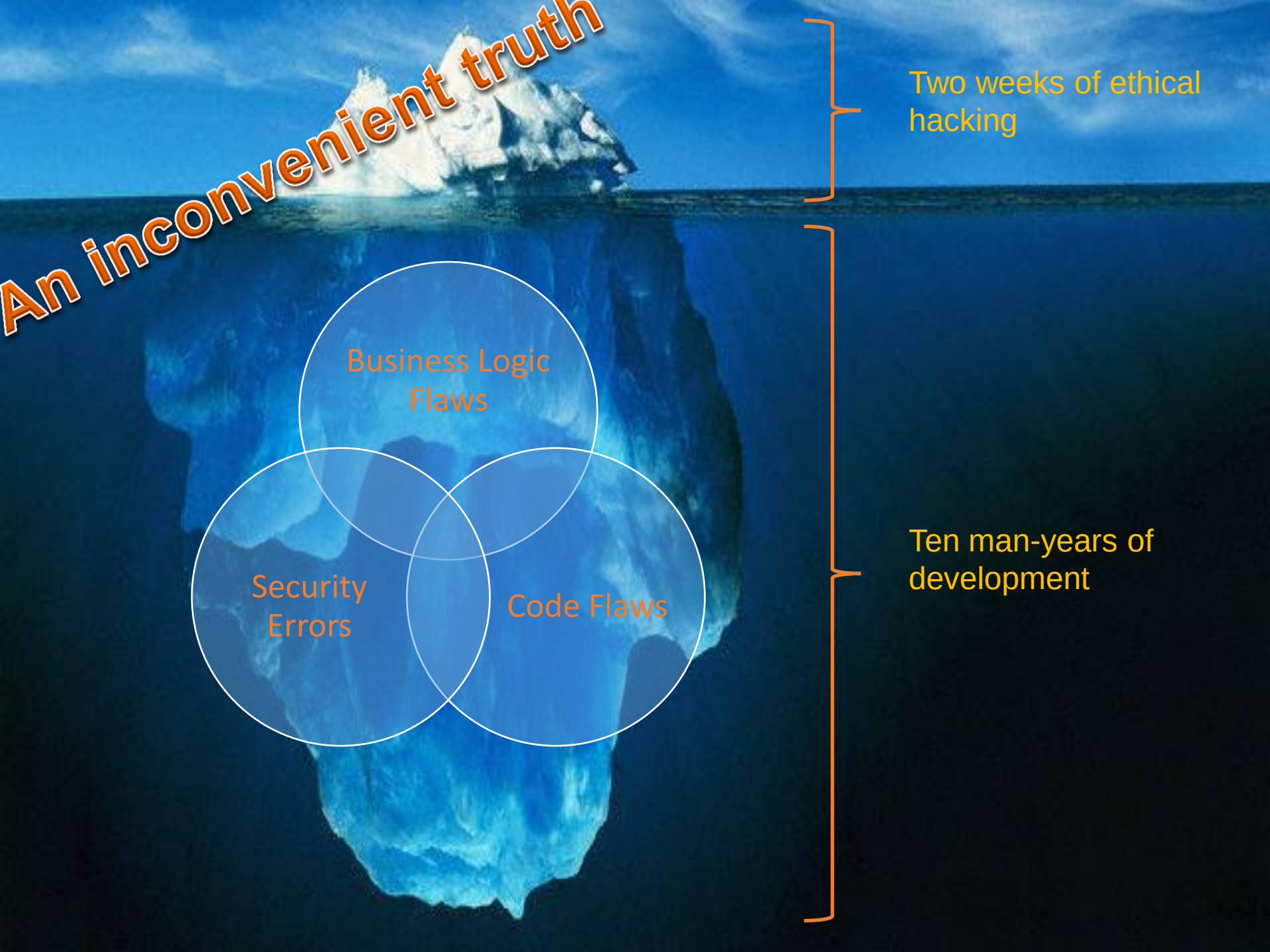
We Use SSL Encryption

Only protects data between site and user not the web application itself

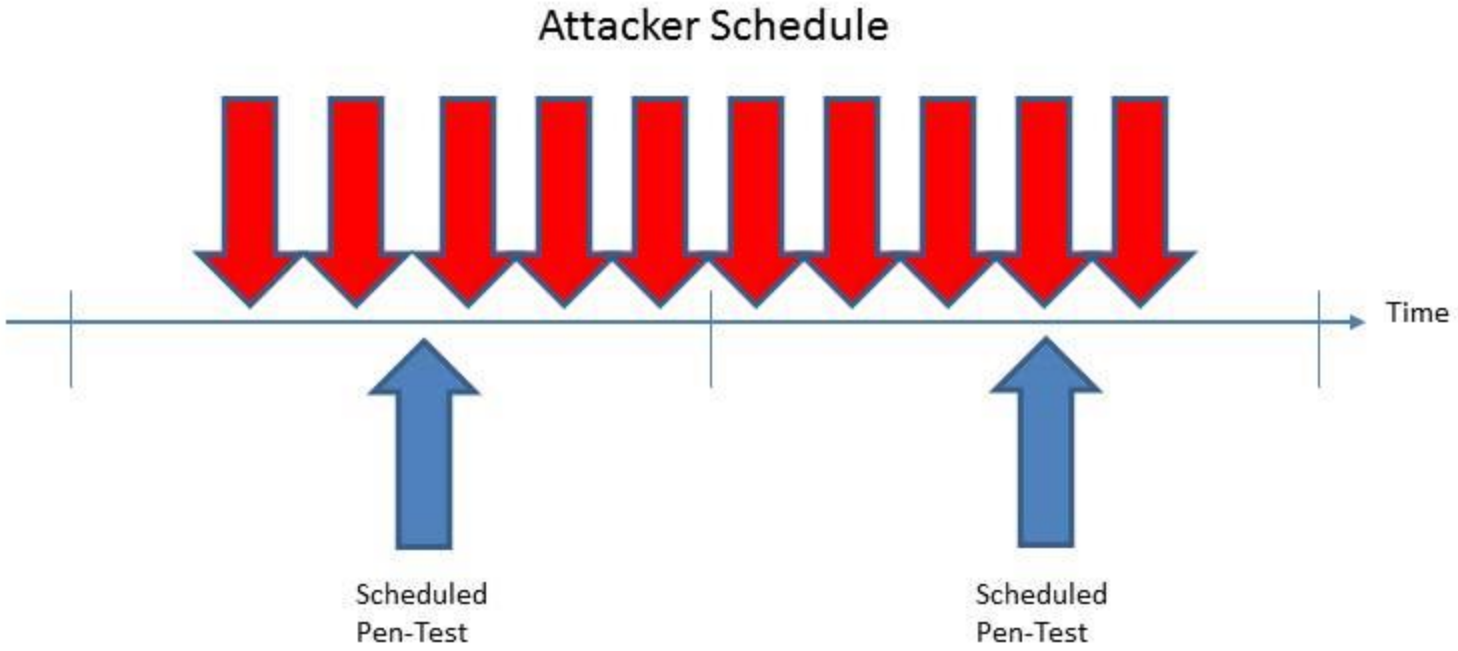
BC RISK ADVISORY

- Asymmetric Arms Race

- A traditional end of cycle / Annual pentest only gives minimal security…..
- There are too many variables and too little time to ensure “real security”.


An inconvenient truth
Two weeks of ethical hacking
Business Logic Flaws
Security Errors
Code Flaws
Ten man-years of development

An Attacker has 24x7x365 to Attack



The Defender has 20 man days per year to detect and defend

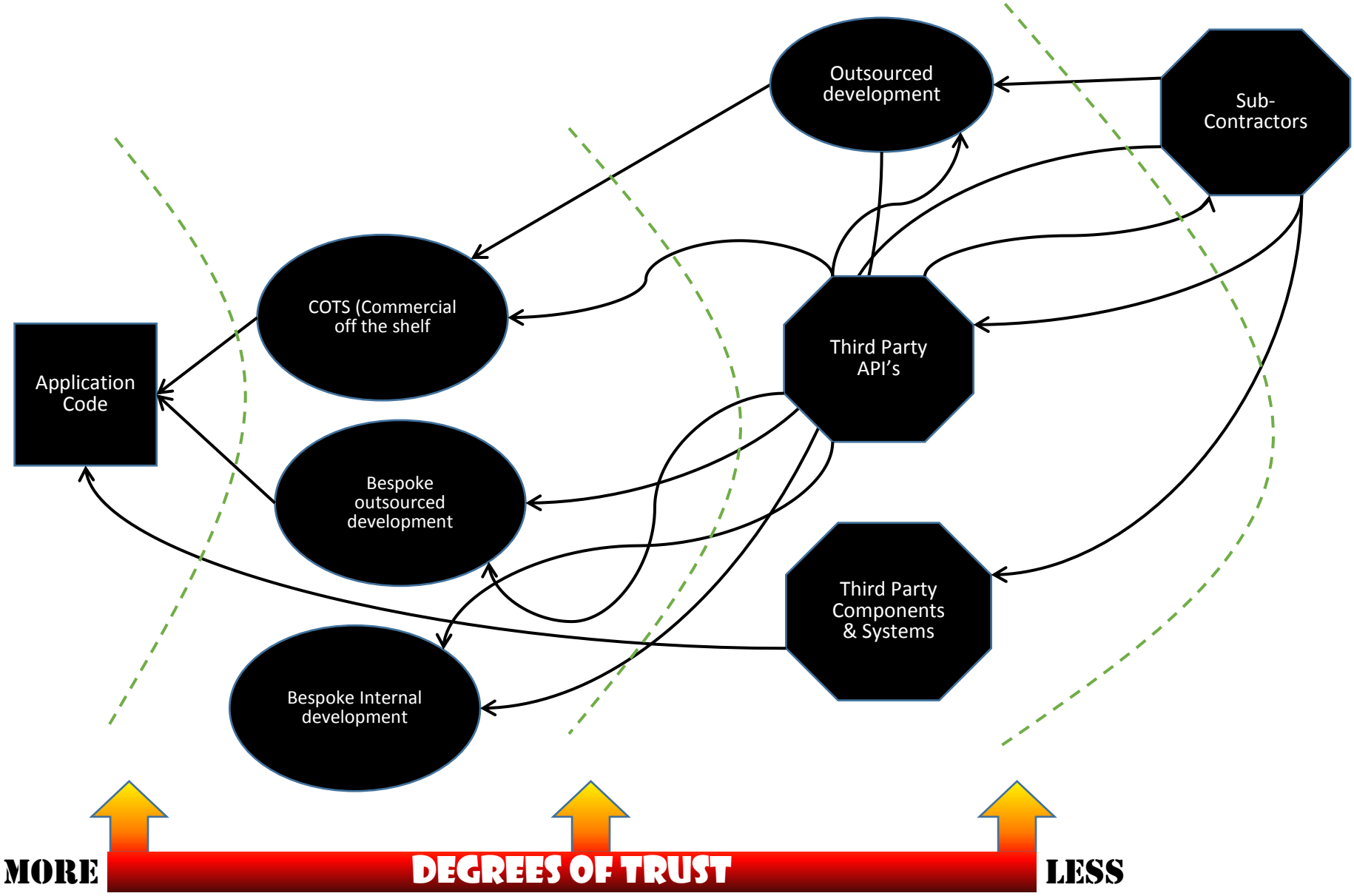
Who has the edge?

"We need an Onion"

SDL	*Design review*
	Threat Modeling
	Code review/SAST
	Pentesting/DAST
Live/Ongoing	*Continuous/Frequent monitoring/Testing*
	Manual Validation
	Vulnerability management & Priority
	Dependency Management ….

We need more than a Penetration test.

You are what you eat



You may not let some of the people who have developed your code into your offices!!

“We can’t improve what we can’t measure”

Information flooding

(Melting a developers brain, White noise and “compliance”)

Doing things right != Doing the right things

“Not all bugs/vulnerabilities are equal”
(is HttpOnly important if there is no XSS?)

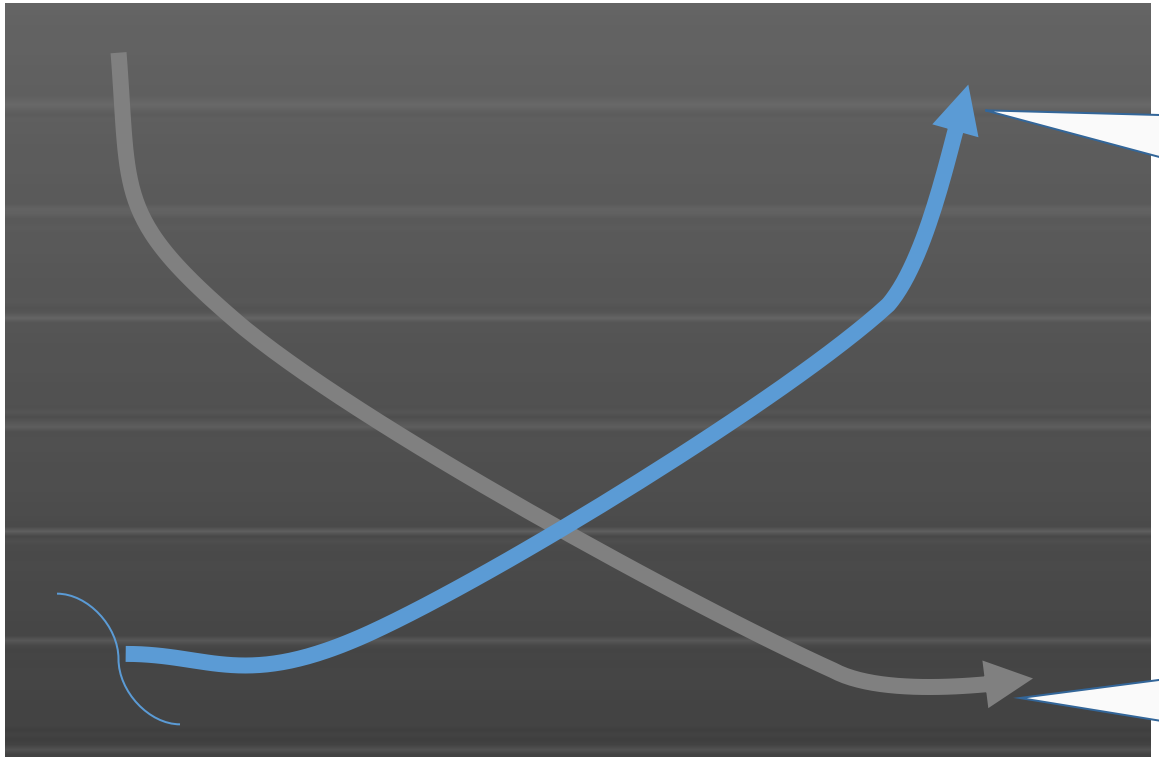
Contextualize Risk
(is XSS /SQLi always High Risk?)

Do developers need to fix everything?

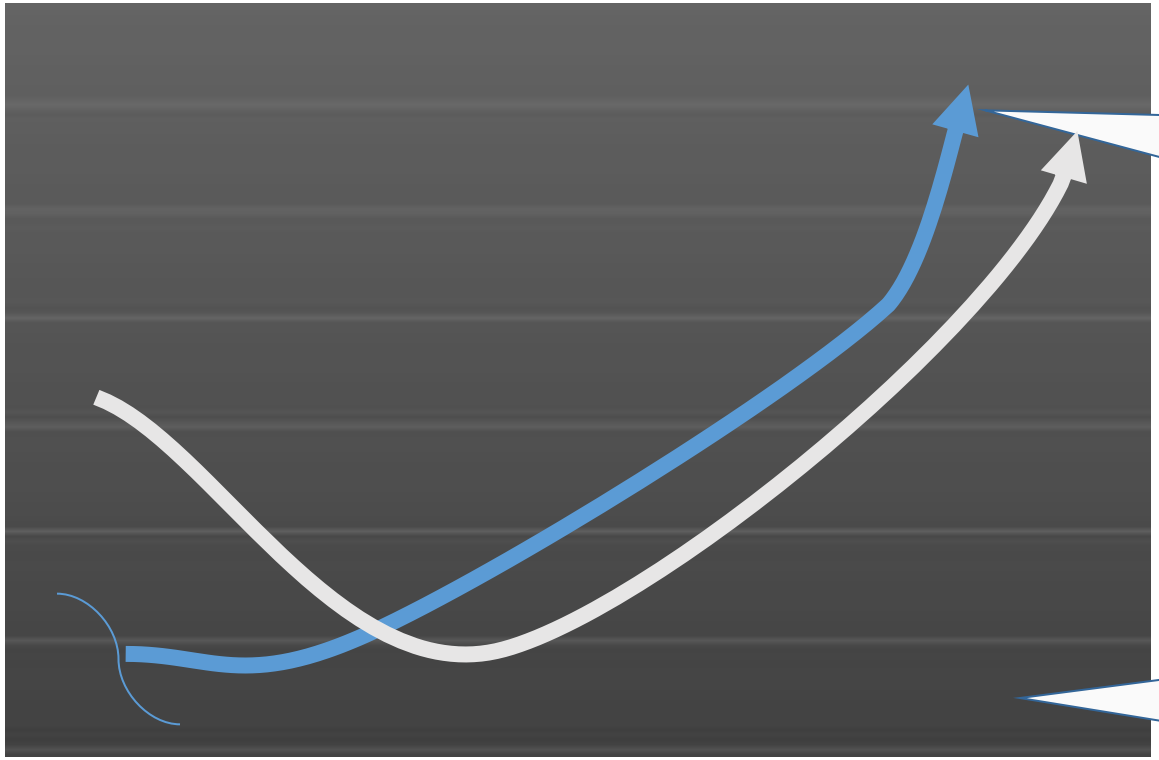
- ***Limited time***
- ***Finite Resources***
- ***Task Priority***
- ***Pass internal audit?***

White Noise

Ideal world


Information security spend
Security incidents (business impact)

Real world


Information security spend
Security incidents (business impact)

Application Vulnerabilities Overview

- Application security vulnerabilities can be roughly broken down into 4 categories.
- Application **Infrastructure**
  - Application infrastructure misconfigured
  - Data passed between browser and server not secured
- Application **Controller/Server Tier** not coded Securely
  - Broken Authentication and Session Management
  - Business object references (identifiers) not properly secured
  - Failure to Restrict URLs Properly
  - Unvalidated Redirects and Forwards
- Vulnerabilities at the **Browser Level**
  - Unvalidated data becomes a script executed on the browser
  - Logged in user's session is able to be forged
- Vulnerabilities at the **Persistence Tier**
  - Database access not properly written to use SQL securely
  - Data not stored in a cryptographically secure way

Developer Security?

- Developers rarely get application security training in school
- The protocols we use for web development are insecure
- The languages we use for web development are insecure
- The frameworks we use for web development are insecure
- Developers rarely get prescriptive security requirements at work
- Developers rarely get good assessment technology to verify if they are writing secure code and applications

Recipe for Disaster!

Secure Application Design Principles

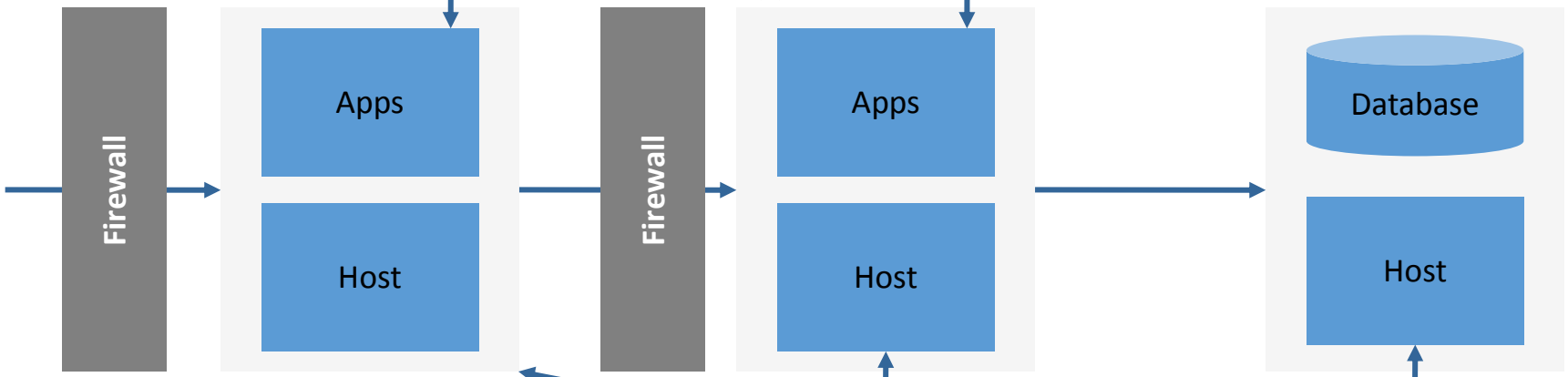
Practice least privilege	Applications should execute with the *Least Privilege* required to perform a job
Employ secure defaults	Choose appropriate features for users and ensure that these features are secure
Validate data from all sources	Always assume that data from any source is malicious and validate it before use
Fail to a secure mode	Design applications to fail to a secure state and never disclose confidential data or provide elevated privledges
Prevent information leakage	An unintentional revelation of information about the way an application works
Practice defense in depth	Use multiple layers of security instead of a single mechanism
Secure the weakest link	Secure your application to prevent it from being the "weakest" link
Escape/Encode	Convert data that is used by parsers into non-executing context

Web application security risks

Blurring traditional boundaries	Organizations are exposing internal data and critical functionality to the public Internet through web application deployments
Data privacy	Weak security controls may be exploited by skilled attackers to access sensitive information or perform unauthorized activities on your organizations' systems
Impact of a security breach	Loss of customer confidence and reputational damage via the negative publicity associated with a security breach

Web Application Security

Securing the application		
Input validation	Session mgmt	Authentication
Authorization	Config mgmt	Error handling
Secure storage	Auditing/logging	XSS Defense

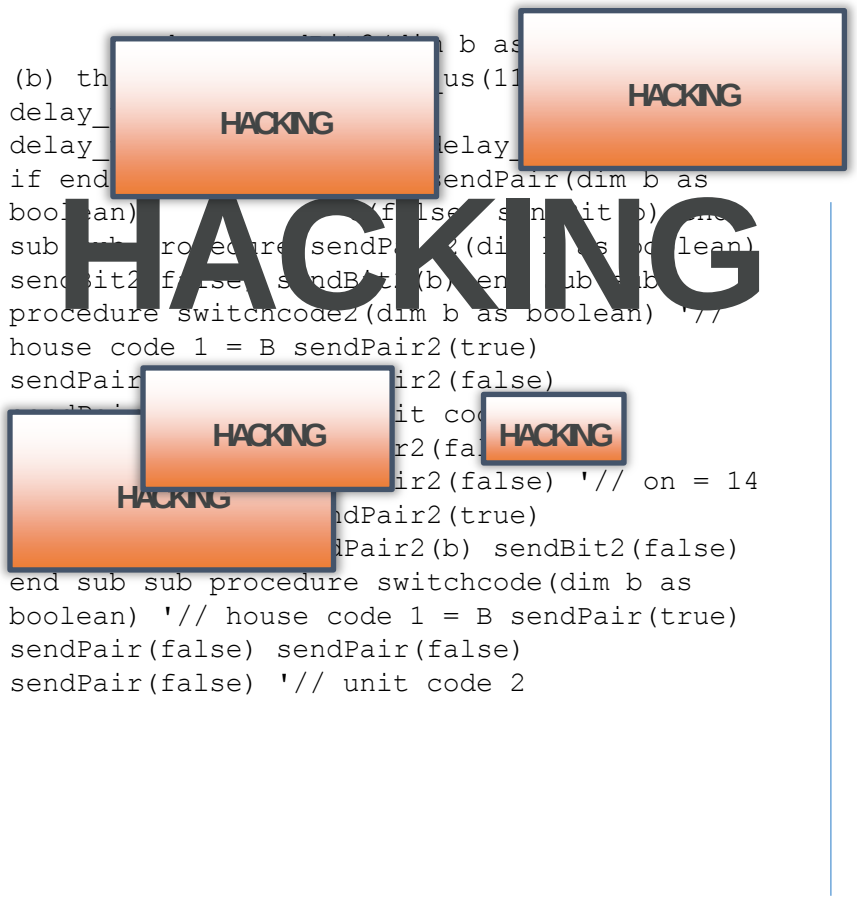


Securing the network
Router
Firewall
Switch

Securing the host		
Patches/updates	Accounts	Ports
Services	Files/directories	Registry
Protocols	Shares	Auditing/logging

BCG RISK ADVISORY

COMMON VULNERABILITIES HACKERS EXPLOIT



OWASP
The Open Web Application Security Project

1. Injection
2. Cross-site scripting
3. Broken authentication/session management
4. Insecure direct object references
5. Cross site request forgery
6. Security misconfiguration
7. Insecure cryptographic storage
8. Failure to restrict URL access
9. Insufficient transport layer security
10. Un-validated redirects and forwards

BCG RISK ADVISORY

CLOUD SECURITY

SOCIAL APPS

MOBILE SECURITY

DATA PRIVACY

SOFTWARE ASSURANCE

NEW Challenges

RISK ADVISORY

More
DEVICES Than
PEOPLE

12.5 Billion

2010

25 Billion

2015

50 Billion

2020

CONNECTED DEVICES

RISK ADVISORY

THE NEW PERIMETER

THE NETWORK IS NO LONGER THE POINT OF CONTROL

PEOPLE

Employees, Contractors
Costumers & Partners

DATA

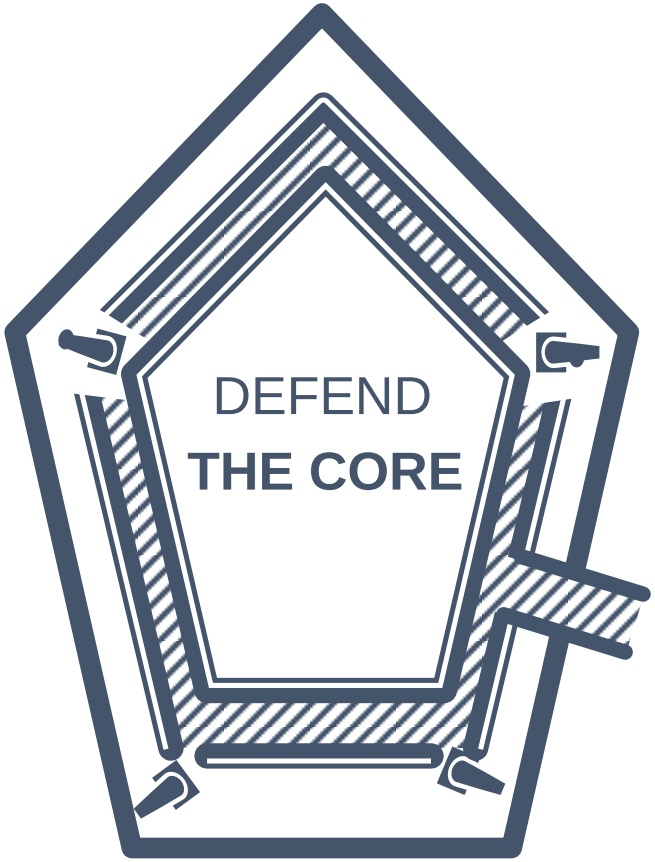
Unstructured & Structured

DEVICES

Phones, Servers,
Laptops, Tablets

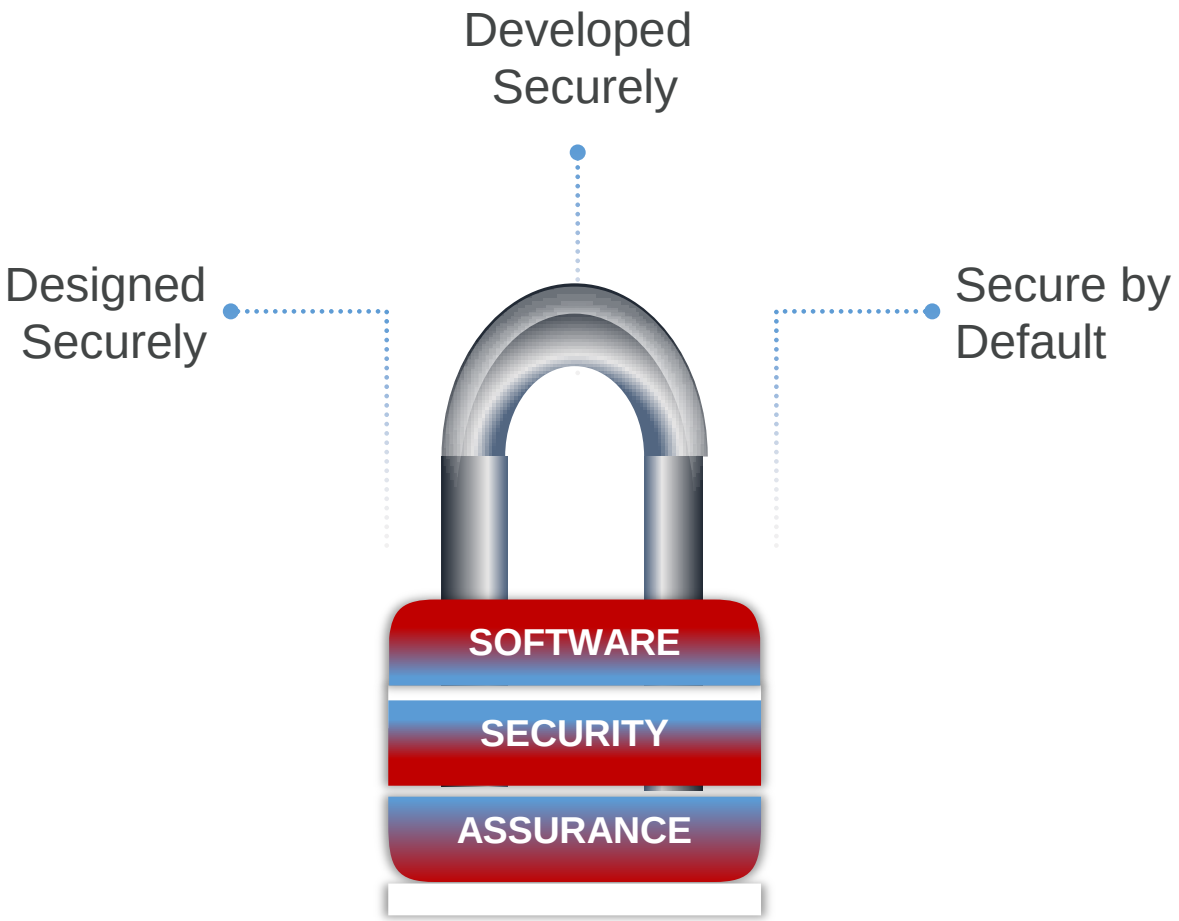
BC RISK ADVISORY

HE WHO DEFENDS EVERYTHING DEFENDS NOTHING



- The network has become the battlefield
- Forcing defense of the entire network
- Low situational awareness on the network
  - Who, What, When, Why ?
- Low awareness increases vulnerability

ASSURANCE IS PART OF THE SOLUTION



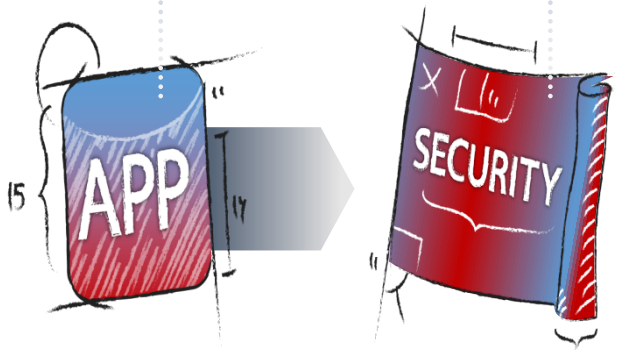
RISK ADVISORY

CRITICAL PATCH **UPDATES**

Cumulative
Incremental Patches

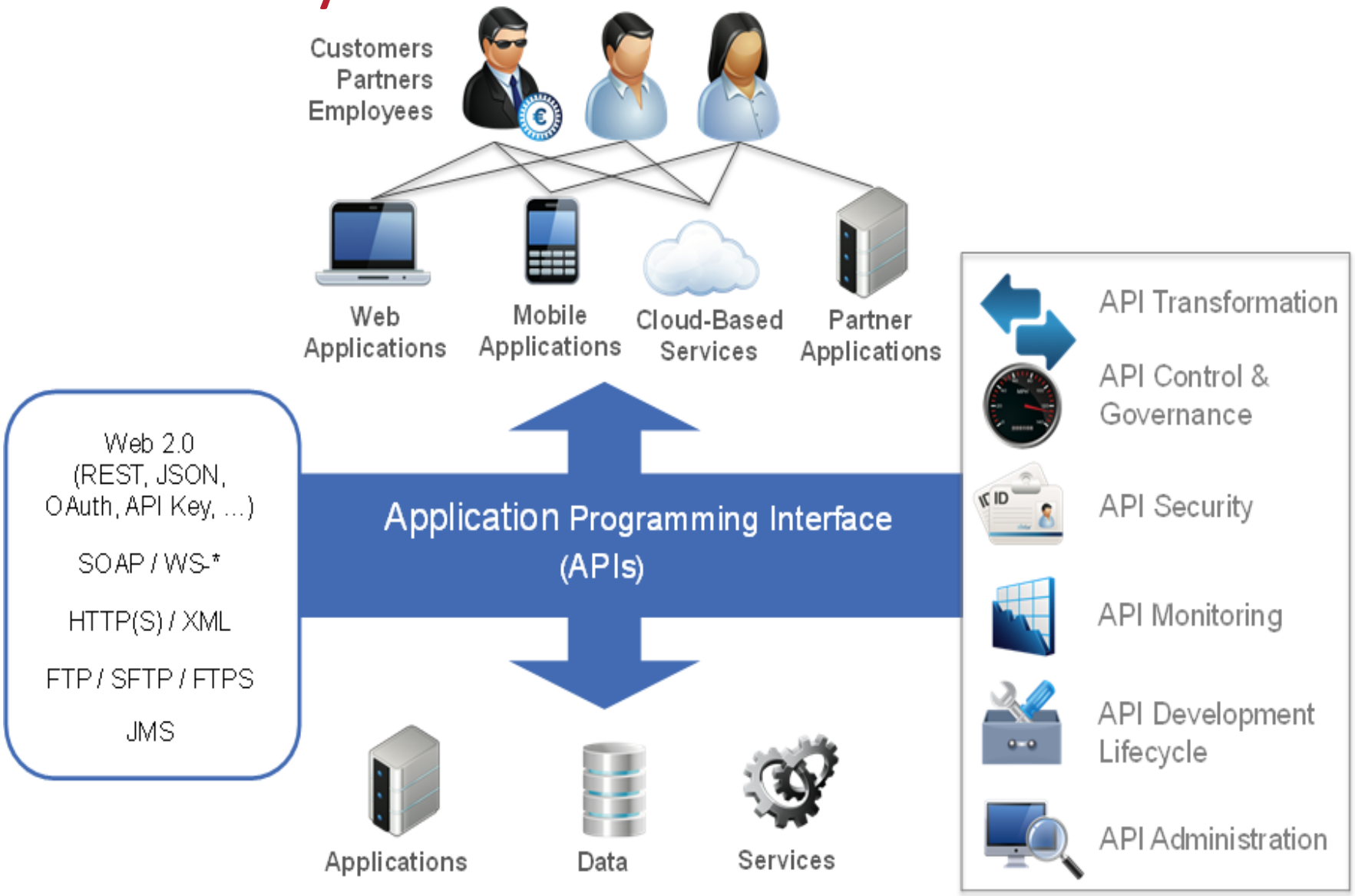
Predictable
Scheduled a year ahead
Quarterly patches

Security focused priority
Most critical patches first
Dynamic schedule



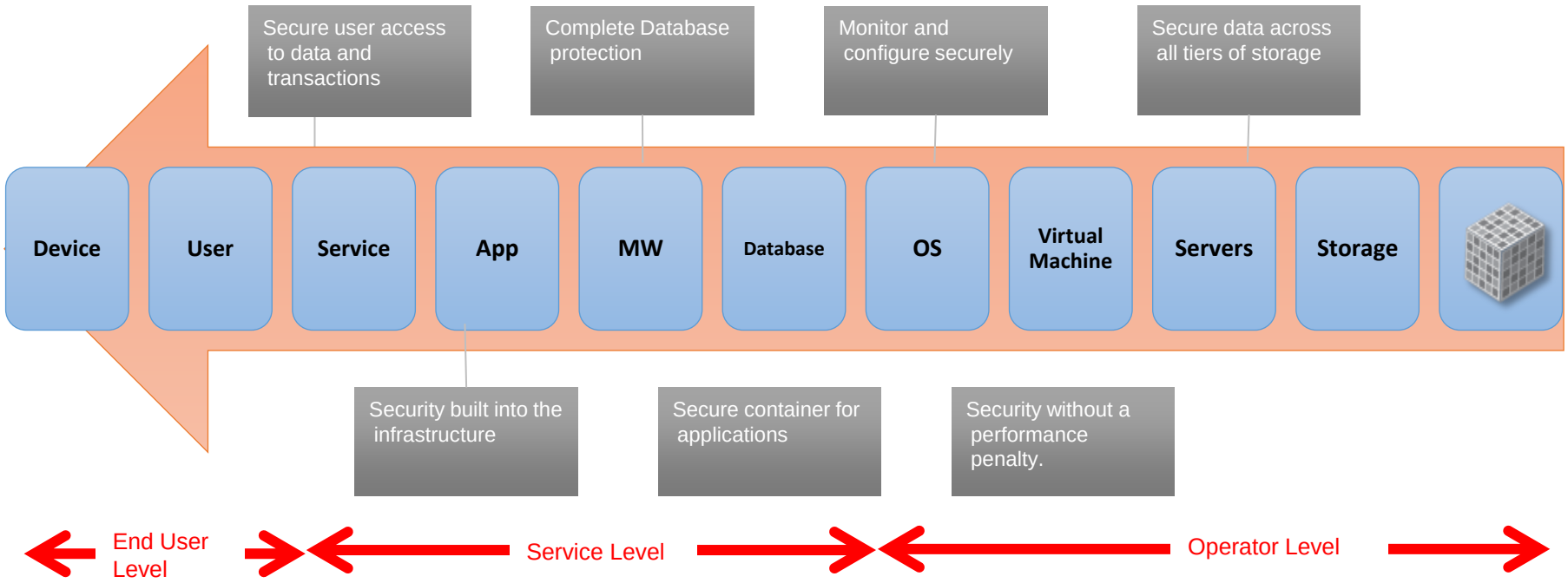
RISK ADVISORY

API Security?



RISK ADVISORY

Identity and Access Management



Identity propagation & consistent access policies

RISK ADVISORY

RECOMMENDATIONS

DON'T SECURE YOURSELF OUT OF BUSINESS

- You can't defend everything
- Assume you are already breached
- Protect your most valuable assets
- Have a plan and execute the plan

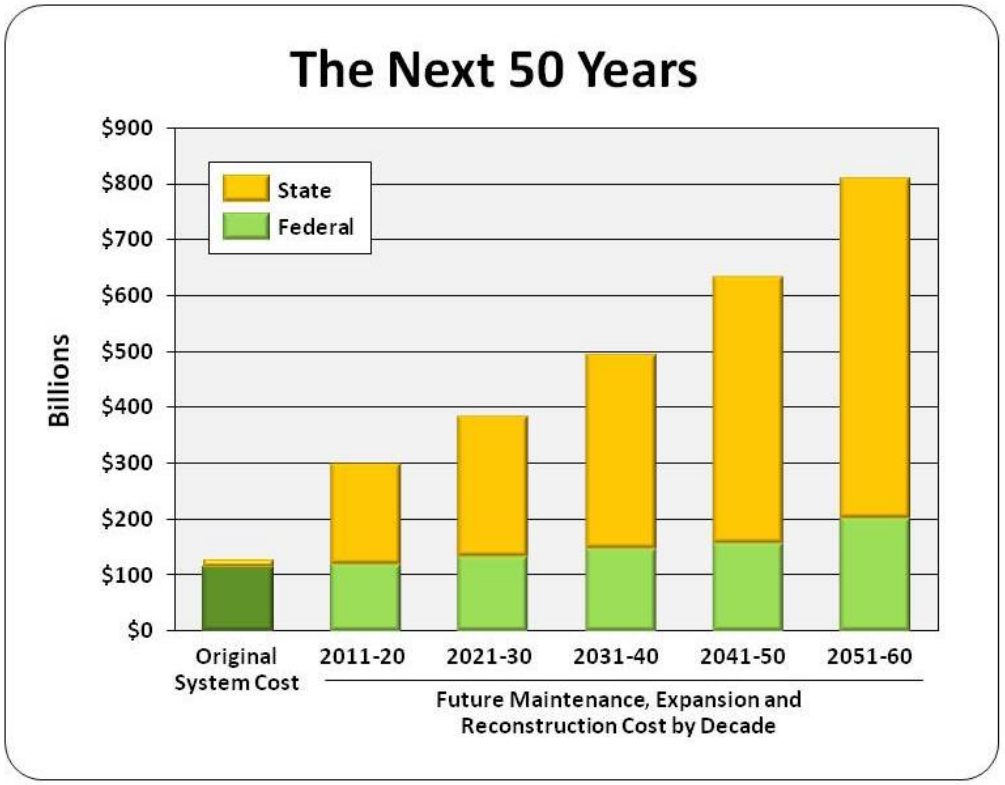
BC RISK ADVISORY

US Interstate Highway System
Initial cost vs. maintenance cost

http://cdmsmith.com/en-US/Insights/Funding-Future-Mobility/Exit-6-Aging-Interstates.aspx

Interstate-related expenditures during the next 50 years will likely reach $2.5 trillion. The interstate system is anything but "paid for"

- http:/cdmsmith.com



BCG RISK ADVISORY

Gratuitous slide to distract you so you can blame your insecure code on me

Baseball + Bat = $1.10
How much is the Bat if it costs $1.00 more than the ball?