

# Conventional Defenses + Unconventional Adversaries == ???

Joshua Corman  
Director, Security Intelligence  
@joshcorman

## FRESHLY OLD: About Joshua Corman

---

- Research Director, Enterprise Security for The 451 Group (Oct '09)
  - Former Principal Security Strategist [IBM ISS]
  - Sold stealth custom malware start-up to ISS in 2002
  
- Industry Experience:
  - Expert Faculty: The Institute for Applied Network Security (IANS)
  - 2009 NetworkWorld [Top 10 Tech People to Know](#)
  - Co-Founder of “Rugged Software” [www.ruggedsoftware.org](http://www.ruggedsoftware.org)
  
- Things I’ve been researching:
  - Compliance vs Security
  - Disruptive Innovations (Virtualization, Cloud, Mobility)
  - The Economics of Information Security
  - Politically motivated Cyber (APT/APA/SMT)
  - Comprehensive Data Security



# Agenda

---

Late Breaking News!

Surviving a Zombie Apocalypse

APTs and Adaptive Persistent Adversaries

The Rise of Chaotic Actors: Understanding Anonymous

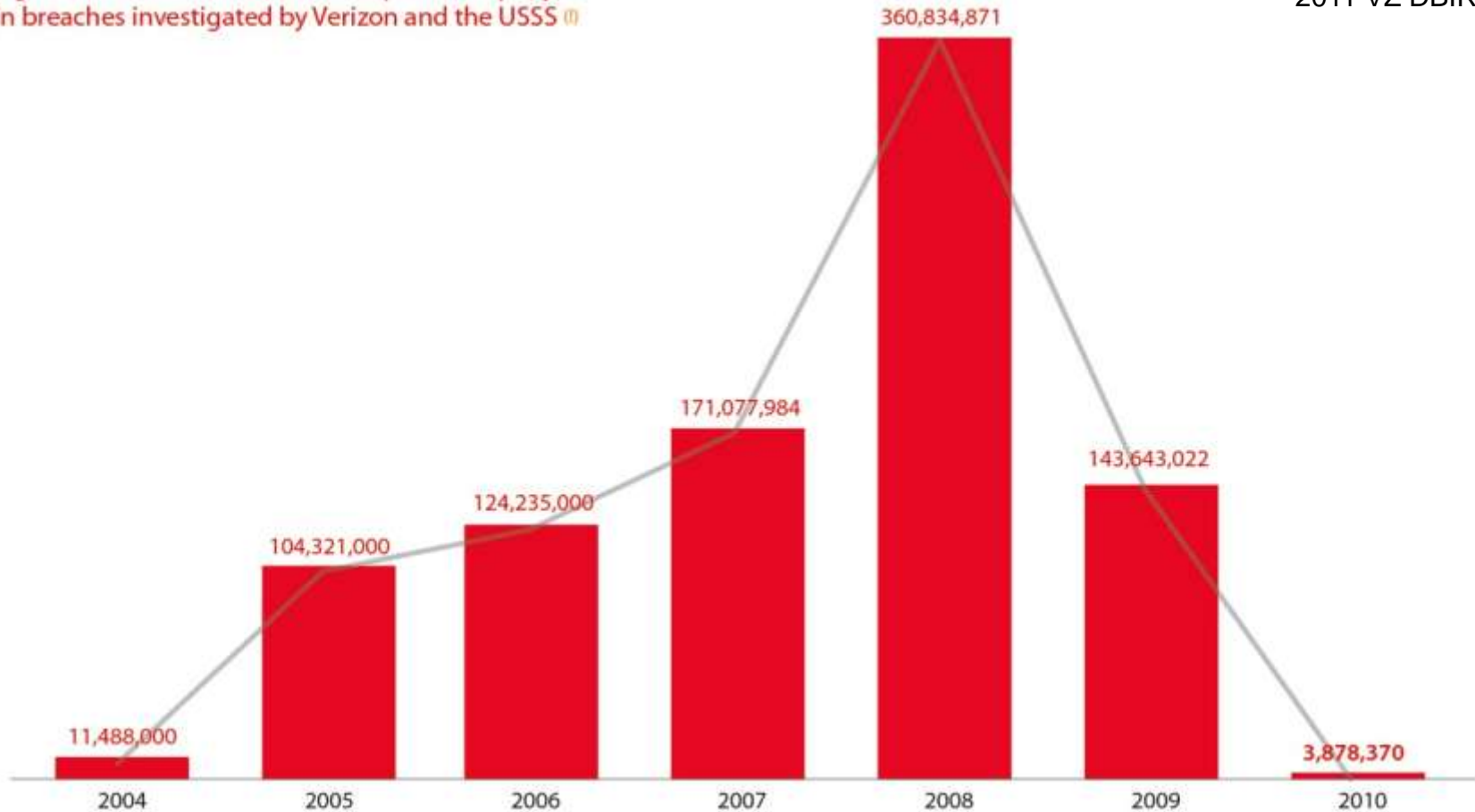
Rugged...

MISSION ACCOMPLISHED!

(no – not really)

Figure 33. Number of records compromised per year in breaches investigated by Verizon and the USSS

2011 VZ DBIR



All-Time High # of Incidents

All-Time Low # of Breached Records

Higher Value Records

All but one thing got worse

MOST cases SMB

	<b>2009</b> <b>141 incidents</b>	<b>2010</b> <b>761 incidents</b>	<b>Delta</b>
Intellectual Property	10	41	31
National Security Data	1	20	19
Sensitive Organizational	13	81	68
System Information	ZERO	41	41

## 2010 Unholy Trinity:

- Google.cn and Operation Aurora
- Stuxnet
- Bradley Manning/WikiLeaks (and Operation Payback)



## 2011:

- Anonymous
- EMC/RSA SecurID
- Sony's Punishment Campaign
- LulzSec
- Lockheed
- IMF



ANONYMOUS



PLAYSTATION®  
Network

---

***20 Slides  
x 20 Seconds  
(6 min 40 sec)***

Joshua Corman  
@joshcorman  
Research Director  
Enterprise Security



RSA PechaKucha Happy Hour

---

# PREPARE



# HOLD THE LINE! ZOMBIES!



# Why Zombies Love PCI: or “No Zombie Left Behind Act”

## SPEAKER:

Joshua Corman  
Research Director  
Enterprise Security  
The 451 Group



PechaKucha Happy Hour





Hungry

Persistent

1 at a time vs...

Why Zombies?

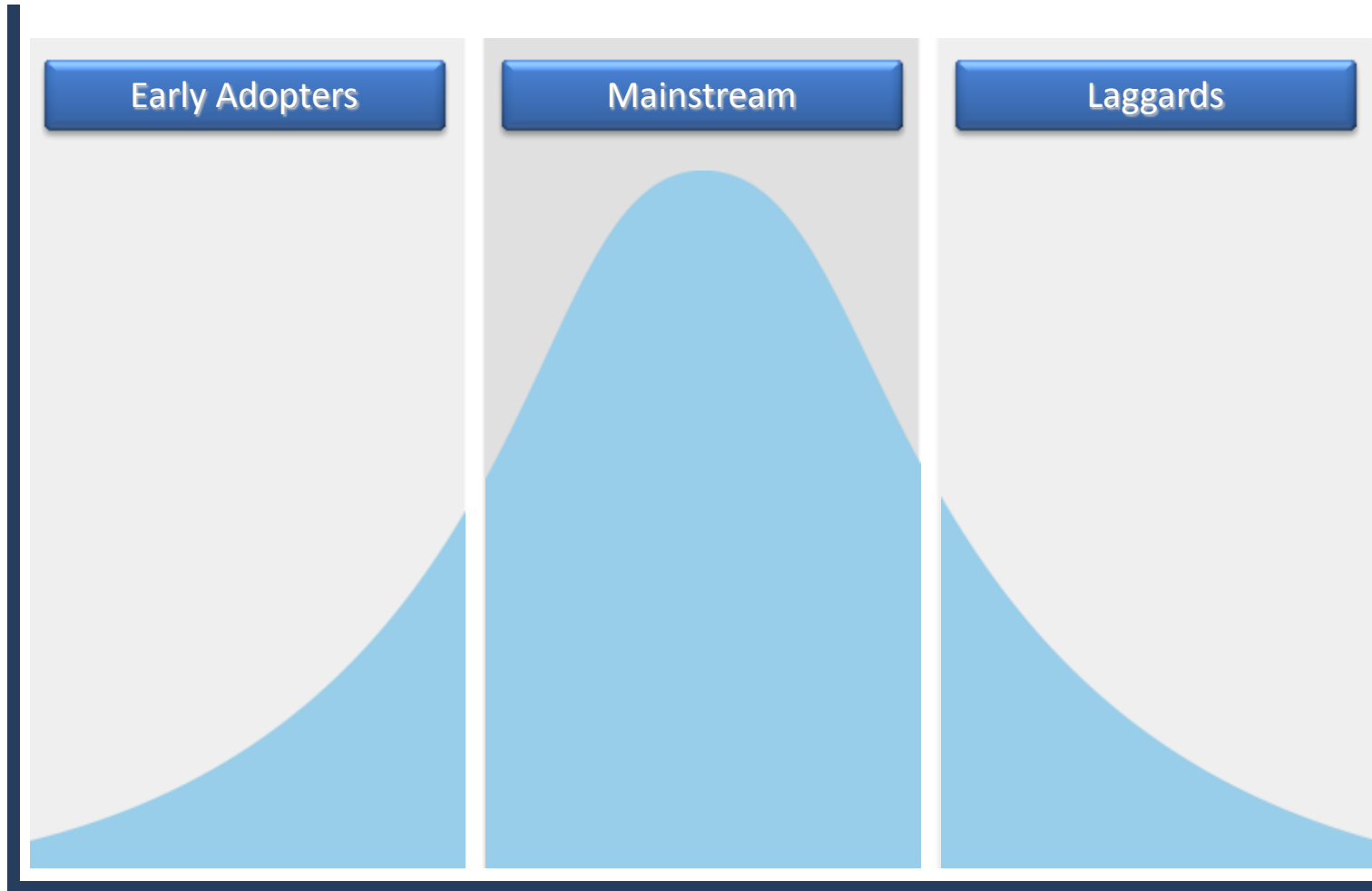
# HOW DANGEROUS IS A ZOMBIE?

## ZOMBIE TYPE

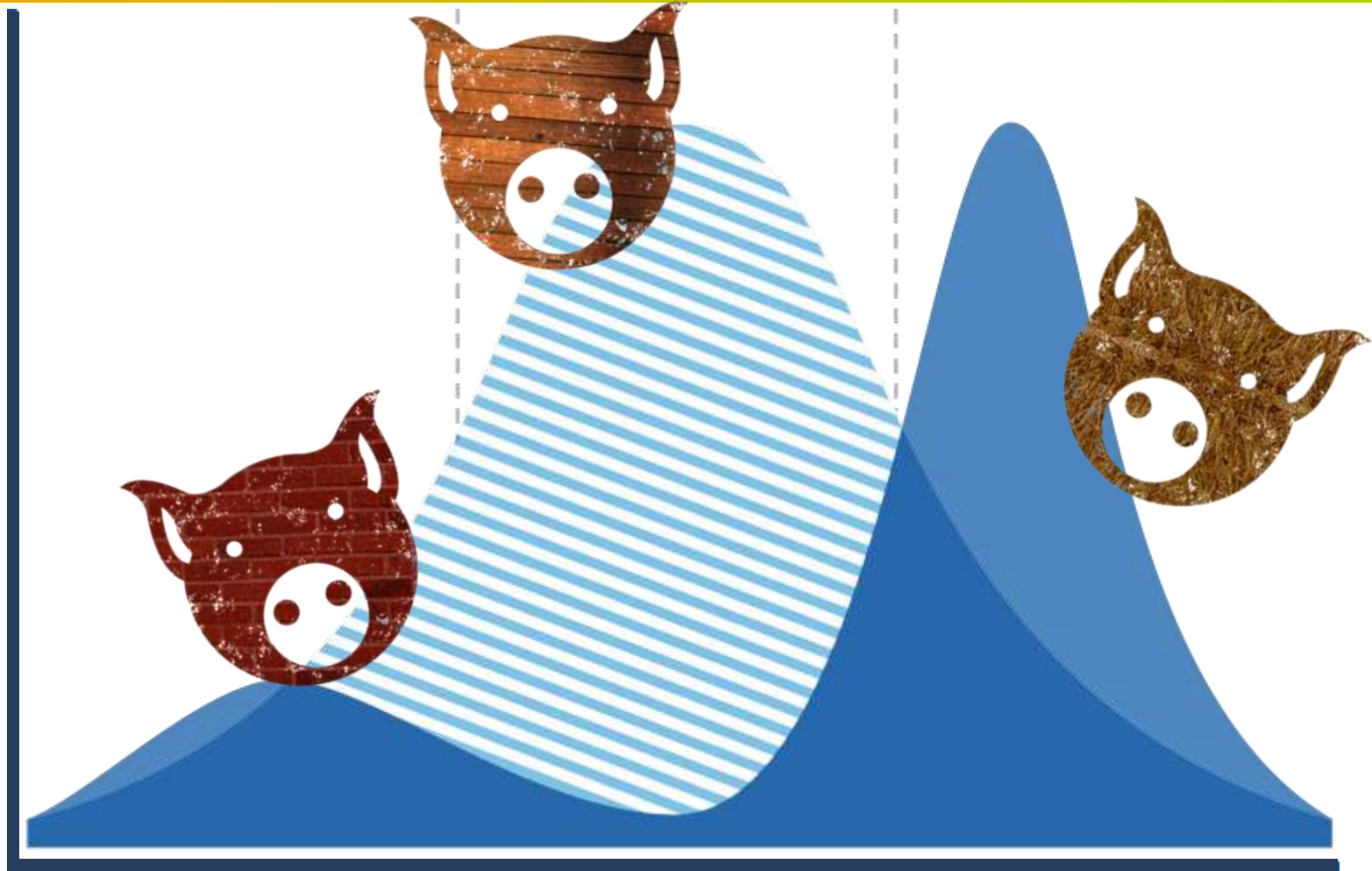
- ⊙ = UNDEAD
- ◻ = DISEASED
- △ = POSSESSED



# Is PCI The No Child Left Behind Act for Information Security?



# When “good enough”... isn’t



# It's all about Zombies



# It's all about Zombies



the 451 group

# Disruptive Changes





# Evolving Threat: Adaptive Persistent Adversaries



# Fear the auditor more than the attacker

CLUELESS STATE  
GOVERNMENTS  
**PRESENT**

WATCH OUT FOR THE  
SOULESS SNAKE OIL  
VENDORS, TOO



THEY'LL PCI  
CERTIFY YOU  
FOR ONLY \$5  
PER IP

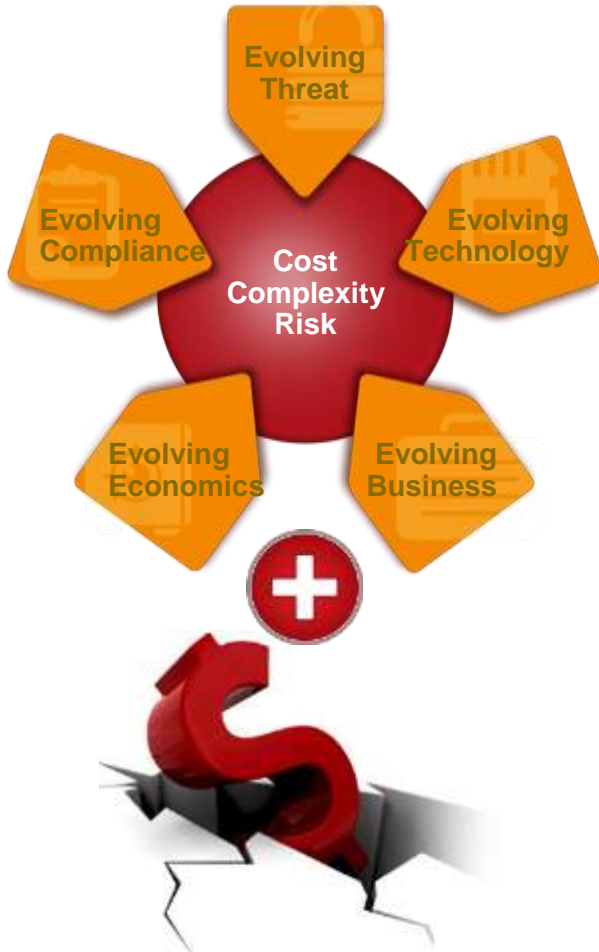
# THE ZOMBIE AUDITORS

AND THEIR CEASELESS HUNGER FOR YOU  
TO ADOPT THEIR MINDLESS RISK TOLERANCE!!!

Original Zombie Art By <http://www.hvw8.com>

**HVW8 ART INSTALLATION**

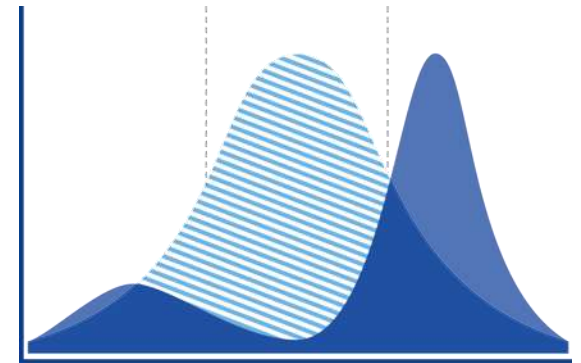
# We broke the Information Security Market



HIPAA  
HITECH  
SOX  
GLB



PCI DSS COMPLIANT



80/20

# Thriller



1984

1994

2004

2014?

Sony Walkman

Sony Discman

iPod

?





94%

89%

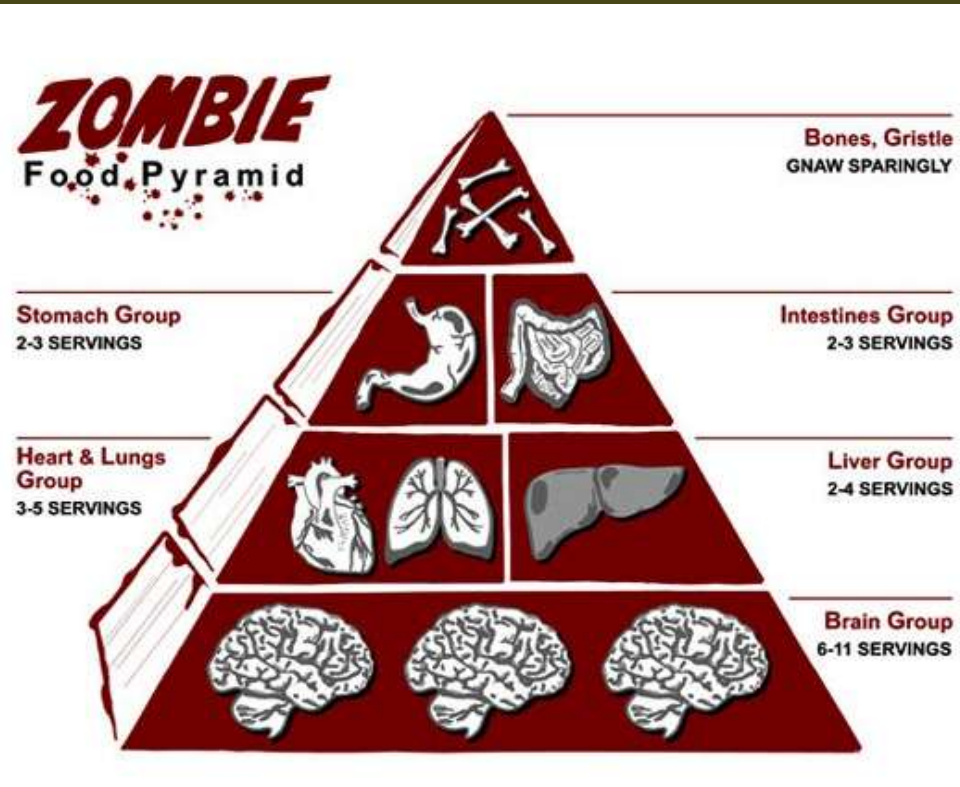
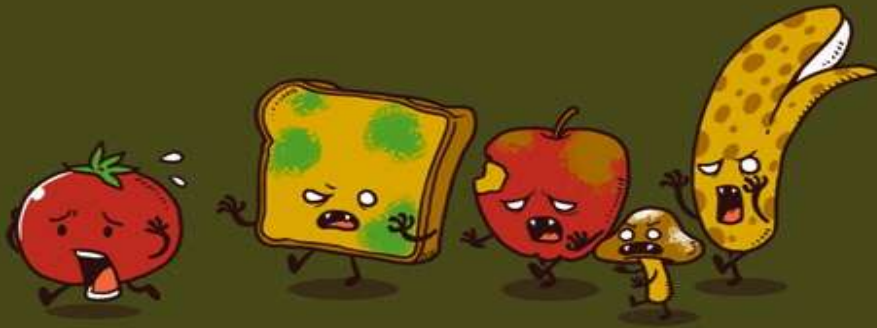
0%



# 2010 DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service.





# Survival Guide/Pyramid



[www.ruggedsoftware.org](http://www.ruggedsoftware.org)



Defensible Infrastructure



the 451 group

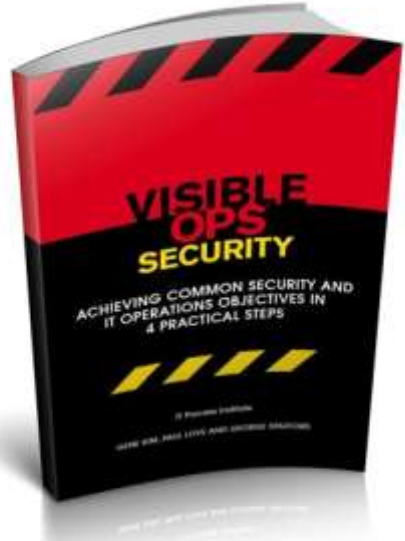


# Survival Guide/Pyramid



**Gene Kim**

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



Operational Discipline

Defensible Infrastructure



the 451 group

# Survival Guide/Pyramid



Situational Awareness

Operational Discipline

Defensible Infrastructure



the 451 group

# Survival Guide/Pyramid

Countermeasures

Situational Awareness

Operational Discipline

Defensible Infrastructure



[jcorman@the451group.com](mailto:jcorman@the451group.com)

@joshcorman

Hungry

Persistent

1 at a time vs...



Surviving The Zombie Apocalypse

# Evolving Threat: Adaptive Persistent Adversaries



**ORDER**

**DISORDER**

**GOOD**

**LAWFUL GOOD**



**NEUTRAL GOOD**

**CHAOTIC GOOD**

**LAWFUL NEUTRAL**

**TRUE NEUTRAL**

**CHAOTIC NEUTRAL**



**EVIL**

**LAWFUL EVIL**

**NEUTRAL EVIL**

**CHAOTIC EVIL**



the **451** group

# Social-Engineer.org

## Security Through Education

Social-Engineer.Org : Security Through Education



[Home](#) [Blog](#) [Framework](#) [Podcast](#) [Newsletter](#) [Resources](#) [CTF](#) [The Team](#) [Sponsors](#) [Contact](#)

*"The basic tool for the manipulation of reality is the manipulation of words."*

## The Official Social Engineering Portal

Social Engineering (SE) is both incredibly complex and amazingly simple.

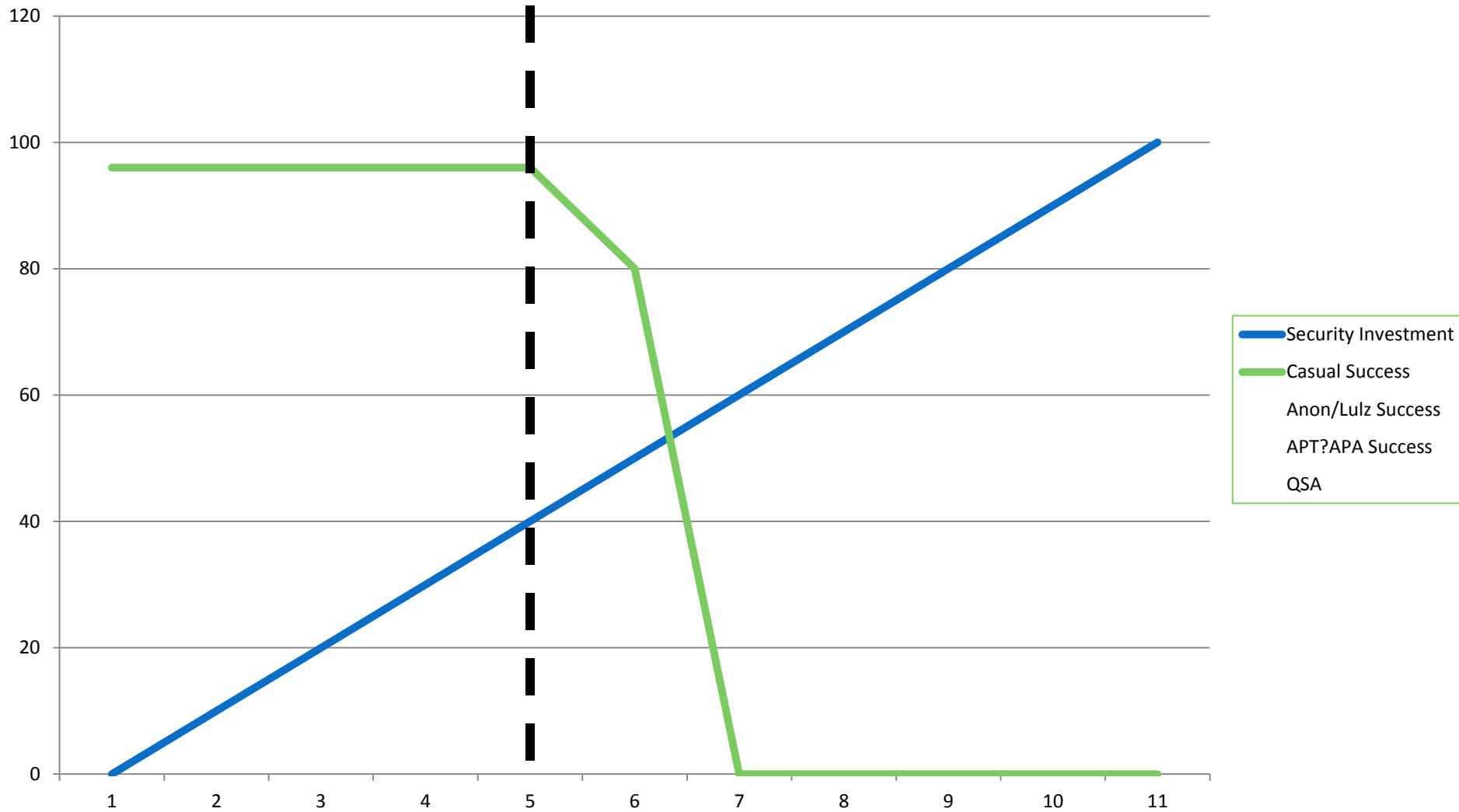
What really is social engineering? We define it as the act of manipulating a person to accomplish goals that may or may not be in the "target's" best interest. This may include [obtaining information](#), gaining access, or getting the target to take certain action.

Due to the mystery surrounding this dark art many people are afraid of it, or they feel they will never be able to accomplish a successful social engineering test. However, every time you try to get someone to do something that is in your interest, you are engaging in social engineering. From children trying to get a [toy from their parents](#) to adults trying to land a job or score the big promotion, all of it is a form of social engineering.

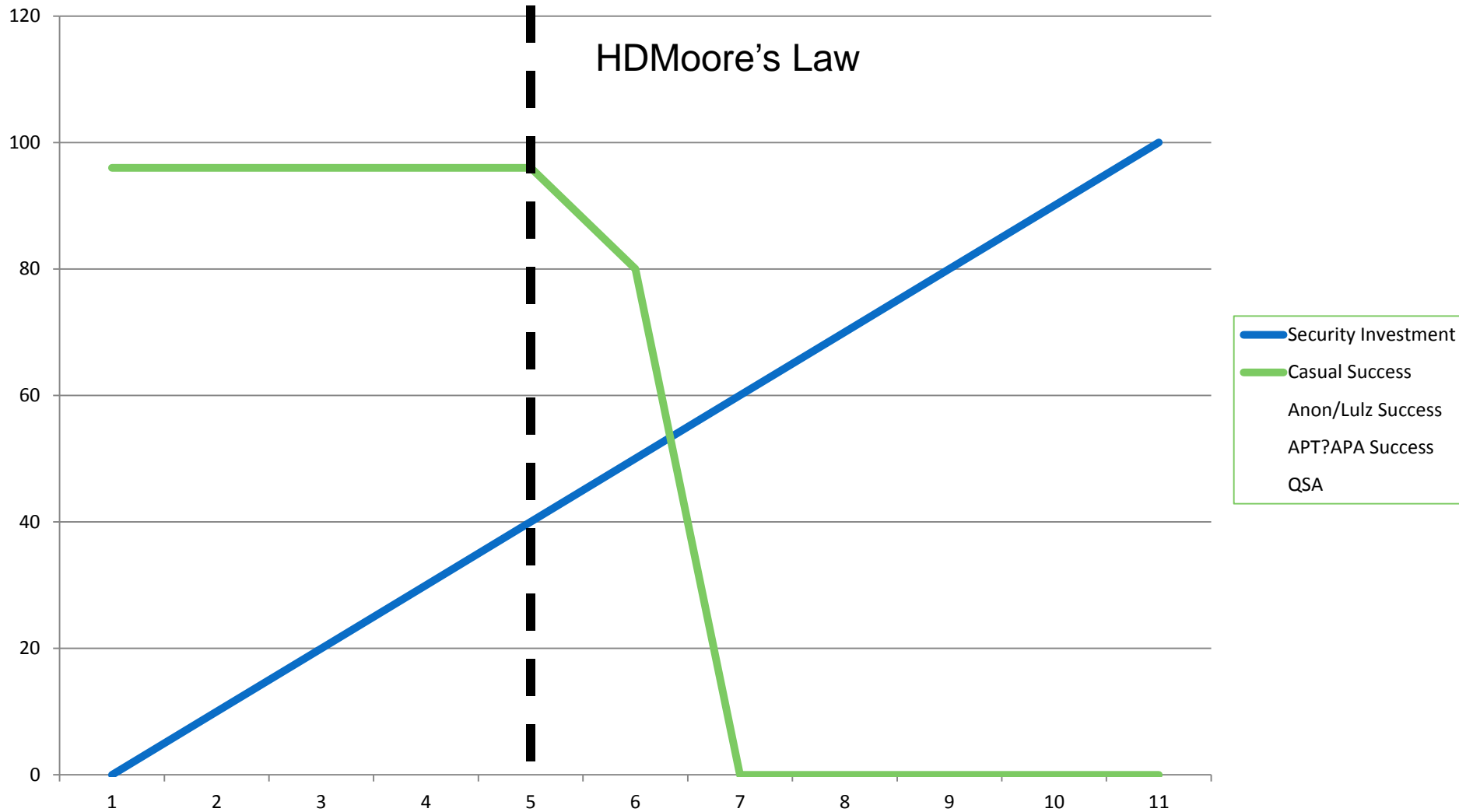




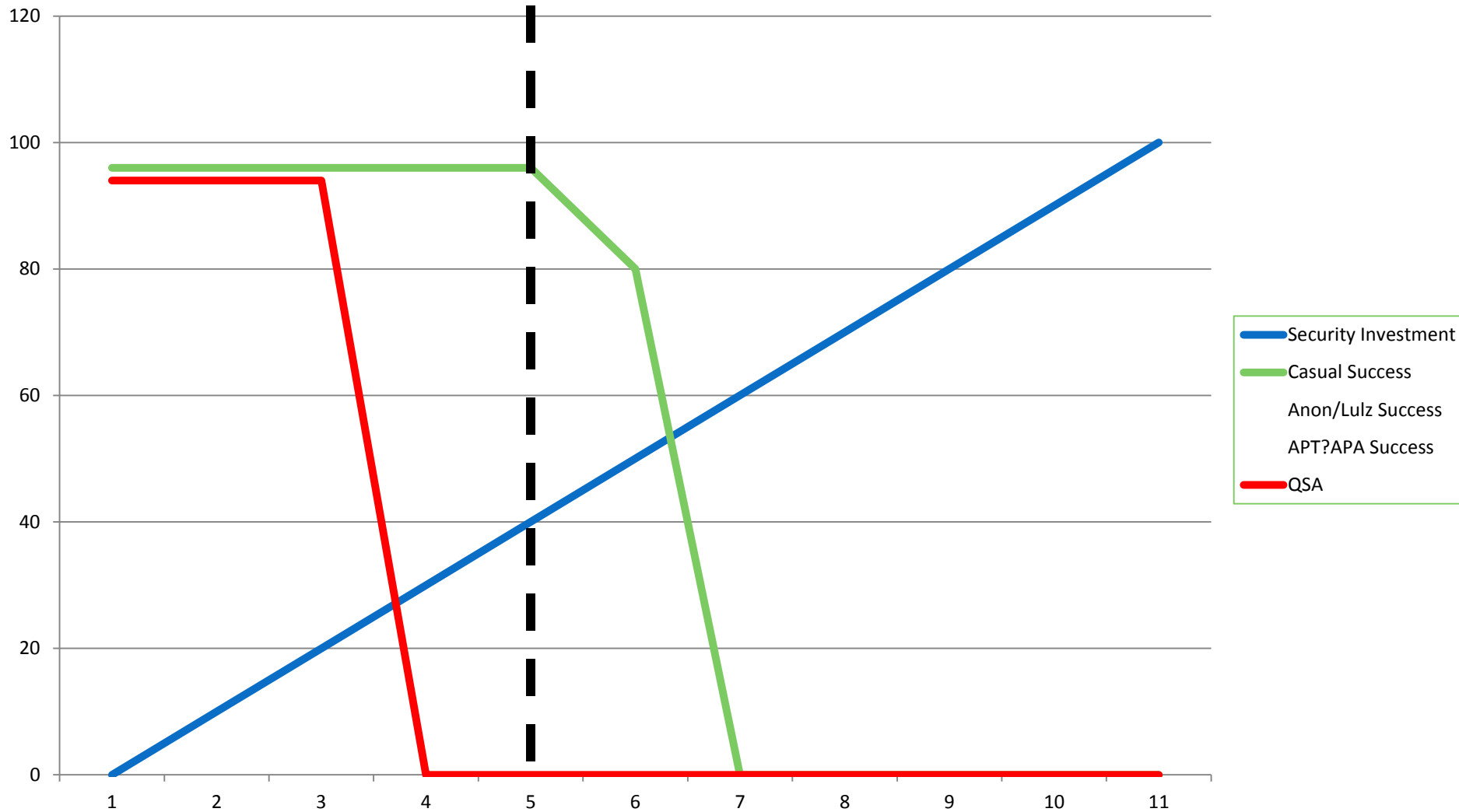
# Attacker Drop-Offs



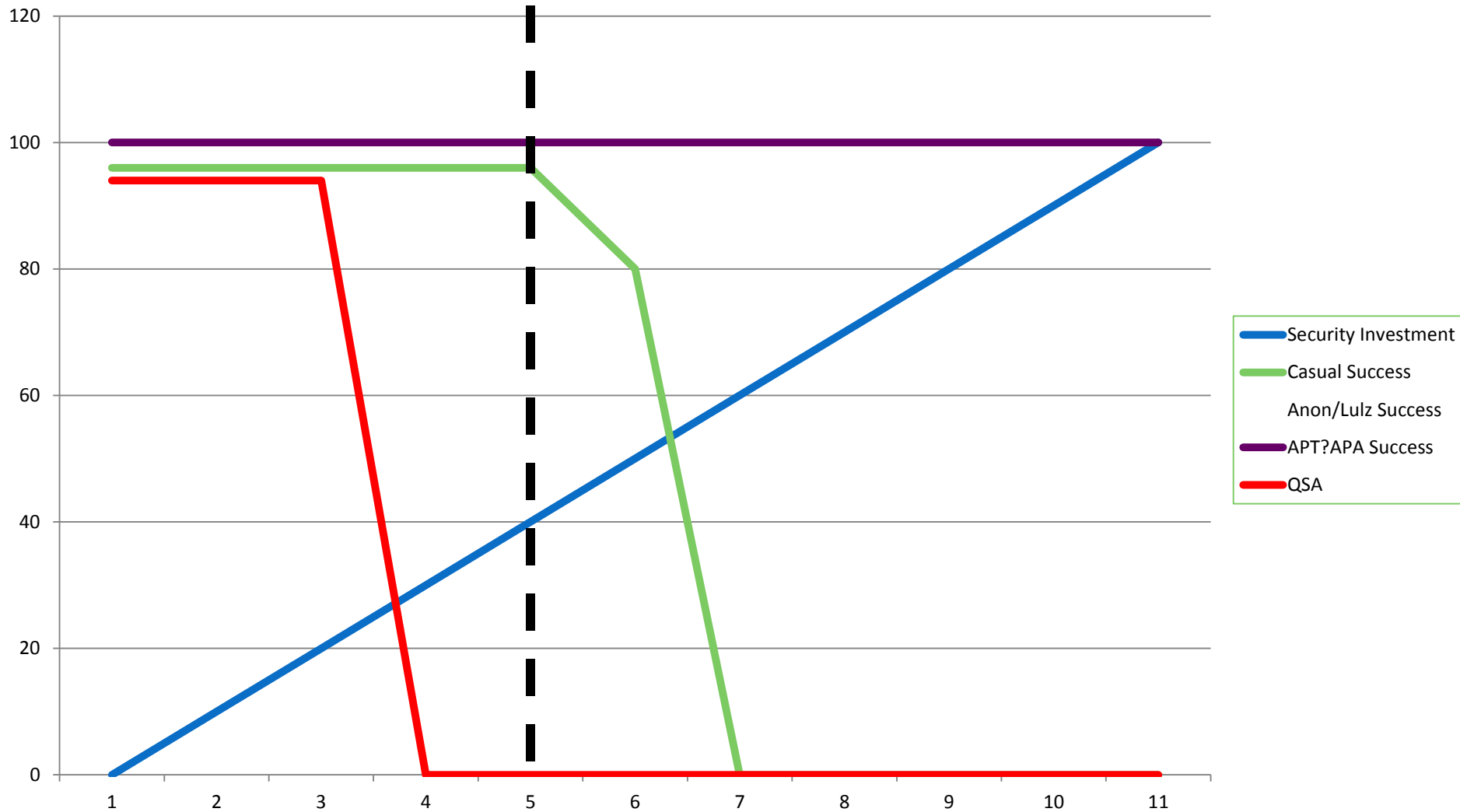
# Attacker Drop-Offs



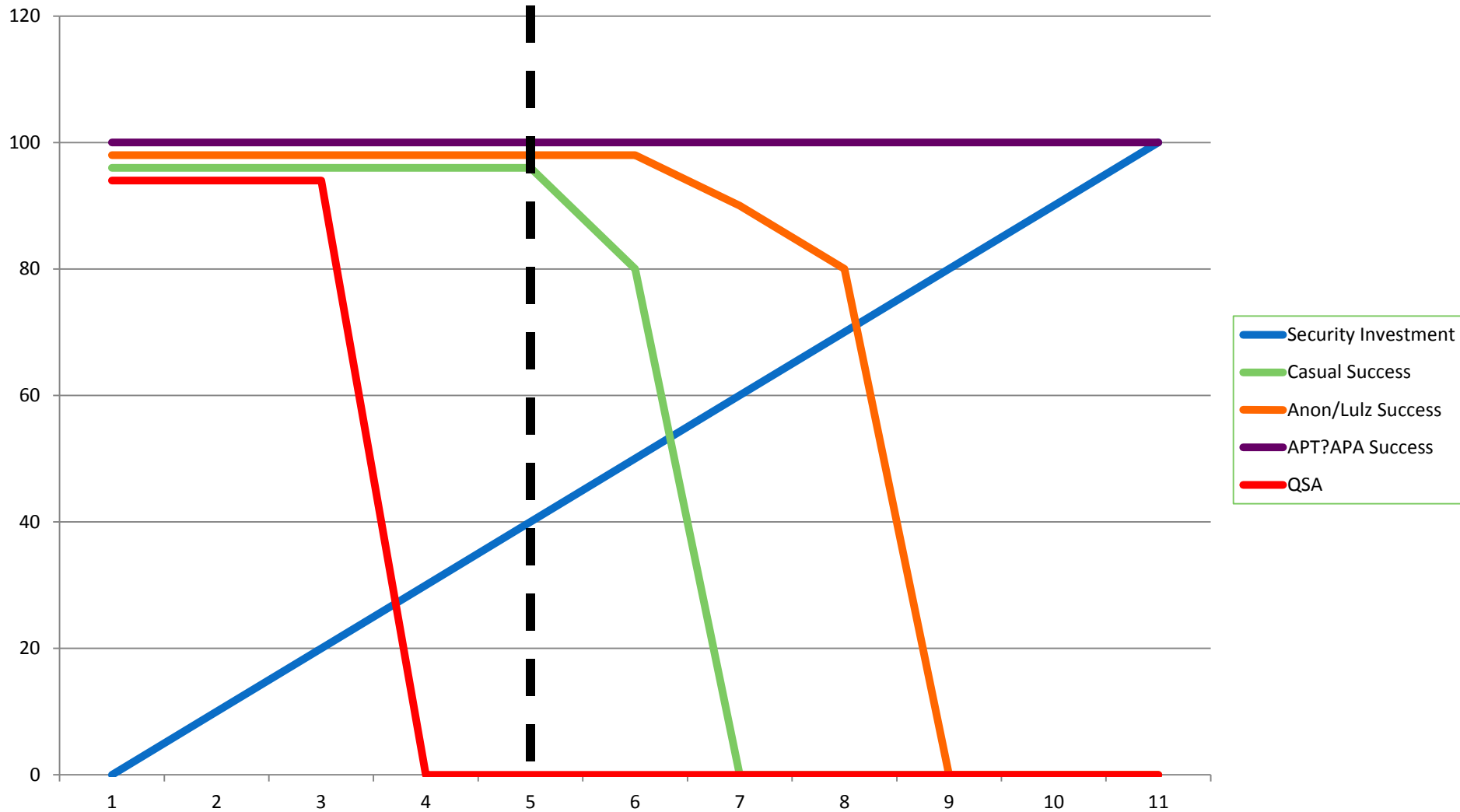
# Attacker Drop-Offs : QSAs



# Attacker Drop-Offs: APTs/APAs



# Attacker Drop-Offs: Chaotic Actors



# What is the Goal...?

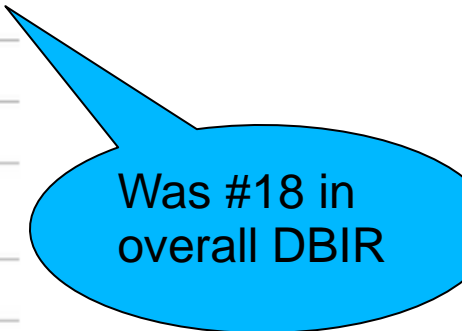


# APT



# Does it matter?

	Category	Threat Action Type	Breaches
1	Misuse	Abuse of system access / privileges	31
2	Hacking	Use of stolen login credentials	28
3	Social	Pretexting	25
4	Hacking	Exploitation of backdoor or command and control channel	24
4	Social	Solicitation / Bribery	24
4	Misuse	Embezzlement, skimming, and related fraud	24
5	Malware	Backdoor (allows remote access / control)	22
5	Malware	Send data to external site / entity	22
5	Malware	System / network utilities ( <u>PsTools</u> , <u>Netcat</u> )	22
6	Malware	<u>Keylogger</u> / <u>Spyware</u> (capture data from user activity)	21
6	Malware	Scan or footprint network	21
6	Hacking	SQL Injection	21



Was #18 in overall DBIR

Top Threat Action Types used to steal INTELLECTUAL PROPERTY AND CLASSIFIED INFORMATION by number of breaches - (excludes breaches only involving payment card data, bank account information, personal information, etc)

# Zombie Proof Housing

<http://all-that-is-interesting.com/post/4956385434/the-first-zombie-proof-house>

Countermeasures

Situational Awareness

Operational Discipline

Defensible Infrastructure





# Zombie Proof Housing

<http://all-that-is-interesting.com/post/4956385434/the-first-zombie-proof-house>



# Zombie Proof Housing

<http://all-that-is-interesting.com/post/4956385434/the-first-zombie-proof-house>

Countermeasures

Situational Awareness

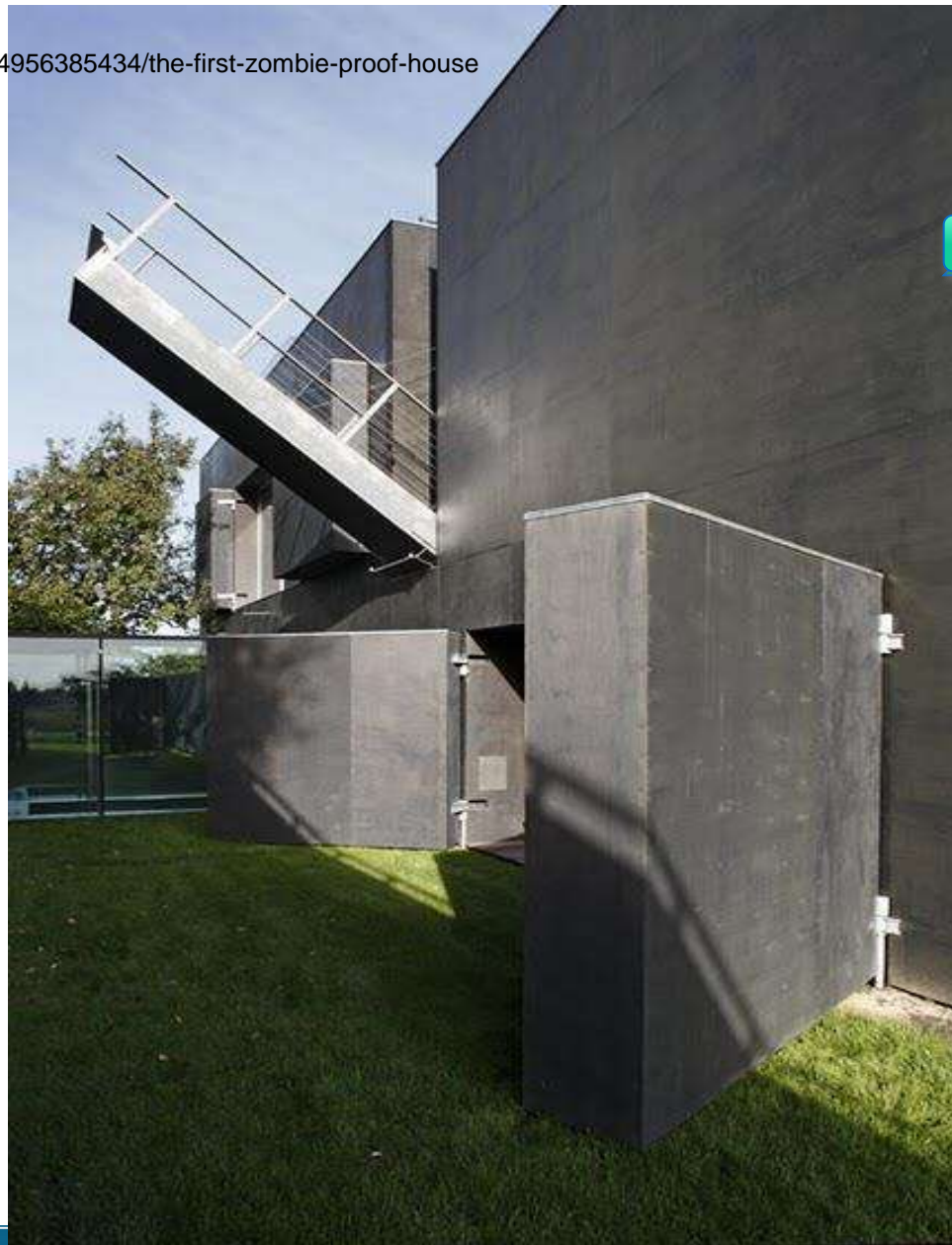
Operational Discipline

Defensible Infrastructure



# Zombie Proof Housing

<http://all-that-is-interesting.com/post/4956385434/the-first-zombie-proof-house>



Countermeasures

Situational Awareness

Operational Discipline

Defensible Infrastructure

# Zombie Proof Housing

<http://all-that-is-interesting.com/post/4956385434/the-first-zombie-proof-house>

Countermeasures

Situational Awareness

Operational Discipline

Defensible Infrastructure



# Zombie Proof Housing

<http://all-that-is-interesting.com/post/4956385434/the-first-zombie-proof-house>

Countermeasures

Situational Awareness

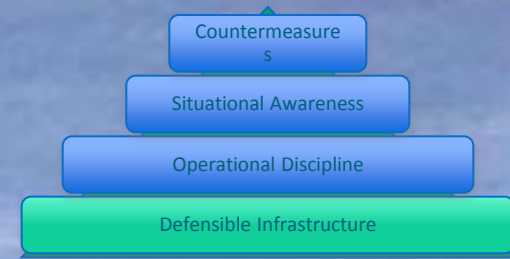
Operational Discipline

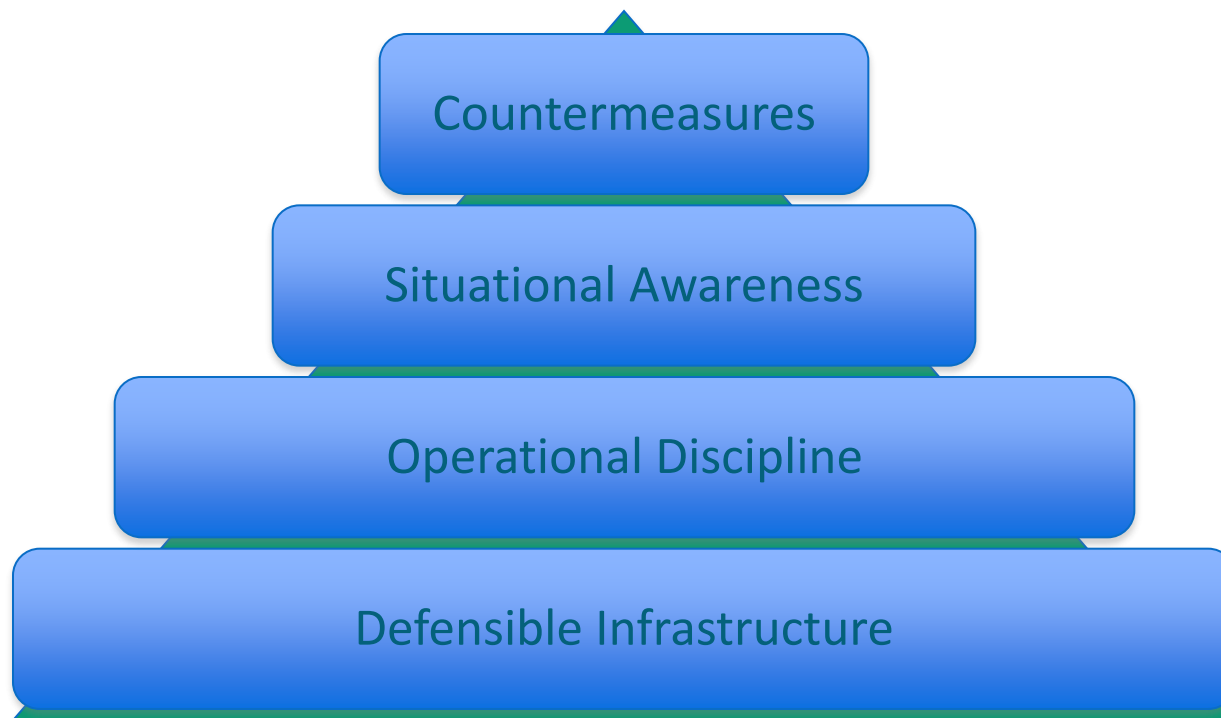
Defensible Infrastructure



# Zombie Proof Housing

<http://all-that-is-interesting.com/post/4956385434/the-first-zombie-proof-house>



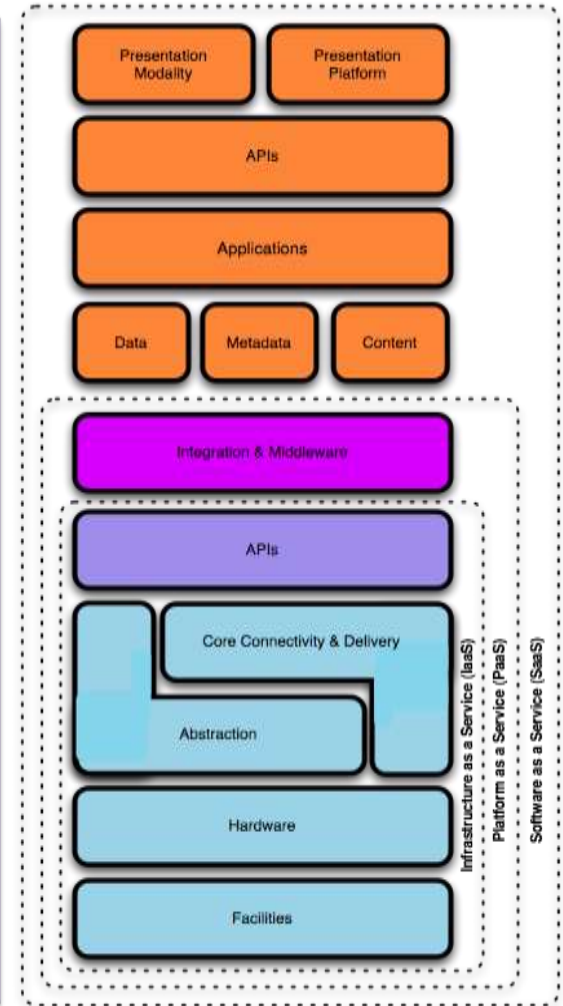


A real use case of 'better security' in the face of adaptive adversaries [http://www.the451group.com/report\\_view/report\\_view.php?entity\\_id=66991](http://www.the451group.com/report_view/report_view.php?entity_id=66991)

**Application Security**



**CSA Cloud Model**







# **Rugged Software Development**

Joshua Corman, David Rice, Jeff Williams

2010

**USA 2009** 20-24 April | Moscone Center | San Francisco





“What is missing from software security?”

**CULTURAL INFORMATION**

PRACTICE OR **IDEA** OR CONCEPT

THEORIES PRACTICES HABITS SONGS

**NATURAL SELECTION**

EXAMPLES MIGHT INCLUDE THOUGHTS IDEAS

CHARLES DARWIN'S IDEAS

**SELF-PROPAGATING**

SURVIVAL AND COMPETITION INFLUENCE THEM

**MEME**







Secure software is critically important to almost every aspect of life.





LT CL DE RES<sup>VE</sup> R. RODOLPHE

# COMBATS



“A fortress mentality will not work in cyber. **We cannot retreat behind a Maginot Line of firewalls...**If we stand still for a minute, our adversaries will overtake us.”

-William Lynn, U.S. Deputy Secretary of Defense  
January 2010



CURRENT SOFTWARE



**RUGGED SOFTWARE**

# CURRENT SOFTWARE



Boulanger



**RUGGED SOFTWARE**



**CURRENT SOFTWARE**



**RUGGED SOFTWARE**



...so software not only needs to be...



FAST

# AGILE





**Are You Rugged?**



**HARSH**



UNFRIENDLY

# **THE MANIFESTO**

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

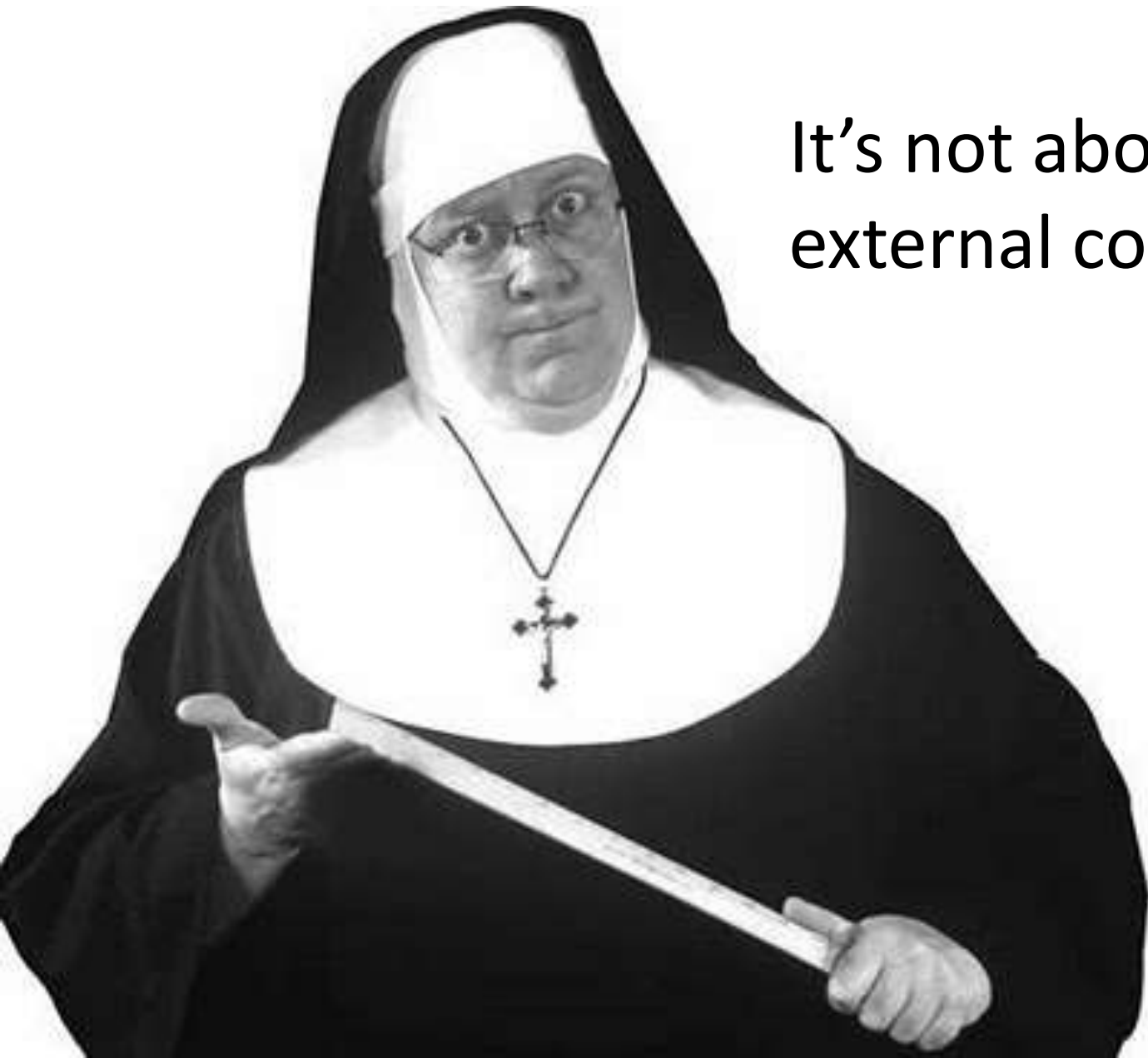


Rugged?

**WHAT IS RUGGED?**



It's not about style, it's about the result.



It's not about  
external compliance...

# RULES

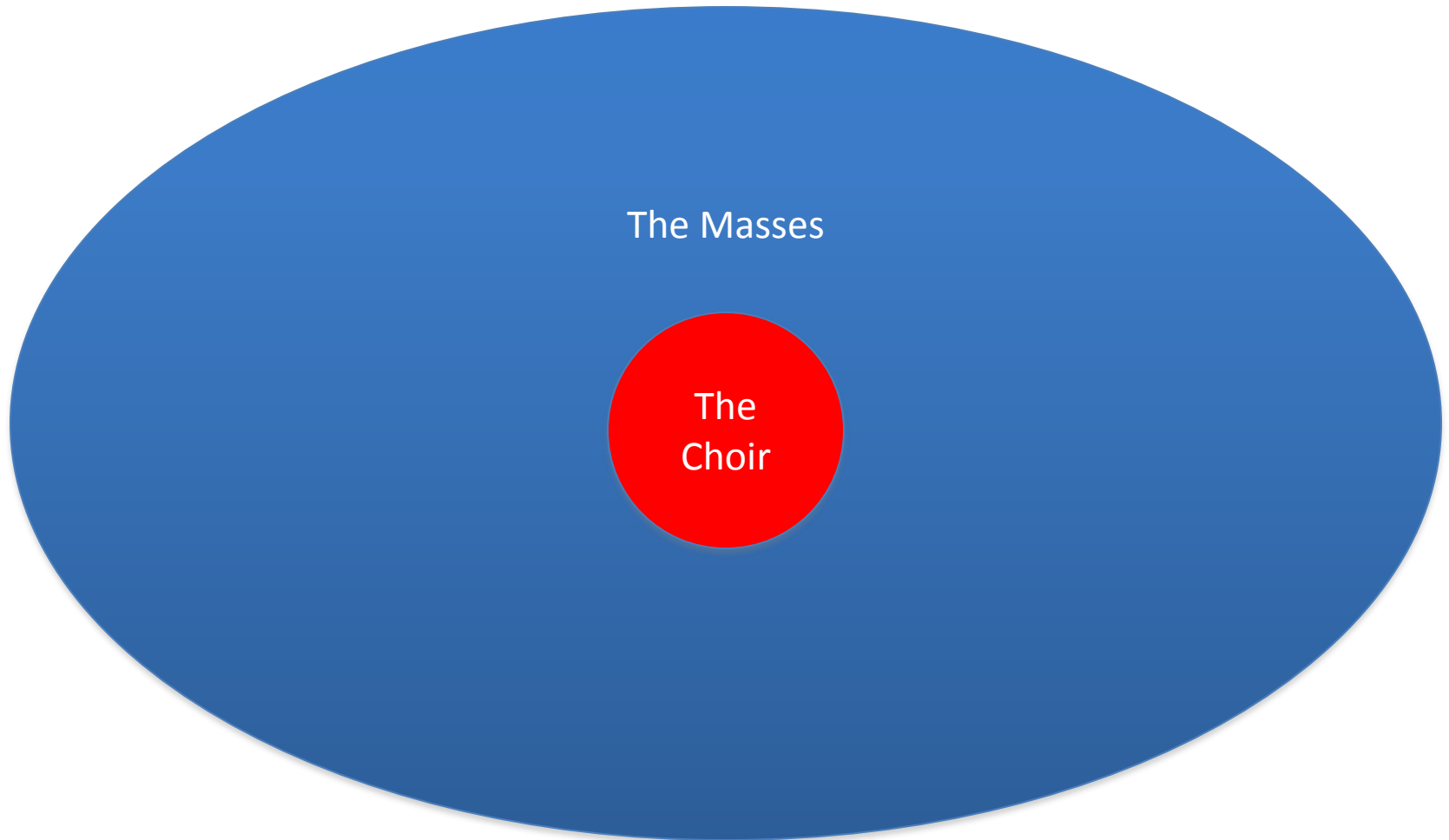
1. YOU CAN....

2. YOU CAN'T...

3. YOU CAN....

4. YOU CAN'T

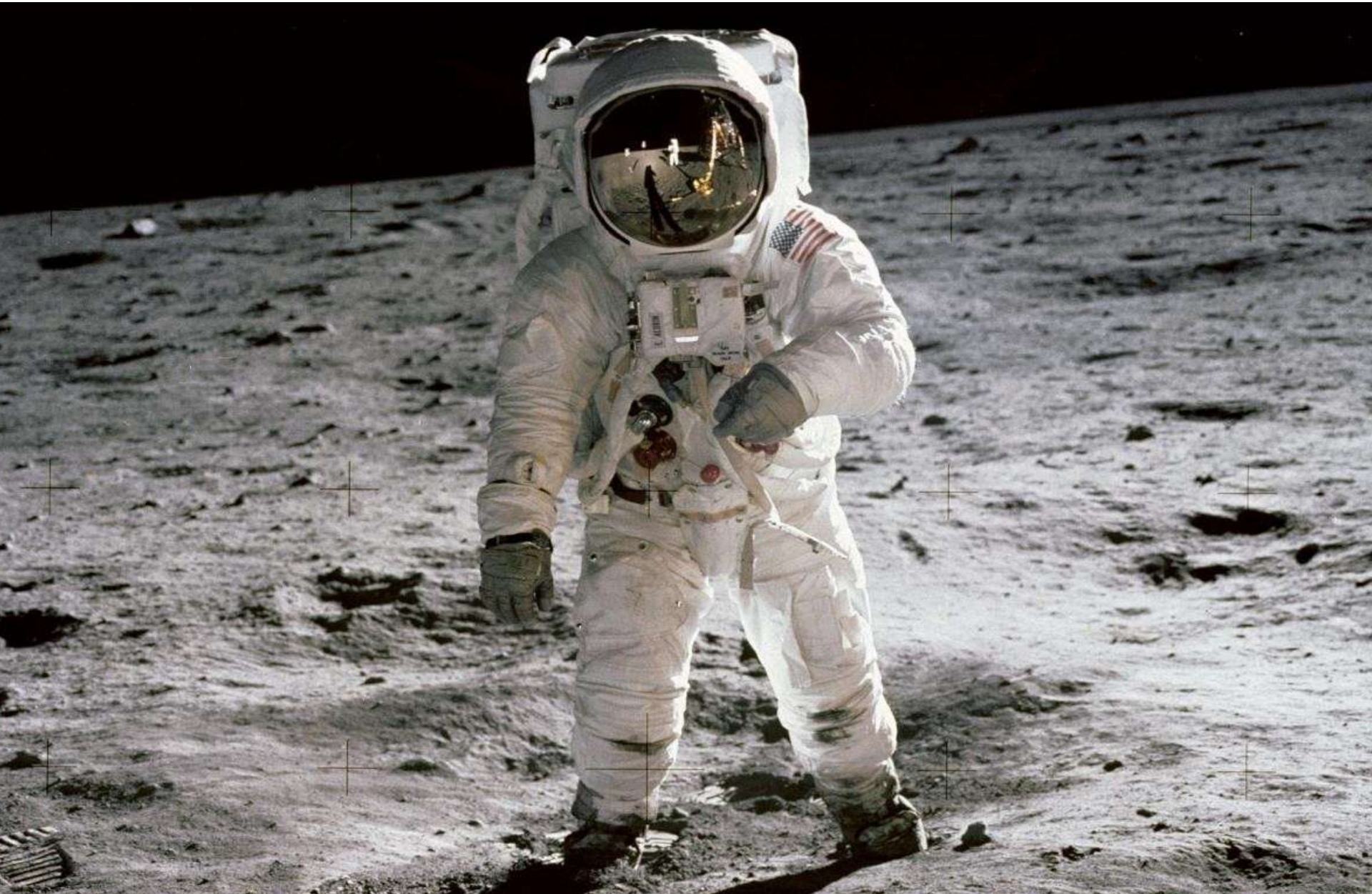
# 1) Beyond the choir



## 2) Beyond technology

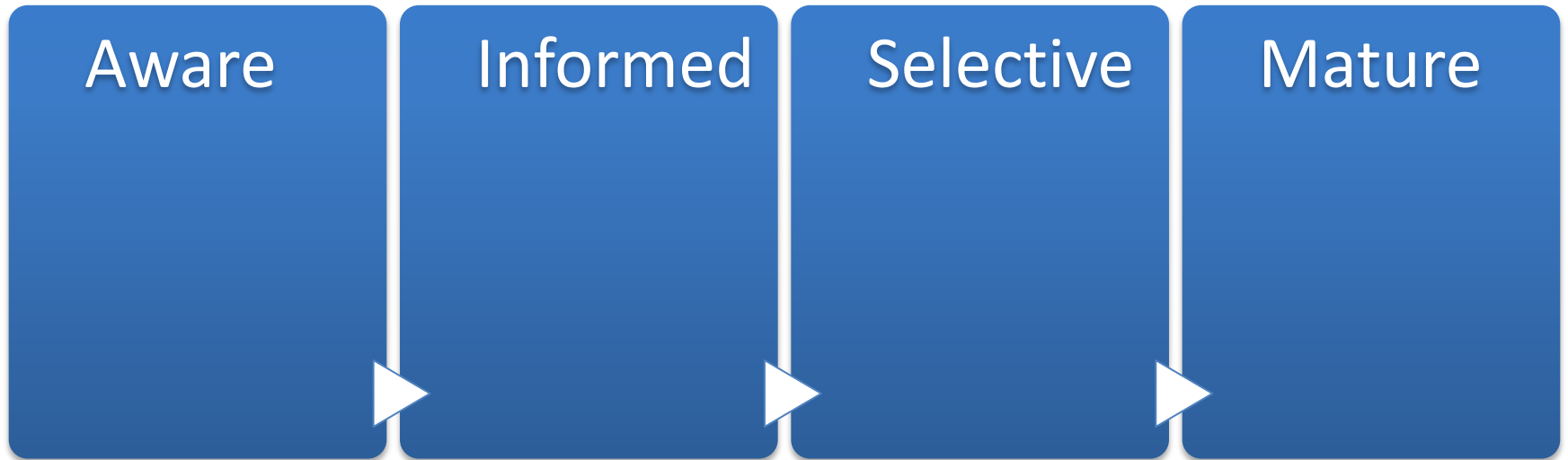


### 3) Aspirational





# The Journey



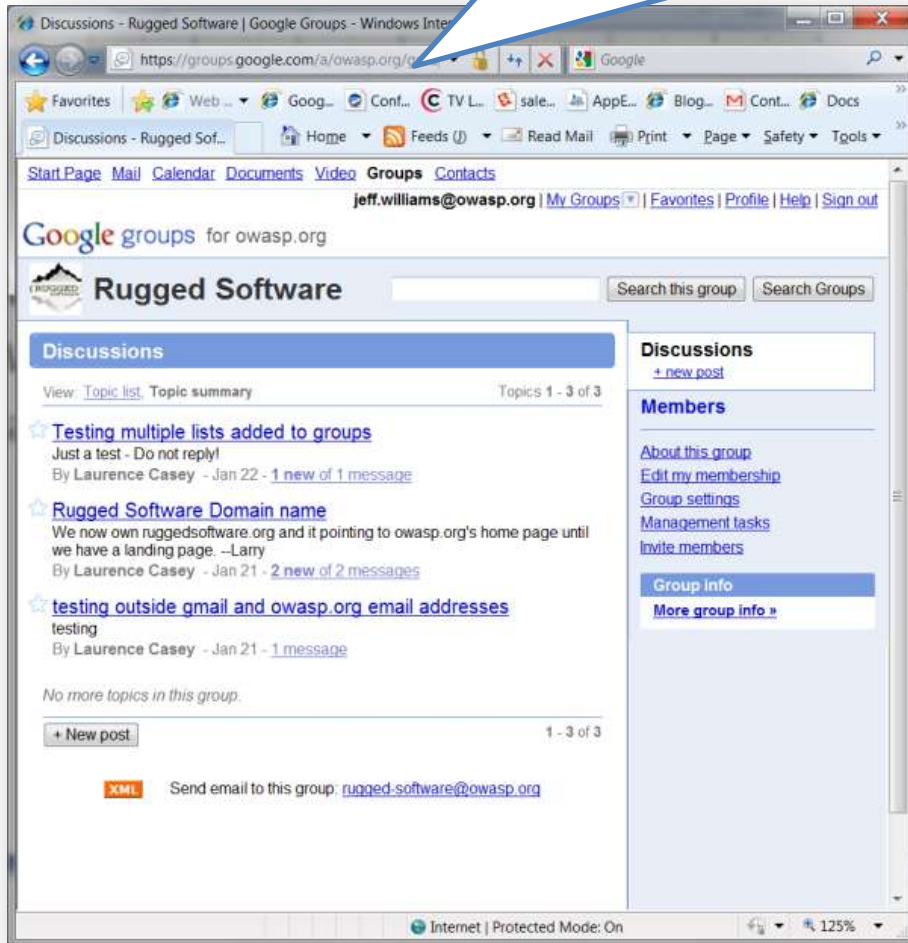
**GETTING INVOLVED**



<http://ruggedsoftware.org>

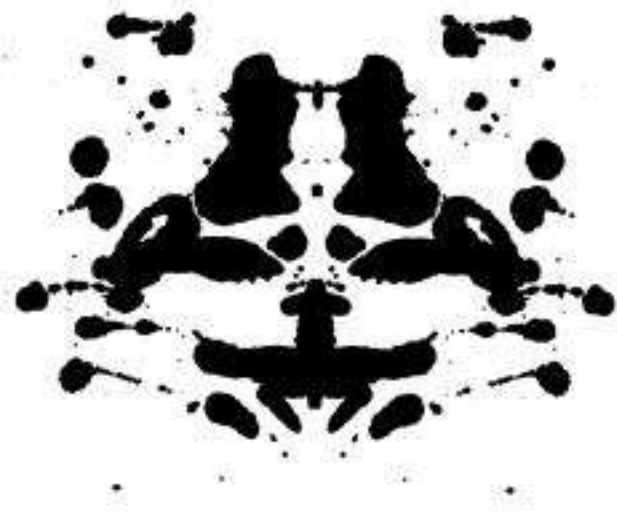
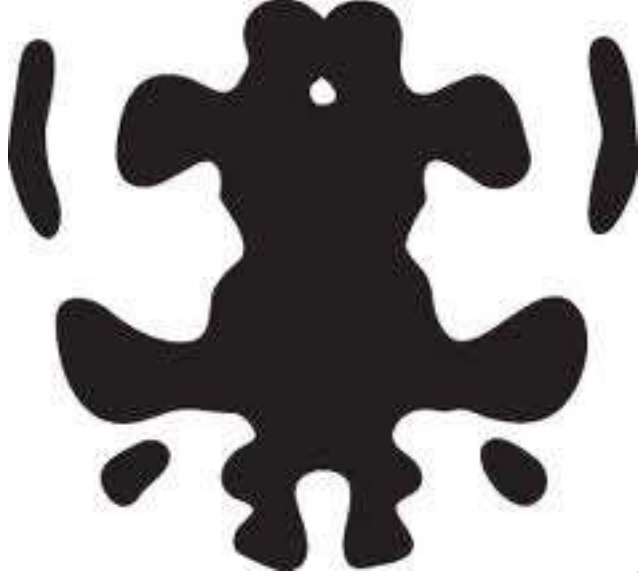
Twitter: @RuggedSoftware

<https://groups.google.com/a/owasp.org/group/rugged-software>



# Google Groups

A Rugged Rorschach  
“What does Rugged mean  
to you?”



# What can Rugged qualities be?

- Supportability – easy to troubleshoot and fix
- Resilience – can handle high loads at unexpected times
- Recoverability – is built to fail gracefully and recover quickly
- Flexibility – can easily be updated
- Security – can withstand accidental or malicious misuse
- Longevity – will serve its purpose for many years to come, that does not assume the ability to update or replace it.

# Rugged Communities

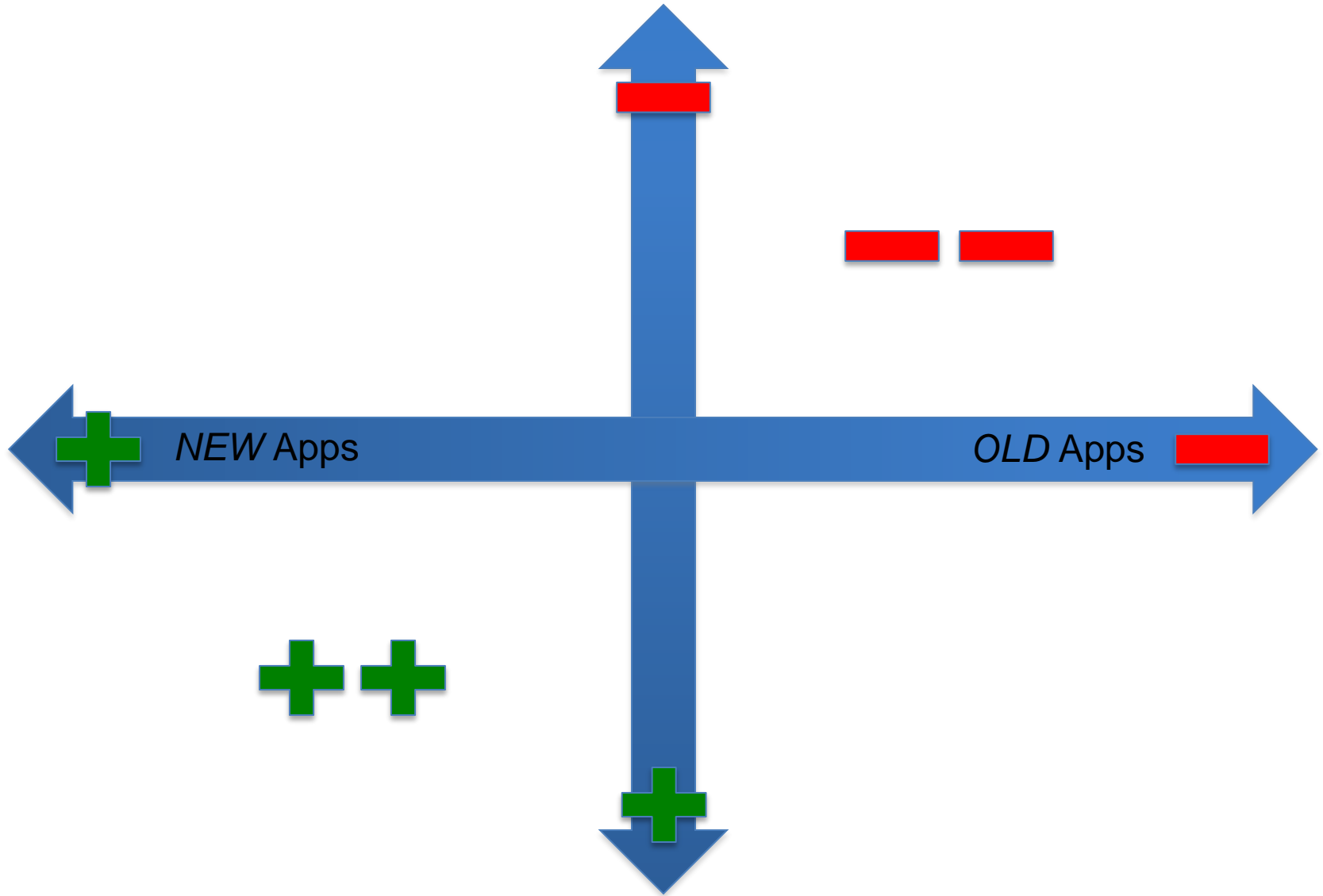
- Developers
  - the hearts and minds - the hands on the keyboards
- Development Executives
  - an asset to pursuing your SDLC
- Students and Universities
  - starting your careers with a head start
- IT Practitioners
  - securing the support and budgets you need
  - identifying the software you deserve
- Procurement
  - demanding Rugged infrastructure from your providers
- Citizens
  - Something my mother in law and neighbors understand



Supply  
and



Code we *WRITE*



Code we *BUY*



# *The Rugged Manifesto*

*I am rugged... and more importantly, my code is rugged.*

*I recognize that software has become a foundation of our modern world.*

*I recognize the awesome responsibility that comes with this foundational role.*

*I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.*

*I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.*

*I recognize these things - and I choose to be rugged.*

*I am rugged because I refuse to be a source of vulnerability or weakness.*

*I am rugged because I assure my code will support its mission.*

*I am rugged because my code can face these challenges and persist in spite of them.*

*I am rugged, not because it is easy, but because it is necessary... and I am up for the challenge.*

# Rugged



**[www.ruggedsoftware.org](http://www.ruggedsoftware.org)**

*The Beginning of the End: Driving an Era of Rugged Software*

<http://www.the451group.com/intake/rugged/>

- The Manifesto
- An untapped resource for consumers of software and clouds
- An opportunity for cloud and hosting providers

# Q&A

**THANK YOU**

[jcorman@akamai.com](mailto:jcorman@akamai.com) @joshcorman @RuggedSoftware