

HOW TO PREPARE FOR INEVITABLE CYBER ATTACK

JASON SMOLANOFF

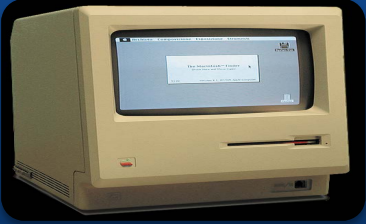


JOHN STARK



johnreedstark
CONSULTING, LLC

ROADMAP FOR TODAY



INITIAL THOUGHTS



QUICK RECAP OF THE THREAT



SOME IMMEDIATE RECOMMENDATIONS

EXTRAORDINARY PROBLEM: GROWING EXPONENTIALLY



THE DATA BREACH WORLD



ALPHABET SOUP

O	B	N	W	P	Z	P	I	N	X	C	F	N	Y	S
U	J	F	H	O	Y	Y	L	O	E	V	W	A	Z	T
E	C	T	V	V	P	Z	Y	S	E	C	V	T	F	A
V	H	C	P	A	Z	M	J	J	M	X	X	S	Y	T
K	V	W	R	V	U	S	S	S	T	X	U	W	U	E
A	W	N	S	I	R	P	V	I	O	D	E	F	I	A
A	R	W	P	Z	X	A	I	U	F	L	I	G	Y	G
F	I	N	R	A	T	R	U	S	Y	B	C	O	M	S
Z	P	J	G	Q	W	Z	N	Q	F	C	L	K	E	A
A	P	V	G	C	S	B	G	B	F	A	Z	C	F	D

LAWS & REGULATIONS



Paradigm shift







WHERE TECHNOLOGICAL
INFRASTRUCTURE HAS
EXPANDED DRAMATICALLY

WHERE DATA-POINTS
RESIDE ON MULTIPLE
PLATFORMS



WHERE DATA
BREACHES DON'T
DEFINE VICTIM
COMPANIES; HOW
THEY RESPOND TO
THEM DOES

HACKING: THE GOOD OLD DAYS



The original "Denial of Service" Attack

©2000 iStockphoto.com

Account Takeover.

A Dire Online Crime



TODAY'S DATA BREACHES



- State-sponsored and Industrial Espionage
- Theft of IP, Emails
- Leaks of Confidential Information
- Lost Laptops, Servers, Backup Tapes
- Unauthorized Access, Clandestine Malware
- Cyber-extortion
- Insider Trading
- Hacktivism
- DOS (much easier)

TODAY'S TARGETS

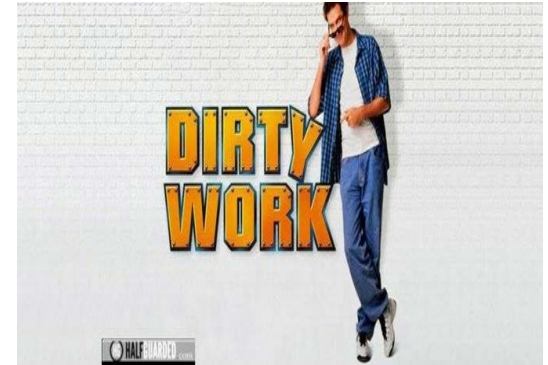
Financial Info



Logons/Passwords



Embarrassing Info



Intellectual Property



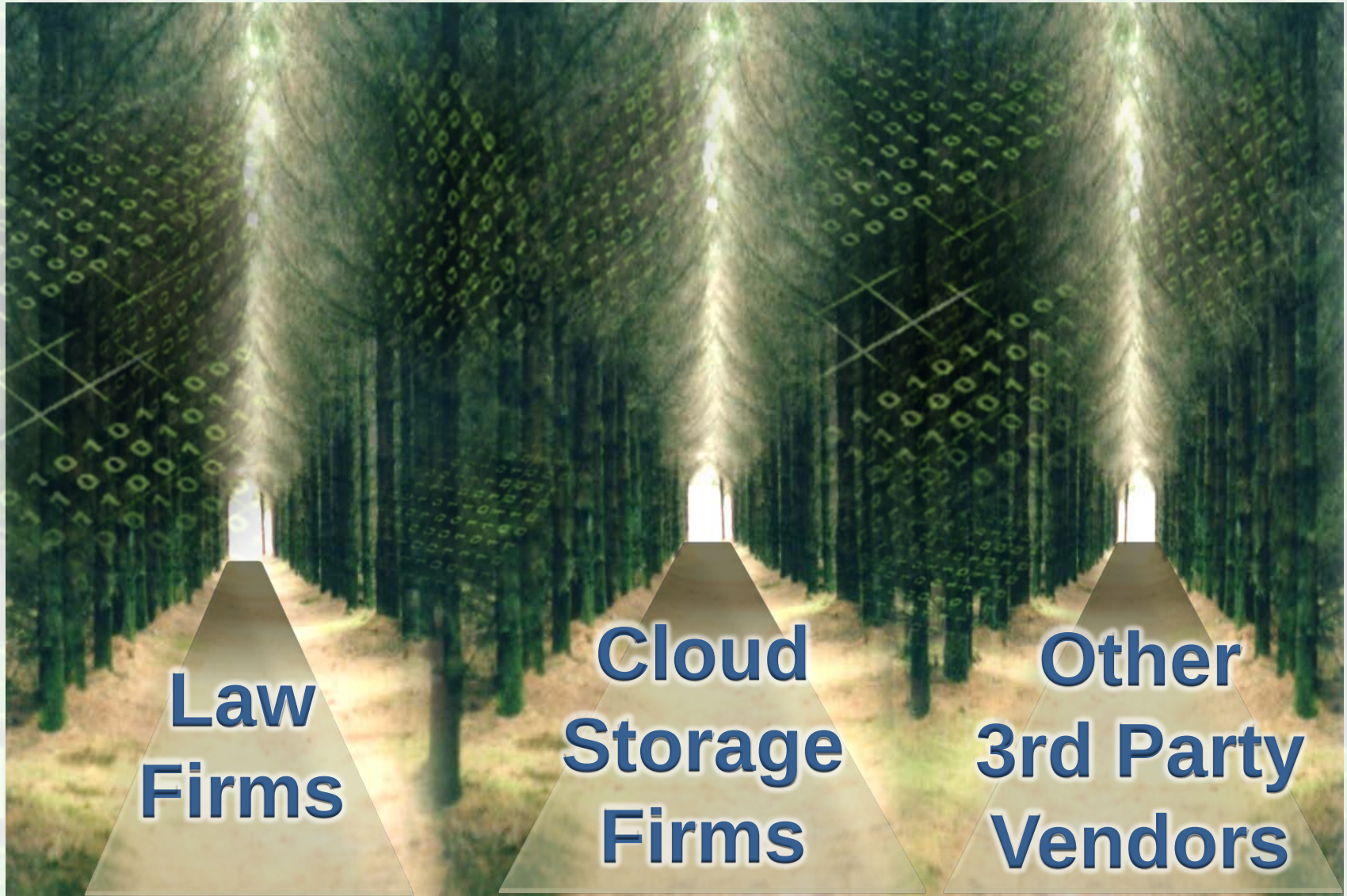
Emails



Shoot First, Ask Questions Later



NEW ATTACK VECTORS AND PATHWAYS



**Law
Firms**

**Cloud
Storage
Firms**

**Other
3rd Party
Vendors**

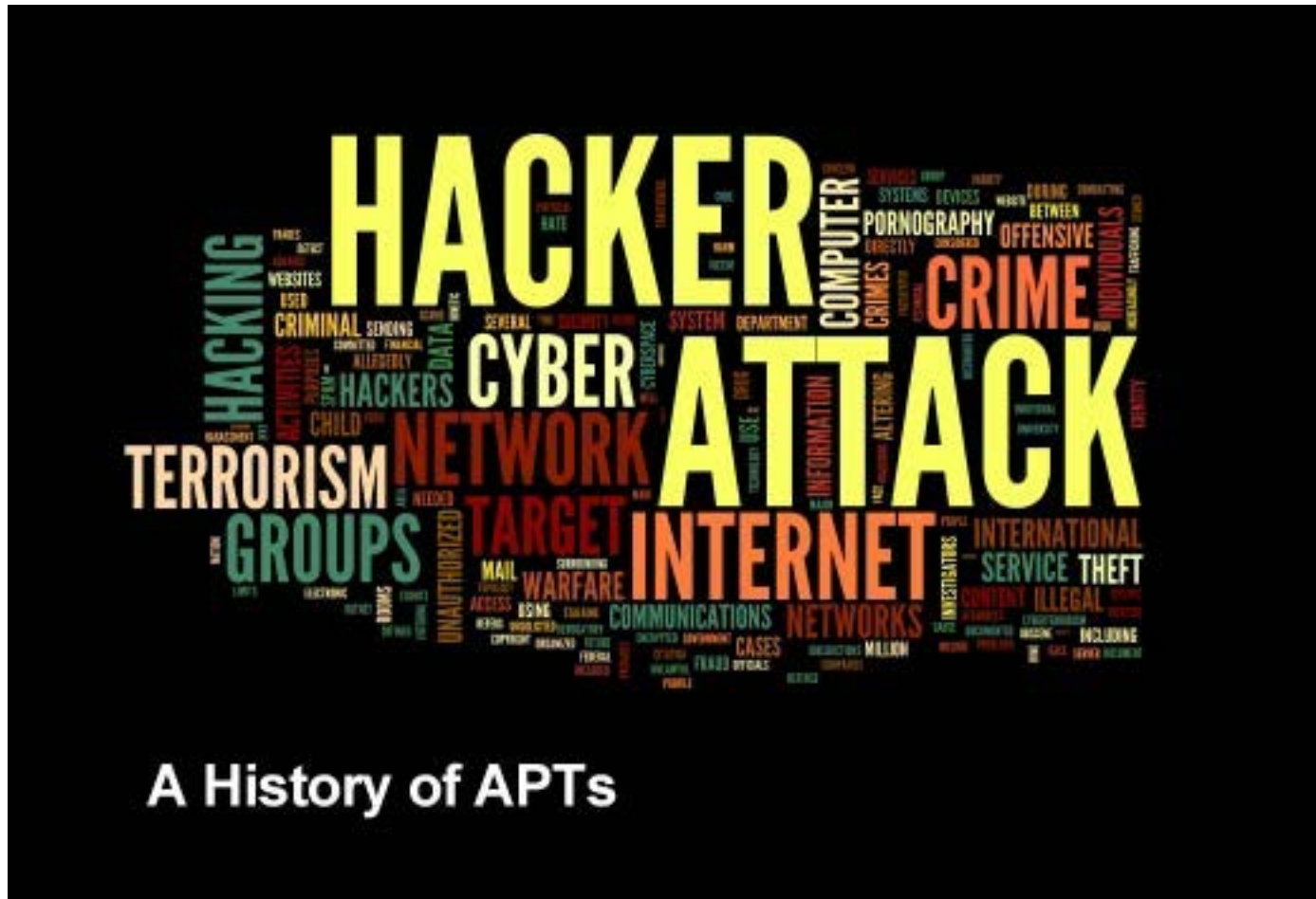
POLLING QUESTION #1

(CPE REQUIREMENT)

My company is well-prepared to defend against cyber-attacks:

- 1) Strongly Agree**
- 2) Agree**
- 3) Disagree**
- 4) Strongly Disagree**

FOUR ADVERSARY CLASSIFICATIONS: STATE SPONSORED



FOUR ADVERSARY CLASSIFICATIONS:

ORGANIZED CRIME



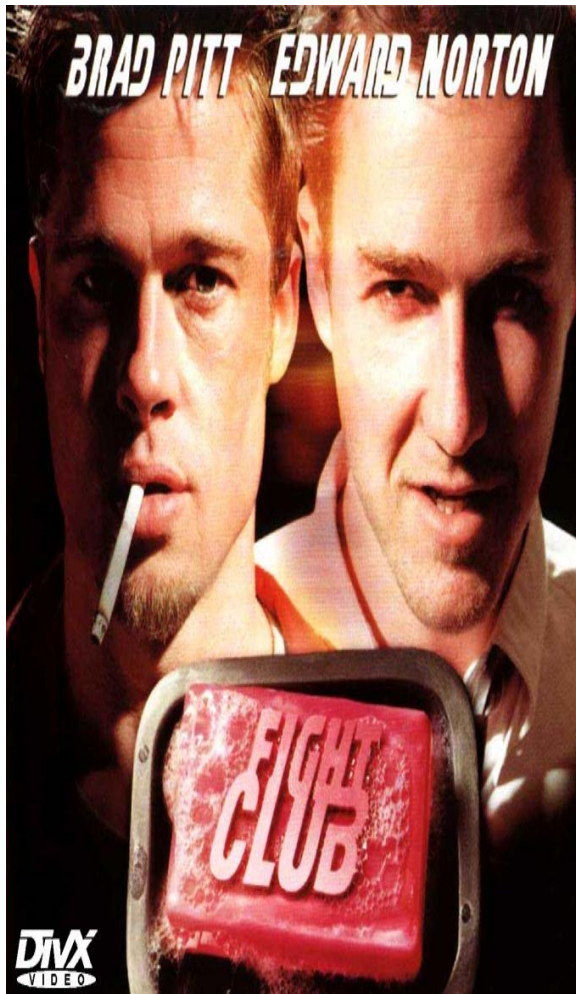
FOUR ADVERSARY CLASSIFICATIONS:

HACTIVISTS



FOUR ADVERSARY CLASSIFICATIONS:

INTERNAL THREAT



BLENDED ATTACK TACTICS



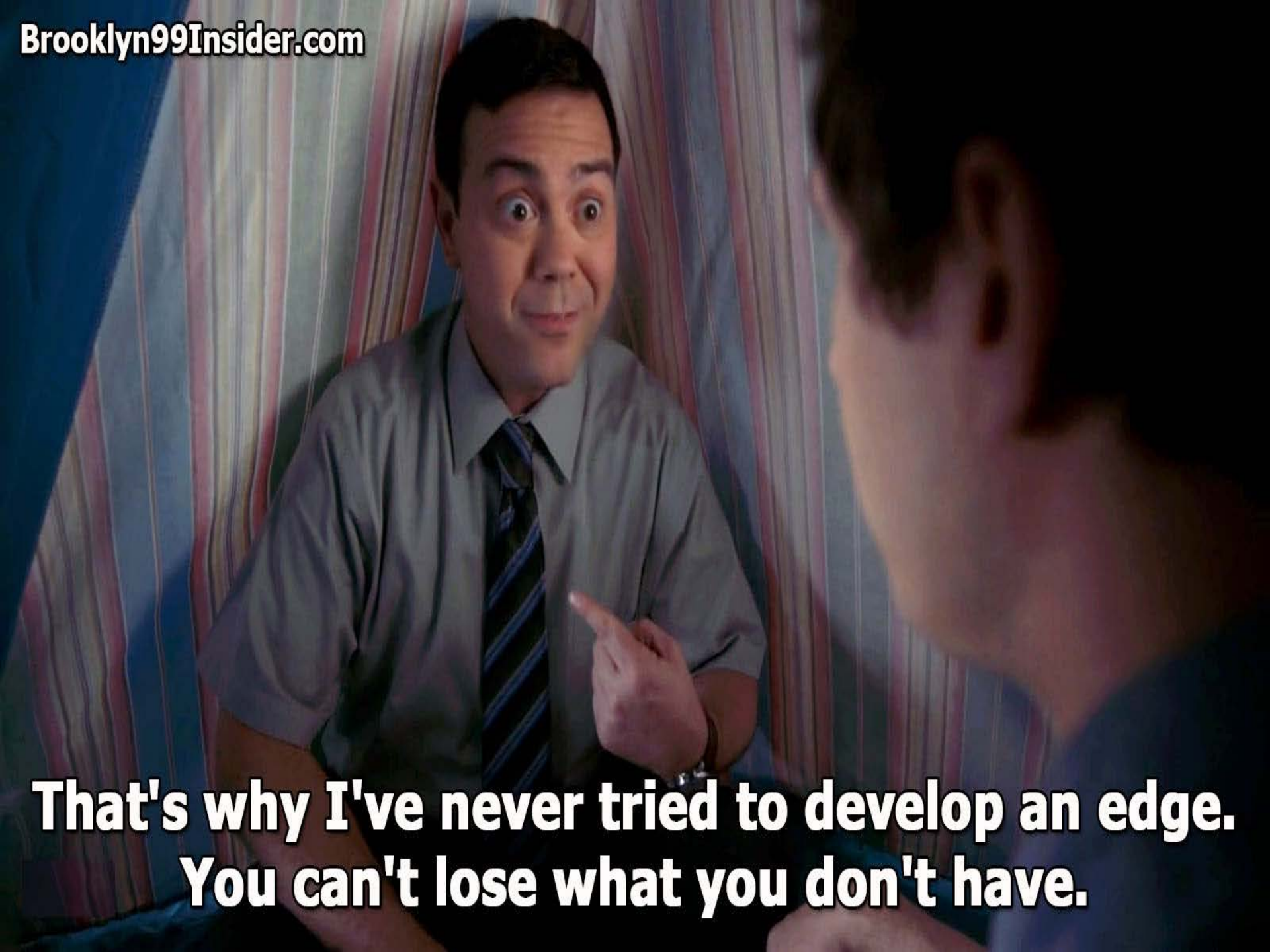
Stealth Attacks



**False Flag Ops to
Gather Intel**



**Target
Communications and
Infrastructure**

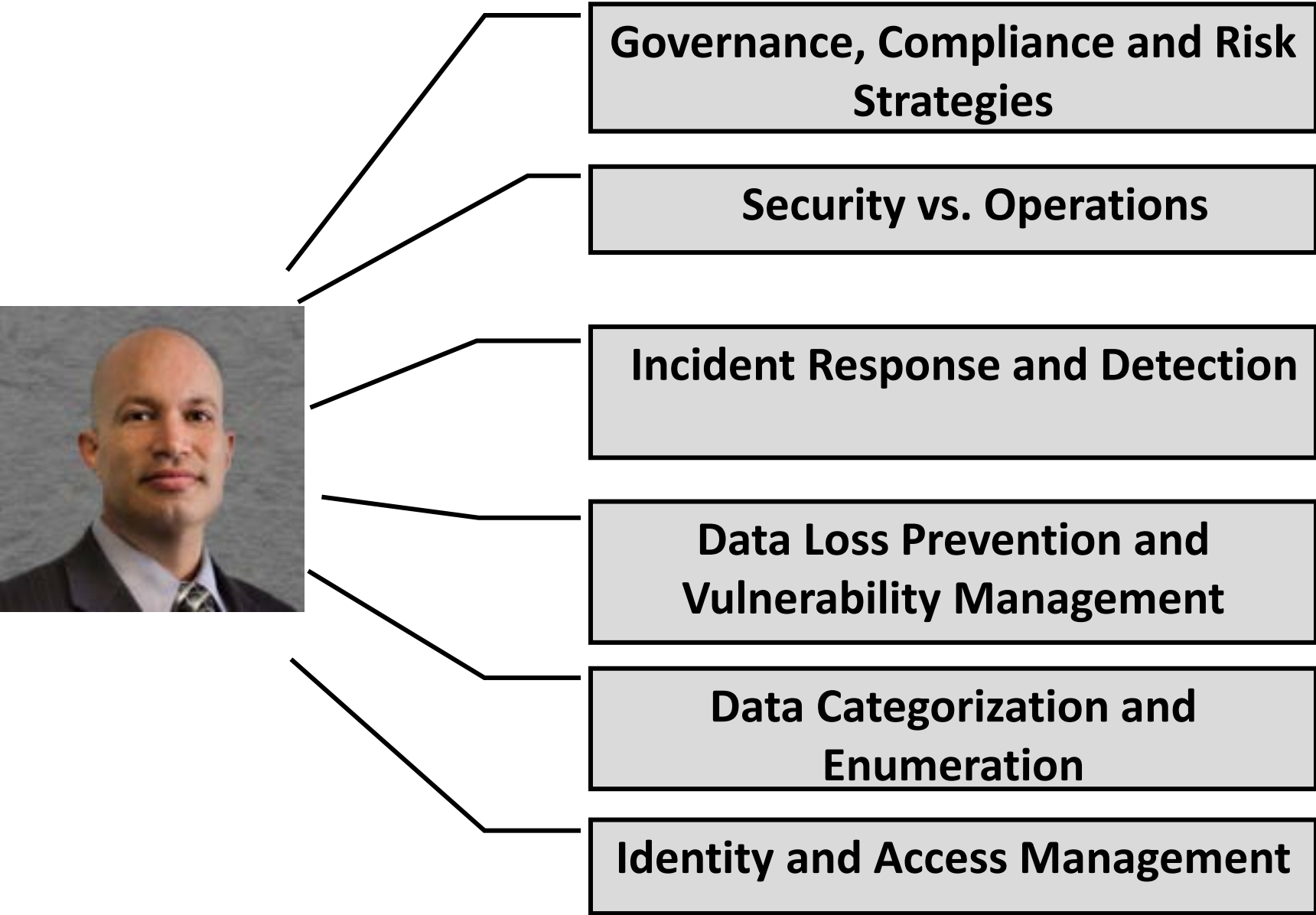
A still from the TV show Brooklyn Nine-Nine. Captain Raymond Holt (Jeffrey Tambor) is sitting in a chair, looking surprised with wide eyes. He is wearing a light blue short-sleeved shirt and a dark blue striped tie. He is pointing his right index finger towards Jake Peralta (Jake Gyllenhaal), who is in the foreground, seen from the back of his head and shoulder. The background consists of vertical striped curtains in shades of blue, red, and white.

**That's why I've never tried to develop an edge.
You can't lose what you don't have.**

CYBER RISK MANAGEMENT



Typical Considerations



Governance, Compliance and Risk Strategies

Security vs. Operations

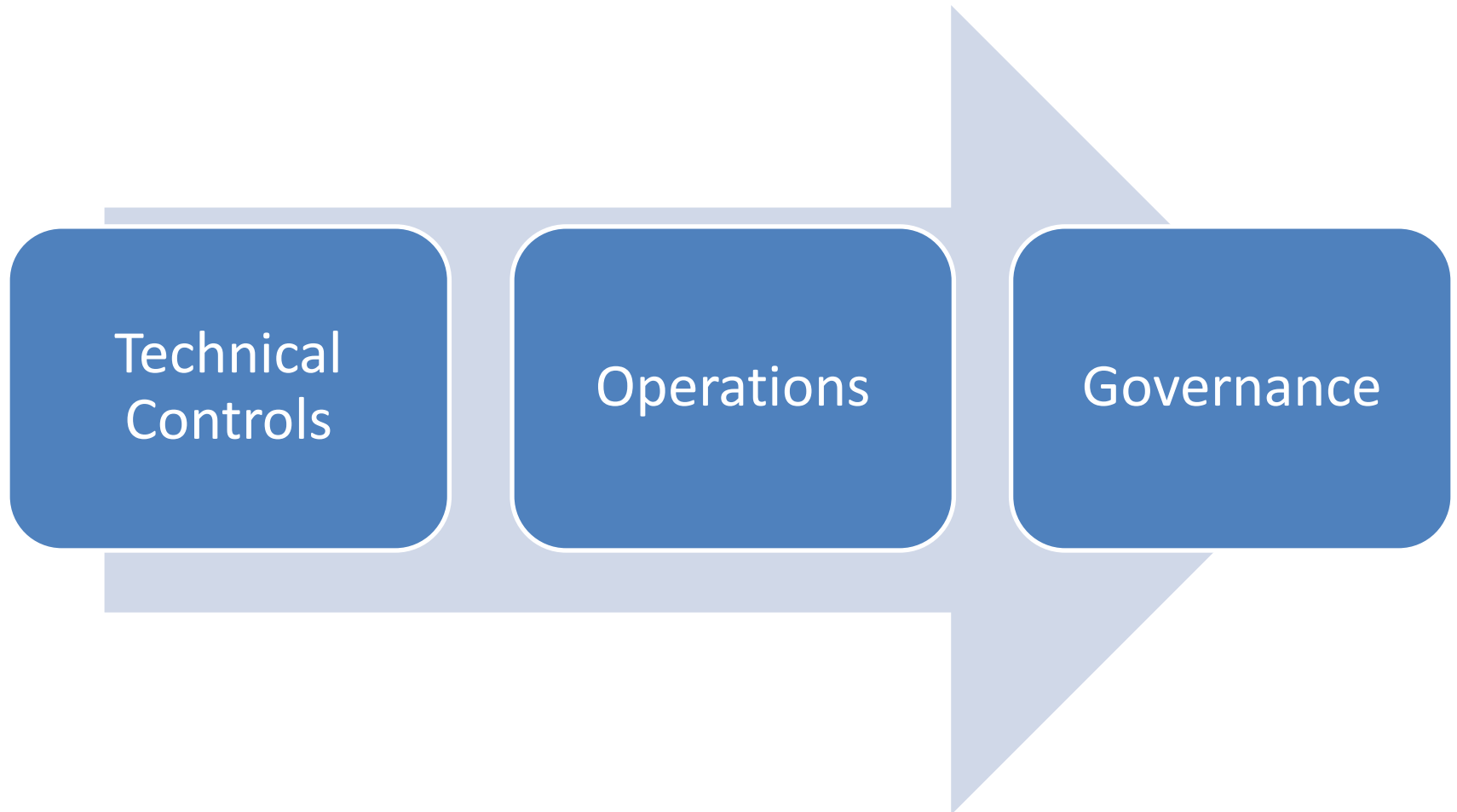
Incident Response and Detection

Data Loss Prevention and Vulnerability Management

Data Categorization and Enumeration

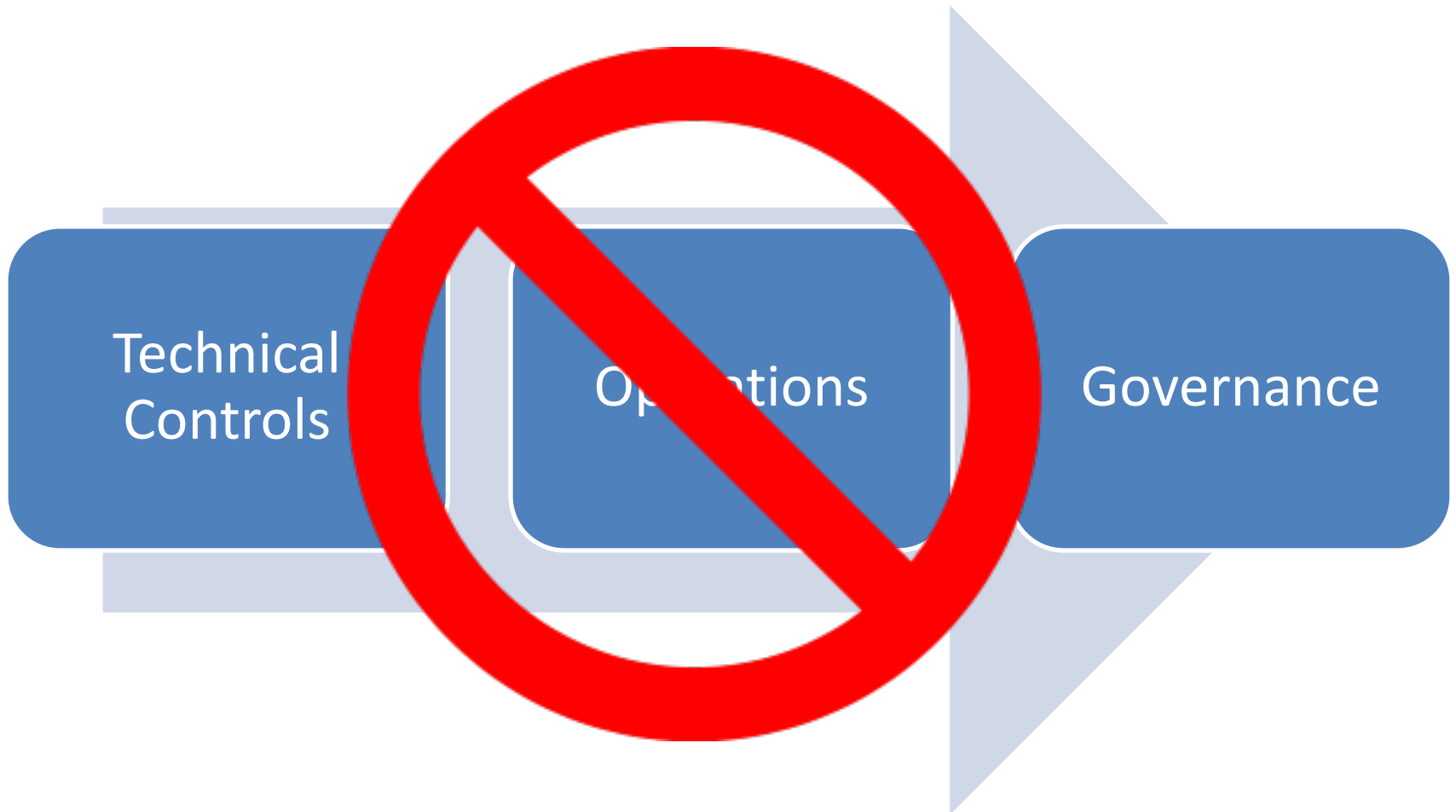
Identity and Access Management

Tool Based Strategy?

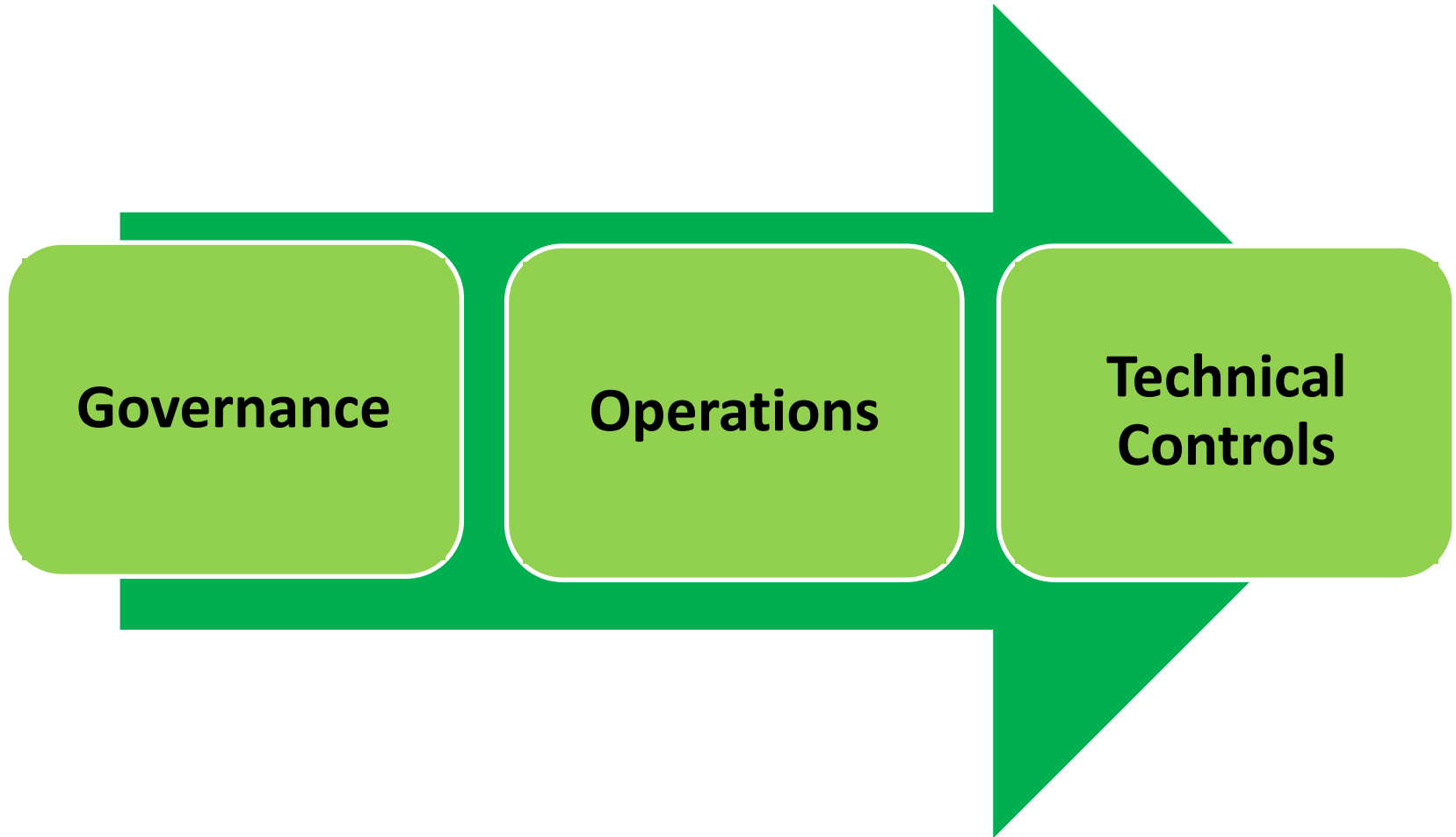


Most Data Breaches Occur Based Upon This Strategy!

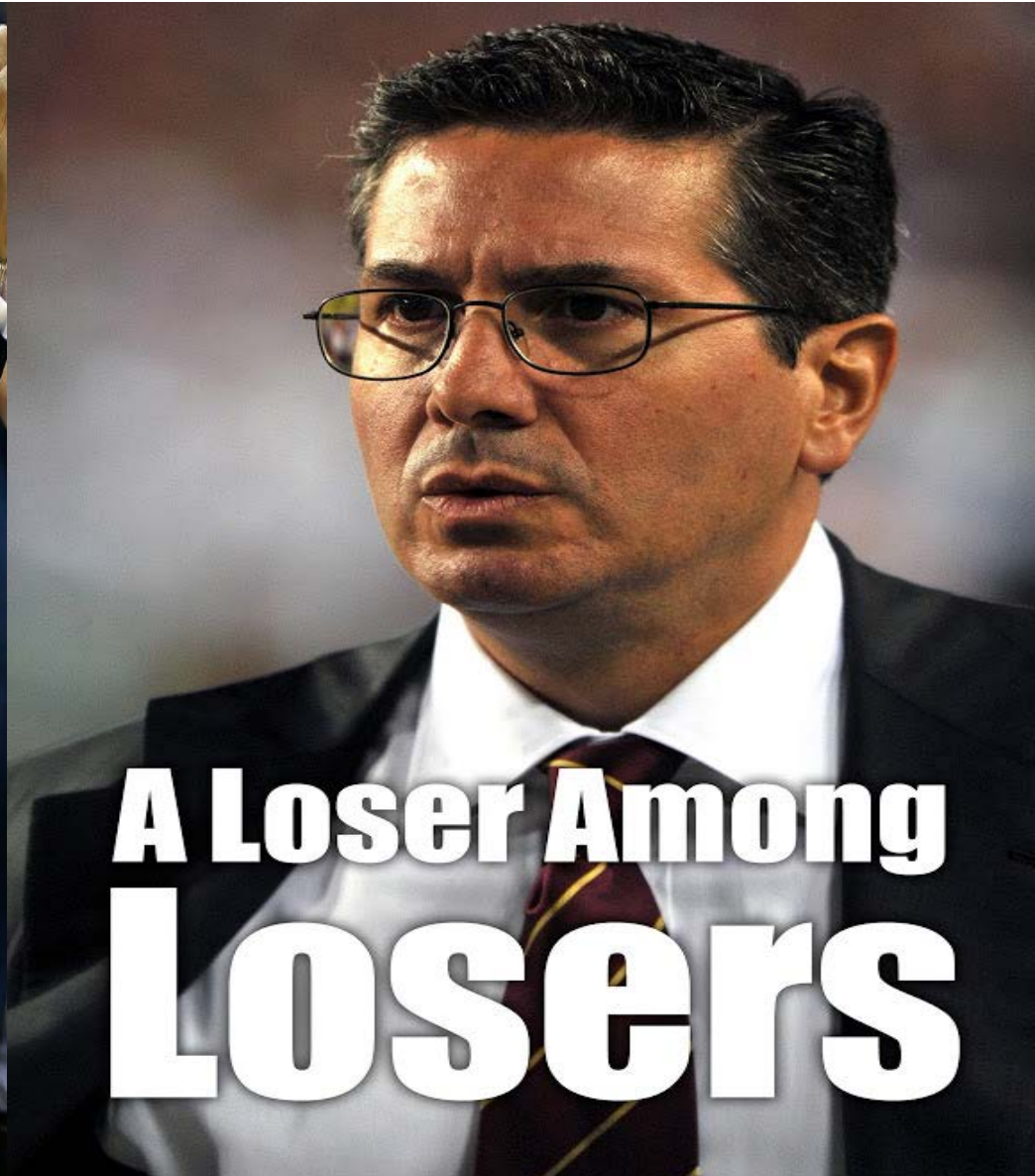
Tool Based Strategy?



Most EFFECTIVE Strategy to Mitigate Risk



TOP DOWN COMMITMENT?



Limitations of Internal Resources

A man's
got to
know
his
LIMITATIONS



FLEXIBLE IT SECURITY BUDGETING



INCIDENT RESPONSE PLAN



Response Team Components

IT

Security

Legal

Crisis
Communications

Forensic Experts

Outside Counsel

INCIDENT RESPONSE FIRM ON SPEED DIAL



INCIDENT RESPONSE REPORTING LINES

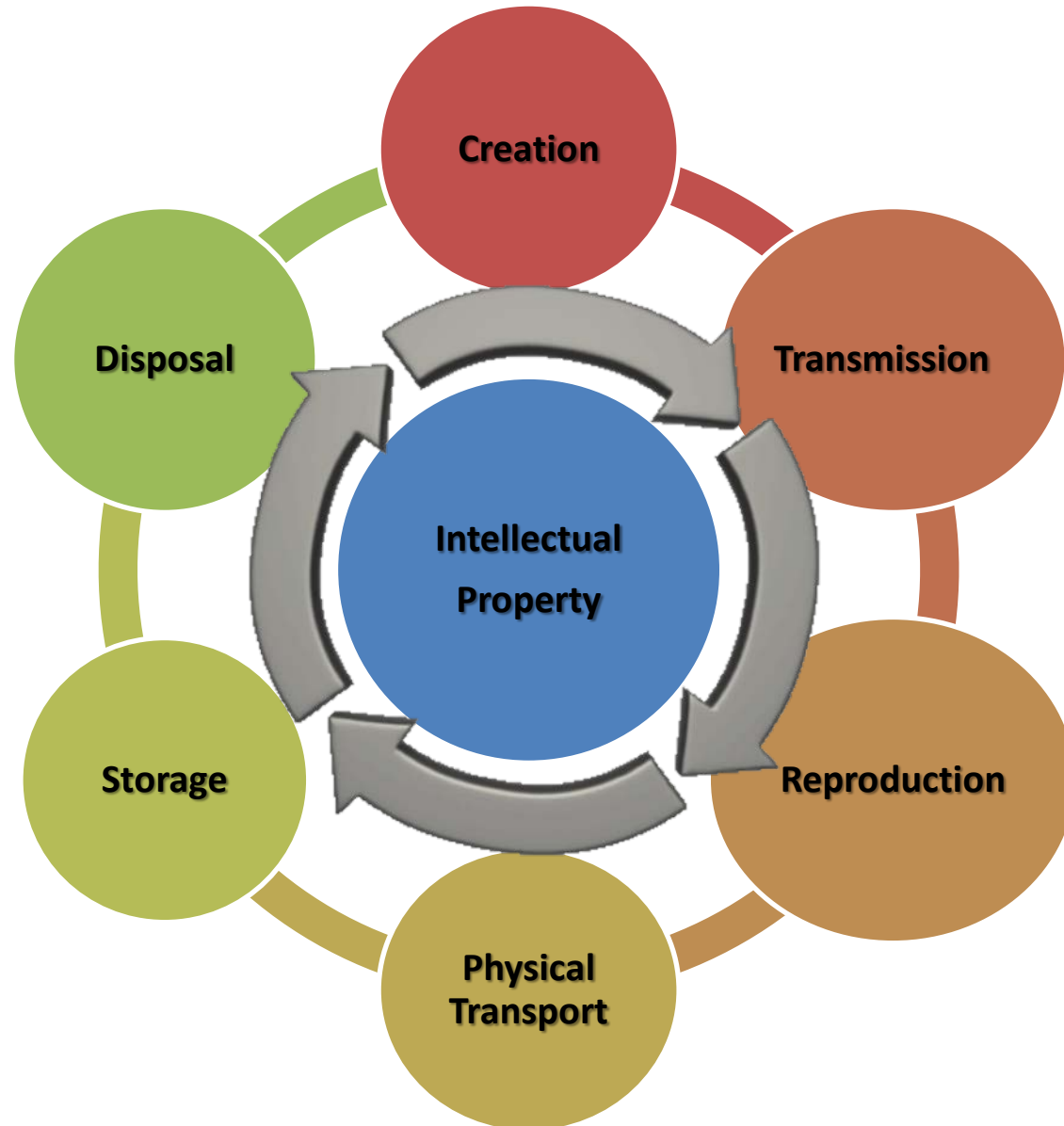


"Yes, I am employee of the month again. And yes, I'm the one who chooses the employee of the month. And no, I don't see a conflict of interest."

DATA MAPPING



Locate Sensitive/Regulated Data/Key Assets?



ORG CHARTS

THE MICHAEL CORLEONE FAMILY

KEY TO ACTIVITY CODE

- A. CURRENTLY IN JAIL FOR NARCOTICS
- B. AWAITING TRIAL FOR NARCOTICS
- C. PREVIOUS CONVICTION FOR NARCOTICS
- D. SUSPECTED OF BEING ACTIVE IN NARCOTICS
- E. GAMBLING
- F. SHYLOCKING
- G. LABOR RACKETEERING
- H. VENDING MACHINES AND/OR JUKE BOXES
- I. EXTORTION, STRONG ARM AND MURDER
- J. COUNTERFEITING
- K. CRIMINALLY RECEIVING
- L. ALCOHOL TAX VIOLATIONS

BOSS



MICHAEL CORLEONE
ALIAS
"DON CORLEONE"

SUCCESSOR TO:

VITO CORLEONE
ALIAS
"DON CORLEONE"
FBI # 397385
DECEASED

UNDERBOSS
FREDO CORLEONE



CONSIGLIERI
THOMAS HAGEN



SANTINO CORLEONE
ALIAS
"SONNY"
FBI # 473001
DECEASED

CAPO REGIME

FORMER:

PETER CLEMENZA
ALIAS
"FAT CLEMENZA"
FBI # 100375
DECEASED



SALVATORE TESSIO
ALIAS
"SAL"
FBI # 320611
DECEASED

PRESENT:



AL NERI
FBI # 563241
(G, K)



ROCCO LAMPONE
FBI # 326412
(G, I)



FRANK PENTANGELI
ALIAS
"FRANKIE FIVE ANGELS"
FBI # 641323
(E, G, H, K)

BUTTONS - SOLDIERS



LUCA BRASI
FBI # 63432
DECEASED
PAULI GATO



FBI # 742611
DECEASED
FRANCIS FORDUCCI
ALIAS
"THE KID"
FBI # 324511



ANGELO GRANELLI
ALIAS
"THE TROJAN"
FBI # 436561
(A, E)



GINO FREDONNA
ALIAS
"PRETTY BOY"
FBI # 223314
DECEASED



FRANK DARRA
ALIAS
"FRANKIE DARE"
FBI # 204325
(A, C, G)



CHRIS PENARRI
ALIAS
"THE MANAGER"
FBI # 416311
(H, I)



NINO ARNELDI
ALIAS
"THE PATCH"
FBI # 312112
(G, H, I)



RICARDO SIMINNI
ALIAS
"POWDER"
FBI # 723412
(H, I)



GINO CORSETTA
FBI # 611294
(A, B)



SABASTINO SABELA
FBI # 533495
(A, B, C, D)



ALPHONSE EVOLLONI
ALIAS
"AL OVE"
FBI # 177123
DECEASED



DONATO TOLENTINICCI
FBI # 134375
(G, H, I)



VICTOR VINATTONI
ALIAS
"VICKY VEAL"
FBI # 177321
GO



FRANK CORTEALE
FBI # 463011
(H, I)



BARTOLO NENI
ALIAS
"O'NEAL"
FBI # 647073
(A, B, C)



LAWRENCE TIPPARI
FBI # 892538
(I, K)



PETER LEONE
ALIAS
"THE LION"
FBI # 360644
(A, B, C, D)



GAETANO DE LUNA
ALIAS
"GARY DEE"
FBI # 892668
(E, F)



CALOGERO RADENI
FBI # 144176
(H)



ETTORE RAOENI
ALIAS
"OILY HAND"
FBI # 493493
(F)



JOSEPH BRONSKI
ALIAS
"JOEY JAIL"
FBI # 467032
DECEASED



GAETANO SIRILLO
FBI # 936000
(H, I)



CASSANDROS FRACCA
ALIAS
"DAVID GELLY"
FBI # 428933
(H, I)



ROBERTO NELENZA
ALIAS
"THUNDER BOB"
FBI # 339933
(E, F, G, I)



RAFILO GERNZO
FBI # 416230
(I)



SALVATORE PLUMARI
ALIAS
"SALLY PEE"
FBI # 210077
(L)



NATALE PARRI
ALIAS
"FAT NAT"
FBI # 445512
(H, I)



TONY DINEGIO
ALIAS
"TONY DING"
FBI # 133401
(E, H, I)



CHARLES LOCIRNO
FBI # 136311
DECEASED



WILLIAM CICCII
FBI # 473289
(E, F, G, I)



CARMINE CORONDA
ALIAS
"THE PLUNGE"
FBI # 179205
(E, H, L)



SAMUEL COROCCO
FBI # 329661
(E, H)



ALPHONSE BARINO
ALIAS
"AL BARRET"
FBI # 279532
(G)

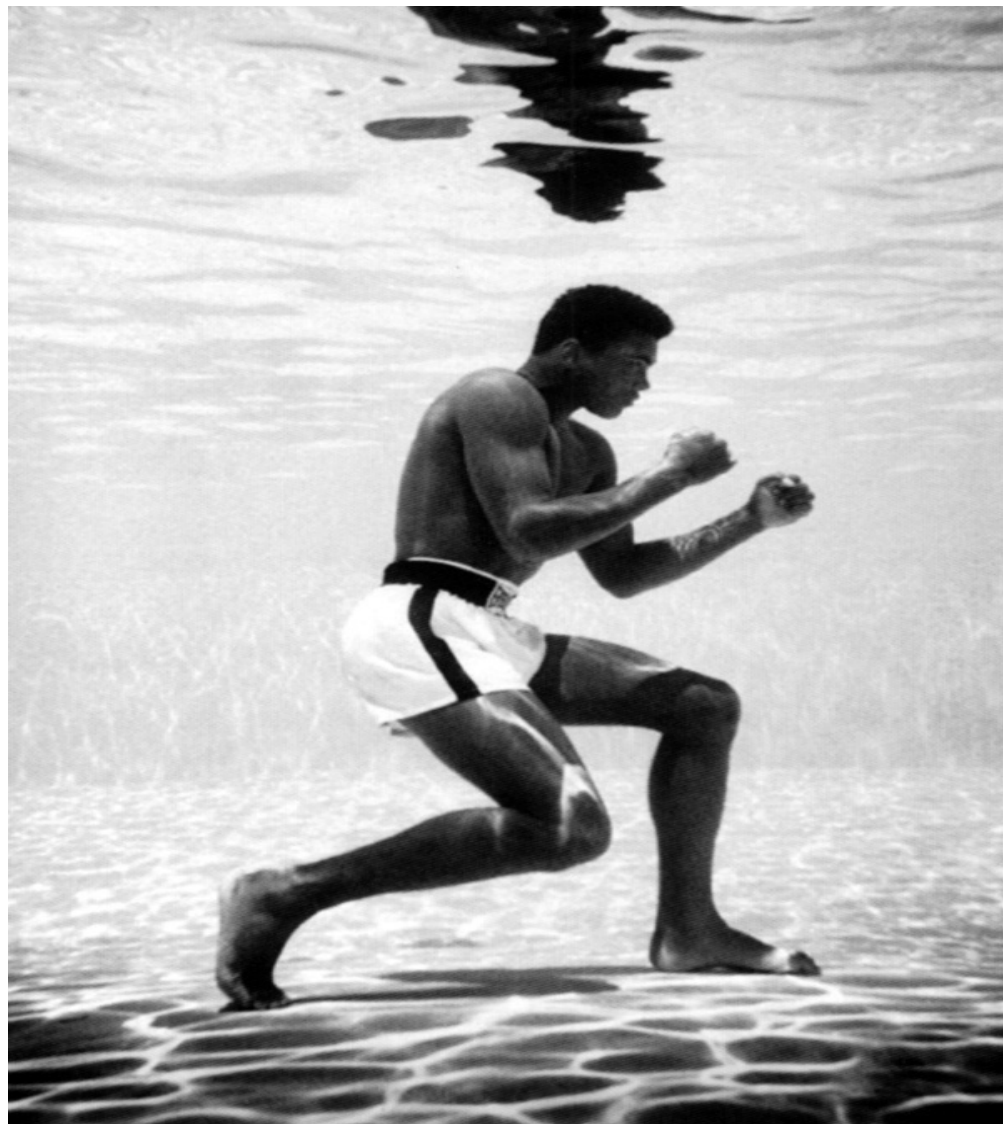


CARMEN DELLA
FBI # 146372
(G)



CRISTOFORO D'BINNA
FBI # 432411
(H, I)

TRAINING PROGRAMS



DRILLS & TABLE-TOP EXERCISES

Springfield Daily Examiner

JUNE 26, 1981 "THE PLACE FOR NEWS" 25 CENTS

ARMY HERO RETIRES



Announces HulkaBurger Franchise

By STEVE BENNETT

After 27 years in the army, local hero Sgt. Joe Hulka has announced his intentions to "turn in his fatigues."

Well known for his courageous actions in Czechoslovakia, Sgt. Hulka has told the Examiner that "There's big bucks in burgers, and Springfield's the

(continued on page 2)

POLLING QUESTION #2

(CPE REQUIREMENT)

My company has a difficult time hiring skilled cybersecurity personnel:

- 1) Agree**
- 2) Disagree**
- 3) Don't Know**

PERSONNEL CONTINUITY

BUDGET FOR RECRUITMENT, HIRING & RETENTION



BUSINESS CONTINUITY PLAN



POLLING QUESTION #3

(CPE REQUIREMENT)

My Company undergoes pen testing:

- 1) Annually**
- 2) Occasionally**
- 3) Has Done so Once or Twice**
- 4) Don't Know**

PENETRATION TESTING/RISK ASSESSMENTS



3RD PARTY DUE DILIGENCE



PHYSICAL SECURITY

INEXORABLY LINKED TO CYBERSECURITY

People

- Insiders: background checks
- Outsiders: sign-in

Places

- Video surveillance
- Keycard access

Things

- Off-site storage
- Old data disposal



DOCUMENT YOUR PREPARATION EFFORTS



Yes!



No!

LAW ENFORCEMENT LIAISON

PRE-BREACH



STAY CURRENT



POLLING QUESTION #4 (CPE REQUIREMENT)

My company has cyber insurance:

- 1) Agree**
- 2) Disagree**
- 3) Don't Know**

WANTED

Cyber Insurance

CYBER INSURANCE: WHY?

- ✓ To Transfer Unmitigated & Unwanted risks
- ✓ To Fill Gaps not Currently Covered
- ✓ To Reduce Risk of Financial & Other Losses
- ✓ CGL May Be Inadequate



CYBER INSURANCE PHENOMENON

- ✓ Market is immature and evolving
- ✓ 50+ insurance companies offering
- ✓ No standard policy language



CYBER INSURANCE/D&O INSURANCE



**Directors and
Officers
Insurance**

CYBER INSURANCE: BOARD OF DIRECTORS

- ✓ Wachtell February 14, 2017 Report
- ✓ Critical aspect of board's risk oversight role
- ✓ Increased expectation of engagement
- ✓ Key aspect of *risk appetite framework*



CYBER INSURANCE COST

- ☑ Like car insurance . . .
- ☑ What kind of car?
- ☑ Who is the driver?
- ☑ How many miles per week?
- ☑ What is the deductible?
- ☑ What are the coverage limits?
- ☑ What is the state of cybersecurity?



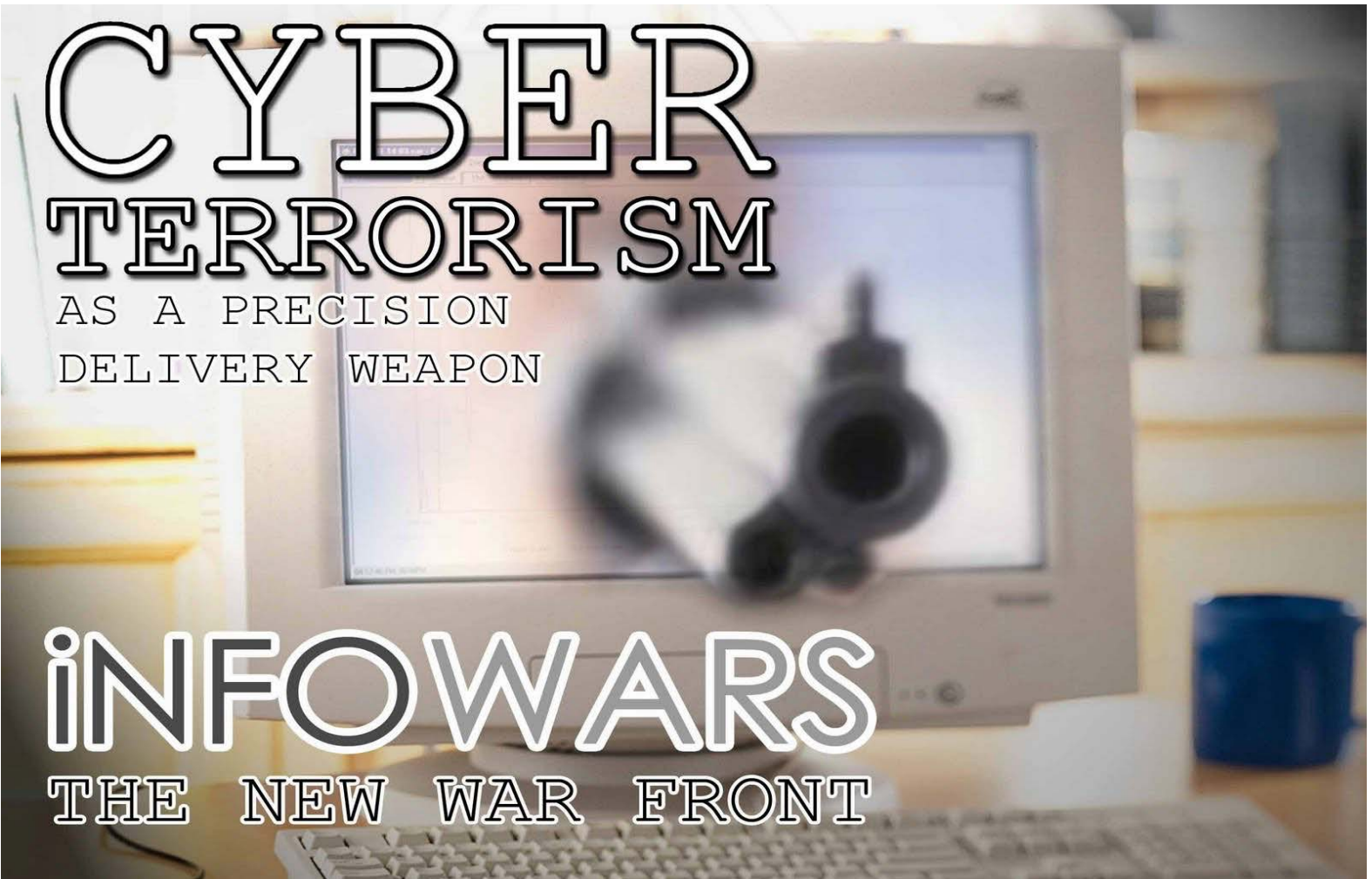
CYBER INSURANCE DILIGENCE



SOME DETAILS . . .

- ☒ How much can your company afford?
- ☒ What type of coverage is needed (Liability? Breach response? Fines and penalties?)
- ☒ What triggers coverage (Stolen laptop or flash drive? APT? Cloud data?)
- ☒ Exclusions?
- ☒ Type of data covered (Public? IP?)
- ☒ Selection of legal/forensic team (Who chooses? Panel?)
- ☒ Notification/ID Monitoring

CYBER EXTORTION/TERRORISM

A computer monitor is the central focus, displaying a blurred image of a handgun. The text 'CYBER TERRORISM' is overlaid in large, white, outlined letters. Below it, 'AS A PRECISION DELIVERY WEAPON' is written in smaller, white, outlined letters. At the bottom, 'iNFOWARS' is written in large, white, outlined letters, and 'THE NEW WAR FRONT' is written below it in smaller, white, outlined letters. The background is a blurred office setting with a keyboard and a blue mug visible.

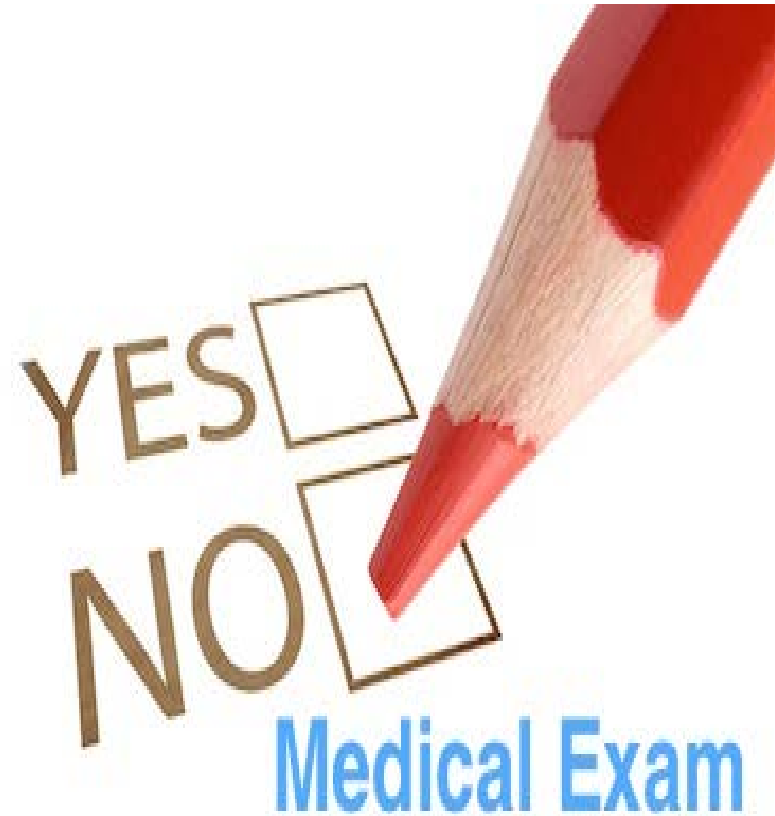
CYBER
TERRORISM

AS A PRECISION
DELIVERY WEAPON

iNFOWARS

THE NEW WAR FRONT

VIGOROUS UNDERWRITING PROCESS



Request “Retroactive” Coverage for Prior, Unknown Breaches



CYBER INSURANCE BATTLEGROUND ISSUES

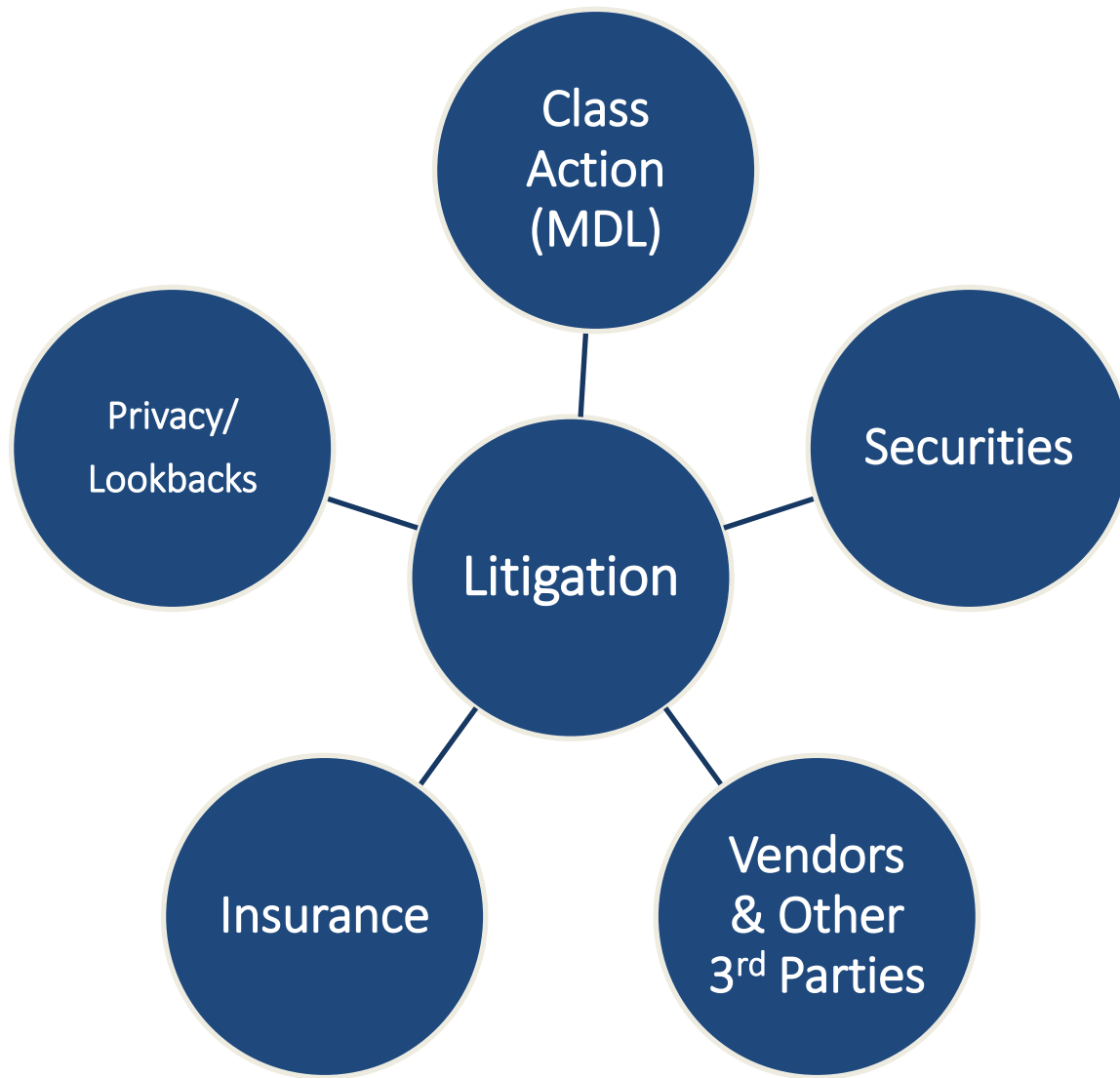
- ☑ Security Requirements (no standard)
- ☑ Act of War and Terrorism Exclusions
- ☑ 3rd Party Acts and Omissions (e.g. cloud)
- ☑ Statutory Damages Coverage (per violation)



COUNSEL AS QUARTERBACK



TYPES OF LITIGATION



SOME LEGAL QUESTIONS

Did an unauthorized party:

- Access
- Acquire
- Misuse
- Disclose PII/PHI

Does investigation show:

- Material compromise
- Actual loss or injury to consumer
- Material risk of ID theft or fraud
- Significant risk of financial, reputational, other harm



SOME LEGAL QUESTIONS

☑ WHO NEEDS NOTICE OR UPDATES?

☑ VICTIMS, BOARD, REGULATORS, BOARD, LAW ENFORCEMENT, INSURANCE CARRIERS, SUPPLIERS, EMPLOYEES, PUBLIC, INTERNAL TEAM? WHEN?

☑ WHAT IS COVERED BY PRIVILEGE?

☑ REPORTS OF INVESTIGATION?

☑ DOCUMENTATION FOR INSURANCE COMPANY?

☑ ALLOW FBI APPLIANCE ATTACH? PROVIDE SYSTEM/IOC COPIES TO LAW ENFORCEMENT?



john@johnreedstark.com

jason.smolanoff@kroll.com

