

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Not Go Quietly: Surprising Strategies and Teammates to Adapt and Overcome

SESSION ID: STR-R01

David Etue

VP Corporate Development Strategy
SafeNet, Inc.
@djetue

Joshua Corman

Chief Technology Officer
Sonatype
@joshcorman



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Context



SafeNet



Sonatype

A story of a CISO...

- ◆ This presentation tell the story of a CISO
- ◆ THIS CISO is fictional...
- ◆ ...but all the stories are REAL examples from real security programs



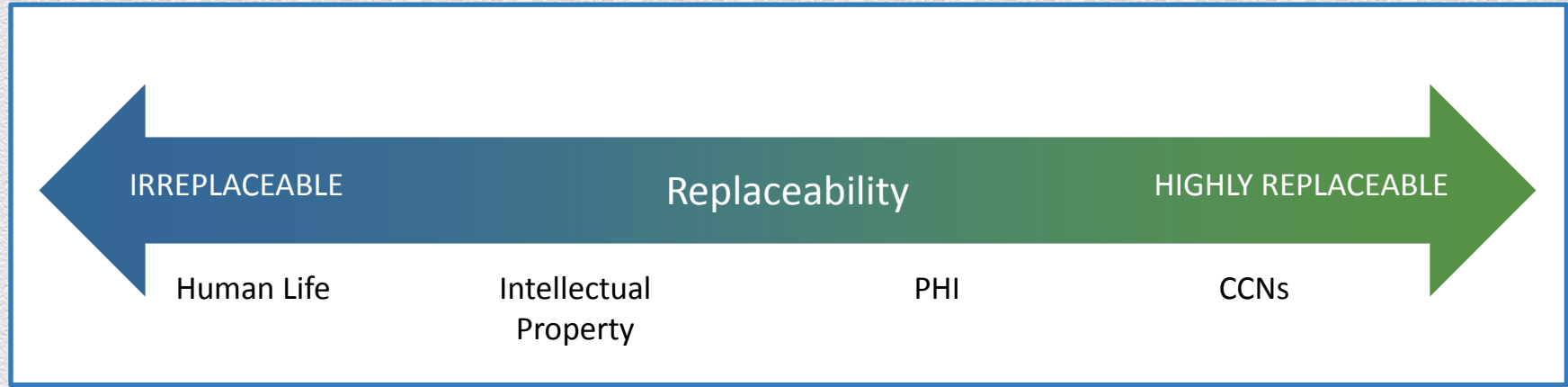
Depressed? You are not alone...



Forces of Constant Change



Consequences: Value & Replaceability



<http://blog.cognitivedissidents.com/2011/10/24/a-replaceability-continuum/>

Feel Like Surrendering?



A Modern Pantheon of Adversary Classes

WHO: Actor Classes

Nation States	Competitors	Organized Crime	Script Kiddies	Terrorists	"Hacktivists"	Insiders	Auditors
---------------	-------------	-----------------	----------------	------------	---------------	----------	----------

WHY: Motivations

Financial	Industrial	Military	Ideological	Political	Prestige
-----------	------------	----------	-------------	-----------	----------

WHAT: Target Assets

Credit Card #s	Web Properties	Intellectual Property	PII/Identity	Cyber Infrastructure	Core Business Processes
----------------	----------------	-----------------------	--------------	----------------------	-------------------------

HOW: Methods

"MetaSploit"	DoS	Phishing	Rootkit	SQLi	Auth	Exfiltration	Malware	Physical
--------------	-----	----------	---------	------	------	--------------	---------	----------

NOTE: More Complete Version @ <http://slidesha.re/1fgu6rb>

Profiling a Particular Actor

WHO: Actor Classes

Nation States	Competitors	Organized Crime	Script Kiddies	Terrorists	"Hacktivists"	Insiders	Auditors
---------------	-------------	-----------------	----------------	------------	---------------	----------	----------

WHY: Motivations

Financial	Industrial	Military	Ideological	Political	Prestige
-----------	------------	----------	-------------	-----------	----------

WHAT: Target Assets

Credit Card #s	Web Properties	Intellectual Property	PII/Identity	Cyber Infrastructure	Core Business Processes
----------------	----------------	-----------------------	--------------	----------------------	-------------------------

HOW: Methods

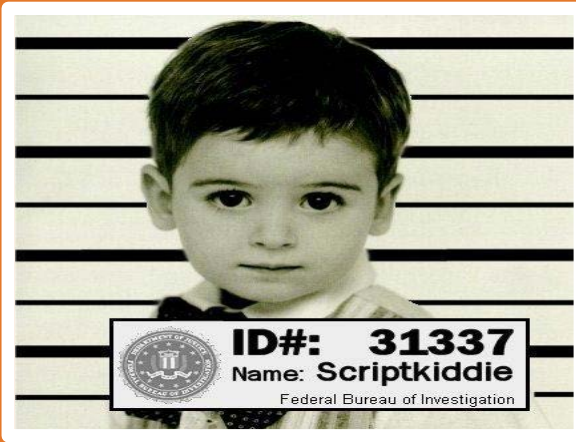
"MetaSploit"	DoS	Phishing	Rootkit	SQLi	Auth	Exfiltration	Malware	Physical
--------------	-----	----------	---------	------	------	--------------	---------	----------

NOTE: More Complete Version @ <http://slidesha.re/1fgu6rb>

Script Kiddies (aka Casual Adversary)

Script Kiddie

5



Skiddie

Profit, Prestige

CCN/Fungible

"MetaSploit", SQLi, Phishing

Organized Crime

Organized Crime

50



Organized Crime

Profit

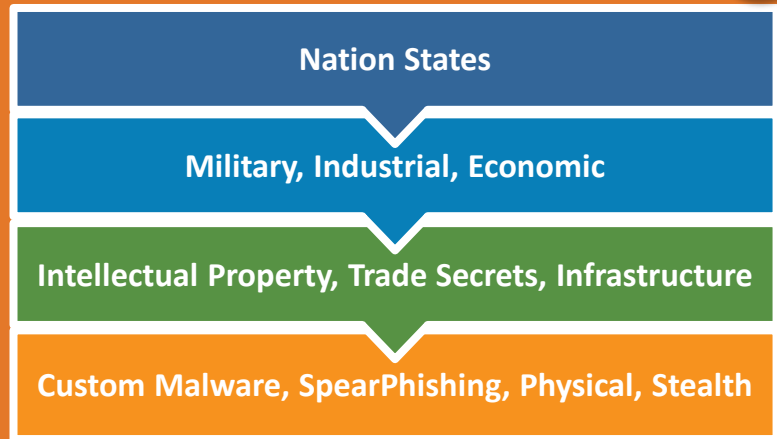
Fungible, Banking

Malware, Botnets, Rootkits

Nation States (Adaptive Persistent Adversaries)

Nation States

50



Hacktivists Chaotic Actors

Chaotic Actors

10



Chaotic Actors

Ideological and/or LULZ

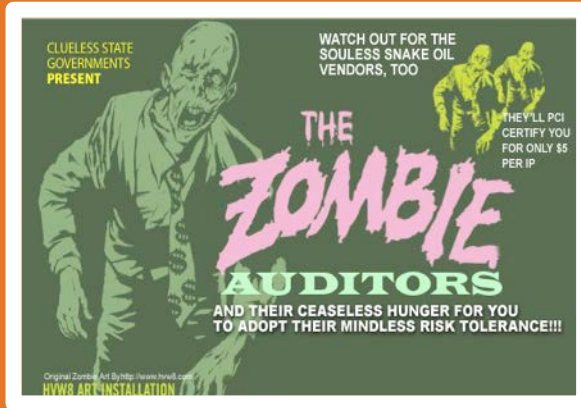
Web Properties, Individuals, Gov't Policy

DoS, SQLi, Phishing, Pranks

Auditors/Assessors/QSA

Auditors

1



Auditor

Profit, Compliance

ONLY "In Scope" E.g. CCN (Credit Card #s)

Checklist

Attacker Power - HD Moore's Law

- ◆ **Moore's Law:** Compute power doubles every 18 months
- ◆ **HDMoore's Law:** Casual Attacker Strength grows at the rate of MetaSploit



Do not go gentle into that not so good night...







Defensible Infrastructure





Gene Kim

MULTIPLE AWARD-WINNING CTO, RESEARCHER, VISIBLE OPS CO-AUTHOR, ENTREPRENEUR & FOUNDER OF TRIPWIRE



Operational Excellence

Defensible Infrastructure



Situational Awareness

Operational Excellence

Defensible Infrastructure





**Counter-
measures**

Situational Awareness

Operational Excellence

Defensible Infrastructure



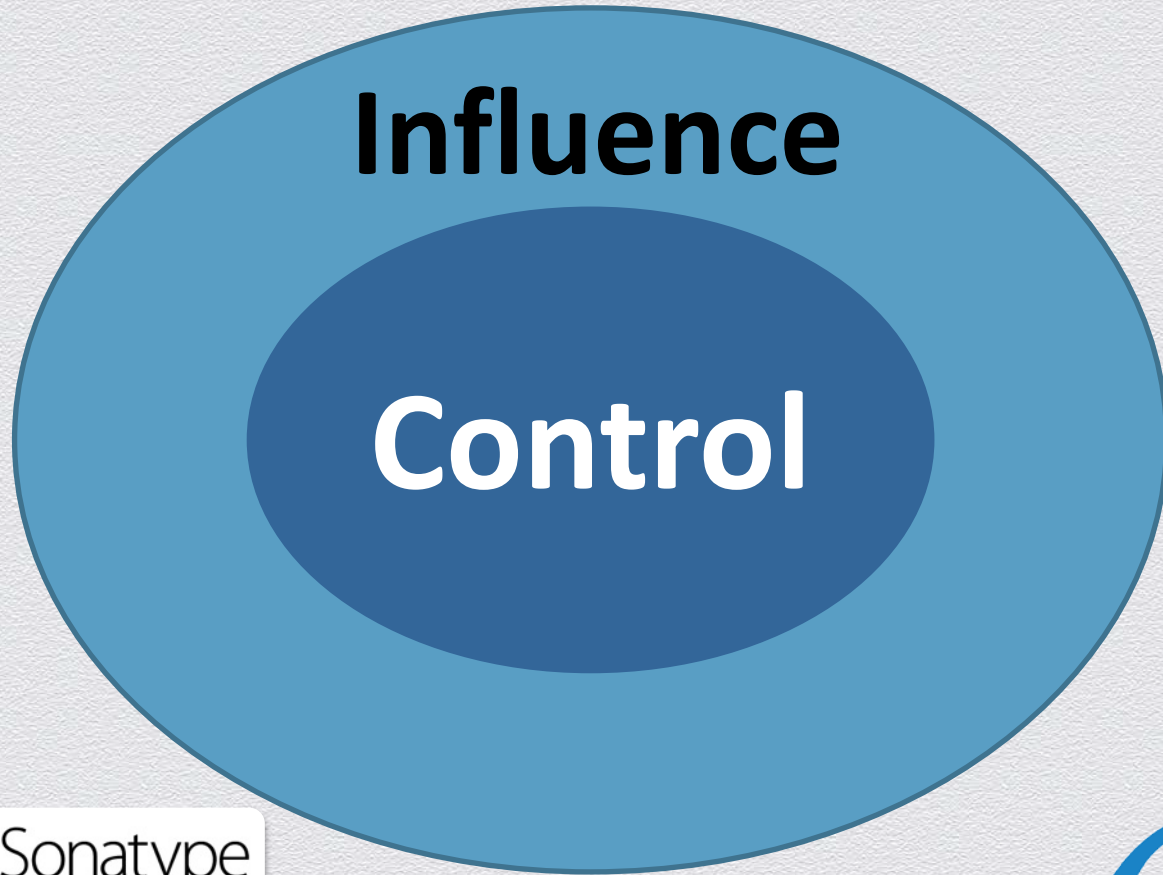


Sphere of Control



Control

Sphere of Influence vs. Control



“Rage, rage against the dying of the light”



Control “Swim Lanes”

Desired

- AV
- FW
- IDS/IPS
- WAF
- Log Mngt
- File Integrity
- Disk Encryption
- Vulnerability Assessment
- Multi-Factor Auth
- Anti-SPAM
- VPN
- Web Filtering
- DLP
- Anomaly Detection
- Network Forensics
- Advanced Malware
- NG Firewall
- DB Security
- Patch Management
- SIEM
- Anti-DDoS
- Anti-Fraud
- ...

Leverage Points

Compliance (1..n)

Productivity

“ROI”

Breach / QB sneak

Outcomes

PCI

PHI

“IP”

Web

...

Control & Influence “Swim Lanes”

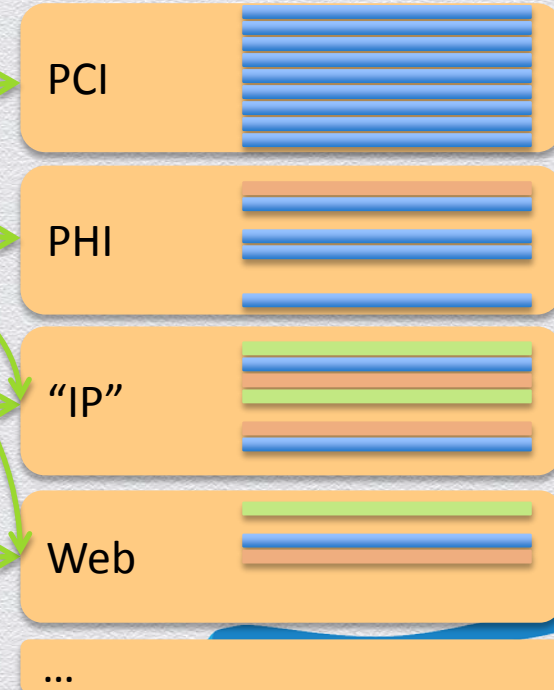
Desired



Leverage Points



Outcomes



Under-tapped Researcher Influence

Desired

AV
FW
IDS/IPS
WAF
Log Mngt
File Integrity
Disk Encryption
Vulnerability Assessment
Multi-Factor Auth
Anti-SPAM
VPN
Web Filtering
DLP
Anomaly Detection
Network Forensics
Advanced Malware
NG Firewall
DB Security
Patch Management
SIEM
Anti-DDoS
Anti-Fraud
...

Litigation

Legislation

Open Source

Hearts &
Minds

Academia

Leverage Points

Compliance (1..n)

Productivity

DevOps

"ROI"

Breach / QB sneak

"Honest Risk"

General Counsel

Procurement

Disruption

Outcomes

PCI

PHI

"IP"

Web

...

Its Easier with Teammates

Alone?



Team?



Surprising Teammates

Executives

CIO	CFO	General Counsel	CTO	R&D	Operations	Sales	Business Owner
-----	-----	-----------------	-----	-----	------------	-------	----------------



Supporting Cast

DevOps	Procurement	Compliance	Internal Audit	Risk Mgmt	Crisis Mgmt	Open Source	Academia	Gov't Affairs
--------	-------------	------------	----------------	-----------	-------------	-------------	----------	---------------

DEFENDER: General Counsel

General Counsel



25



General Counsel

Due Care, Defensible Risks

Intellectual Property, Trade Secrets, Sensitive

Policy, LDoS, Contracts, AttorneyClientPriv

DEFENDER: Procurement / Supply Chain

Procurement



Procurement

Cost Reduction, Employer Interests

All Things Procured: SaaS, COTS, Services

RFPs, T&Cs, SLAs, "Gating"

DEFENDER: Chief Information Officer

CIO



CIO

Stability, Order, Support Business

All Infrastructure

GRC, Standards, Policy, Change Mngt, Process

DEFENDER: Chief Technology Officer

CTO



CTO

Innovation, Differentiation, Adoption

IP, Trade Secrets, Code, Platforms

SDLC, Standards, Code/Tech Selection, Research

DEFENDER: Chief Financial Officer



DEFENDER: Senior Vice President, Sales

SVP Sales



15



SVP Sales

Retire Quota, Drive Revenue

Customer Data, "Goods"

Customer Compliance, \$DEALS, Roadmaps

DEFENDER: Internal Audit

Internal Audit



Internal Audit

Strict Compliance

Scoped Data & Environments

CheckLists, Interviews, Policies

DEFENDER: DevOps

DevOps



DevOps

Faster Faster, Velocity, Efficiency

Code, Deploys, Environments

Automate, Orchestrate, ChaosMonkey, Teamwork

Counter-measures



Situational Awareness



Operational Excellence



Defensible Infrastructure



Battle: PCI Compliance

Auditors 05

Script Kiddie 01



ID#: 31337
Name: Scriptkiddie
Federal Bureau of Investigation

Skiddie


Profit, Prestige

CCN/Fungible

"MetaSploit", SQLi, Phishing



Internal Audit 05



Internal Audit

Strict Compliance

Scoped Data & Environments

CheckLists, Interviews, Policies

AT DEFEAT

Battle: Intellectual Property

Nation State 50

ADAPTIVE	PERSISTENT
	UNDETERRED
ADVERSARIES	
GOAL-ORIENTED	PATIENT
DELIBERATE	

Nation State / Espionage

Military, Industrial, Economic

IP, Trade Secrets, Infrastructure

Custom Malware, SpearPhishing,
Physical, Stealth



Internal Audit 05

DEFEAT

A photograph of a woman in a black blazer and white shirt, sitting at a desk and working on a laptop. A blue credit card is visible in the background.

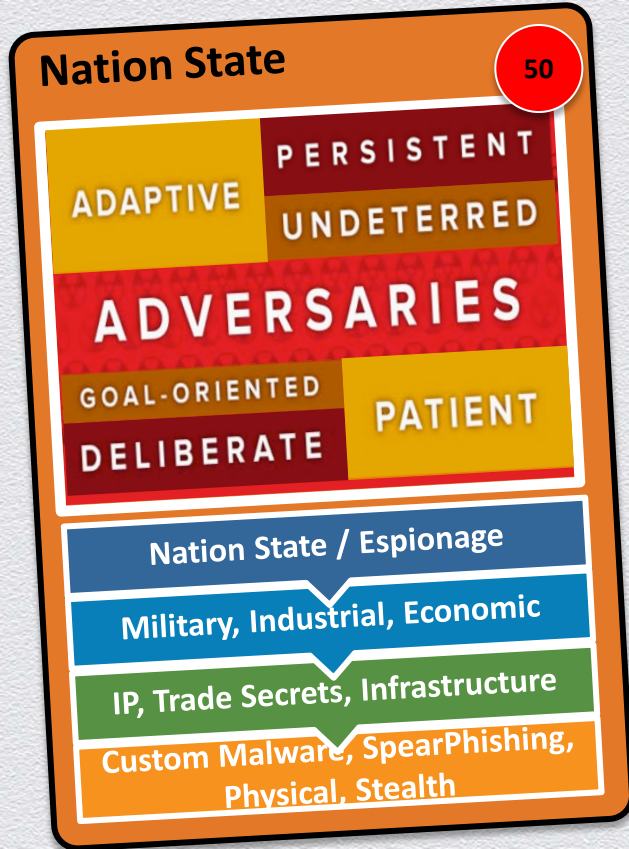
Internal Audit

Strict Compliance

Scoped Data & Environments

CheckLists, Interviews, Policies

Battle: Intellectual Property Round 2



Battle: Web Properties

DEFEAT

Chaotic Actors +20



Chaotic Actors

Ideological and/or LULZ

Websites, People, Gov't Policy


DoS, SQLi, Phishing, Pranks



DEFEAT

Procurement 20

DevOps 50



DevOps

Faster Faster, Velocity, Efficiency

Code, Deploys, Environments

Automation, Orchestration, Teams

Case Study: Gaining Situational Awareness

- ◆ CISO: "There is a difference between reacting and hunting. If you're reacting, you're done. We knew we had to go hunting, and that meant we had to do things differently."
- ◆ Teammates:
 - ◆ Business Owner: Understood adversary
 - ◆ Operations: Deploy BigFix for Power Management (GREEN!) AND security
 - ◆ Compliance: Repurposed SIEM and other compliance tools
 - ◆ CIO: Driven by Productivity
- ◆ Result: One of the most advanced automated attack identification and classification systems developed at the time



Case Study: Using Customers To Your Advantage

- ◆ Large Financial CISO: “Only getting investment in InfoSec where required by ‘compliance’”
- ◆ Teammates:
 - ◆ VP of Sales: Worked with to include customer contractual obligations in scope of compliance
 - ◆ General Counsel: Determine committed customer contractual obligations, measured risk
 - ◆ Audit: Added customer contractual obligations to scope of audit
- ◆ Result: Significantly increase in information security investment—demanded by Sales

Case Study: “DevOps” Chaotic Good

- ◆ F100 Insurance “Chaos Monkey”: “We spend ZERO on securing anything but mandatory PCI controls & scope; therefore I must infect the org w/ Card Data.”
- ◆ Teammates:
 - ◆ LOB CTO: WAFaaS can accelerate your PCI 6.6 & TimeToMarket
 - ◆ General Counsel: We must take reasonable steps to keep our secrets secret
 - ◆ CIO: If we fund a Visible Ops program, we’ll run more efficiently & be complaint
- ◆ Result: More sane/balanced security posture, more agility/efficient IT

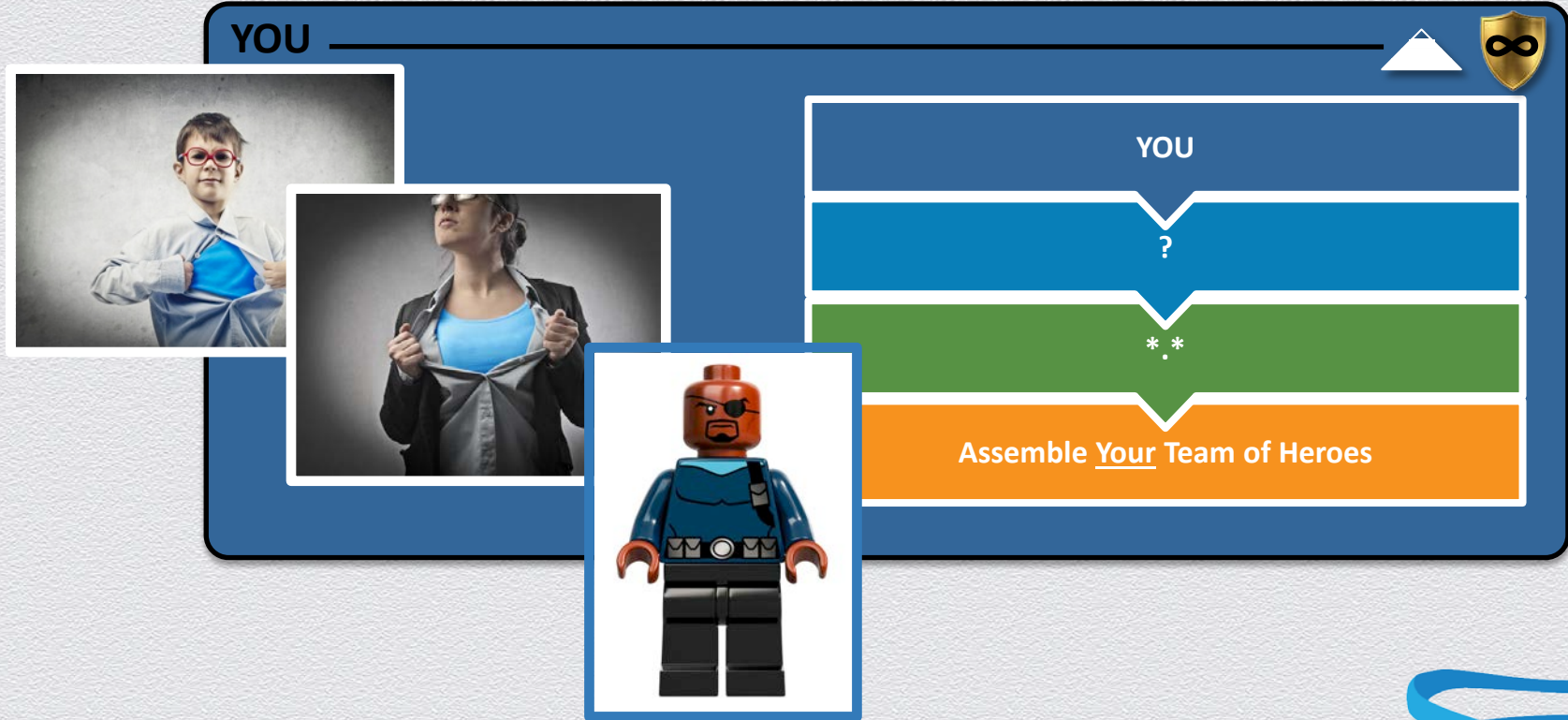
Case Study: Changing Report Structure

- ◆ CISO: “Reporting into CIO ignored Data Security and 3rd Party Risk”
- ◆ Teammates:
 - ◆ General Counsel: Heavier concern focus Data Classification/Security
 - ◆ Procurement: More stringent 3rd Party Service Provider Security, Ts & Cs
- ◆ Greater Board Level Visibility & Access to Drive Table Top Exercises

Case Study: Adversary Driven!

- ◆ Large Scale European Financial Services CISO: “Despite a large scale information security investment, we were still losing”
- ◆ Teammates:
 - ◆ Business Owners: Determine likely adversaries—organized crime for financial fraud
 - ◆ Risk: Determine potential financial losses due to various fraudulent attacks
 - ◆ Application Development: Shared investment with information security to tie broad information security controls with application specific security and fraud prevention
- ◆ Result: Significantly more effective information security program resulting in lower fraud without significant increase in investment

CISO: The New “Nick Fury”



Apply

- ◆ Who Is Your Team?
- ◆ Identify at least one opportunity to leverage a new swim lane
- ◆ Identify at least one new teammate to recruit and make a hero
- ◆ Identify one opportunity this year to influence each layer of the pyramid



Everyone Has The Chance To Be the Hero
In Their Own Story!

Thank You & Additional Resources

- ◆ Adversary ROI: [[SlideShare](#)] [[RSA US 2012 Online on YouTube](#)]
- ◆ Supply Chain Security: Policy and Program Development [[Free Research from IANS](#)]
- ◆ Rugged Software – Are you Rugged? [[Website](#)]
- ◆ [Do not go gentle into that good night](#) by Dylan Thomas

David Etue
@djetue

Joshua Corman
@joshcorman



RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

**Back-Up
Will Delete by Final**

Internal Audit



05



Internal Audit

Strict Compliance

Scoped Data & Environments

CheckLists, Interviews, Policies

DevOps



50



DevOps

Faster Faster, Velocity, Efficiency

Code, Deploys, Environments

Automation, Orchestration, Teams

Risk Management



??



Risk Management

Support Business Intent

Risk Identified & Prioritized Assets

Risk Models, Metrics, "TableTops"

CTO



20



CTO

Innovation, Adoption

IP, Trade Secrets, Code, Platforms

SDLC, Research, Tech Selection

CFO



05



CFO

Responsible & Lawful Fiduciary

Financials Integrity, "Material"

Audit, Process, "Purse Strings"

SVP Sales



15



SVP Sales

Retire Quota, Drive Revenue

Customer Data, "Goods"

Customer Compliance & \$DEALS

General Council



20



General Counsel

Due Care, Defensible Risks

IP, Trade Secrets, Sensitive

Policy, Contracts, AttorneyClientPriv

Procurement



20



Procurement

Cost Reduction, Employer Interests

All Things Procured: COTS, Services

RFPs, T&Cs, SLAs, "Gating"

CIO



20



CIO

Stability, Order, Support Business

All Infrastructure

GRC, Policy, Change Mngt

Nation State

50

ADAPTIVE

PERSISTENT
UNDETERRED

ADVERSARIES

GOAL-ORIENTED

DELIBERATE

PATIENT

Nation State/Espionage

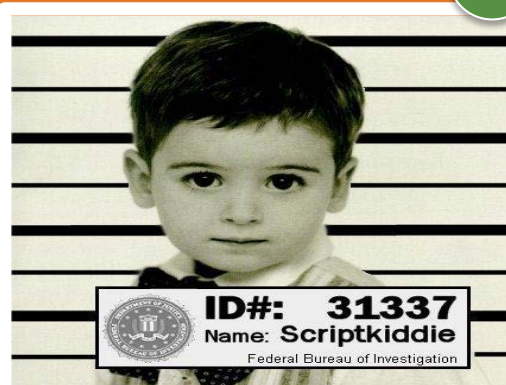
Military, Industrial, Economic

IP, Trade Secrets, Infrastructure

Custom Malware, Stealth, *.*

Script Kiddie

05



Skiddie

Profit, Prestige

CCN/Fungible

"MetaSploit", SQLi, Phishing

Organized Crime

50



Organized Crime

Profit

Fungible, Banking

Malware, Botnets, Rootkits

Chaotic Actors

10



Chaotic Actors

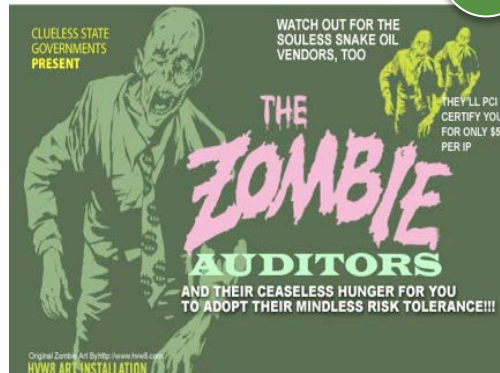
Ideological and/or LULZ

Websites, People, Gov't Policy

DoS, SQLi, Phishing, Pranks

Auditors

01



Auditor

Profit, Compliance

ONLY "In Scope" (Credit Card #s)

Checklist