



Closing Address: Cybersecurity and Internal Controls

Special guest lecturer:

John Reed Stark, President of John Reed Stark Consulting, the author of “The Cybersecurity Due Diligence Handbook” and the former Head of the SEC’s Cybersecurity Enforcement Unit

DATA BREACH RESPONSE, C-SUITES AND THE BOARD: LESSONS, CAVEATS AND REMINDERS





Part One
**Cybersecurity and
Data Breach
Response
Background**



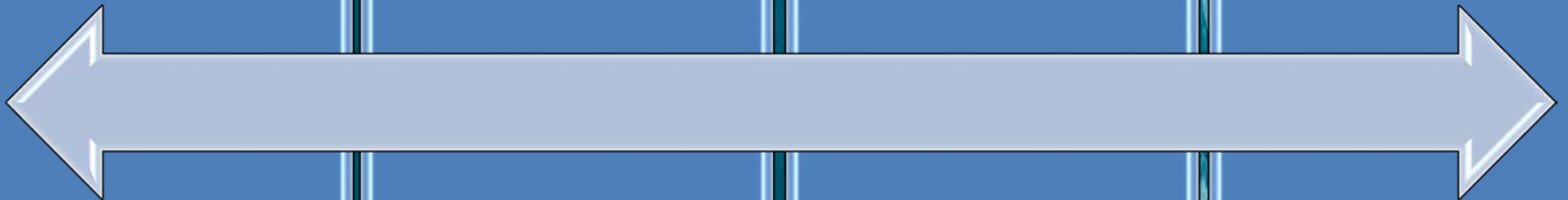
Part Two:
**Upside Down
World of Data
Breaches**



Part Three:
**Data Breach
Response
Workflow**



Part Four:
**A New Paradigm
& Asking the Right
Questions**





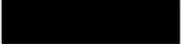








Part One:

Background

EXTRAORDINARY PROBLEM: GROWING EXPONENTIALLY



Selected data breaches by number of consumers/user accounts

COMPANY	SIZE OF BREACH	YEAR DISCLOSED
Yahoo*	 3 billion	2016-17
Yahoo*	 500 million	2016
Marriott	 500	2018
Equifax	 143	2017
Heartland Payment Sys.	 130	2009
LinkedIn	 117	2016
Sony	 100	2011
TJX	 90	2007
Anthem	 80	2015
J.P. Morgan	 76 [†]	2014
Target	 70 [‡]	2013

Death
and
Taxes





Threat

security

crime protection

breach

protect

attack

danger

phishing

laptop

technology

business

warning

data

cyber

criminal

virus

unlock

privacy

bomb

stealing

hacker

hacking

hacked

digital

surveillance

steal

vulnerability

hack

malware

fraud

web

firewall

confidential

leak

password

software

defense

encryption

person

spy

aggression

concept

burglar

symbol

pc

theft

robber

code

information

identity

com

online

alert

searching

internet

network

secrecy

antivirus

thief



**STATE
SPONSORED**

The image features a central red padlock with a blue chain, set against a dark blue background with a grid of binary code (0s and 1s) and red, smoky-like patterns. The word "ransomware" is written in a large, white, sans-serif font across the middle of the image.

ransomware

[illegible]

01100110	
00000110	
0010000100000010010	
11001110110100001110	
011001100111010101011	00000110
0000011010000101001	1001010
0101101001011011100	01000110
1111000100000011011	000100
000001101111011001	10000000
00000100100000000	00000000
1100101001000000	10
001000000110001	1
110001000000100	0
00001011001000	0
110100101110011	
10000101000001	
11011000010111	
10000010010010	
1010010111001	
000101000001	
0111010000101	



INSIDER TRADING



HACKTIVIS TS



INTERNAL THREAT/BAD LEAVERS





**Financial
Info**



**Emails/
Passwords**



**Embarrassing
Info**



**Intellectual
Property**



**Denial of
Service**



**Shoot First,
Ask Questions
Later**



Part Two:

**The Upside Down
World of Data Breaches**

FINANCIAL/HEALTHCARE/PCI REGULATORY COMPLIANCE



LAWS & REGULATIONS



GDPR



**Data Protection
Officer (DPO)**



Compliance



25 May 2018



Data Breaches

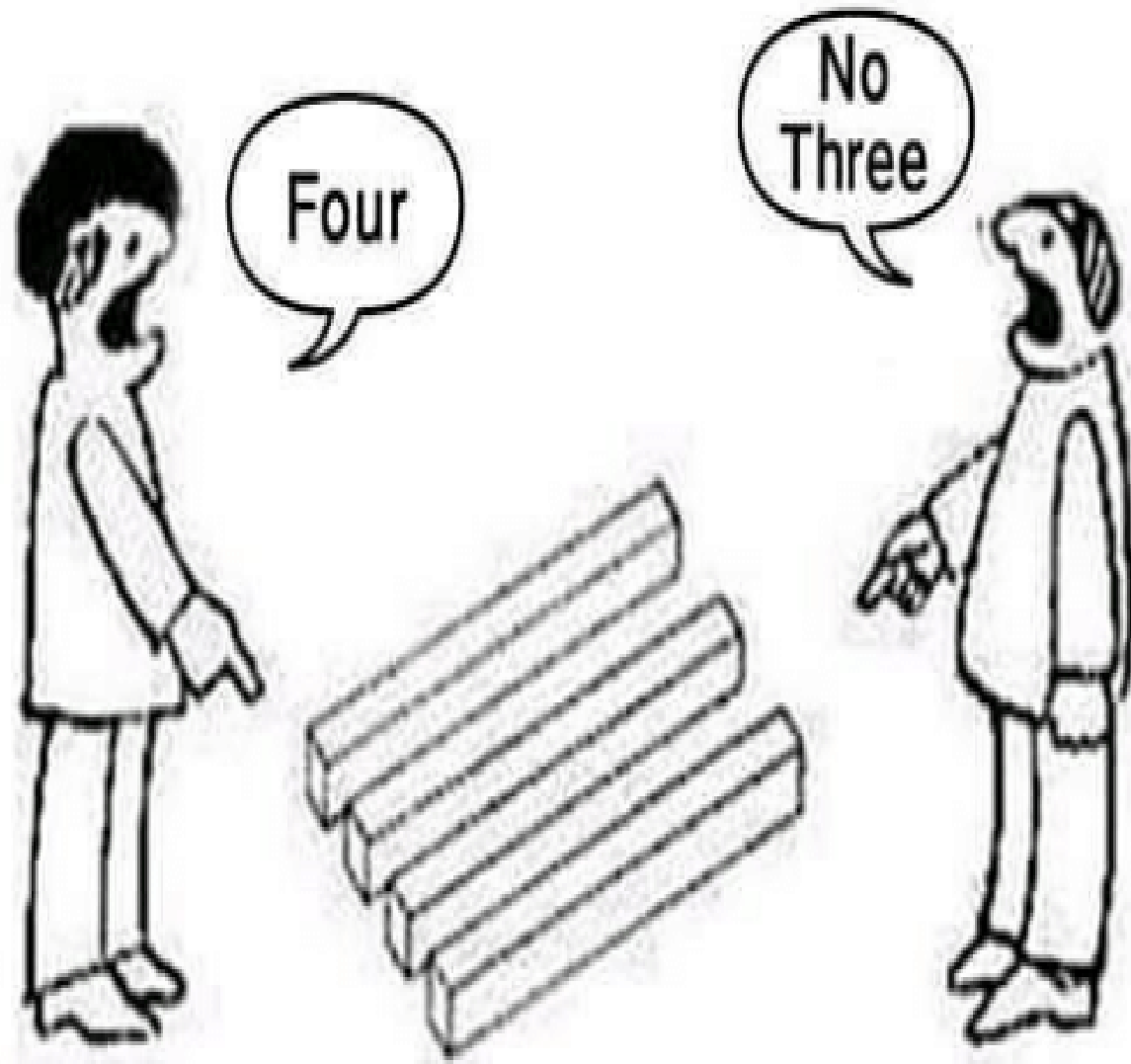


Personal Data

It is really confusing!!!



Payment Card
Industry - Data
Security Standard



The PFI logo consists of the letters "PFI" in a bold, white, sans-serif font, centered within a red square. The square has a thin blue border and is set against a blue background that tapers to the right.

PFI

Contractually Bound to Hire PFI



PFI Beholden to Brands (Not Victim)

The word "VICTIM" is written in large, bold, black capital letters using a marker. It is written on a piece of white, crumpled paper that is set within a square frame. The frame has a blue border and is part of a larger blue banner that tapers to the right.

Victim Company Pays



CONGRESSIONAL INTEREST IS INTENSE

- ✓ Hearings
- ✓ Chronology
- ✓ 36 senators asked DOJ & SEC to investigate Equifax Execs Who Sold stock Before Public Knew About Breach



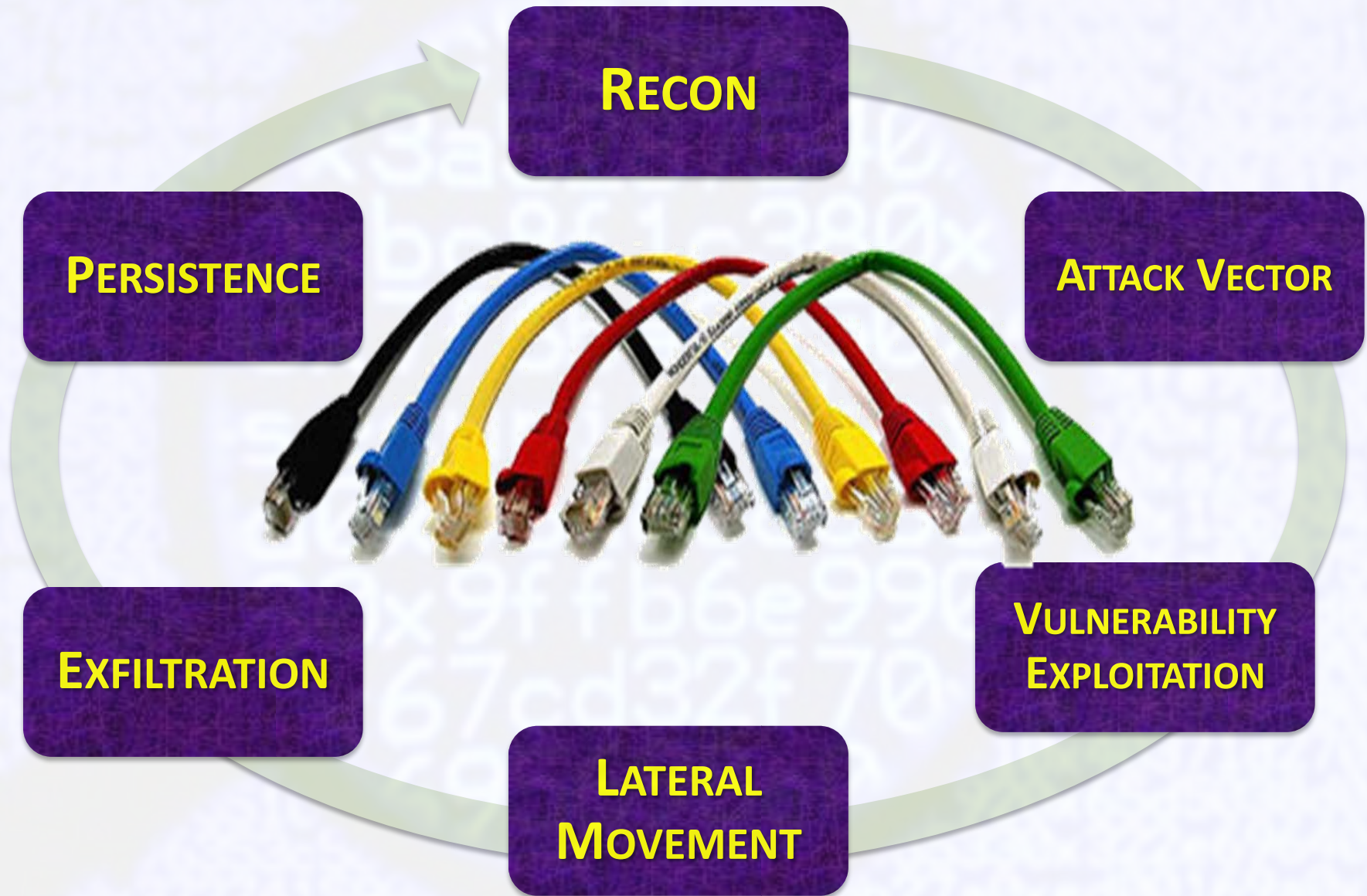


“The Equifax breach is one of the most egregious examples of corporate malfeasance since Enron.”

Part Three:

Data Breach Workflow

IR SEQUENCE OF EVENTS



**Multiple
Back
Doors**

**Multiple
Infected
Machines**

**Stop the
breach**



**Who is at
fault?**



**When will
the other
shoe drop?**



**Is management
in control of
the situation?**



*Am I going to
lose my job?*



**What will
consumers
think? The
public? Our
shareholders?**



**How to
Respond
W/o
Disruption?**



Remediate
malware,
Block IP
Addresses

Rebuild
compromised
systems

Reset
compromised
account
credentials

Initiate
Network and
Host
Monitoring



Preservation



Malware Scans



**Find Artifacts,
Remnants,
Fragments**



DATA BREACH



**Malware Reverse
Engineering**



**Exfiltration
Analysis**



Remediation





Disparate Logs



**Volatile Memory
Capture**



**Scattered Active and
Deleted File attributes**



**Normal User/Admin
Activity**



Suspect Events



**Voluminous Time
Stamps**

CSI:

CRIME SCENE INVESTIGATION



**Spoofed IP
Addresses**



Registry Entries



**Obfuscated
Network Traffic**

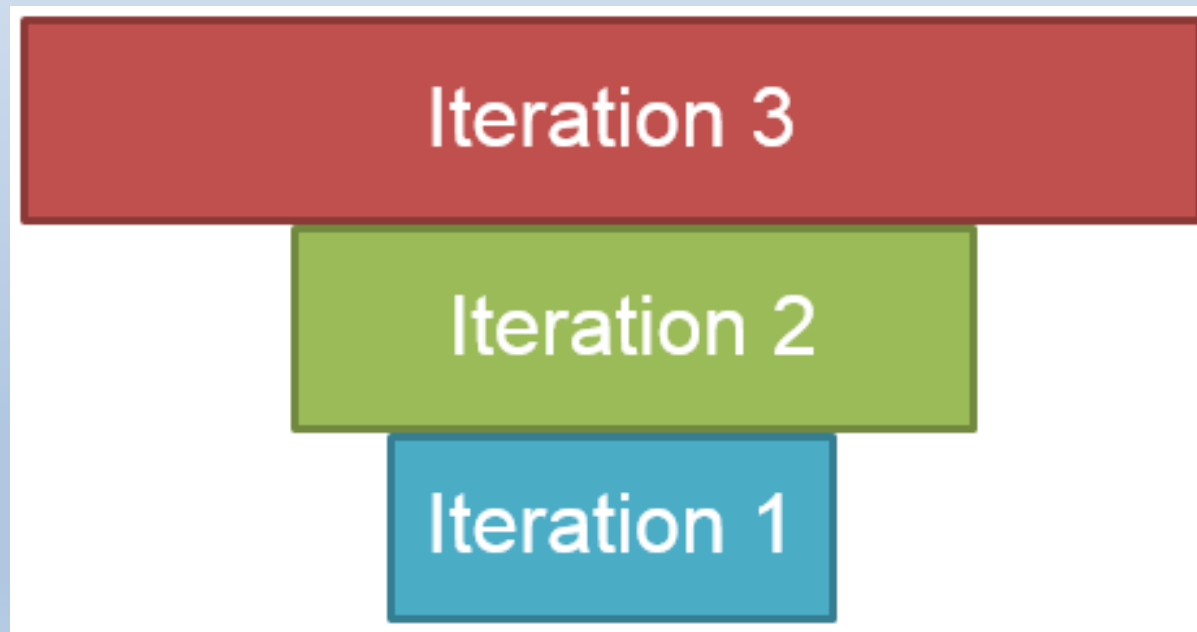
DIGITAL FORENSICS:

LATHER – RINSE -- REPEAT



LATHER -- *RINSE* -- REPEAT

Iterative process of digital forensics, malware reverse engineering, monitoring and scanning





Identify Indicators of Compromise (IOCs), examine network traffic and logs, scan hosts for these IOCs



When this effort discovers additional infected systems, those systems are forensically imaged and analyzed, and process repeats . . .



CONSTITUENCY CANDOR IS PARAMOUNT

CANDOR

can·dor [kan-der]

noun

1. the state or quality of being frank, open, and sincere in speech or expression; candidness.
2. freedom from bias; fairness; impartiality.

CONSTITUENCY NOTIFICATIONS



CUSTOMER



**VENDORS
WANTED**



CAVEAT

SECONDARY DISCLOSURE CONSIDERATIONS

- ❗ PCI Audit
- ❗ Cybersecurity Due Diligence
- ❗ Whistleblowers
- ❗ Law Enf Actions
- ❗ Contractual Negotiations
- ❗ Special Relationships



Part Four:

Cyber: Boards, C-Suite & the SEC, a New Approach





Press Release



SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures

FOR IMMEDIATE RELEASE

2018-22

Washington D.C., Feb. 21, 2018 — Yesterday, the Securities and Exchange Commission voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

"I believe that providing the Commission's views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors," said SEC Chairman Jay Clayton. "In particular, I urge public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."

The guidance provides the Commission's views about public companies' disclosure obligations under existing law with respect to matters involving cybersecurity risk and incidents. It also addresses the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and Regulation FD and selective disclosure prohibitions in the cybersecurity context.

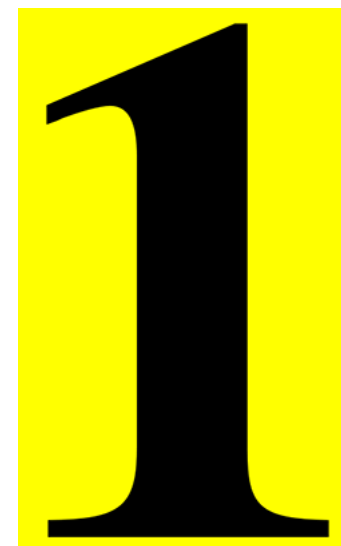
###

More About This Topic

- [Cybersecurity, the SEC and You](#)

Related Materials

- [Cybersecurity Interpretive Guidance](#)
- [Chairman Clayton Statement](#)





Newsroom

Press Releases

Public Statements

Speeches

Testimony

Spotlight Topics

Media Kit

Press Contacts

Events

Webcasts

What's New

Media Gallery

▶ RSS Feeds

▶ Social Media

Press Release



SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls

FOR IMMEDIATE RELEASE

2018-236

Washington D.C., Oct. 16, 2018 — The Securities and Exchange Commission today issued an investigative report cautioning that public companies should consider cyber threats when implementing internal accounting controls. The report is based on the SEC Enforcement Division's investigations of nine public companies that fell victim to cyber fraud, losing millions of dollars in the process.

The SEC's investigations focused on "business email compromises" (BECs) in which perpetrators posed as company executives or vendors and used emails to dupe company personnel into sending large sums to bank accounts controlled by the perpetrators. The frauds in some instances lasted months and often were detected only after intervention by law enforcement or other third parties. Each of the companies lost at least \$1 million, two lost more than \$30 million, and one lost more than \$45 million. In total, the nine companies wired nearly \$100 million as a result of the frauds, most of which was unrecoverable. No charges were brought against the companies or their personnel.

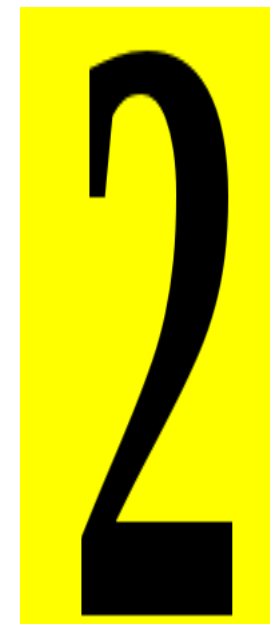
The companies, which each had securities listed on a national stock exchange, covered a range of sectors including technology, machinery, real estate, energy, financial, and consumer goods. Public issuers subject to the internal accounting controls requirements of Section 13(b)(2)(B) of the Securities Exchange Act of 1934 must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly. The FBI estimates fraud involving BECs has cost companies more than \$5 billion since 2013.

"Cyber frauds are a pervasive, significant, and growing threat to all companies, including our public companies," said SEC Chairman Jay Clayton. "Investors rely on our public issuers to put in place, monitor, and update internal accounting controls that appropriately address these threats."

Stephanie Avakian, Co-Director of the SEC Enforcement Division, said, "In light of the facts and circumstances, we did not charge the nine companies we investigated, but our report emphasizes that all public companies have obligations to maintain sufficient internal accounting controls and should consider cyber threats when fulfilling those obligations."

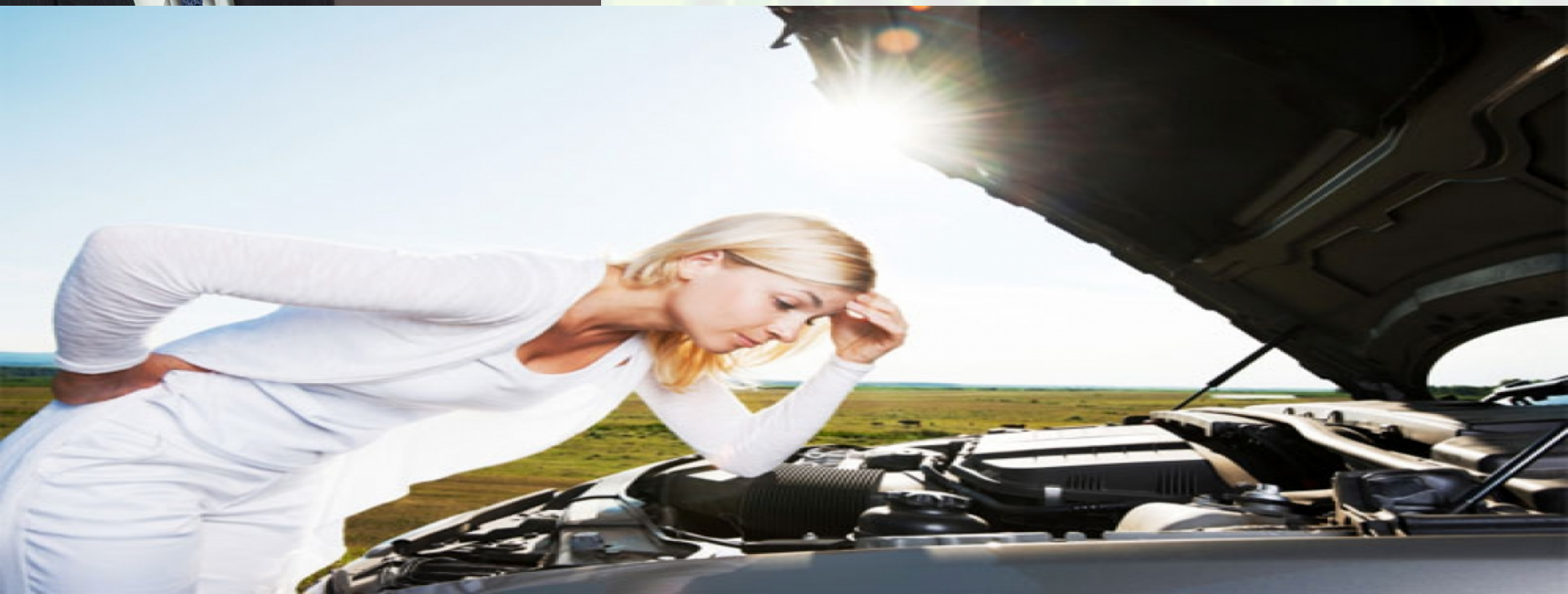
Related Materials

- Report of Investigation





***“According to the SEC, the development of effective disclosure controls and procedures “is best achieved when a **company’s directors**, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face.”
(February 2018 SEC Guidance)***





Exchange Act Rules 13a-14 and 15d-1455 require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures,⁵⁶ and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures. ***These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact.*** In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.



Design and Effectiveness of
Disclosure Controls

THE SEC ADVISED THAT PUBLIC ISSUERS SUBJECT TO THE INTERNAL ACCOUNTING CONTROLS REQUIREMENTS OF THE EXCHANGE ACT “MUST CALIBRATE THEIR INTERNAL ACCOUNTING CONTROLS TO THE CURRENT RISK ENVIRONMENT AND ASSESS AND ADJUST POLICIES AND PROCEDURES ACCORDINGLY.”

IT ALSO DIRECTLY INDICATED ITS POSITION THAT CYBERSECURITY FALLS SQUARELY WITHIN THE INTERNAL CONTROL FRAMEWORK, STATING “OUR REPORT EMPHASIZES THAT ALL PUBLIC COMPANIES HAVE OBLIGATIONS TO MAINTAIN SUFFICIENT INTERNAL ACCOUNTING CONTROLS AND SHOULD CONSIDER CYBER THREATS WHEN FULFILLING THOSE OBLIGATIONS.”

[illegible]

FINANCIAL AUDIT

Audit
Committee

Financial
Expertise

Periodic,
Independent
Financial Audit





**Cybersecurity
Committee**

**Cyber
Expertise**

**Periodic,
Independent
Cyber Audit**

Conclusion:

The Right Questions

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

CAPOREGIME

FORMER:

PETER CLEMENZA
ALIAS
"FAT CLEMENZA"
FBI # 100375
DECEASED



SALVATORE TESSIO
ALIAS
"SAL"
FBI # 320611
DECEASED

PRESENT:



AL NERI
FBI # 563241
(G, I, 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 # 436601
(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



ALPHONSE EVOLLONI
ALIAS
"AL OVE"
FBI # 77123
DECEASED



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



VICTOR VINATTONI
ALIAS
"VICKY VEAL"
FBI # 173210
(G, H, I)



BARTOLO NENI
ALIAS
"O'NEAL"
FBI # 547073



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



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



CALOGERO RADENI
FBI # 1176176
(F)



JOSEPH BRONSKI
ALIAS
"JOEY JAIL"
FBI # 467032



CASSANDROS FRACCA
ALIAS
"DAVID GELLY"
FBI # 428935
(H, I)



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



RAFILO GERNO
FBI # 416230
(I)



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



NATALE PARRI
ALIAS
"FAT NAT"
FBI # 441111
(M)



CHARLES LOCIRNO
FBI # 136311
DECEASED



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



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



SAMUEL COROCCO
FBI # 329661
(E, H)



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



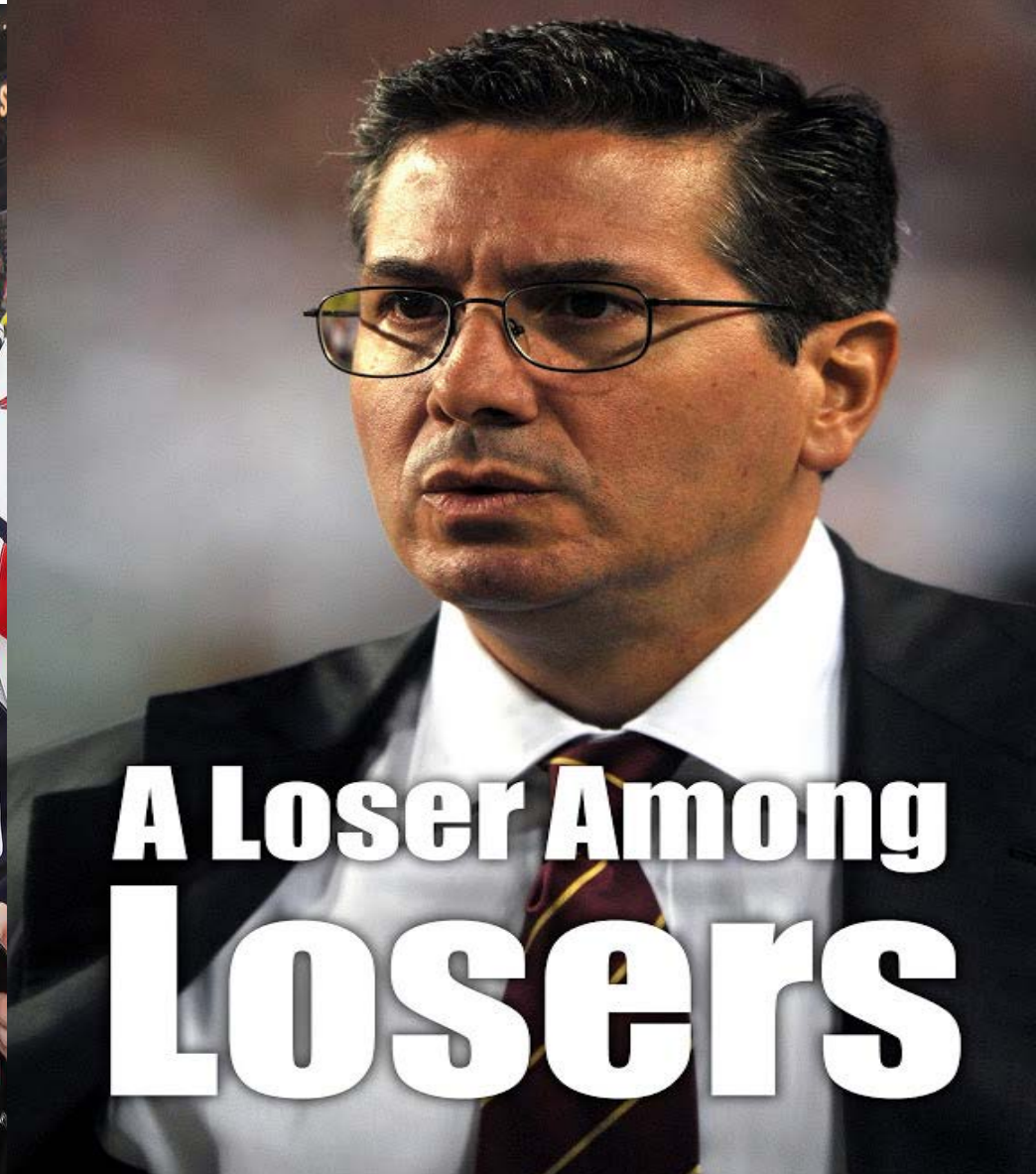
CARMEN DELLA
FBI # 146372
(G)



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

WHO'S ACCOUNTABLE?

TOP DOWN COMMITMENT?



**A Loser Among
Losers**

WANTED

**Cyber
Insurance**

??????????



**Transfer
Risk**

**Fill Gaps .
..**

**CGL May Be
Inadequate**

**Mitigate
Losses**





How much cyber insurance can your company afford?



Type of coverage? Liability? Breach response? Fines and penalties?



Coverage triggers? Stolen laptop? APT? Cloud issue?



Exclusions?



Who chooses lawyers? Forensic teams? Panels?

VIGOROUS CYBER-UNDERWRITING PROCESS

Life Insurance



COMPLEX INSURANCE DOCUMENTATION & INTERPHASE



CYBER-INSURANCE BATTLEGROUND ISSUES



NIST

Security Requirements
(no standard)

TERROR

Act of War and
Terrorism Exclusions

THIRD
PARTY

3rd Party Acts and
Omissions (e.g. Cloud)

DAMAGES

Statutory Damages
Coverage (per violation)

CYBER INSURANCE KEY POINTS



**Reps and
Warranties**



**Experienced
Broker**



**Understanding
IR Workflow**



INDEPENDENT TESTING/ASSESSMENT?



FIND THE RIGHT PEN TESTER

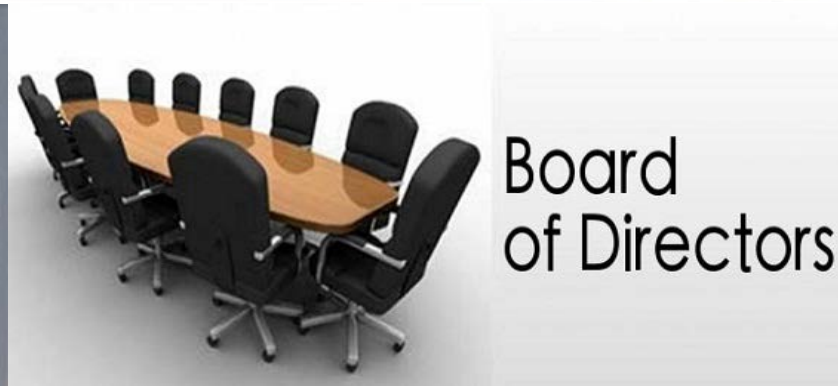
What's in a name? That
which we call a rose,
by any other word
would smell as sweet

- Shakespeare

#1 SKILLSET: EXPERIENCE



#2 SKILLSET: COMMUNICATION SKILLS



#3 SKILLSET: REGULATORY EXPERTISE



#4 SKILLSET: DARK WEB SURVEILLANCE



THIRD-PARTY

SERVICES

Law Firms

Cloud Storage Firms

Other 3rd Party Vendors



**Other
3rd Party
Vendors**

FLEXIBLE IT SECURITY BUDGETING?



INCIDENT RESPONSE PLAN?



DEVELOP A RESPONSE PLAN



Management
Endorsement

- To underscore the mission

Contact Lists

- For members of the response team

Legal Analysis and
Timeline

- Drawn from state or federal law

Categories of Adverse
Events

- To prevent a constant fire drill

"First Steps" Checklists

- To identify priorities

Facilities and Equipment
Lists

- So that response can start immediately

Outreach Plan

- Effective response involves more than just a company's managers and employees

RESPONSE TEAM?



**Technical Incident
Response Team**

Employees

**Independent
Outside Experts**

**From relevant c-
levels of a
company's org chart**

**Information
technology, investor
relations, public
relations, legal etc.**

**Engage experts to
conduct
independent
investigation of the
attack**

**Tasks include data
preservation,
malware analysis,
digital forensic
analysis, reverse
engineering**

INCIDENT RESPONSE FIRM ON SPEED DIAL?

A close-up photograph of a computer keyboard. The central focus is a bright red key with the word "HELP!" printed in white, sans-serif capital letters. The key is slightly raised and has a glossy finish. Surrounding this key are several dark grey or black keys, including one with a right-pointing arrow, one with the letter "N", and one with the letter "Q". The lighting is dramatic, highlighting the red key against the darker background of the other keys.

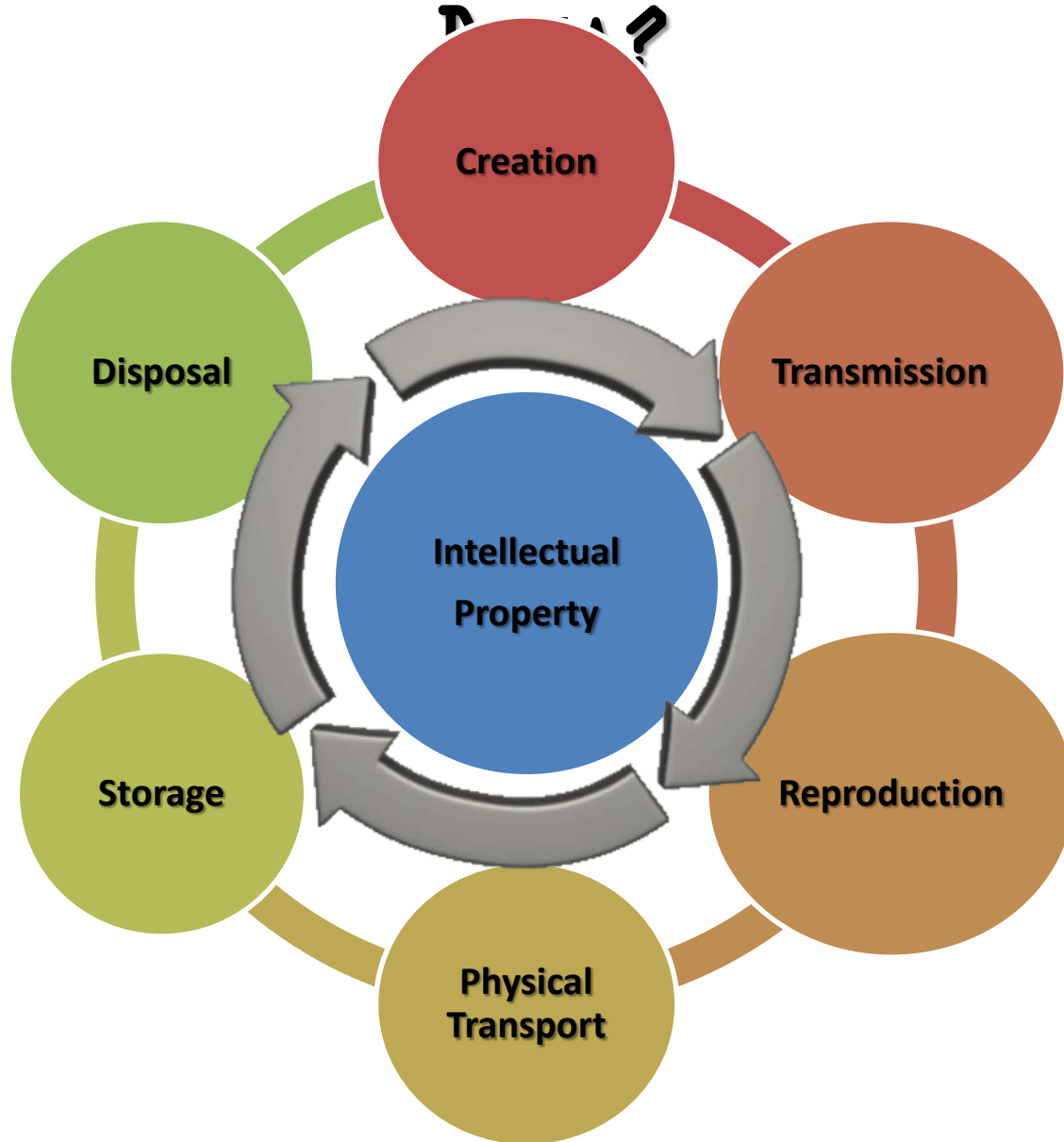
HELP!

LAW ENFORCEMENT LIAISON?

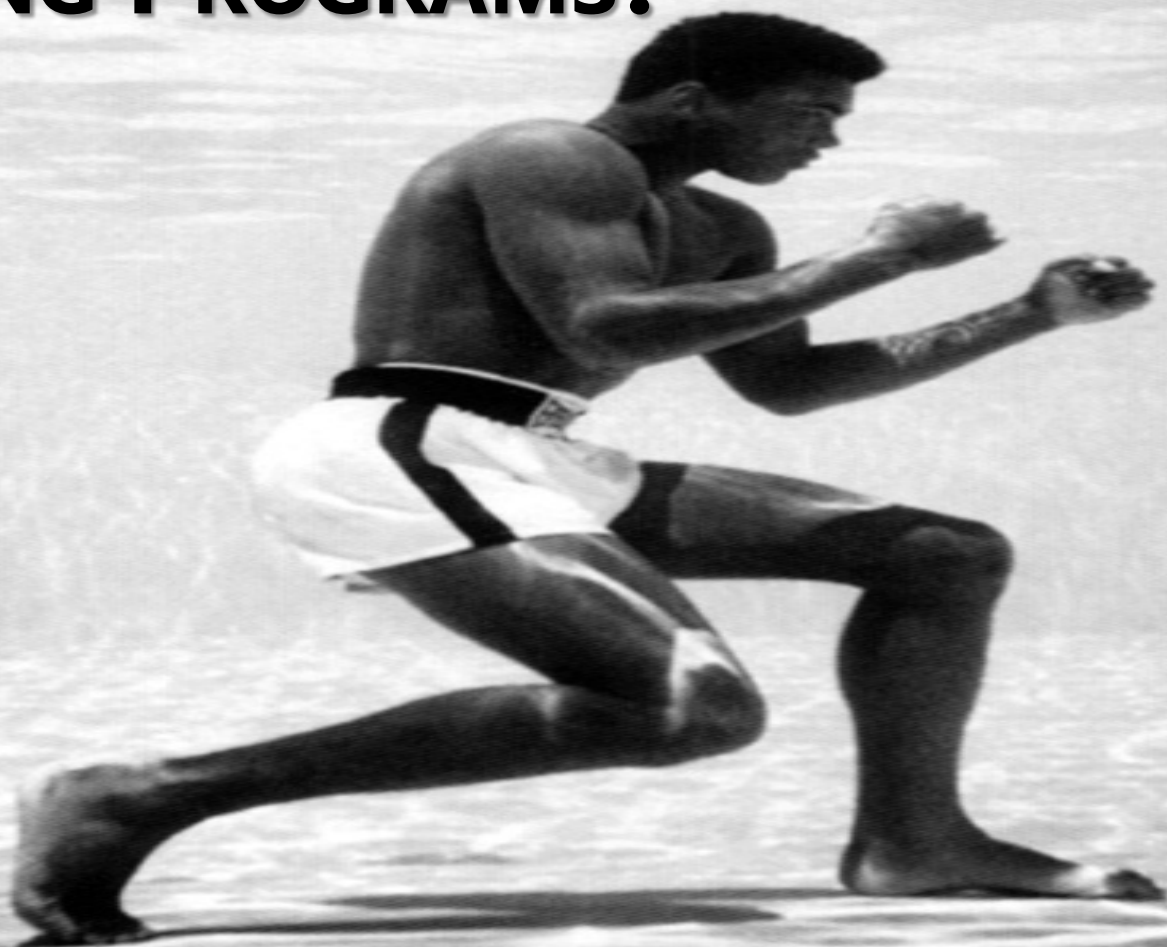
PARAMOUNT: BEFORE AND AFTER



DATA MAPPING/SENSITIVE/REGULATED/KEY



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 22 years in the army, local hero Sgt. Joe Hulka has announced his intention to "turn in his fatigues."

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

(continued on page 2)

PERSONNEL CONTINUITY?

BUDGET FOR RECRUITMENT,
HIRING & RETENTION?






BUSINESS CONTINUITY PLAN?



COMMUNICATION PLAN?



Communicate
/ko-mu-ni-kate/

1. To pass on information, news or thoughts.
2. To spread to another or others.



RESPONSE SHOULD NOT MAKE MATTERS WORSE

Thank You

Based on the information provided, we believe that your personal information may have been impacted by this incident.

Click the button below to continue your enrollment in TrustedID Premier.

Enroll

For more information [visit the FAQ page.](#)

Equifax data breach response...



SKIP THE FINE PRINT



"I wouldn't—there's an awful lot of scary-sounding legalese."

ESTABLISH HIERARCHY: COUNSEL AS QUARTERBACK



LEGAL CHALLENGES

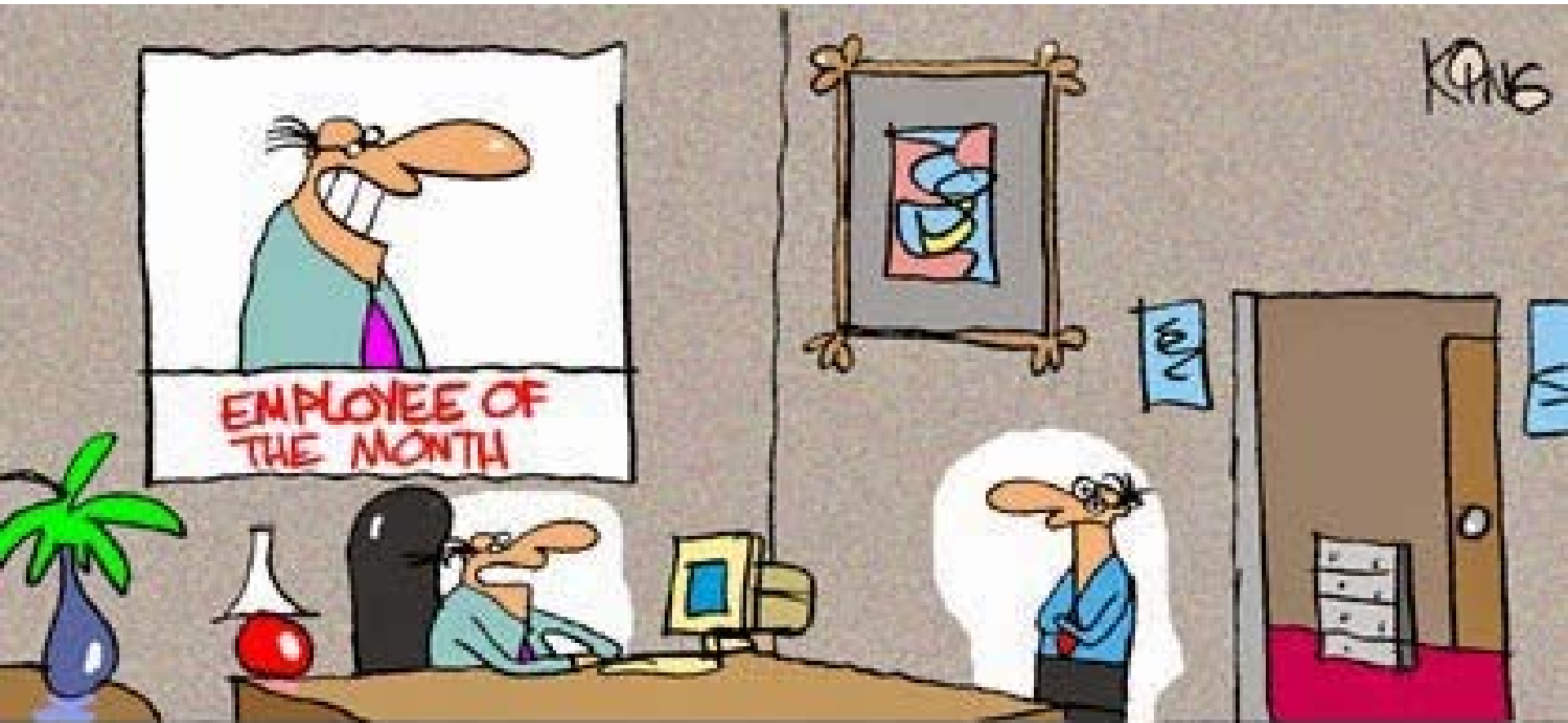
Timing



Desire for Certainty



INDEPENDENT PROCESS



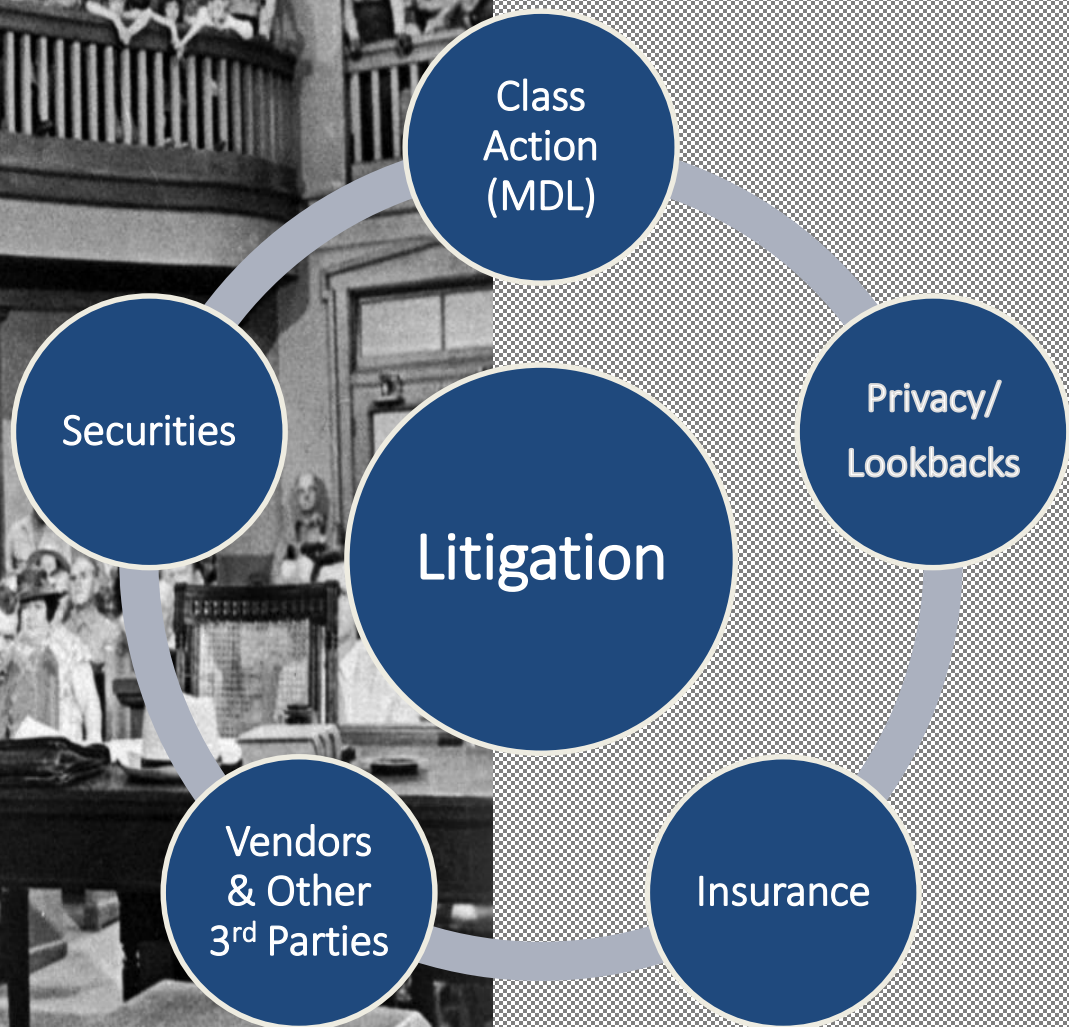
"Yes, I am employee of the month again. And yes, I'm the one who chooses the employee of the month. And no, I don't see a conflict of interest."

MANY 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?**



1919-114





CLASS ACTION RUSH



30+ lawsuits Filed to Date
E.G. Fail to Implement
Reasonable Procedures to
Protect Data; Fail to Notify in
Timely Manner



E.G. Stock Drop; Insider
Trading;
Poor Disclosure

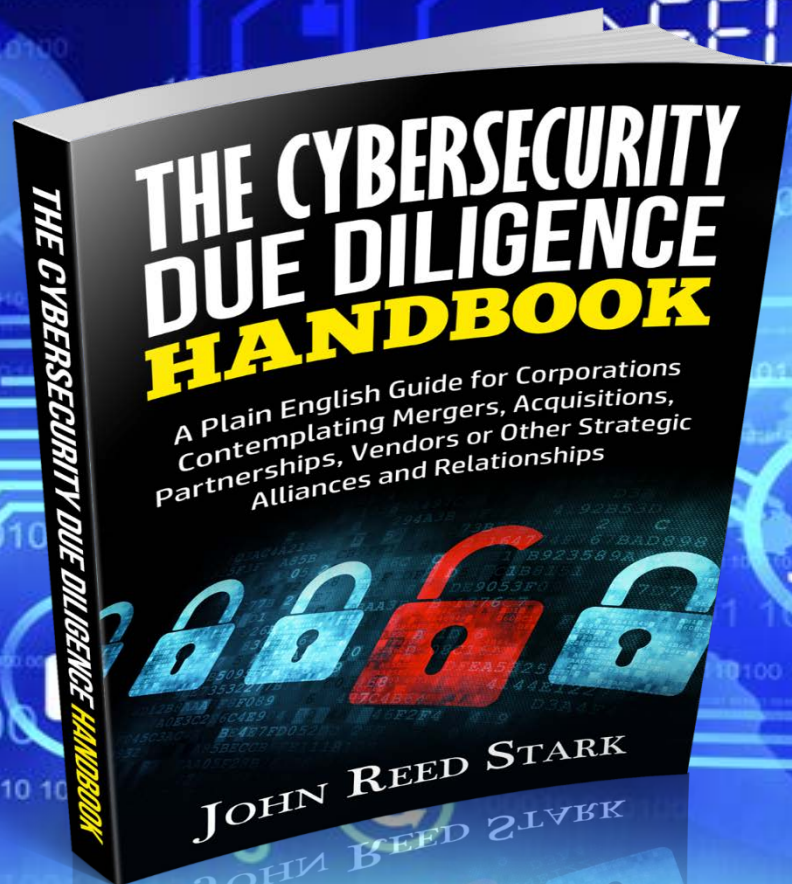
SECURITIES CLASS ACTION

Equifax issued materially false or misleading statements or failed to disclose that Equifax failed to maintain adequate:

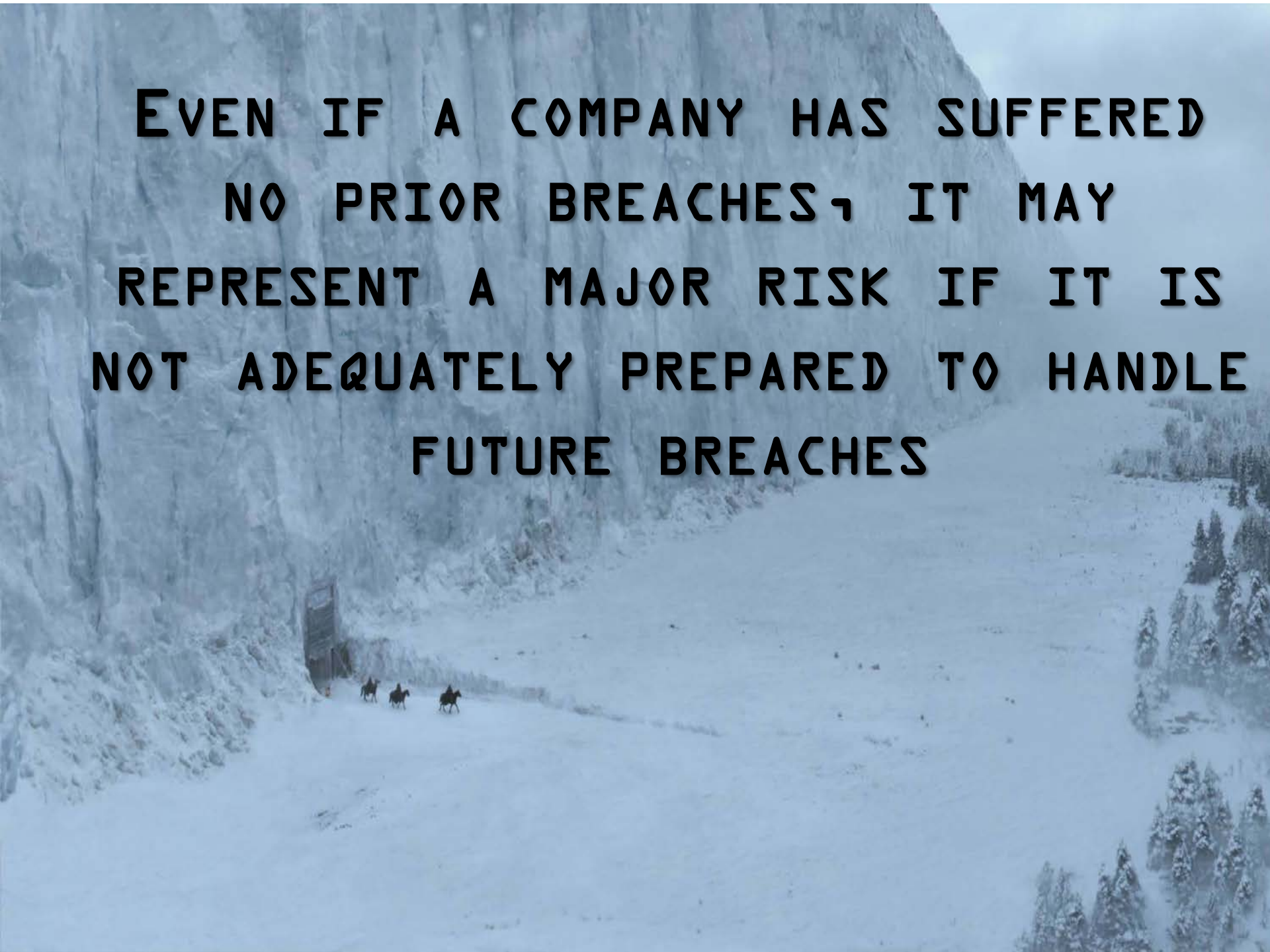
- ✓ **Measures to protect its data system;**
- ✓ **Monitoring systems to detect security breaches; and**
- ✓ **Security systems, controls and monitoring systems in place.**

As a result Equifax's financial statements were materially false and misleading at all relevant times





**EVEN IF A COMPANY HAS SUFFERED
NO PRIOR BREACHES, IT MAY
REPRESENT A MAJOR RISK IF IT IS
NOT ADEQUATELY PREPARED TO HANDLE
FUTURE BREACHES**





johnreedstark
CONSULTING, LLC



Thank you.



ANY QUESTIONS?

Snapple112