Adversary ROI: Evaluating Security from the Threat Actor's Perspective

Josh Corman

Director, Security Intelligence

Akamai

David Etue

VP, Corporate Development Strategy

SafeNet

Session ID: GRC-303

Session Classification: Intermediate

RSA CONFERENCE EUROPE 2012

Agenda

- Context
- Why ROI and ROSI have failed us…
- Adversary ROI
- Categorizing Threat Actors
- Application in the Real World

Context

We Have Finite Resources…We Can Not Protect Everything!

Lufthansa Airbus A380 D-AIMC with the name "Peking" at Stuttgart
Lasse Fuss
http://commons.wikimedia.org/wiki/File:Lufthansa_A380_D-AIMC.jpg

http://commons.wikimedia.org/wiki/File:Fdr_sidefront.jpg

Consequences: Value & Replaceability

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

Misplaced Focus

*"With the breach-a-week over the last two years, the key determinate was nothing YOU did… **but rather was WHO was after you**."*

Why ROI and ROSI have failed us…

Why ROI failed…

$$ROI = \frac{Expected\ \ Returns - Cost\ of\ \ Investment}{Cost\ of\ \ Investment}$$

at Net Present Value for an organization's required Rate of Return

- Most security people aren't finance experts
- Typically applied in a vacuum
- No actual no profit from security investments
- Doesn't determine efficacy of security investment or commensurate investment levels

From the Failure of ROI comes ROSI

- Return on Security Investment (ROSI) created as a well intentioned way to apply risk metrics to ROI

$$ROSI = \frac{(Risk\ Exposure \times \%Risk\ Mitigated) - Solution\ Cost}{Solution\ Cost}$$

- Problems:
  - Attack surface is approaching infinity (not a real number)
  - "Risk Mitigated" can be both subjective and objective
  - Lacks accuracy (see @djbphaedrus Accuracy vs. Precision…)

Practical Application of ROSI

$$ROSI = \frac{(Assumption \times Wild\ \&\ *\$\ Guess) - Hunch}{Hunch}$$

Examples of Failures...

The Adversary Doesn't Care About Your ROI/ROSI

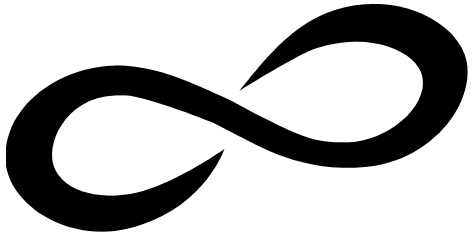
- Adversaries don't care if you spend 4% or 12% of your IT budget on security
- Adversaries are results oriented
- Adversaries care if *they* can get a return on investment from an attack, not you…

Adversary ROI

Why Adversary ROI

- Adversaries want assets - vulnerabilities are a means

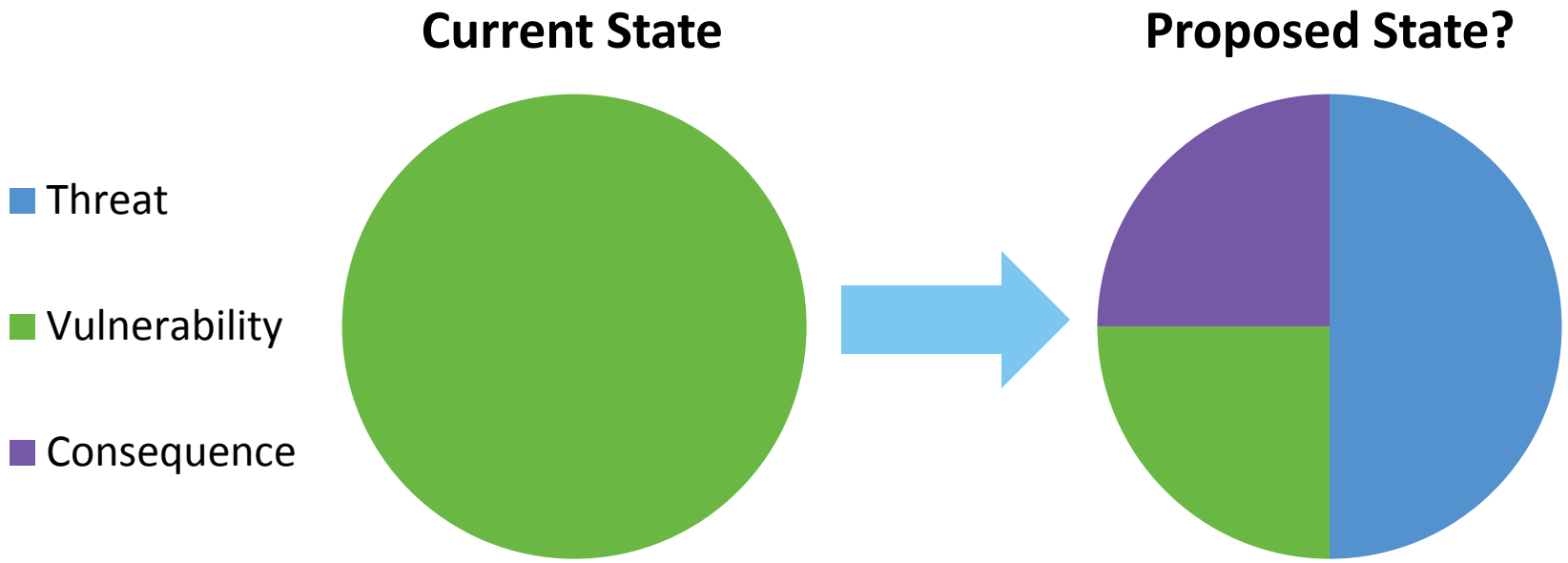
- Our attack surface is approaching infinity



- Adversaries have scarce resources too

Adversary ROI Came About By Looking at Risk

A risk requires a threat and a vulnerability that results in a negative consequence



We have finite resources, and must optimize the entire risk equation for our success!

What is a “Threat”?

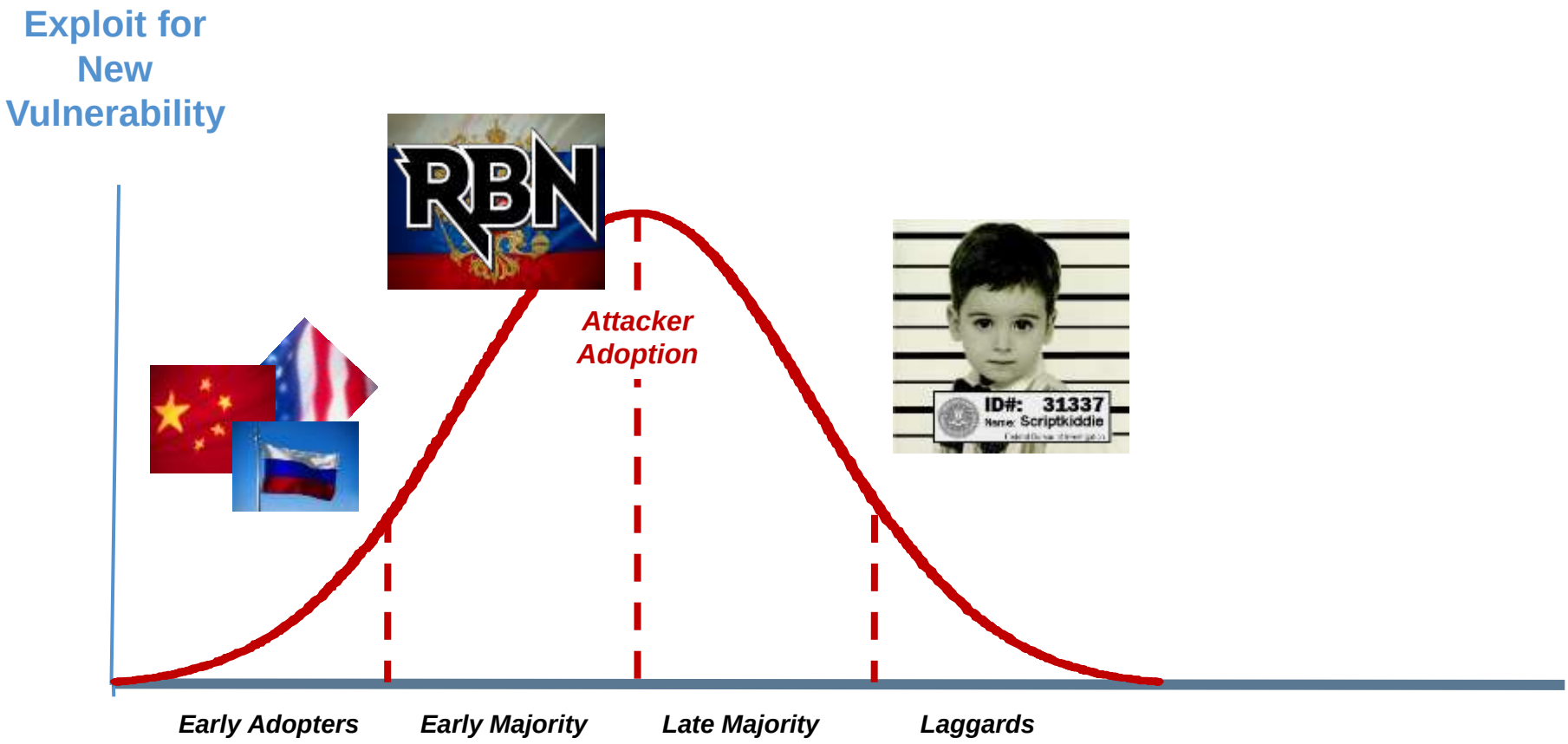
A Threat is an Actor

with a Capability

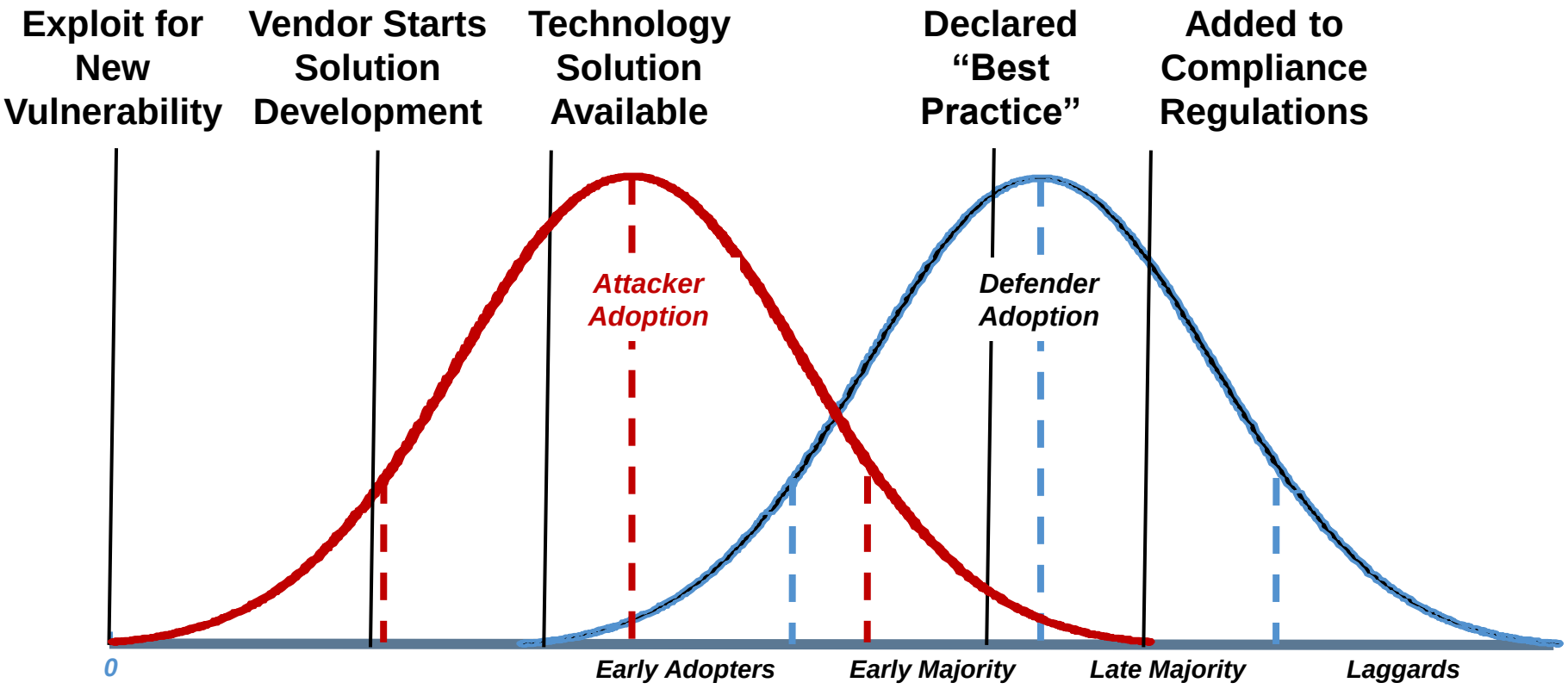
and a Motive

Threats Are A “Who”, Not a “What”

Solely Managing Vulnerabilities Will Never Win

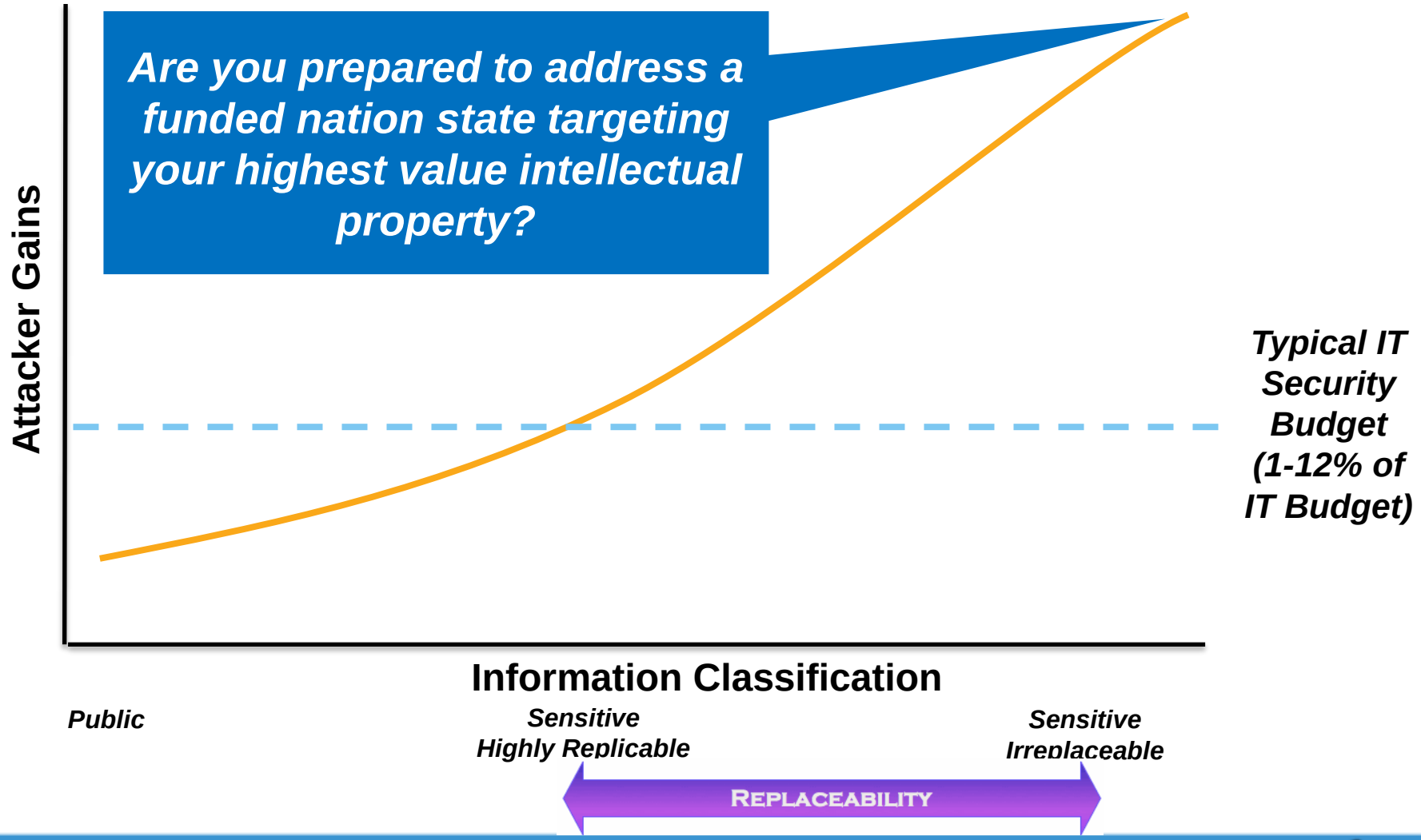


Solely Managing Vulnerabilities Will Never Win



Extensive Lag Between Attack Innovation, Solution, and Adoption

Value Favors the Attacker



The Adversary ROI Equation

$$\text{Adversary ROI} = \left(\frac{\text{Attack Value} \left[\begin{array}{c} \text{Value of Assets Compromised} + \\ \text{Adversary Value of Operational Impact} \end{array} \right] - \begin{array}{c} \text{Cost of} \\ \text{the Attack} \end{array}}{\text{Cost of the Attack}} \right)$$

$$\times \quad \text{Probability of Success}$$

$$- \quad \text{Deterrence Measures} \quad (\%\ \text{Chance of Getting Caught} \times \text{Cost of Getting Caught})$$

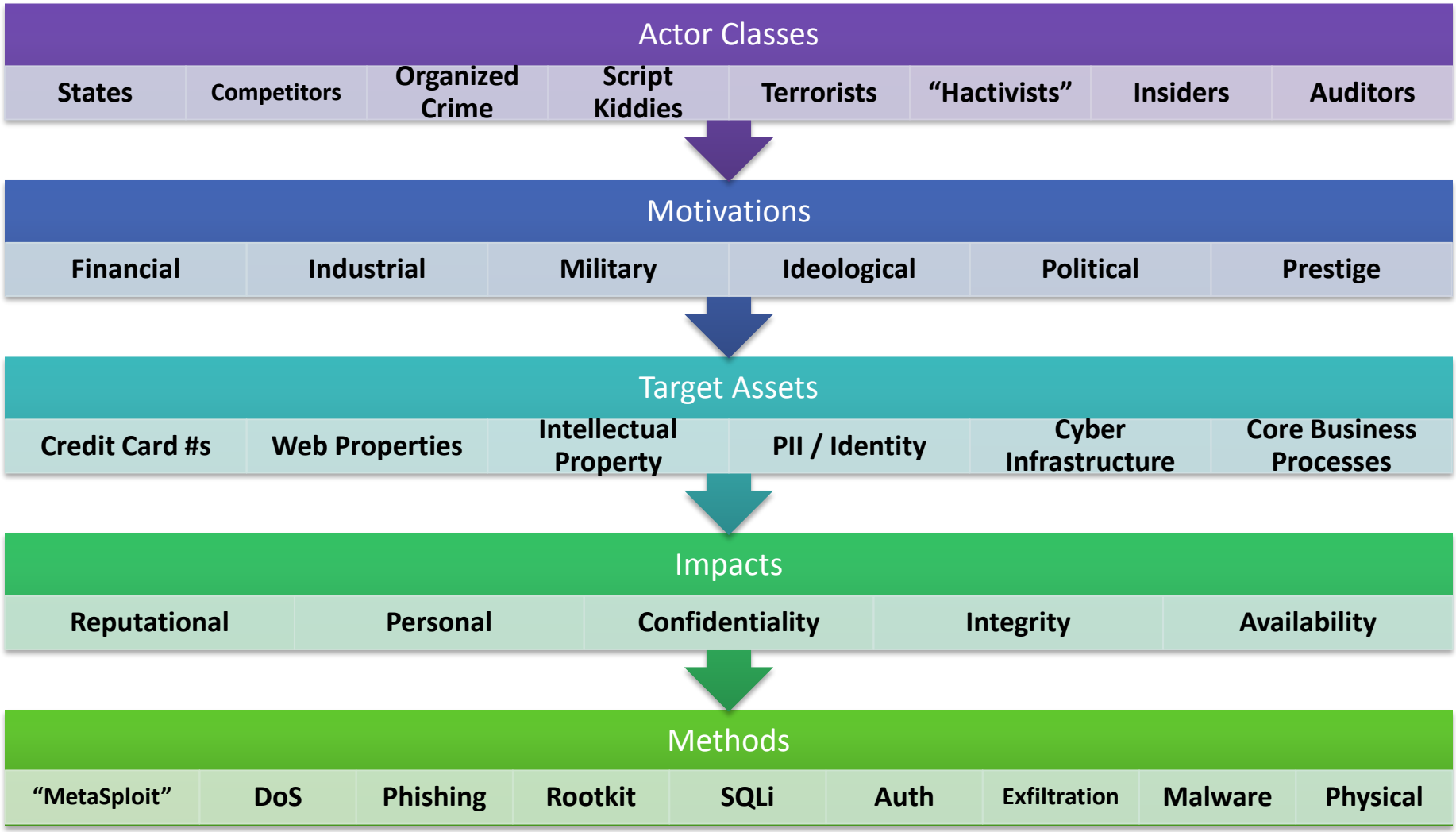
Adversary ROI Example: Bicycle Theft

OR

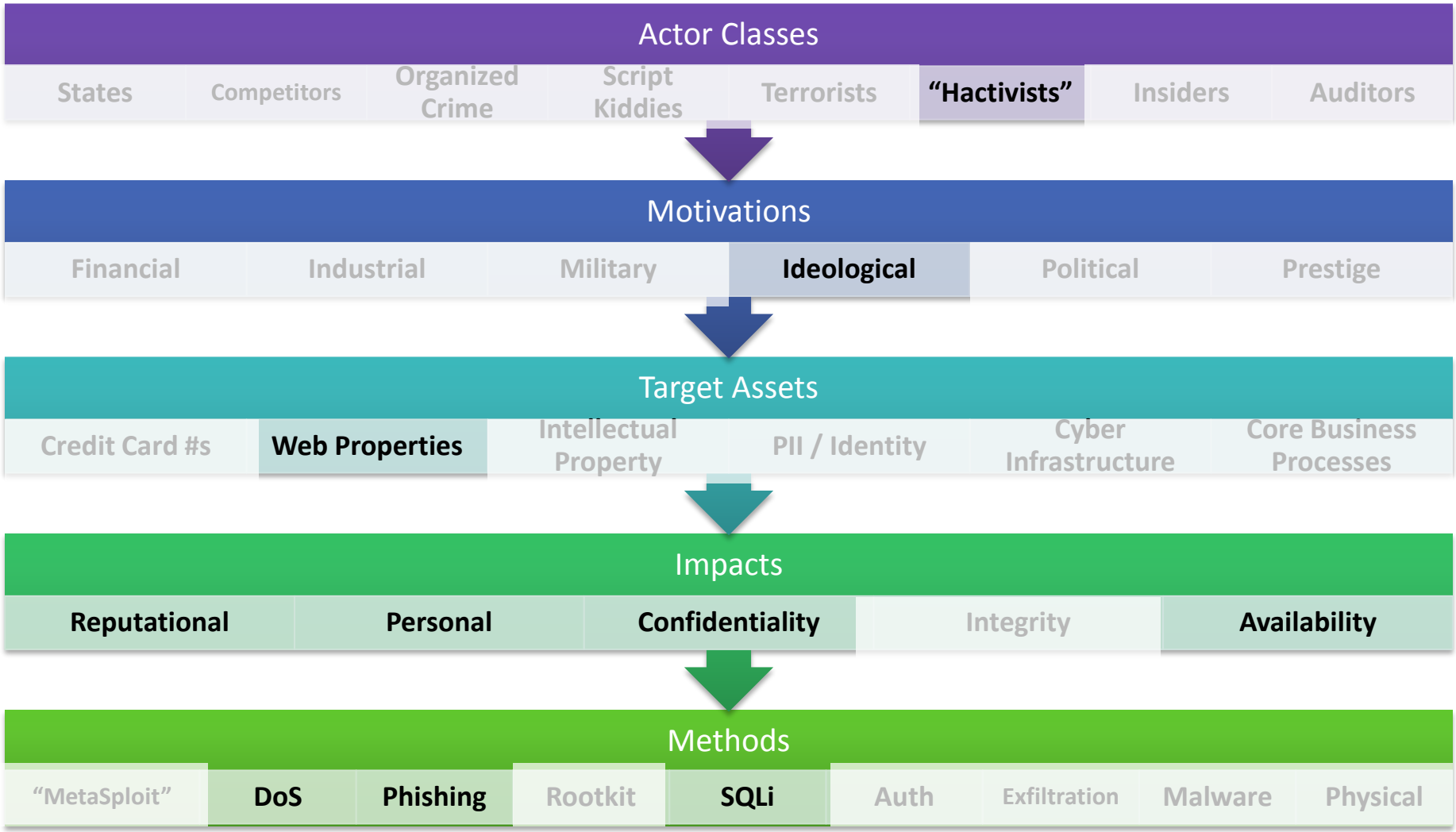
Categorizing Threat Actors


DOGMA

A Modern Pantheon of Adversary Classes



Profiling a Particular Actor



Script Kiddies (aka Casual Adversary)

- Skiddie
- Profit, Prestige
- CCN/Fungible
- Confidentially, Reputation
- “MetaSploit”, SQLi, Phishing

Organized Crime

- Organized Crime
- Profit
- Fungible, Banking
- Confidentially
- Malware, Botnets, Rootkits

Adaptive Persistent Adversaries

State/Espionage

Industrial/Military

Confidentially, Reputation

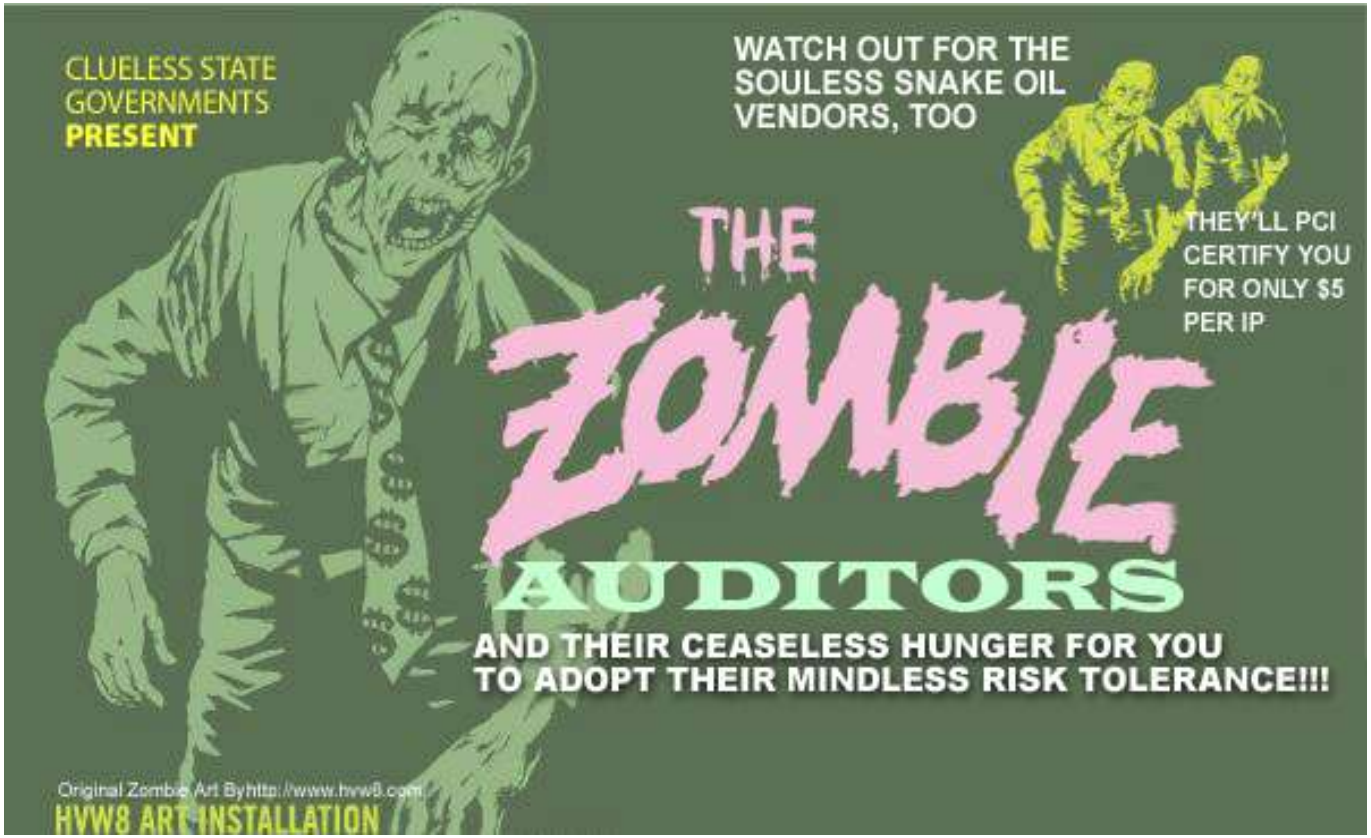
Intellectual Property Trade Secrets Infrastructure

Custom Malware, SpearPhishing, Physical, ++

~~Hactivists~~ Chaotic Actors

- Chaotic Actor
- Ideological and/or LULZ
- Web Properties, Individuals, Policy
- Availability, Confidentiality, Reputation, Personal
- DoS, SQLi, Phishing

Auditors



- Auditor QSA
- Profit
- Credit Card #s
- Distraction, Fines
- CheckList

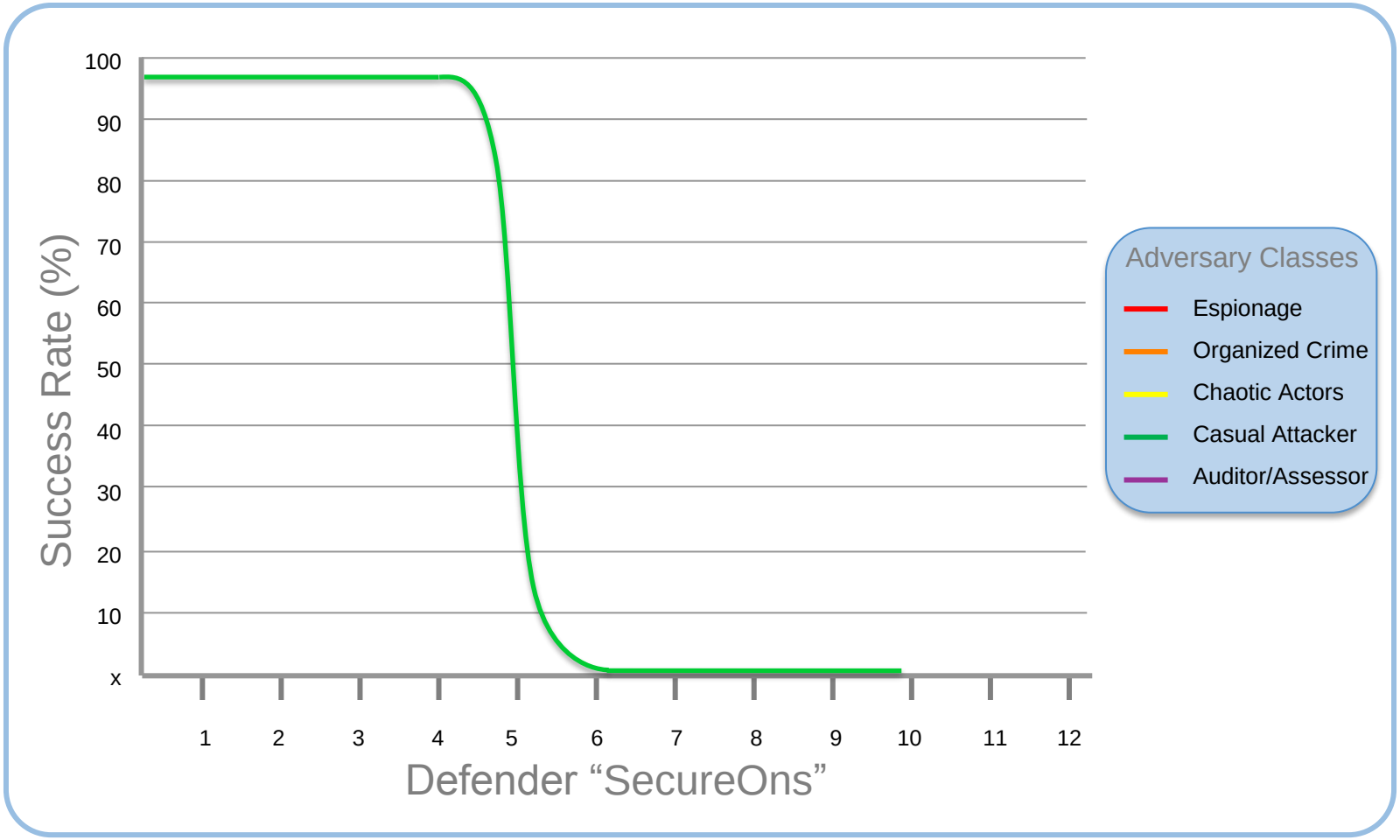
Compare and Contrast Threat Actors

	QSA	Casual Attacker	Chaotic Actor	Org Crime	State APT/APA
Asset Focus	CCNs	CCNs…	Reputation, Dirty Laundry DDoS/Availability	CCNs Banking Fungible $	IP, Trade Secrets, National Security Data
Timeframe	Annual	Anytime	Flash Mobs	Continuous	Long Cons
Target Stickiness	NA	LOW	HIGH	LOW	HIGH
Probability	100%	MED	?	HIGH	?
"Impact"	Annual $	1 and done	Relentless	Varies	Varies

Attacker Power - HD Moore's Law

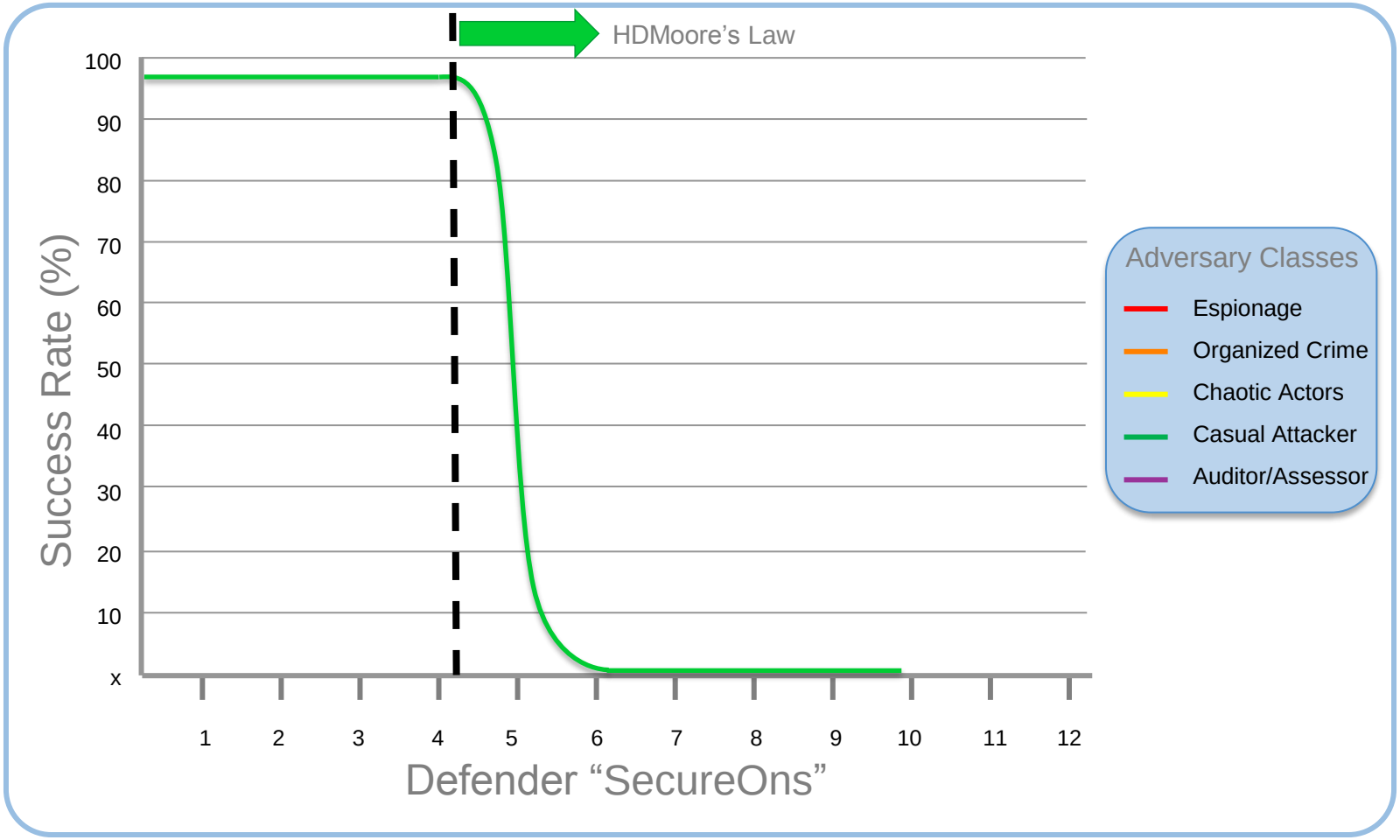
- **Moore's Law:** Compute power doubles every 18 months
- **HDMoore's Law:** Casual Attacker Strength grows at the rate of MetaSploit

HDMoore's Law



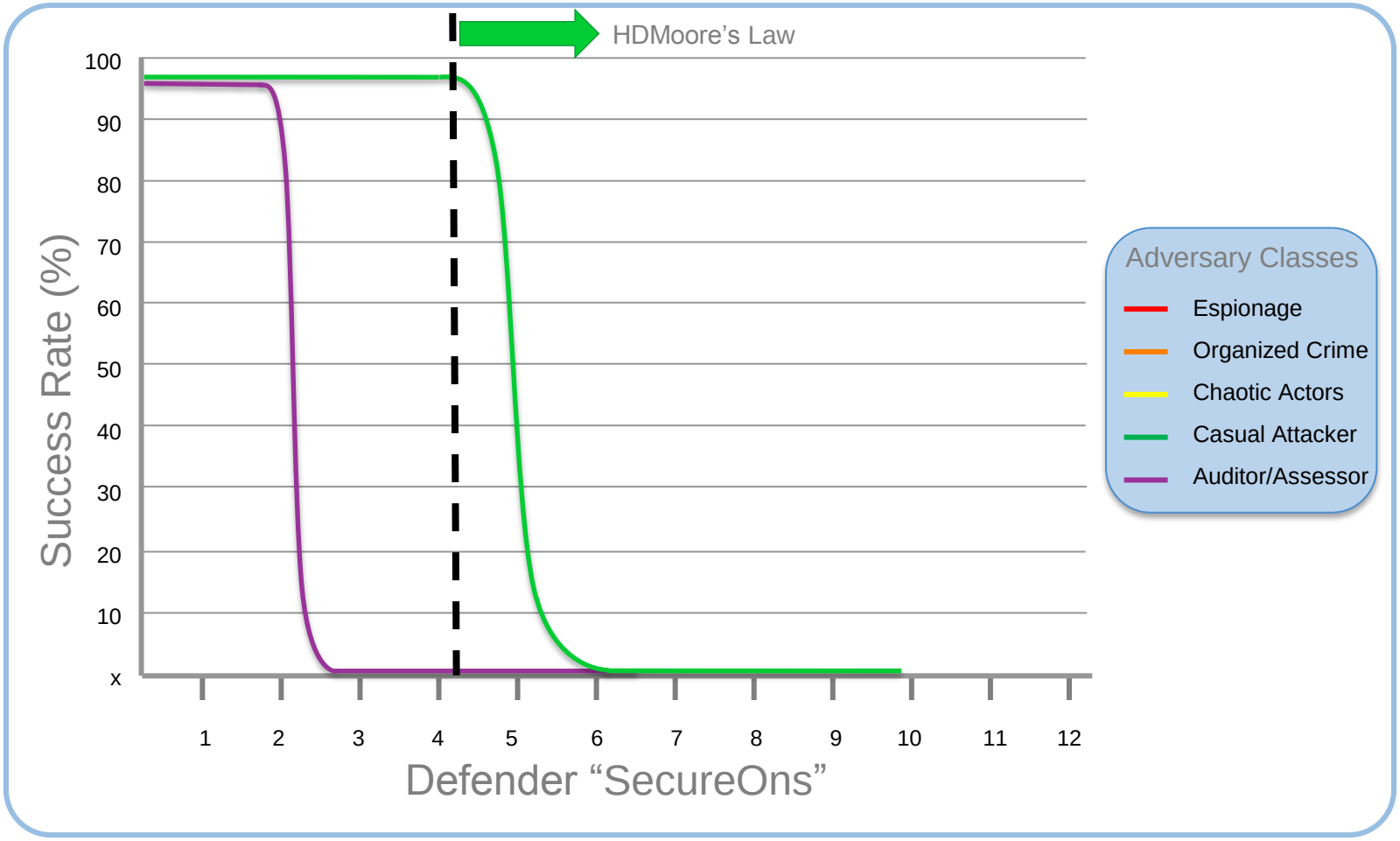
http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

HDMoore's Law (continued)



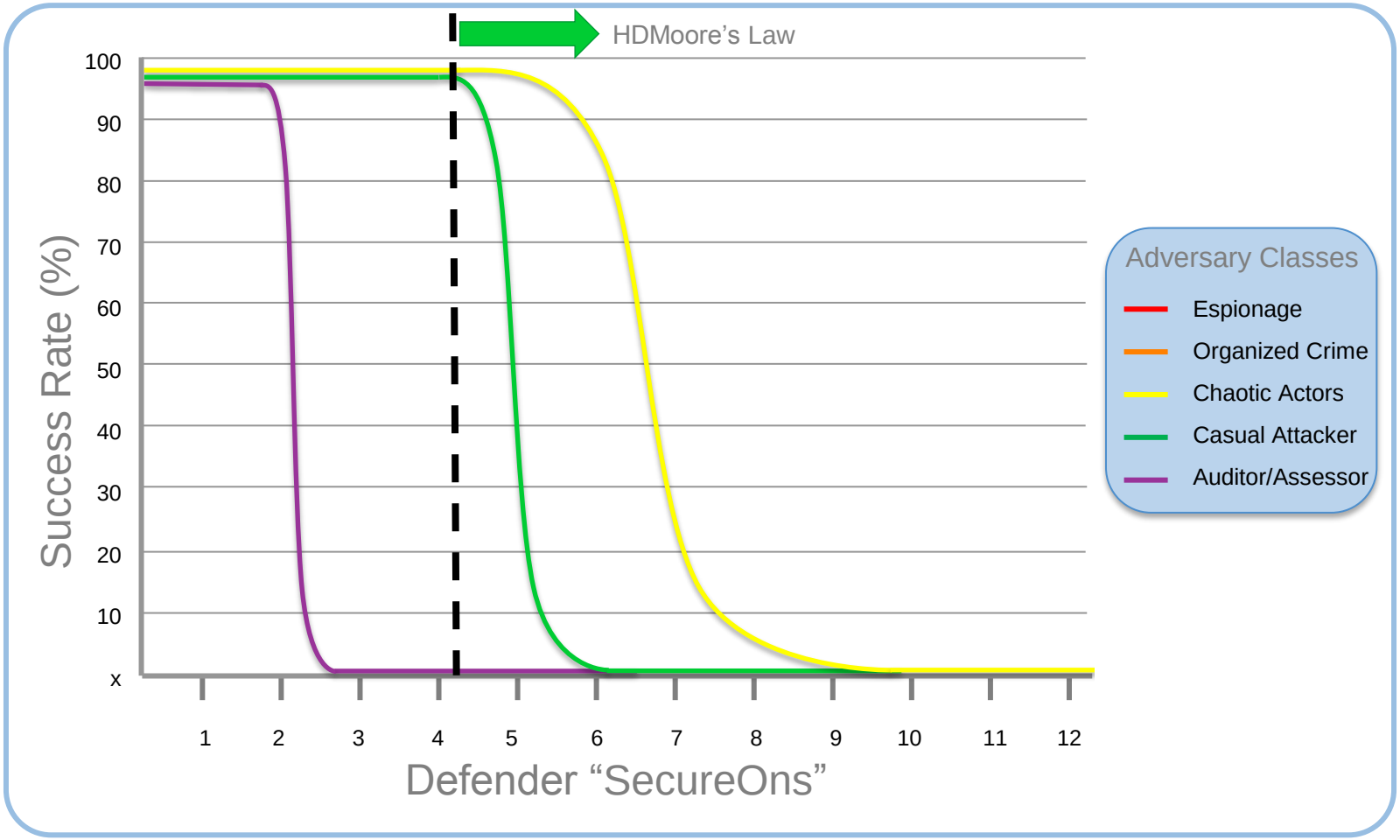
http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

HDMoore's Law (continued)



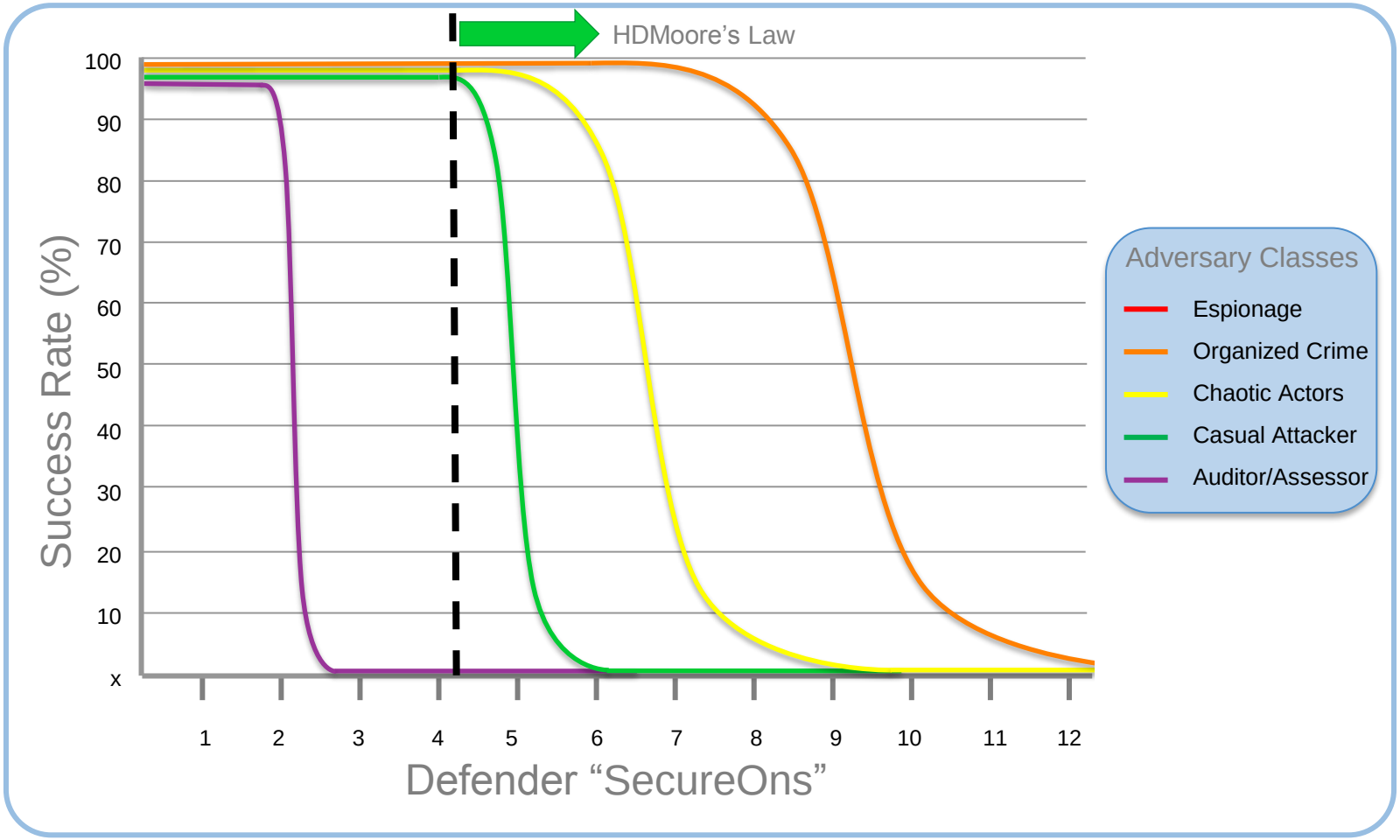
http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

HDMoore's Law (continued)



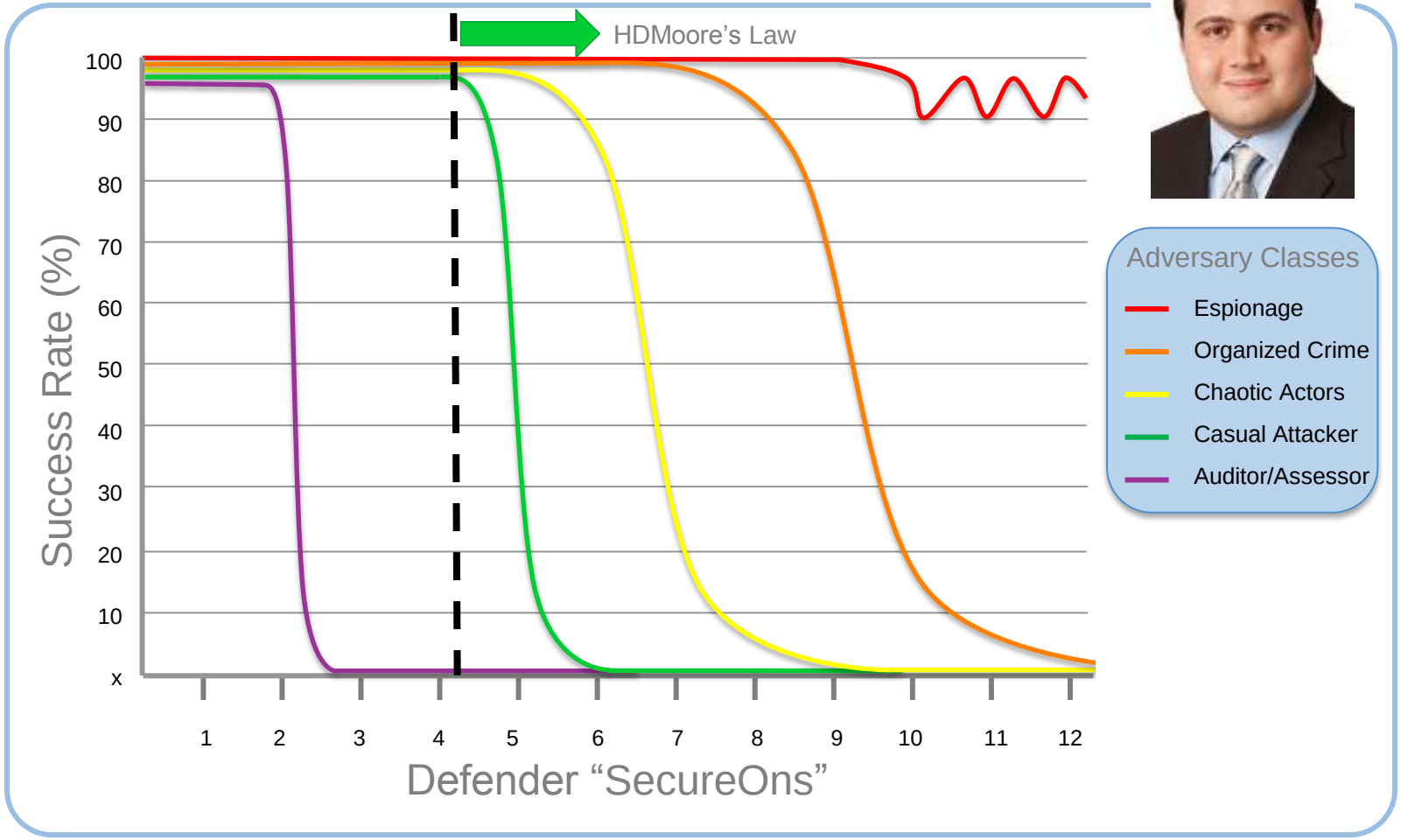
http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

HDMoore's Law (continued)



http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

HDMoore's Law (continued)



http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

Application in the Real World

Does it Matter Who is Attacking?

	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 (PsTools, Netcat)	22
6	Malware	Keylogger / Spyware (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)

Source: Verizon Business Security Blog (post-DBIR), 2011
http://securityblog.verizonbusiness.com/2011/06/23/new-views-into-the-2011-dbir/

Impacting Adversary ROI

It is typically not desirable to make your assets less valuable

$$\text{Adversary ROI} = \left(\frac{\text{Attack Value} \left(\begin{array}{c}\text{Value of Assets Compromised +} \\ \text{Adversary Value of Operational Impact}\end{array} \right) - \begin{array}{c}\text{Cost of} \\ \text{the Attack}\end{array}}{\text{Cost of the Attack}} \right)$$

x Probability of Success

Increase adversary "Work Effort"

- Deterrence Measures (% Chance of Getting Caught x Cost of Getting Caught)

Ability to respond and recover key

Impact of getting caught is typically a government issue

Who Are You Playing Against?

False Flags

http://www.flickr.com/photos/pierre_tourigny/367078204/

VZ DBIR Patching: Evolving Adversary TTPs

"Let's Patch Faster!"

2008	2009	2010
22% Patchable	6 of 90 Patchable	ZERO Patchable
(not 90%)	6.66%	[0]

Barking up the wrong tree?

Source: Verizon Business Data Breach Investigations Report (DBIR), Years 2009-2011

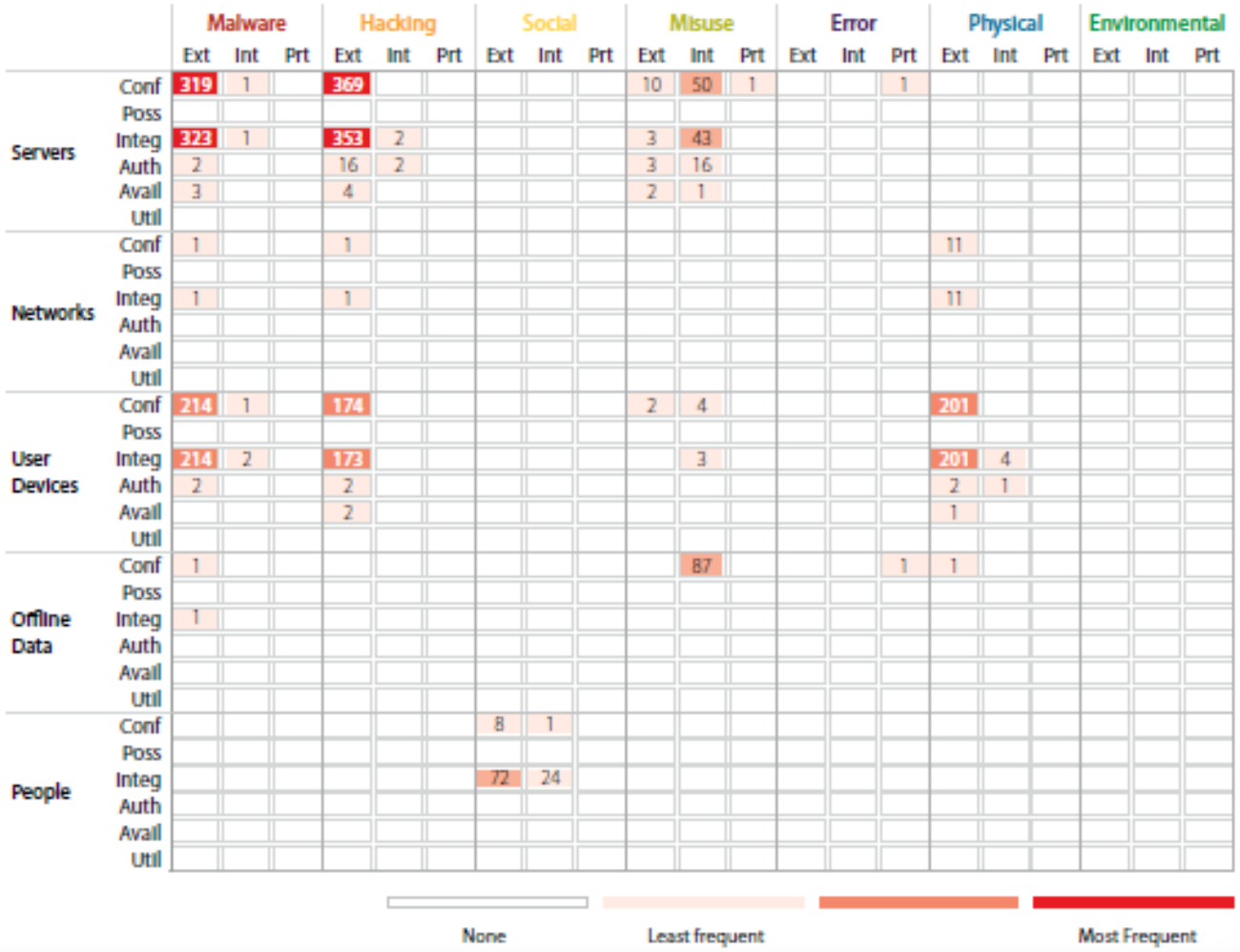
SQLi

We spend under $500m

Source: 2011 Verizon Business Data Breach Investigations Report (DBIR)

2011: Attacks Density (4Realz DBIR Style)

Figure 6. A⁴ Grid depicting the frequency of VERIS Threat Events across 2010 caseload



		Malware			Hacking			Social			Misuse			Error			Physical			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Conf	319	1		369						10	50	1			1						
	Poss																					
	Integ	323	1		353	2					3	43										
	Auth	2			16	2					3	16										
	Avail	3			4						2	1										
	Util																					
Networks	Conf	1			1												11					
	Poss																					
	Integ	1			1												11					
	Auth																					
	Avail																					
	Util																					
User Devices	Conf	214	1		174						2	4					201					
	Poss																					
	Integ	214	2		173							3					201	4				
	Auth	2			2												2	1				
	Avail				2												1					
	Util																					
Offline Data	Conf	1										87				1	1					
	Poss																					
	Integ	1																				
	Auth																					
	Avail																					
	Util																					
People	Conf							8	1													
	Poss																					
	Integ							72	24													
	Auth																					
	Avail																					
	Util																					

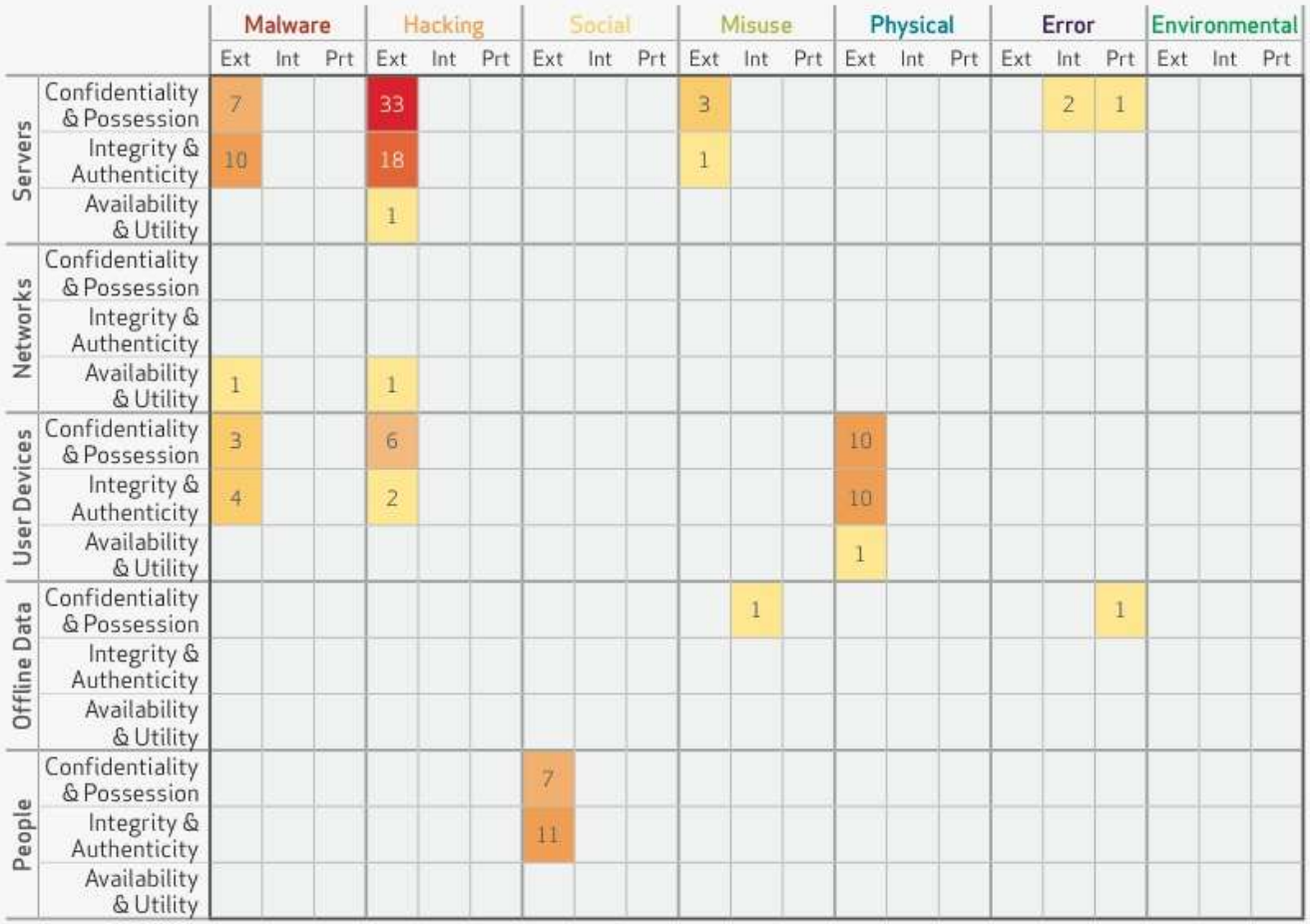
None — Least frequent — Most Frequent

"Only 55 of the 630 possible events have a value greater than 0…90% of the threat space was not in play at all"

Source: 2011 Verizon Business Data Breach Investigations Report (DBIR)

2012: Attacks Density (4Realz DBIR Style)

Figure 9. VERIS A⁴ Grid depicting the frequency of high-level threat events – LARGER ORGS



		Malware			Hacking			Social			Misuse			Physical			Error			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Confidentiality & Possession	7			33						3							2	1			
	Integrity & Authenticity	10			18						1											
	Availability & Utility				1																	
Networks	Confidentiality & Possession																					
	Integrity & Authenticity																					
	Availability & Utility	1			1																	
User Devices	Confidentiality & Possession	3			6									10								
	Integrity & Authenticity	4			2									10								
	Availability & Utility													1								
Offline Data	Confidentiality & Possession											1							1			
	Integrity & Authenticity																					
	Availability & Utility																					
People	Confidentiality & Possession							7														
	Integrity & Authenticity							11														
	Availability & Utility																					

"Only 22 of the 315 possible events have a value greater than 0…93.1% of the threat space was not in play at all"

Source: 2012 Verizon Business Data Breach Investigations Report (DBIR)

2011 VZ DBIR: Non-CCN Asset Type Breakdown

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

Source: 2010 & 2011 Verizon Business Data Breach Investigations Report (DBIR)

2012 VZ DBIR: Non-CCN Asset Type Breakdown

Table 11. Varieties of data compromised by percent of breaches and records

Variety	Label in Fig 32	All Orgs		Larger Orgs	
		Breaches	Records	Breaches	Records
Payment card numbers/data	CardData	48%	3%	33%	1%
Authentication credentials (usernames, pwds, etc.)	Credentials	42%	1%	35%	1%
Personal information (Name, SS#, Addr, etc.)	Personal	4%	95%	27%	98%
Sensitive organizational data (reports, plans, etc.)	OrgData	2%	<1%	22%	<1%
Bank account numbers/data	BankData	2%	1%	10%	1%
System information (config, svcs, sw, etc.)	SysInfo	2%	<1%	15%	<1%
Copyrighted/Trademarked material	Copyright	1%	1%	3%	<1%
Trade secrets	TradeSecret	1%	<1%	12%	<1%
Classified information	Classified	<1%	<1%	2%	<1%
Medical records	Medical	<1%	<1%	2%	<1%
Unknown (specific type is not known)	Unknown	44%	<1%	2%	<1%

Source: 2012 Verizon Business Data Breach Investigations Report (DBIR)

Think About Work Effort/Factor

What Do You Look Like To Different Adversaries?

Real Life Example from a Defense Industrial Base Company

Who Are The Threats?

What Do They Want?

What Are Their TTPs?

Deployed Specific Technology and Processes—Forced Adversary to Change TTPs Or Target Other Organizations

Real Life Technology Examples

Work Effort

- WebLabyrinth

http://code.google.com/p/weblabyrinth/

- SCIT: Self Cleansing Intrusion Tolerance

http://cs.gmu.edu/~asood/scit/

Respond and Recover

- FOG Computing

http://sneakers.cs.columbia.edu:8080/fog/

- Honeyports

http://honeyports.sourceforge.net/

Photo - http://www.flickr.com/photos/shannonholman/2138613419

Neither presenter has any affiliation with these technologies

Adversary ROI – Getting Non-Security Executives Involved

- What protected or sensitive information do we have?
- What adversaries desire the information and why?
- What is the value of the information to the organization?
- How would the adversary value it?
- What are the adversaries capabilities?
- What controls protect the information?

How To Apply To Enrich Current Security Investments

- Enrich incident response
  - Increase aim of incident responders
  - Detect false flags
- Enrich Security Information and Event Management (SIEM)
  - Cluster assets or methods by adversary class - new "pivots" to interpret security events
- Enrich Budgeting
  - More precision in how you apply investment

Apply: Final Thoughts

- Start with a blank slate!
- Engage non-security people
- Identify your most likely adversaries
- Obtain/share adversary centric intel
  - Threat Intelligence
  - Brand/chatter monitoring
  - Information sharing
- Simulate adversary-driven scenarios
  - Table tops/roll playing (w/ Crisis Management)
  - Adversary-Centric Penetration Testing

Thank You / Contact

Josh Corman

@joshcorman

blog.cognitivedissidents.com

David Etue

@djetue

profile.david.etue.net