HACKERS & ATTACK ANATOMY

Geoff Gentry, Regional Director | ggentry@securityevaluators.com

Why is this important?

Attacks

TEXAS INSTRUMENTS

About ISE

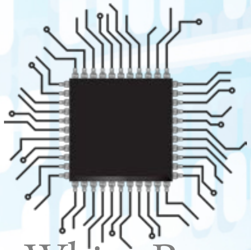
belkin

III. Security vs. Functionality

TARGET

I. Assets vs. Perimeters

IV. Build In vs. Bolt On



II. Black Box vs. White Box

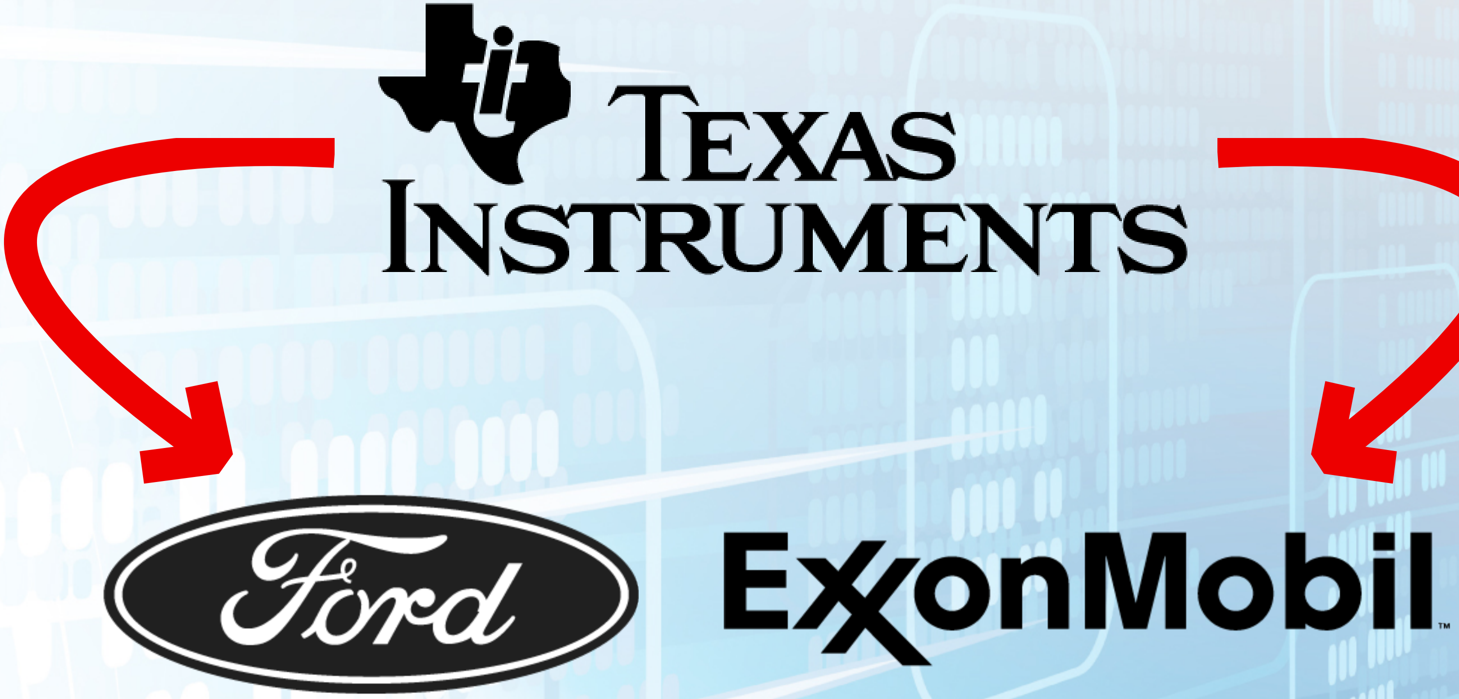
iPhone

V. Ongoing vs. Periodic

HACKED

Texas Instruments

HACKED



Place Speedpass
HERE

PUSH
ON
START
LOCK

About ISE

Perspective

- White box

Analysts

- Computer Scientists; Ethical Hackers

Research

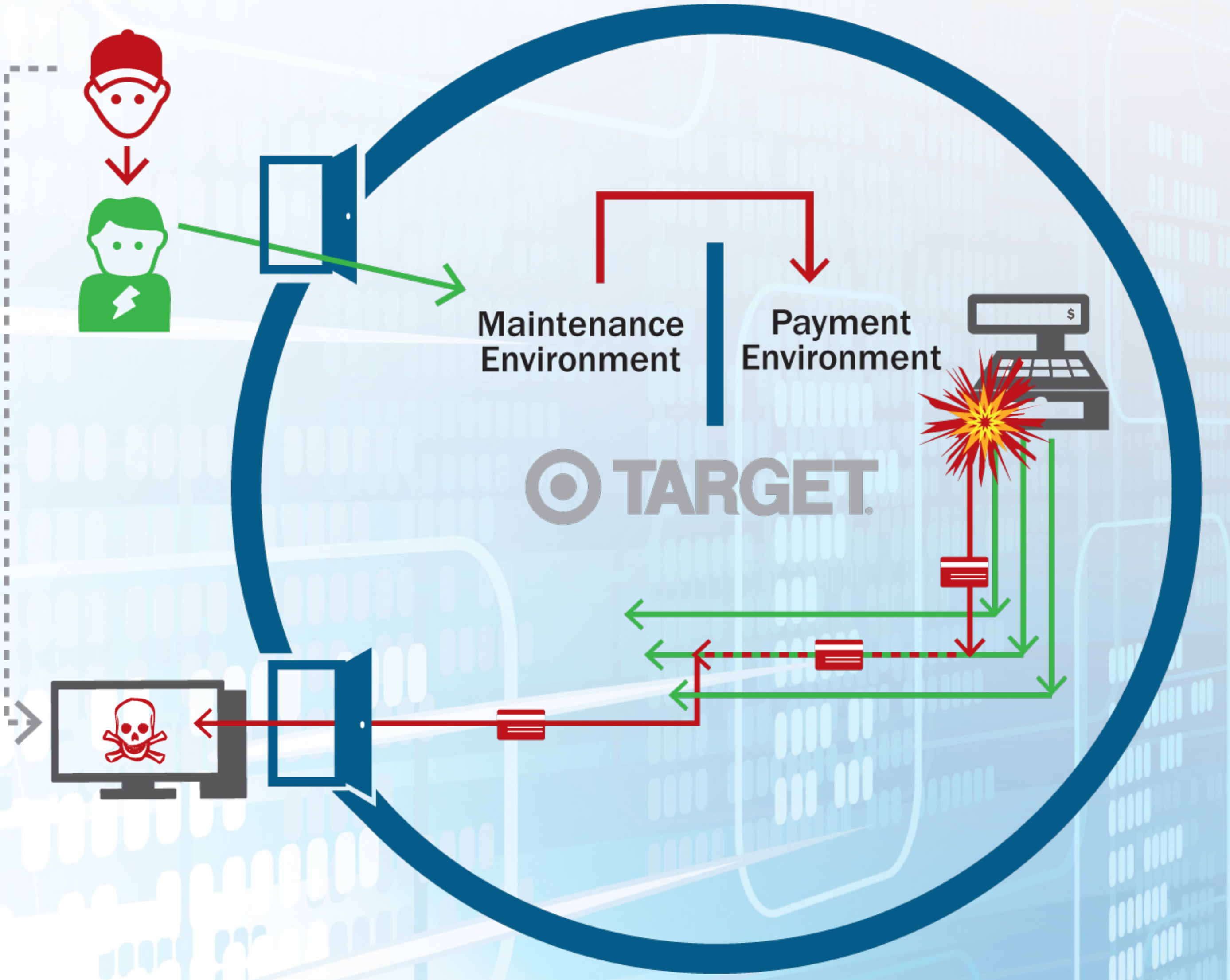
- Recent: Browsers; Routers; Hospital

Customers

- Fortune 500 Enterprises

HACKED

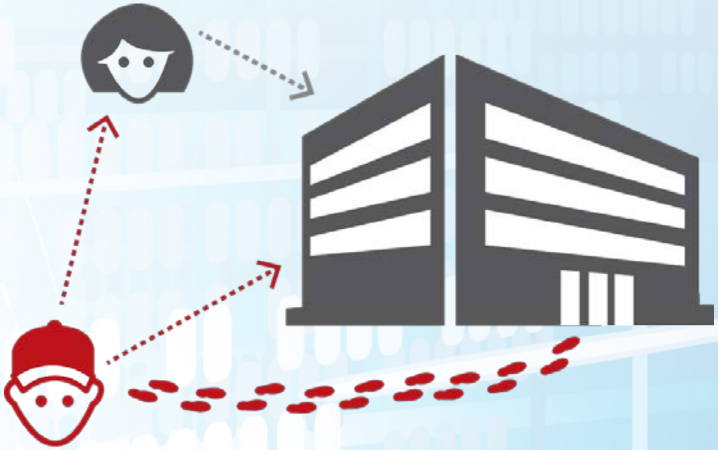
TARGET®


Maintenance Environment
Payment Environment
TARGET
$

I. Secure Assets, Not Just Perimeters

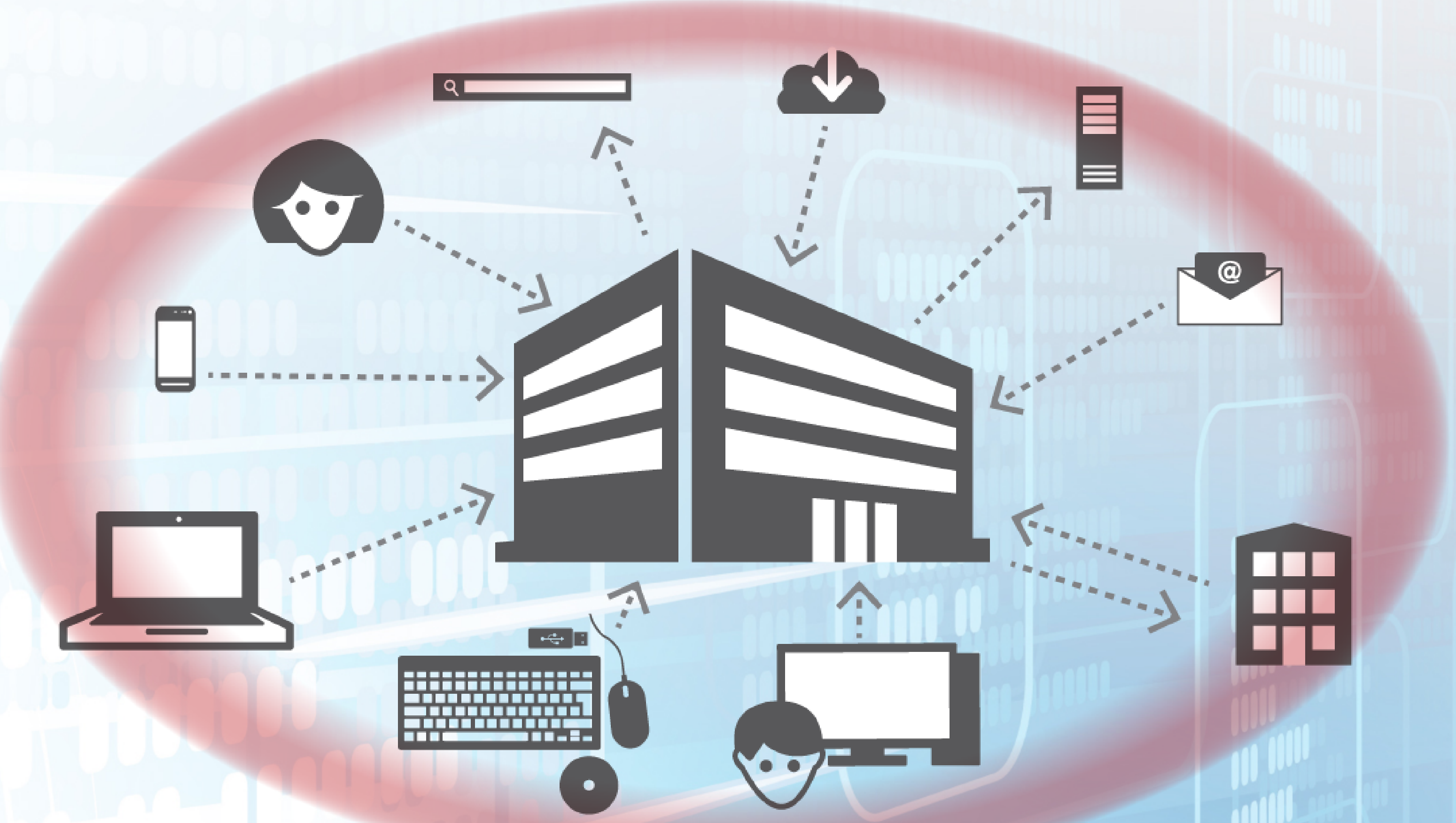
I. Secure Assets, Not Just Perimeters

Traditional Attacks



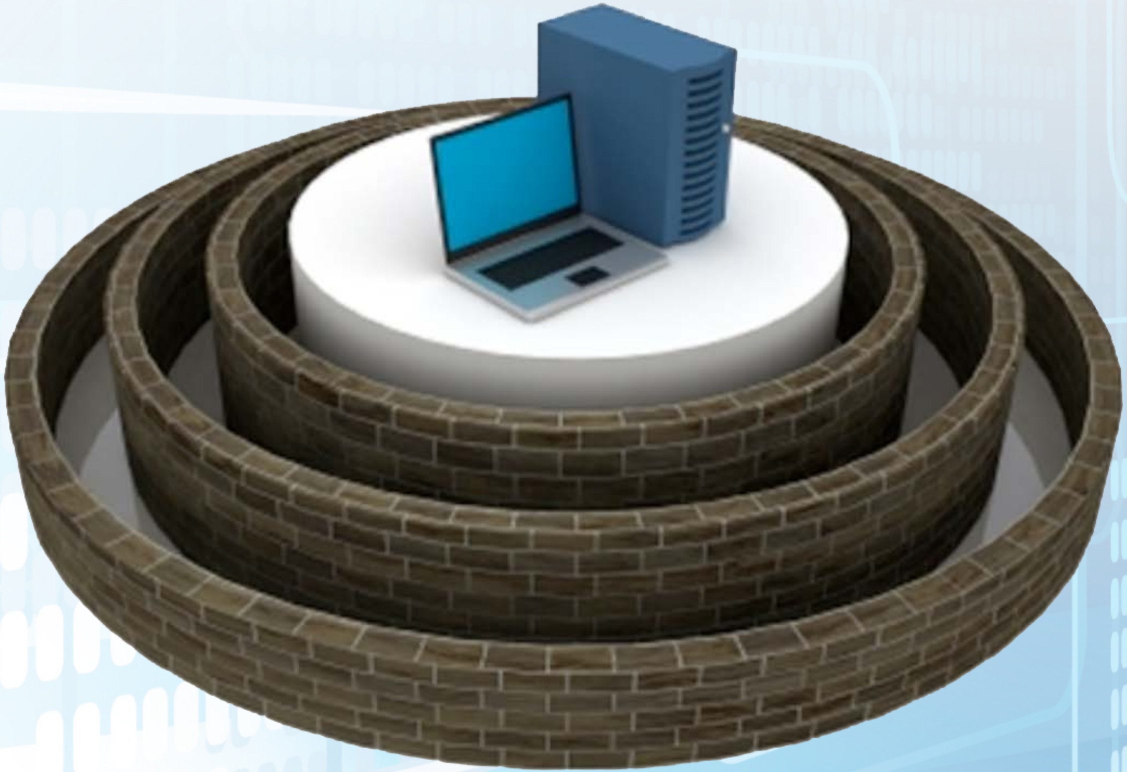
Traditional Defenses

I. Secure Assets, Not Just Perimeters

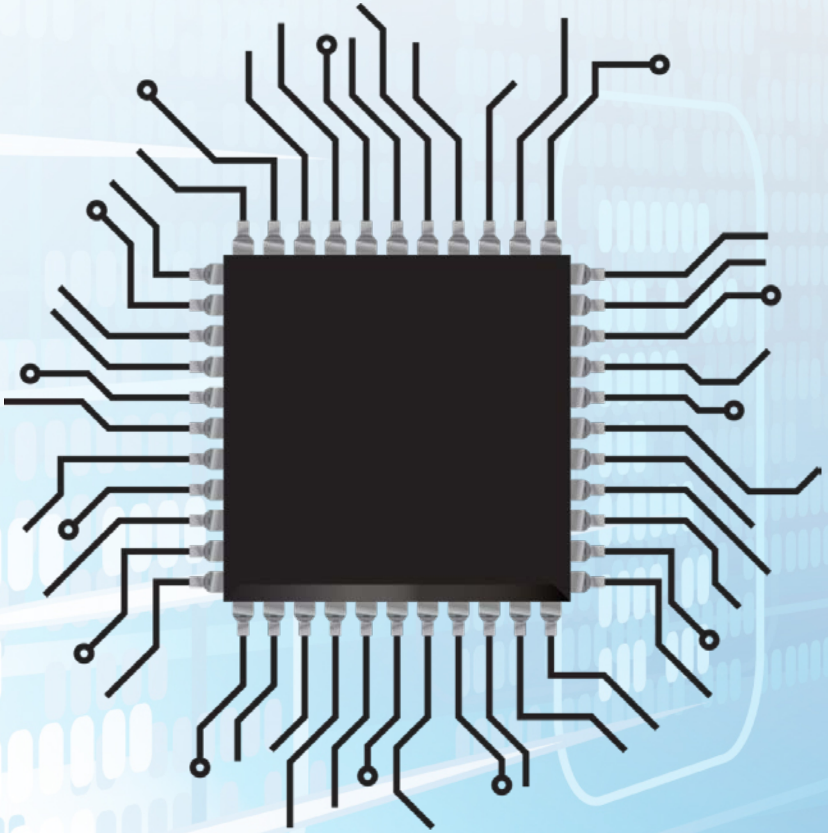


Modern Attacks

I. Secure Assets, Not Just Perimeters



HACKED



II. Black Box Penetration Tests == Good

~~II. Black Box Penetration Tests == Good~~

White box vulnerability assessment == GOOD!

II. Black Box vs. White Box

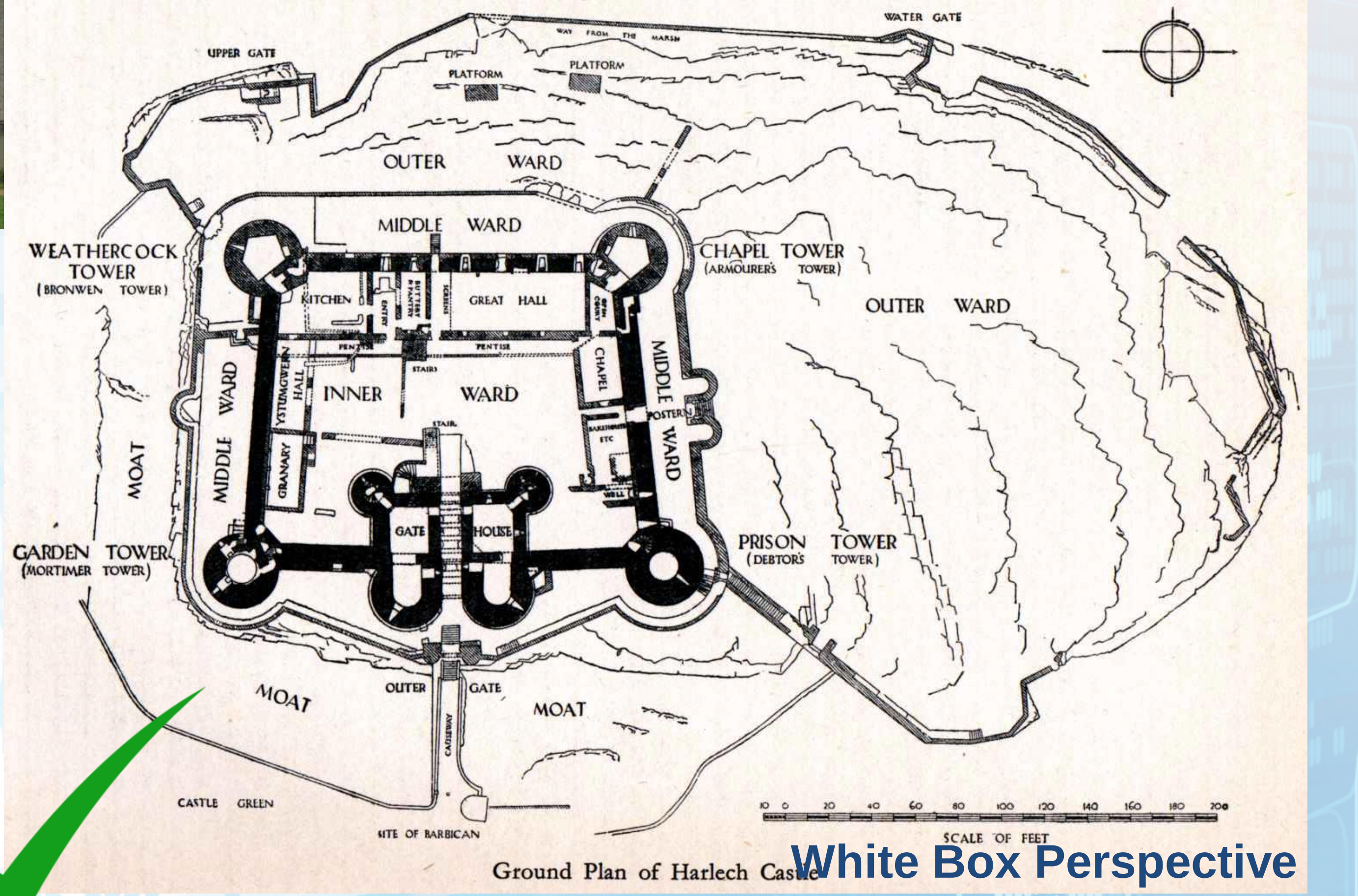
- Access Level
  - Black Box
  - White Box
- Evaluation Types
  - Penetration Test
  - Vulnerability Assessment

II. Black Box vs. White Box

Black Box Perspective

independent security evaluators

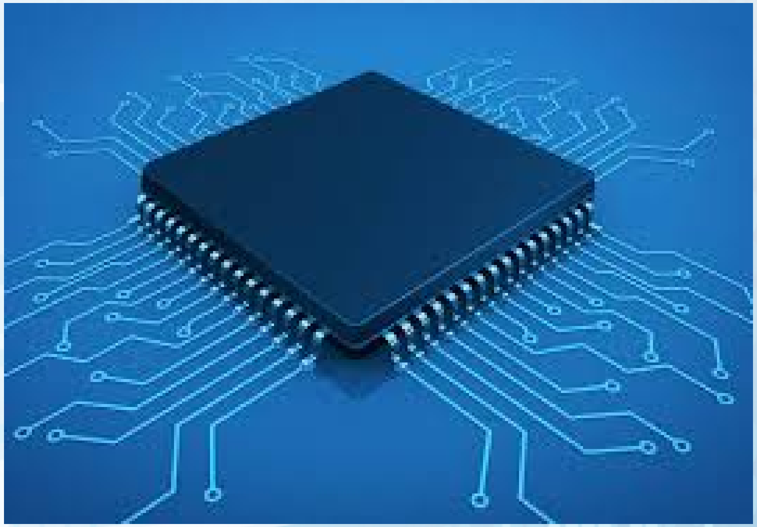
II. Black Box vs. White Box



Ground Plan of Harlech Castle

White Box Perspective

II. Black Box vs. White Box



II. Black Box vs. White Box

	Black Box	White Box
Time/cost	2 mo. / 200 hrs.	2 mo. / 200 hrs.
Severe issues	4 *potential* issues 1 confirmed	11 confirmed
Other issues	none	10 confirmed
Results	no recommendations	21+ mitigation strategies
Completeness/Confidence	very low	high
Cost/issue	200+ hrs.	~9 hrs.
Cost/solution	∞	~9 hrs.

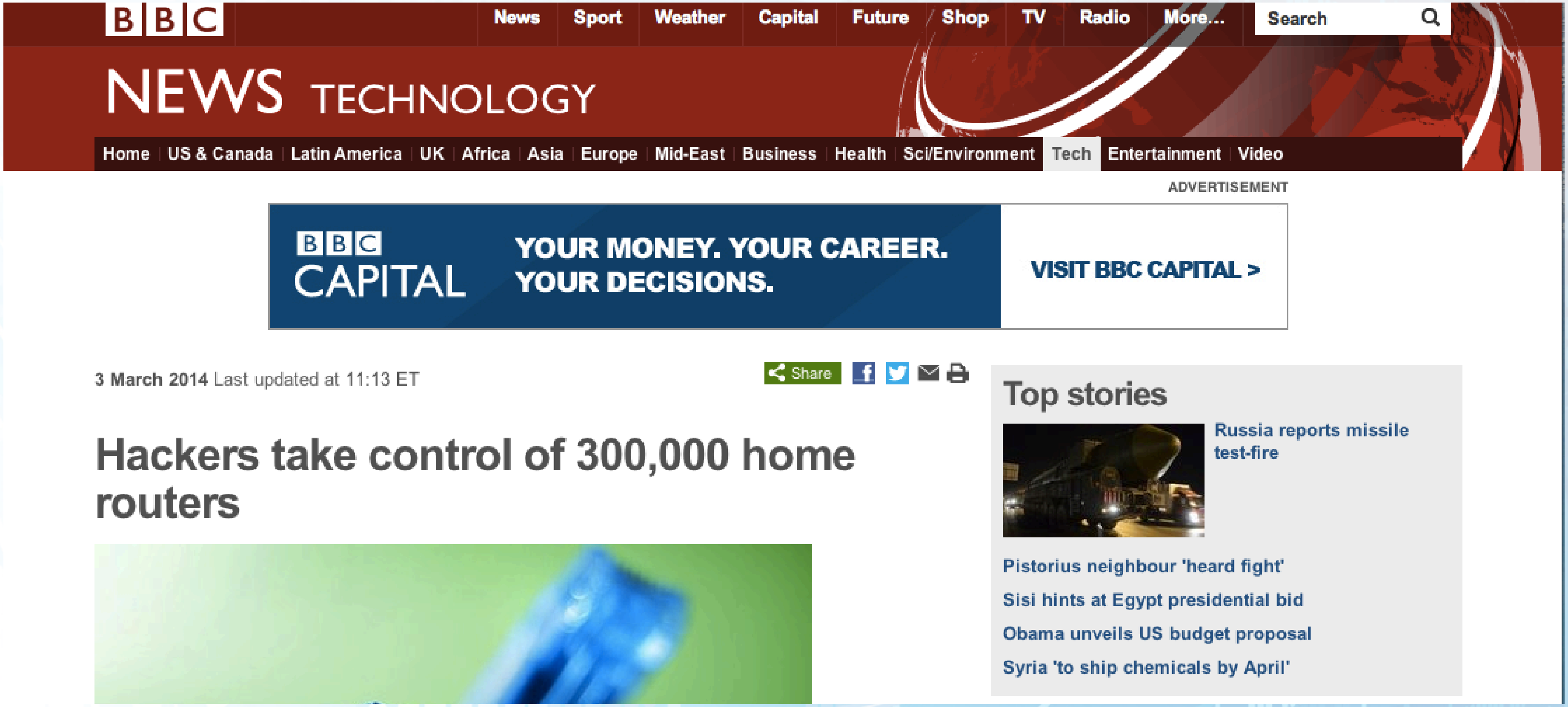
HACKED

SOHO Routers: Outcomes

	Goals	Results
Models	10	13
Attacks	Any	Remote, Local, Both
Compromise	>30%	**100% Broken**

ROUTER	REMOTE ADVERSARY			LOCAL ADVERSARY		
	TRIVIAL	UNAUTHENTICATED	AUTHENTICATED	TRIVIAL	UNAUTHENTICATED	AUTHENTICATED
Linksys WRT310Nv2			X			X
Belkin F5D8236-4 v2			X			X
Belkin N300		X	X	X	X	X
Belkin N900		X	X	X	X	X
Netgear WNDR4700				X	X	X
TP-Link WR1043N			X			X
Verizon Actiontec			X			X
D-Link DIR-865L			X			X
ASUS RT-N56U			X			X
ASUS RT-AC66U			X			X
Linksys EA6500						X
Netgear WNR3500			X	X	X	X
TRENDnet TEW-812DRU			X			X

POINT-CLICK-KILL



3 March 2014 Last updated at 11:13 ET

Hackers take control of 300,000 home routers

Top stories

Russia reports missile test-fire

Pistorius neighbour 'heard fight'

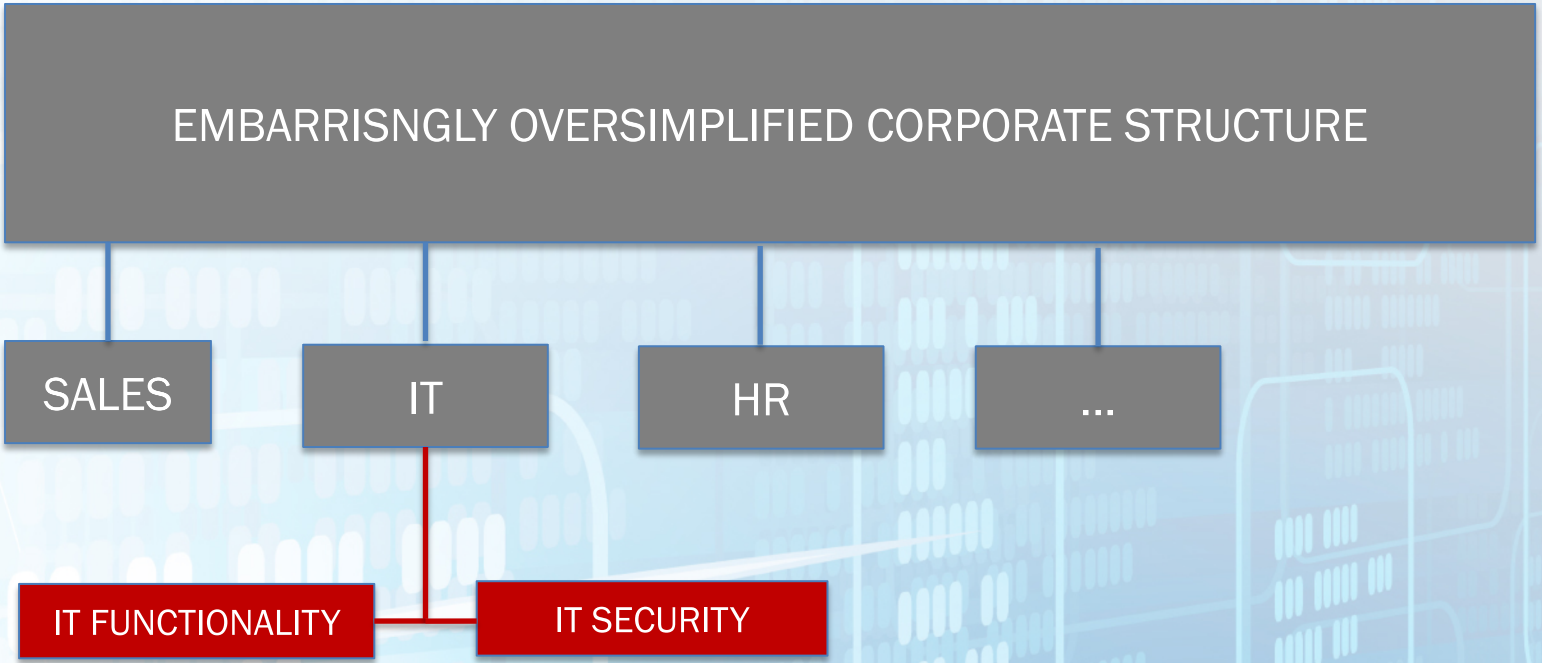
Sisi hints at Egypt presidential bid

Obama unveils US budget proposal

Syria 'to ship chemicals by April'

III. Security vs. Functionality

III. Security vs. Functionality



EMBARRISNGLY OVERSIMPLIFIED CORPORATE STRUCTURE

SALES

IT

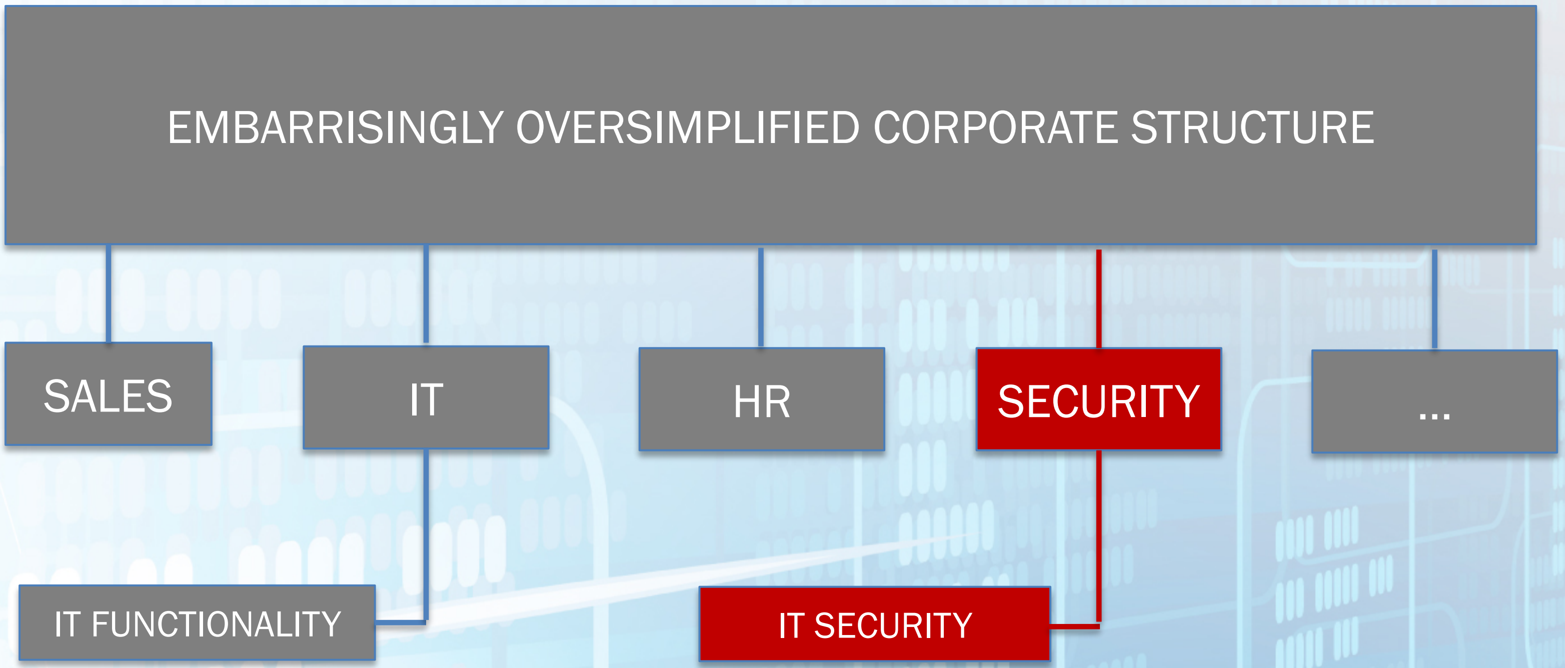
HR

...

IT FUNCTIONALITY

IT SECURITY

III. Security vs. Functionality



EMBARRISINGLY OVERSIMPLIFIED CORPORATE STRUCTURE

SALES

IT

HR

SECURITY

...

IT FUNCTIONALITY

IT SECURITY

III. Security vs. Functionality

CONFLICT IS GOOD!

III. Security vs. Functionality

I. Security Separated From Functionality

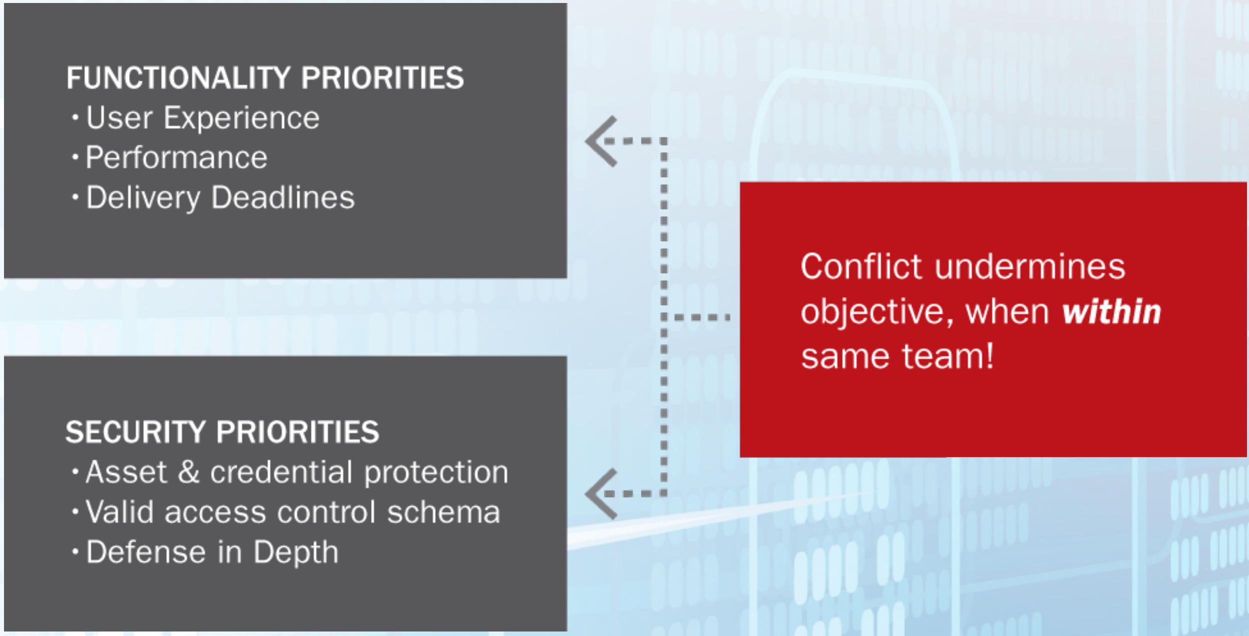
FUNCTIONALITY PRIORITIES

- User Experience
- Performance
- Delivery Deadlines

SECURITY PRIORITIES

- Asset & credential protection
- Valid access control schema
- Defense in Depth

I. Security Separated From Functionality



FUNCTIONALITY PRIORITIES

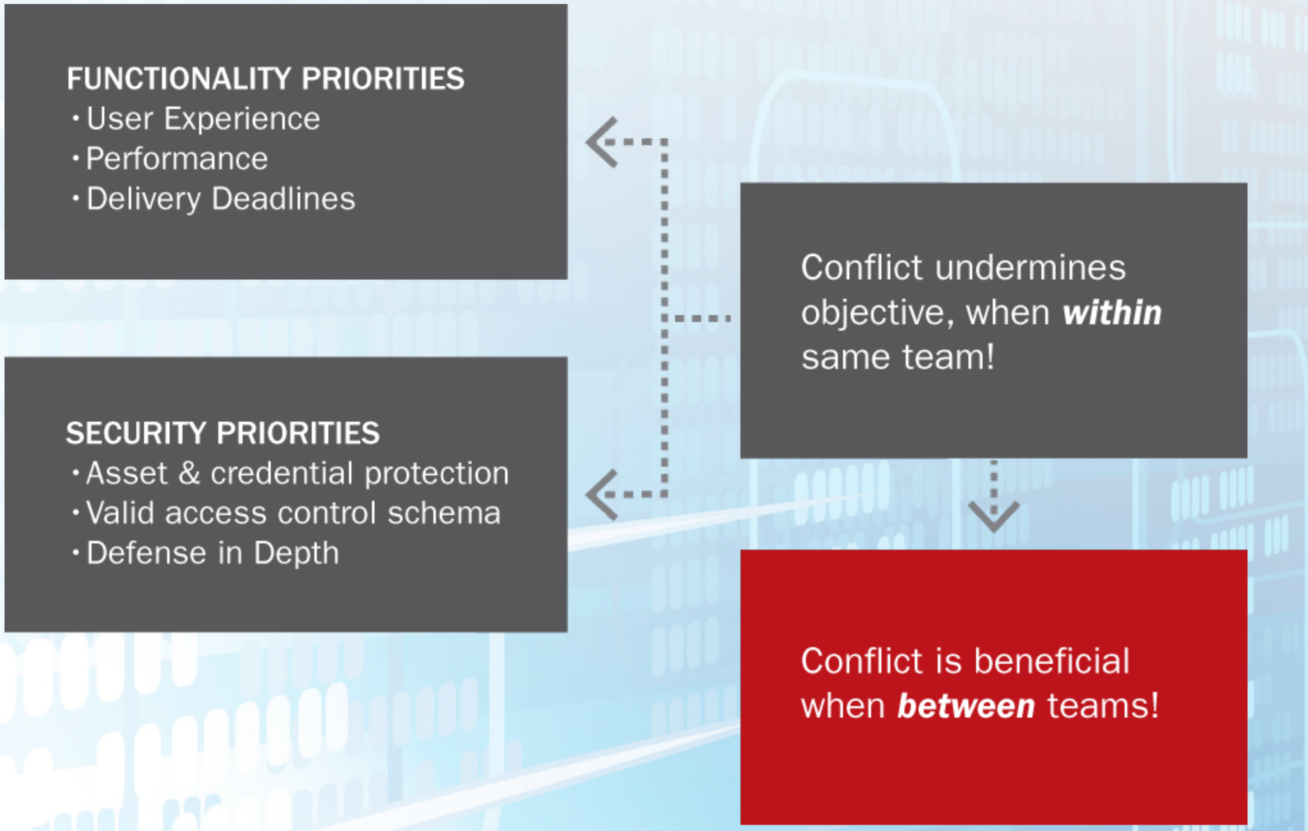
- User Experience
- Performance
- Delivery Deadlines

SECURITY PRIORITIES

- Asset & credential protection
- Valid access control schema
- Defense in Depth

Conflict undermines objective, when ***within*** same team!

I. Security Separated From Functionality



FUNCTIONALITY PRIORITIES
- User Experience
- Performance
- Delivery Deadlines

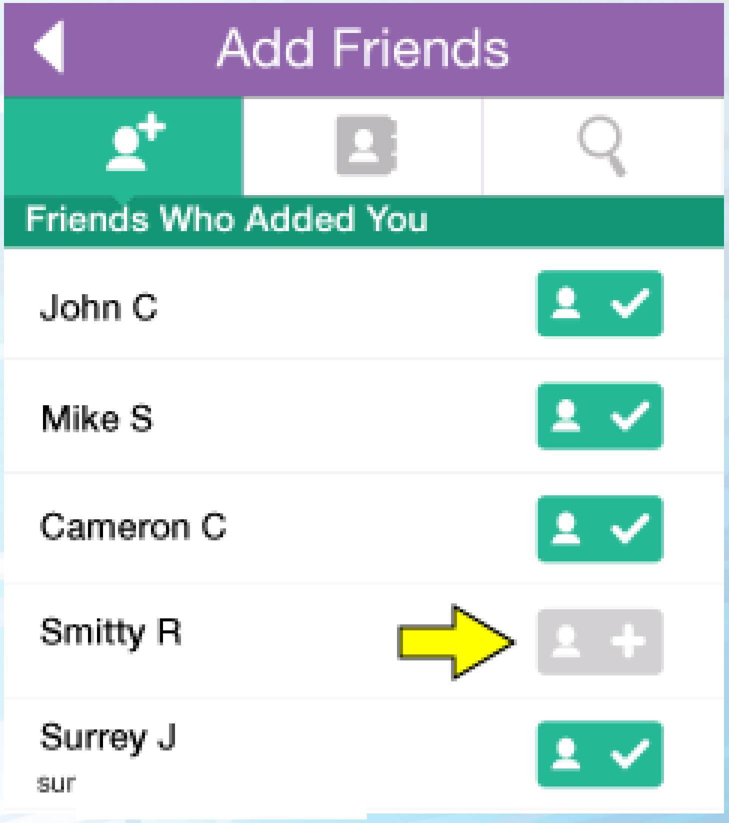
SECURITY PRIORITIES
- Asset & credential protection
- Valid access control schema
- Defense in Depth

Conflict undermines objective, when ***within*** same team!

Conflict is beneficial when ***between*** teams!

HACKED

HACKED



Add Friends

Friends Who Added You

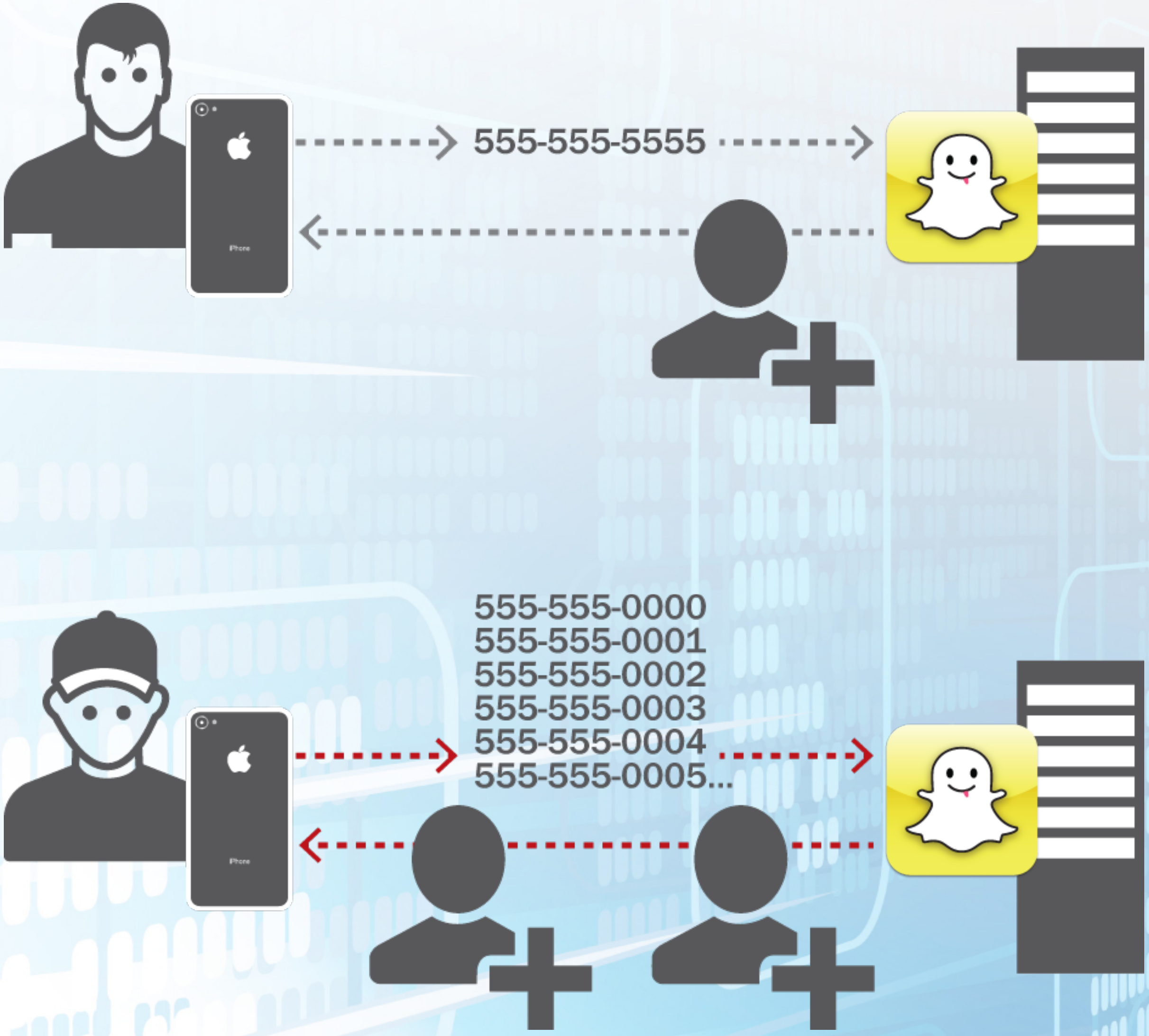
John C

Mike S

Cameron C

Smitty R

Surrey J
sur

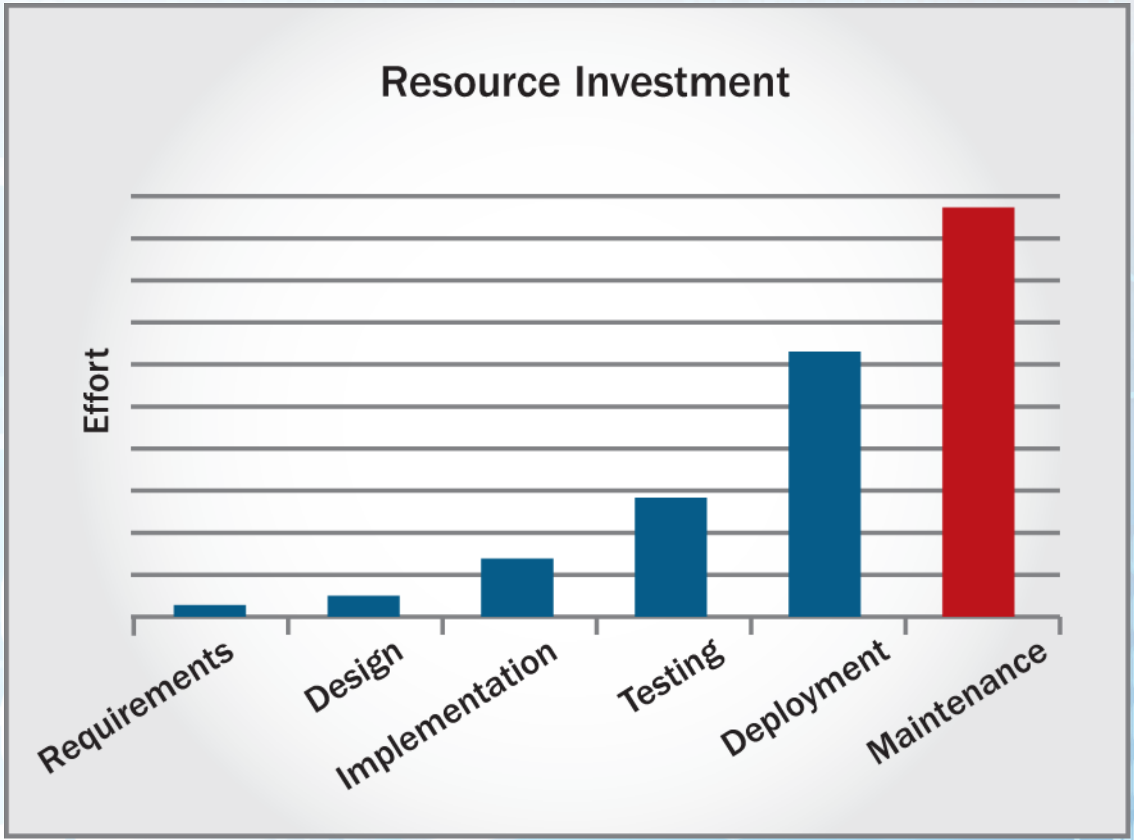


555-555-5555

555-555-0000
555-555-0001
555-555-0002
555-555-0003
555-555-0004
555-555-0005...

IV. “Build It In,” Not “Bolt It On”

IV. "Build It In," Not "Bolt It On"



IV. "Build It In," Not "Bolt It On"

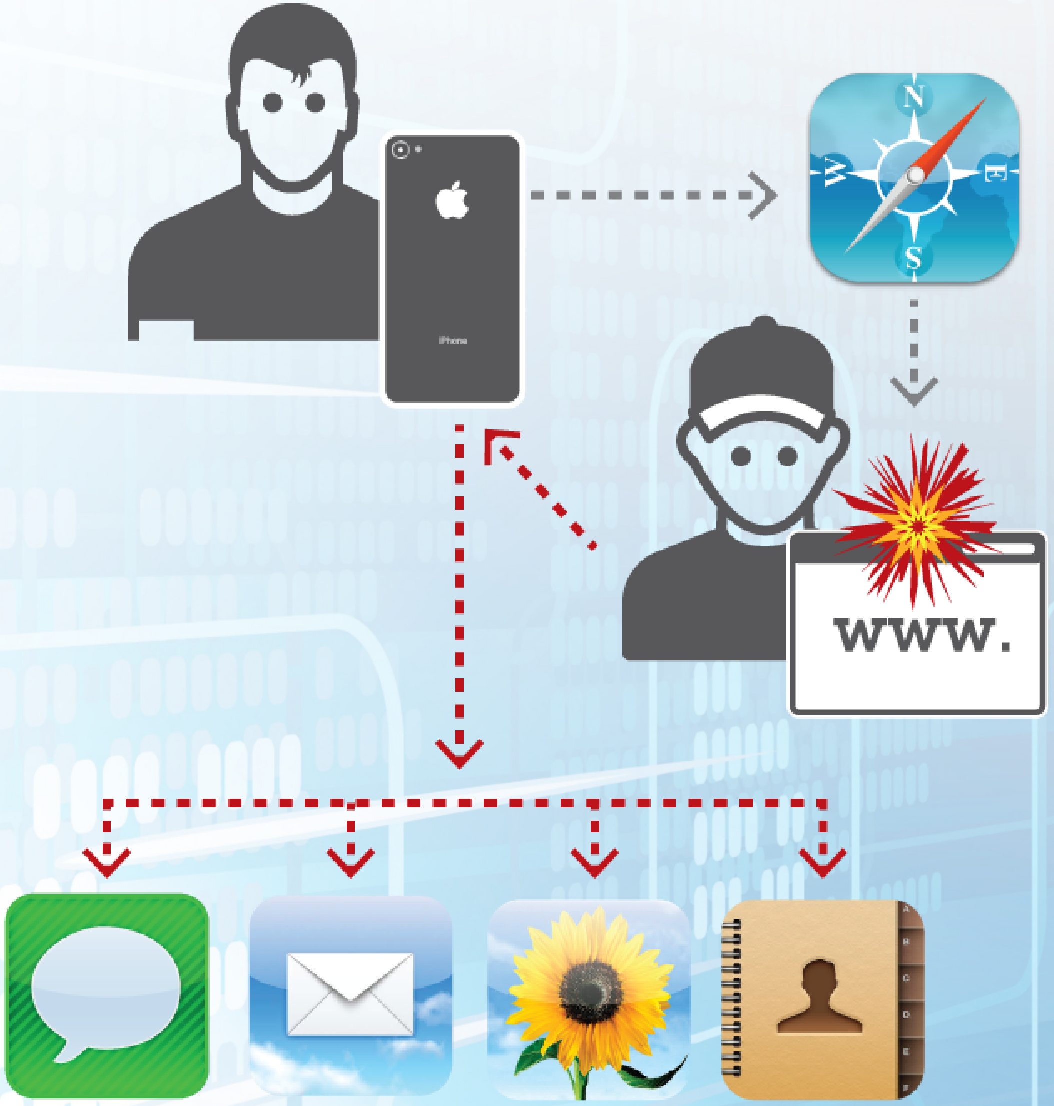
REQUIREMENTS	Determine business & user needs	Develop threat model
DESIGN	Define architecture	Design defense in depth
IMPLEMENTATION	Coding	Audit code
TESTING	System testing	White box vulnerability assessment
DEPLOYMENT	Customer roll-out	Configuration Guidance
MAINTENANCE	Resolve bugs	Iteration Hardening

IV. “Build It In,” Not “Bolt It On”

	Built In	Bolted On
Assessment cost	90%	100%
Assessment overhead	- - -	- - -
Mitigation cost / issue	1x	25x : application 300x : infrastructure

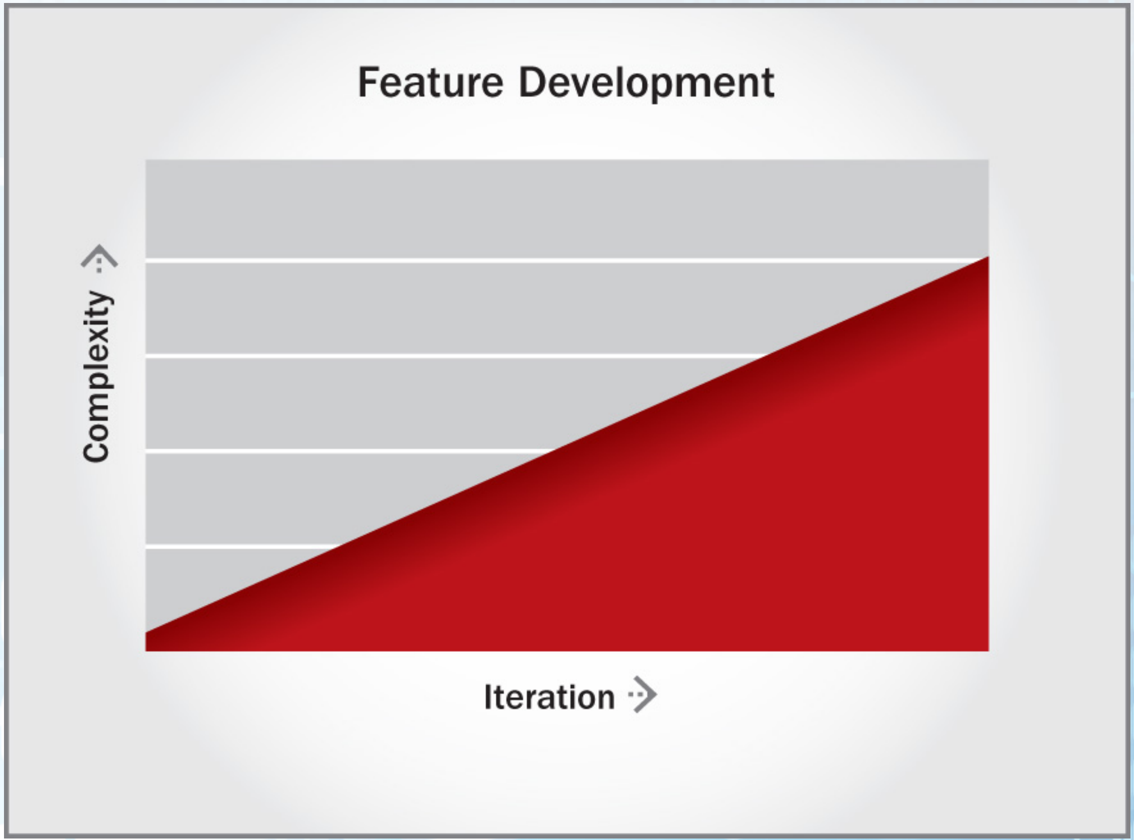
HACKED

iPhone

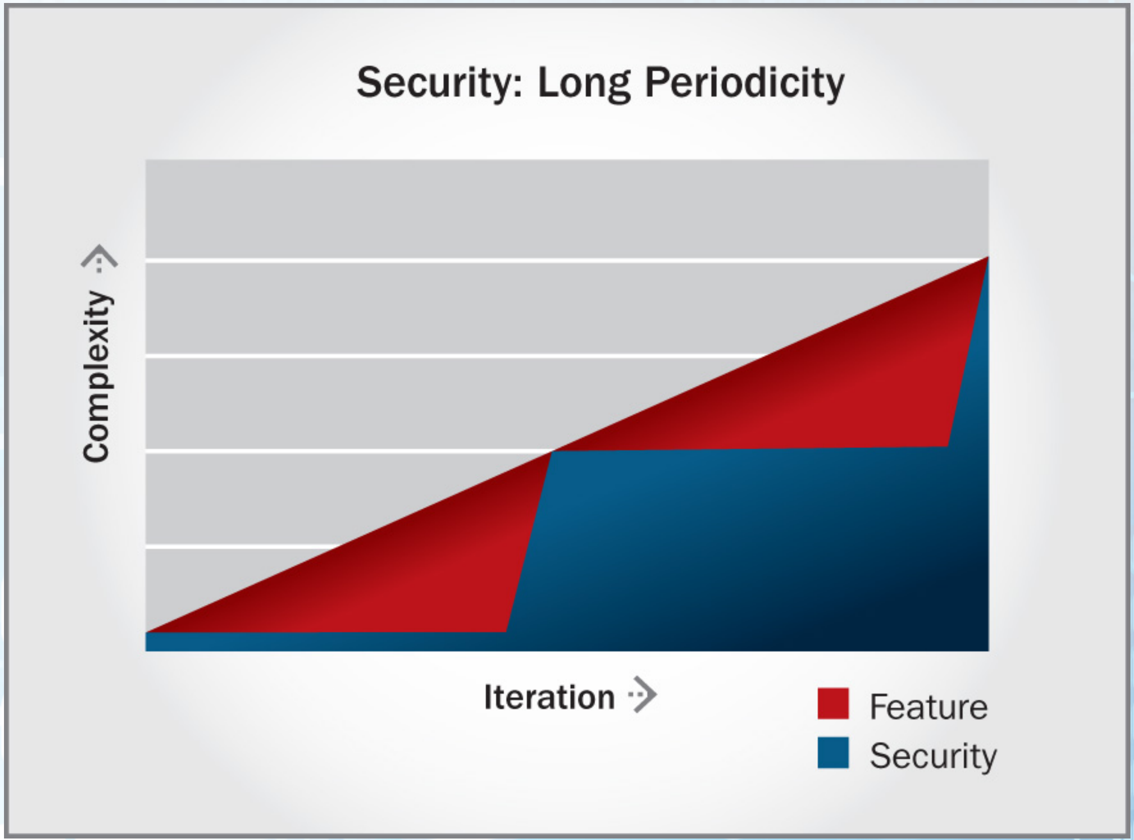

iPhone
N
W
E
S
www.

V. Security as Ongoing Process

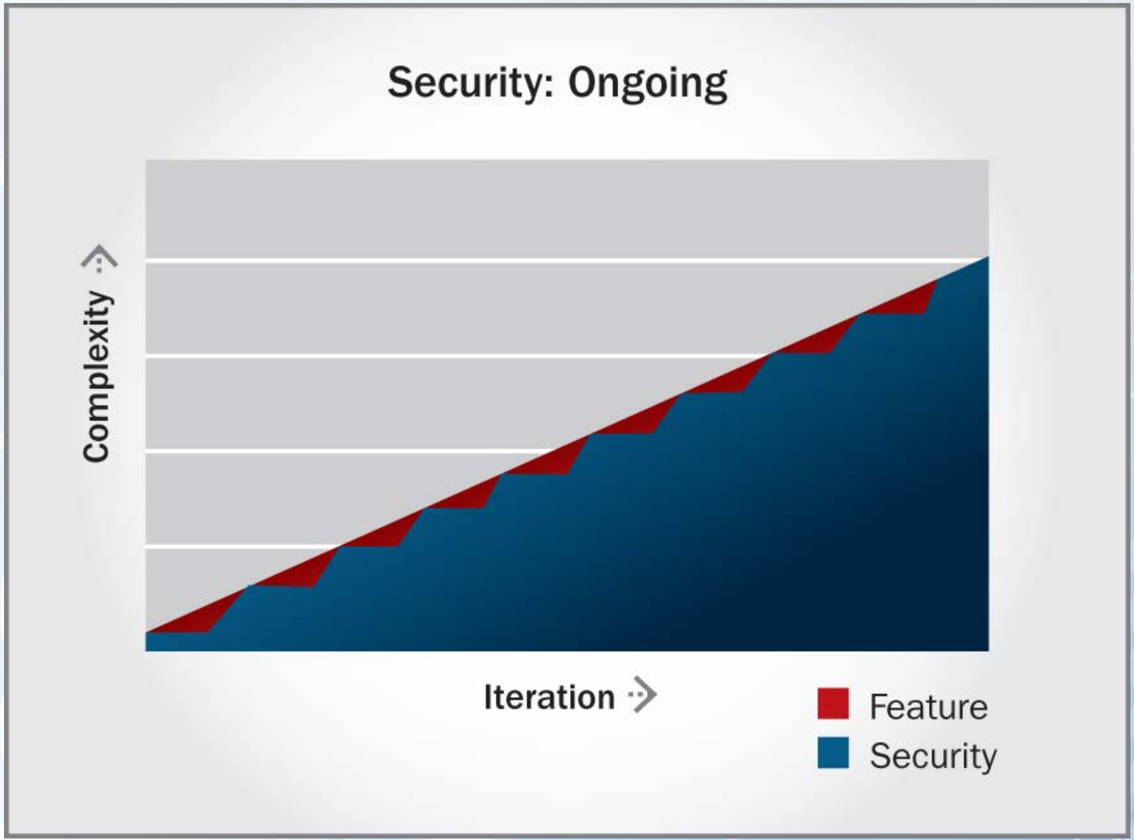
V. Security as Ongoing Process



V. Security as Ongoing Process

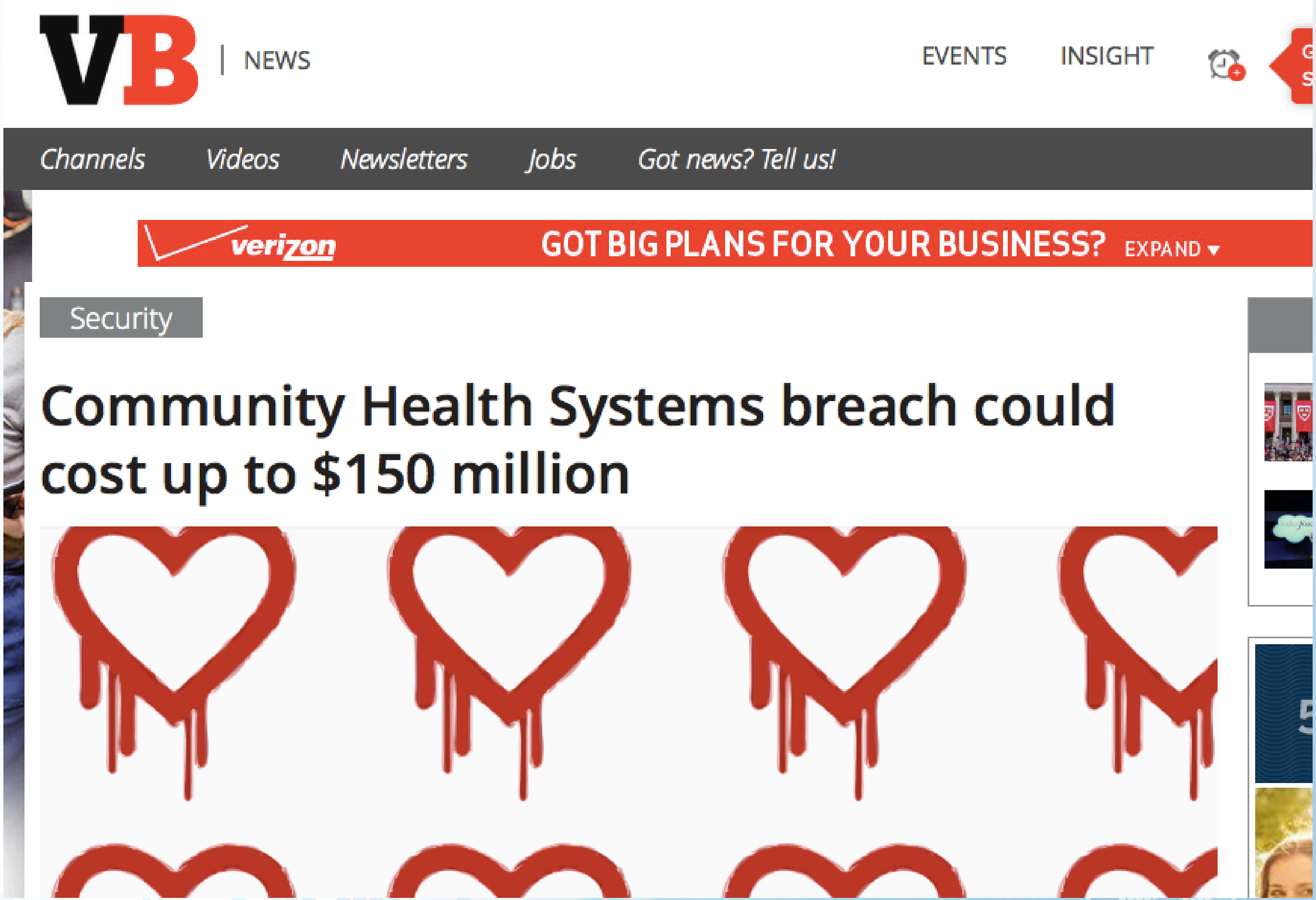


V. Security as Ongoing Process



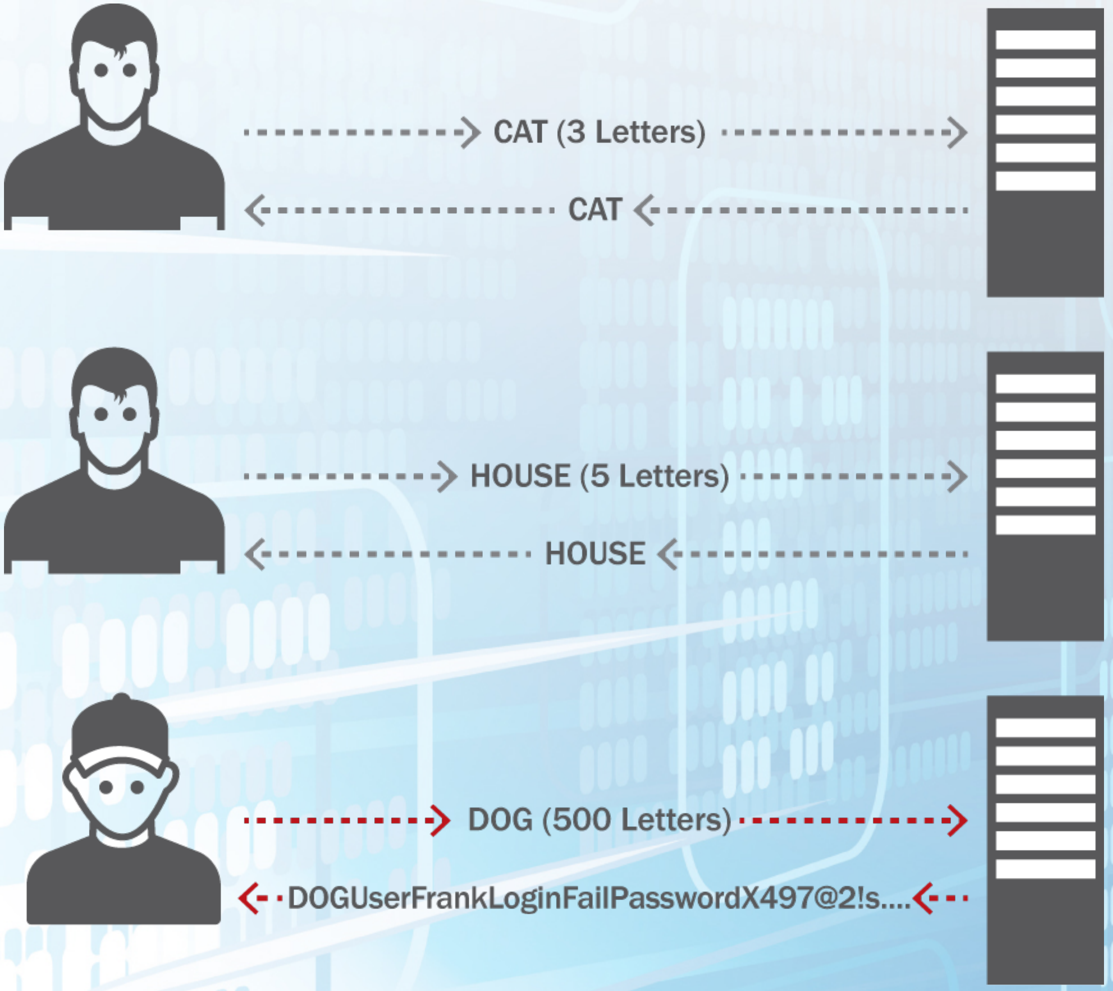
V. Security as Ongoing Process

	Yearly	Bi-yearly	Quarterly
Initial assessment cost	X	X	X
Full scope reassessment cost	90-95%	35-45%	20-30%
Full assessments / year	1	2	4
Cost / year	X (0.9)	X (0.7)	X (0.8)



Security

Community Health Systems breach could cost up to $150 million



CAT (3 Letters)

CAT

HOUSE (5 Letters)

HOUSE

DOG (500 Letters)

DOGUserFrankLoginFailPasswordX497@2!s....

Heartbleed Mitigations

PROVIDERS

- Update to patched version of OpenSSL
- Revoke all SSL certificates
- Get new certificates
- Update all credentials

USERS

- Test all providers, using a tool such as:

https://demo.securityevaluators.com/Heartbleed/

- Change passwords

Get Involved

ggentry@securityevaluators.com