

CYBER INSURANCE

WHAT, WHERE & HOW



CPE Credits

Today's webcast is worth 1 Continuing Professional Education (CPE) credit.

To be eligible for CPE credit, you must:

- Answer **at least 3 of the 4** polling questions (during the webcast) and have a total viewing time of **at least 50** minutes.
- Participants will have the opportunity to download their CPE certificate immediately following the webcast if above requirements are met.
- In accordance with the standards for the National Registry of CPE Sponsors, CPE credit will be granted based on a 50-minute hour.
- We are unable to grant CPE credit in cases where technical difficulties preclude eligibility. CPE Program Sponsorship guidelines prohibit us from issuing credit to those not verified by the technology to have satisfied the minimum requirements listed above.

CYBER INSURANCE ROADMAP FOR TODAY



Background



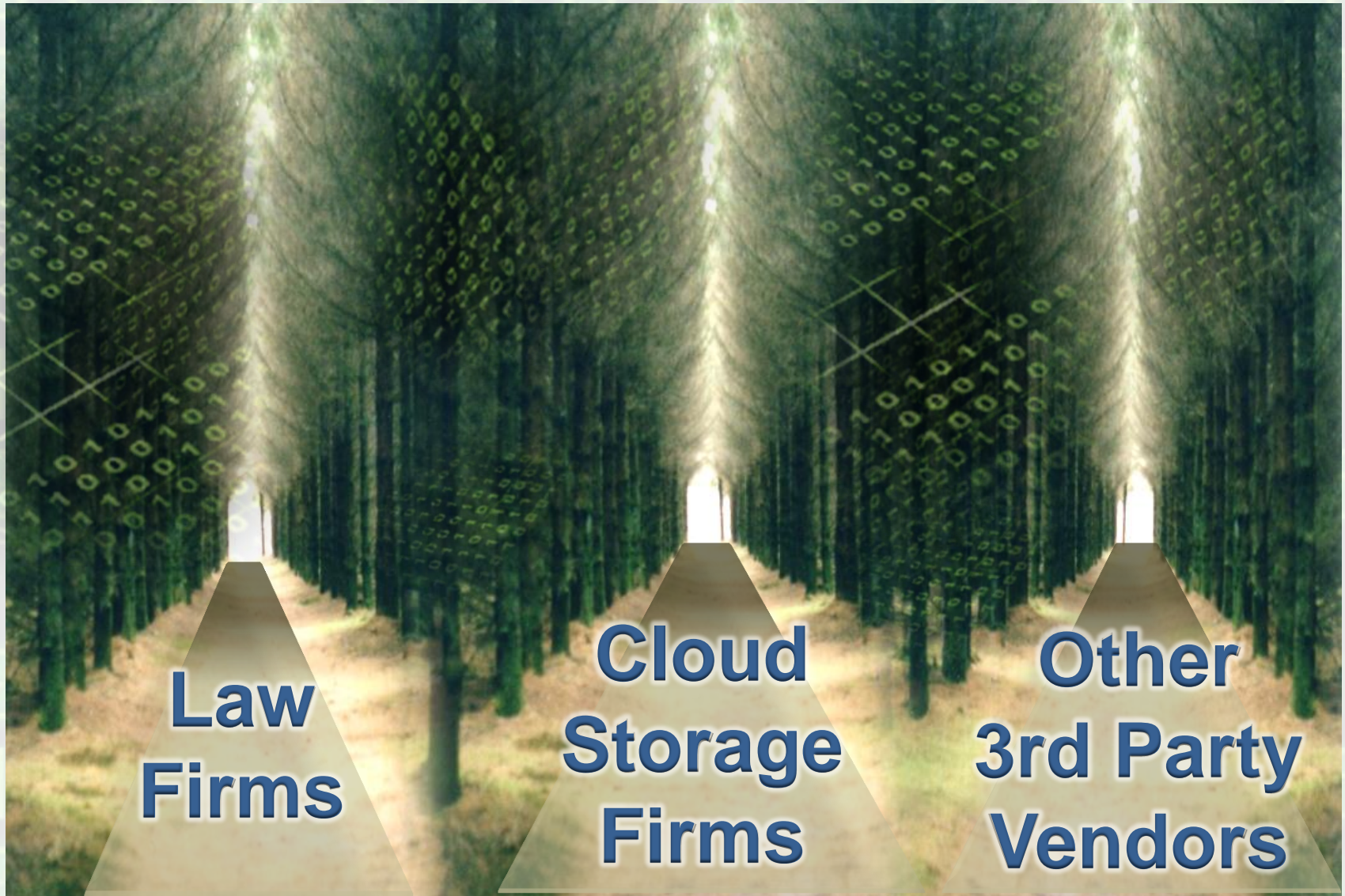
Hot Button Issues



Legal Questions

Death
and
Taxes

NEW ATTACK VECTORS AND PATHWAYS



**Law
Firms**

**Cloud
Storage
Firms**

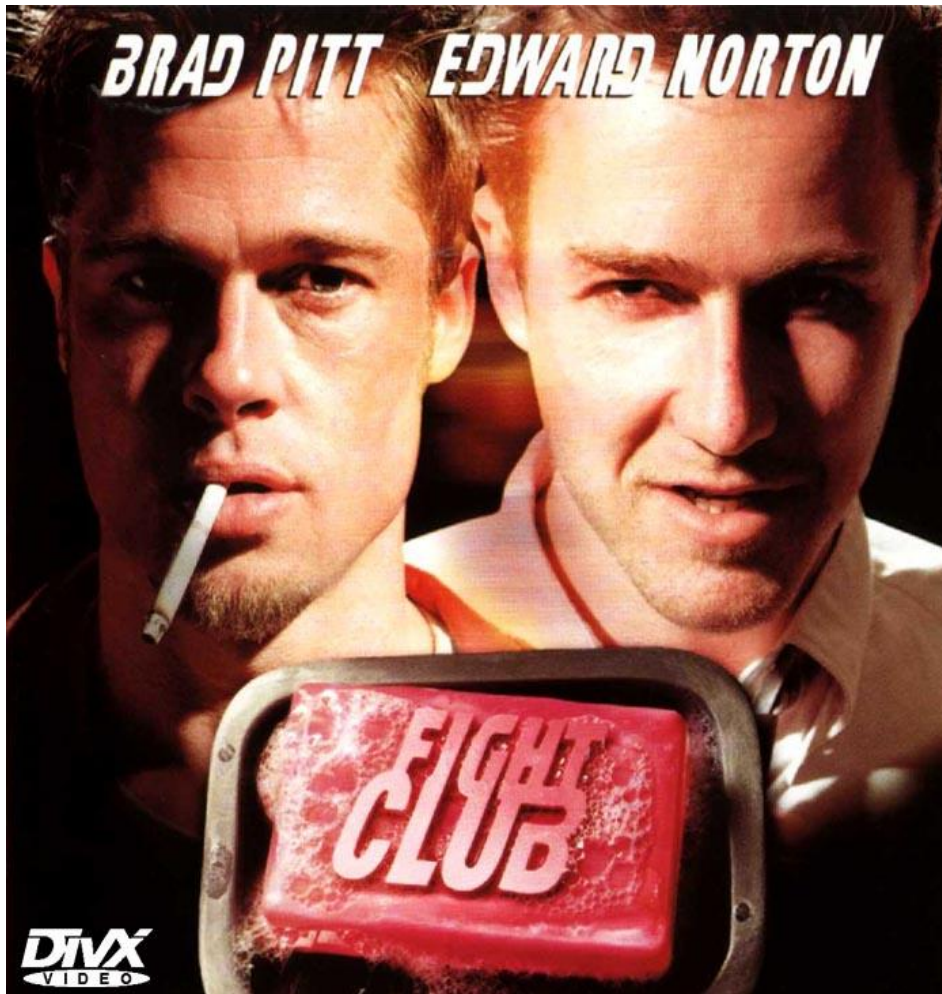
**Other
3rd Party
Vendors**

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**
- **Hactivism**
- **DOS (much easier)**

INTERNAL THREATS



THE DATA BREACH WORLD



POLLING QUESTION #1

(CPE REQUIREMENT)

My company has cyber insurance:

- 1) Yes, and I was part of the process**
- 2) Yes, but I was not part of the process**
- 3) No**
- 4) Don't Know**

CYBER INSURANCE

SOME GENERAL NOTES

CYBER
INSURANCE
CLAIM FORM

Personal Information

Name (Last)	(First)	(Middle Initial)	Home Telephone
Address (Mailing Address)	(City)	(State)	(Zip)
			Other Telephone

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 BASICS

- ☑ Errors and Omissions (failed professional services)
- ☑ Media Liability (IP or trademark infringement)
- ☑ Network Security (consumer data breach, destruction of data, virus transmission, cyber extortion)
- ☑ Privacy Failure (First Party (e.g. forensic investigation, legal advice, notification, loss of profits); Third Party (e.g. lawsuits, regulatory inquiries and class actions))

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 . . .

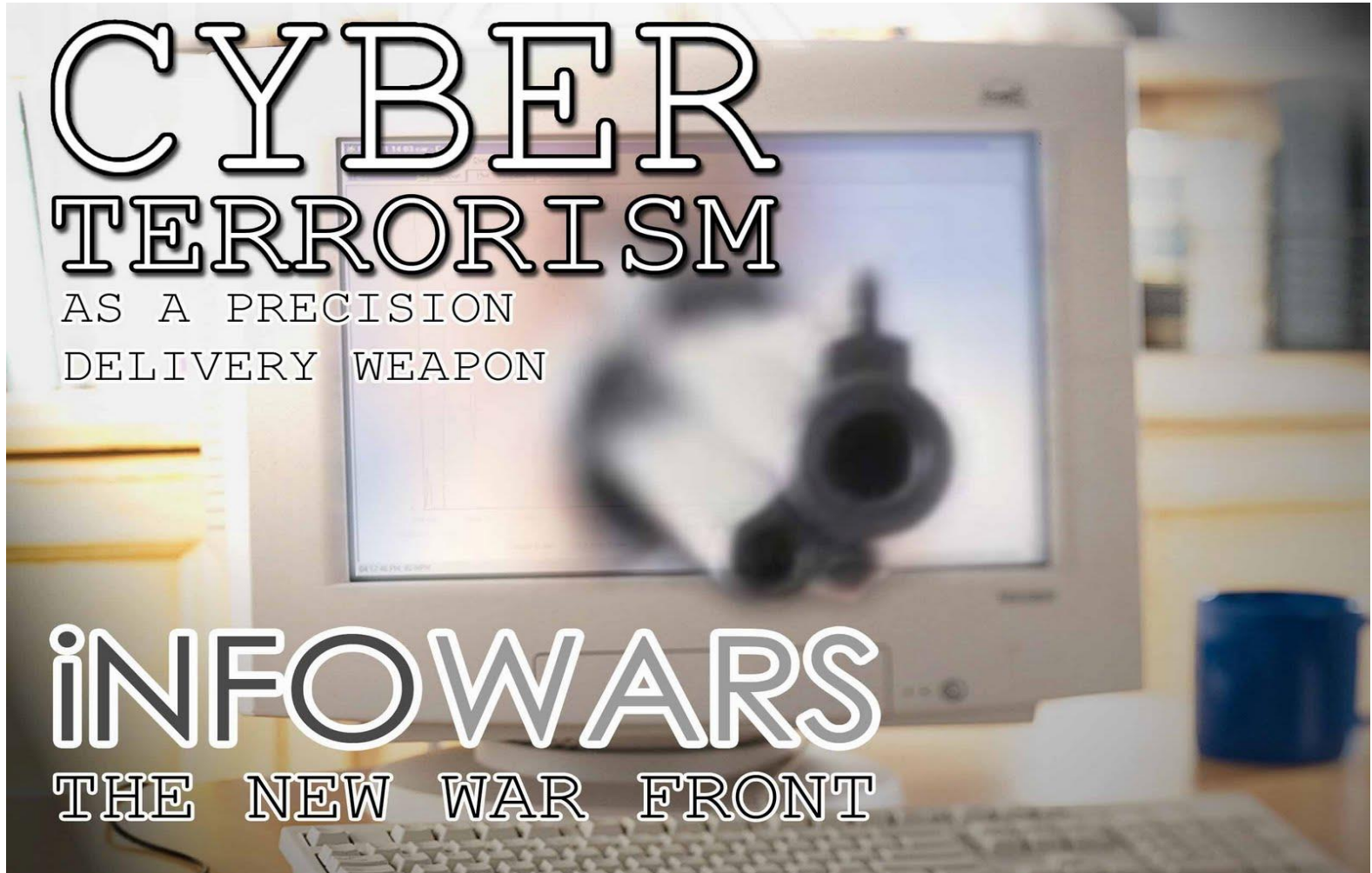
- ☒ How much can your company afford?
- ☒ What type of coverage is needed (Liability? Breach response? Fines and penalties?)
- ☒ What triggers coverage (Stolen laptop or flash drive? APT? Cloud data?)
- ☒ Exclusions?
- ☒ Type of data covered (Public? IP?)
- ☒ Selection of legal/forensic team (Who chooses?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

CYBER INSURANCE

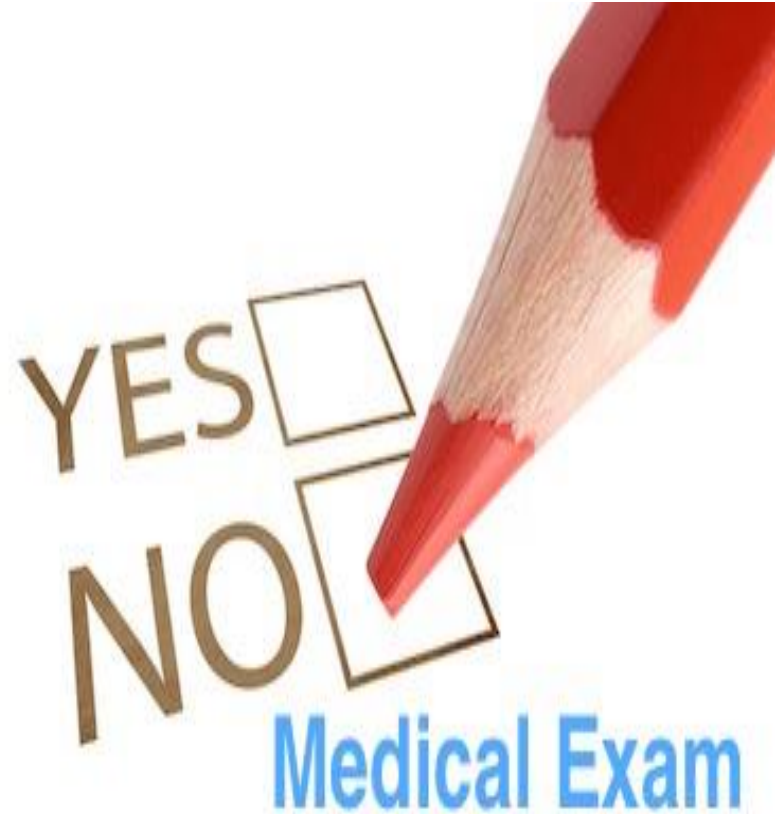
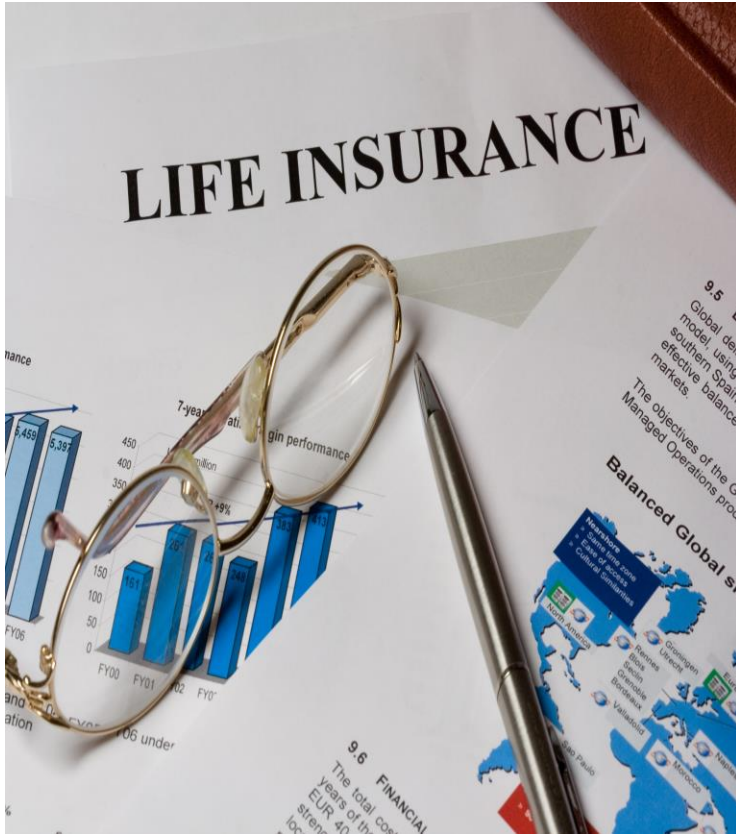
HOT BUTTON ISSUES



CYBER EXTORTION/TERRORISM



VIGOROUS UNDERWRITING PROCESS



Request "Retroactive" Coverage for Prior, Unknown Breaches



“Panel” and “Prior Consent” Provisions



Loss of Data v. Theft of Data

**NOT
RESPONSIBLE
FOR LOSS OR THEFT
OF PERSONAL
PROPERTY**

Vendor Error and Omissions



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)



LEVERAGE? NEGOTIATION?



POLLING QUESTION #2

(CPE REQUIREMENT)

My company has cyber insurance and I understand what is and is not covered:

- 1) Yes**
- 2) No**
- 3) Don't Know**
- 4) My company does not have cyber insurance**

CYBER INSURANCE REVERSE GAP ANALYSIS



DATA BREACH WORKFLOW OVERVIEW

Stop Breach



Preservation



Malware Scan



Find Artifacts



Deconstruct Malware



Determine What Was
Taken



Remediation



INCIDENT RESPONSE WORKFLOW



PRESERVATION



DIGITAL FORENSIC ANALYSIS



LOGGING ANALYSIS



MALWARE REVERSE ENGINEERING



INCIDENT RESPONSE FIRM



SURVEILLANCE



REMEDIATION EFFORTS



POLLING QUESTION #3

(CPE REQUIREMENT)

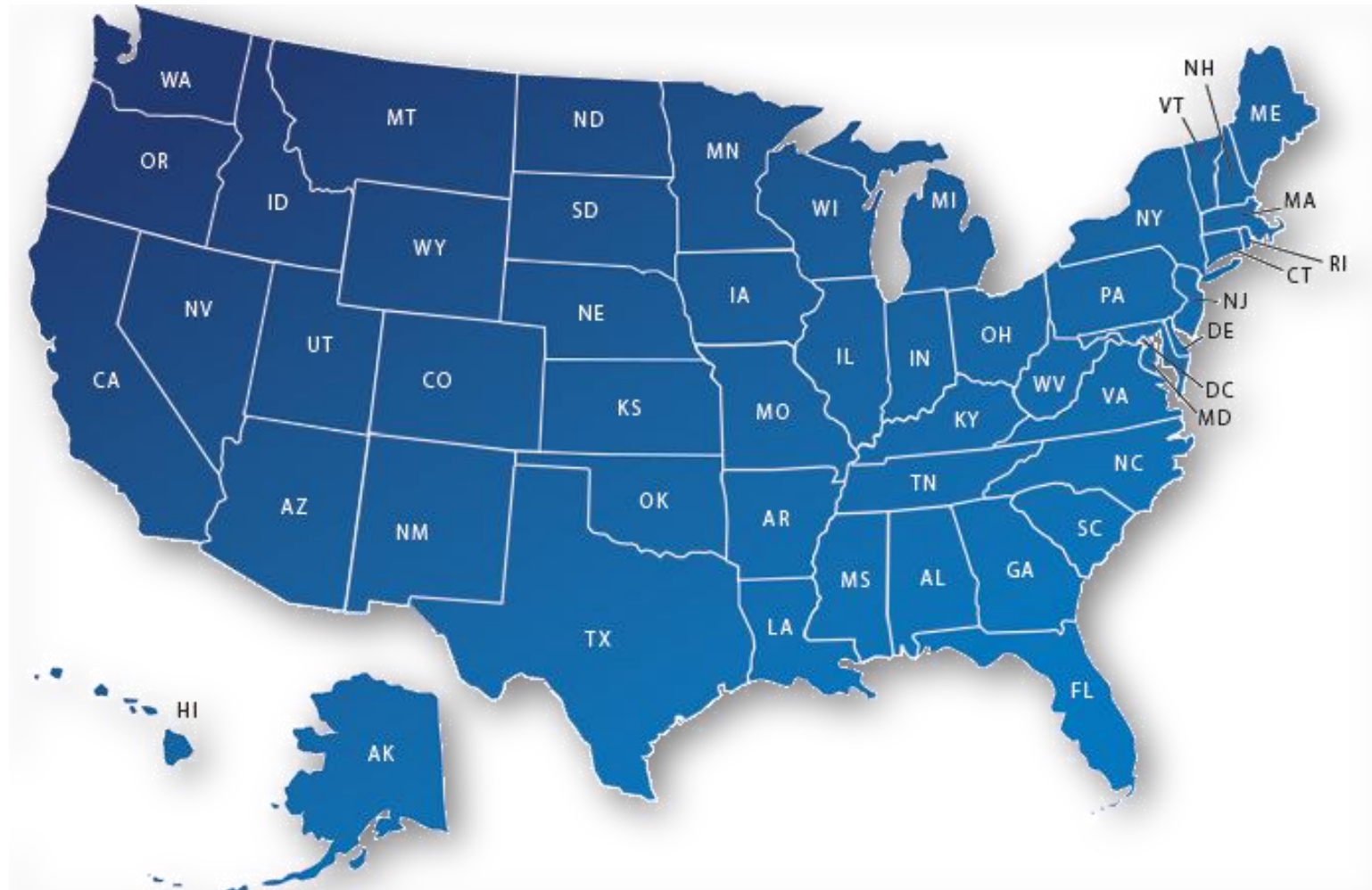
My company has made a cyber insurance claim and we were paid fairly:

- 1) Yes**
- 2) No**
- 3) My company has never made a cyber insurance claim**
- 4) Don't Know**

EXFILTRATION ANALYSIS



STATE REGULATORY COMPLIANCE



FEDERAL REGULATORY COMPLIANCE



PCI COMPLIANCE

PCI Compliance



LAW ENFORCEMENT LIAISON



CONSTITUENCY NOTIFICATIONS



EMPLOYEE
ENGAGEMENT



INDIVIDUAL NOTIFICATION MONITORING SERVICES



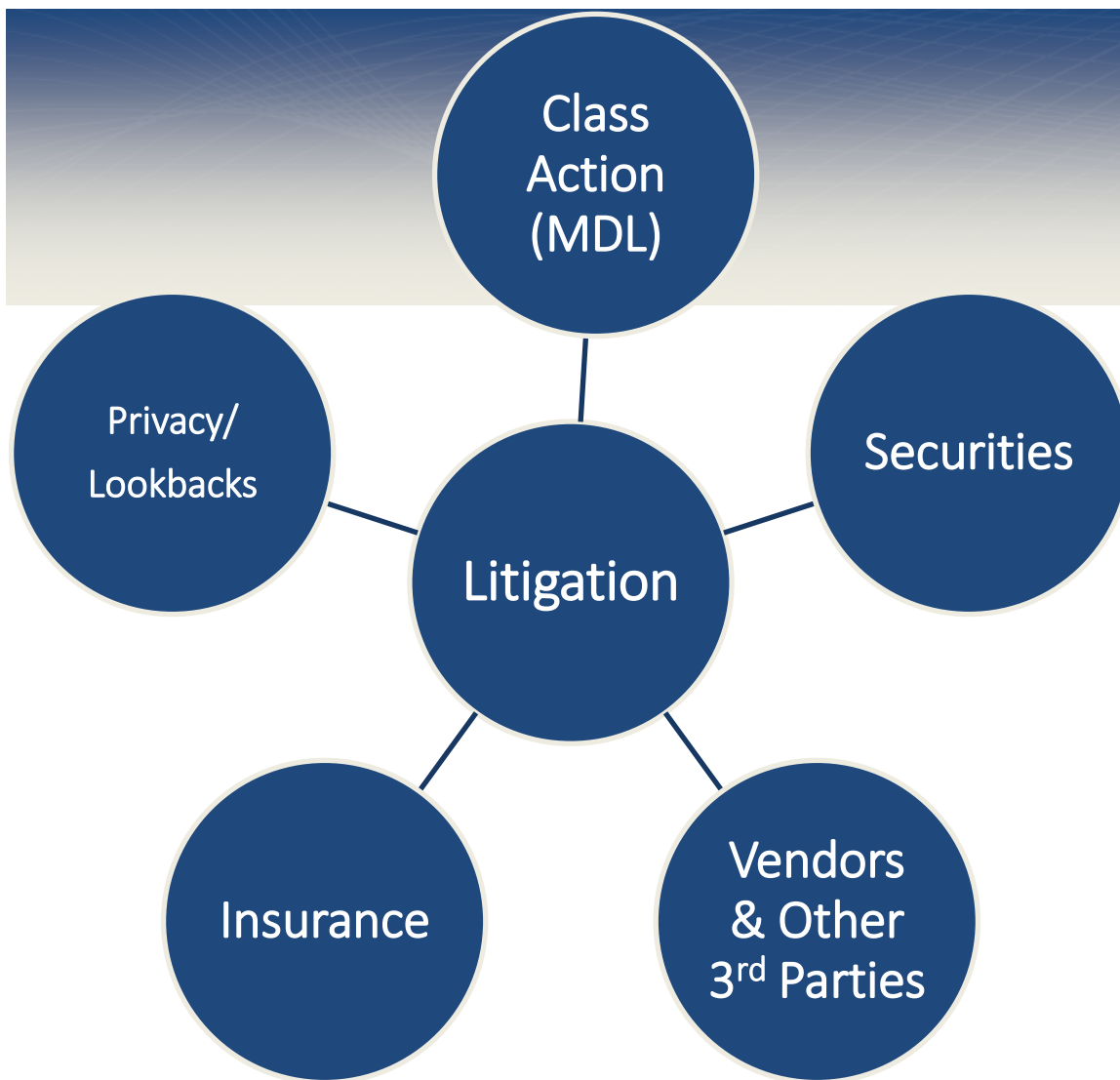
PUBLIC/GOVERNMENT RELATIONS



CYBER INSURANCE 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

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



CRITICALITY OF ATTORNEY CLIENT PRIVILEGE



"Son, I want to talk to you about the birds, the bees,
and the attorney client privilege."

NOTE: BE WARY OF “LOOK-BACKS”



DOCUMENT YOUR PREPARATION/RESPONSE EFFORTS



Yes!



No!

CYBER INSURANCE KEY POINTS

- ☑ Reps and Warranties: Key
- ☑ Experienced Broker: Key
- ☑ Understanding Your IR workflow: Key
- ☑ Counsel Review



MIND THE GAP

POLLING QUESTION #4

(CPE REQUIREMENT)

I am interested in attending the Incident Response Forum on April 4th in DC:

- 1) Agree**
- 2) Disagree**
- 3) I don't care if it is a free ticket, I don't believe you, nothing in life is free, leave me alone . . .**

INCIDENTRESPONSEFORUM.COM

[Home](#) | [Keynote](#) | [Agenda](#) | [Register](#) | [Corp. Sponsors](#) | [Law Firm Sponsors](#) | [Press](#) | [Contact](#) | [Search this site...](#)



Register Now

[KEYNOTE AND FACULTY BIOS](#)

[PAST EVENTS](#)

Incident Response Forum 2017

A Data Breach Response Conference for Legal and Compliance Professionals

****Tuesday, April 4, 2017, The Mayflower Hotel, Washington, D.C.****

Presented by Cybersecurity Docket

Faculty: John Reed Stark

John Reed Stark, President,
John Reed Stark Consulting
LLC; Former Founder and
Chief, SEC Office of Internet
Enforcement



Incident Response Forum 2017 is the first conference of its kind. It is focused solely on the field of Incident Response – the work that begins after a data breach that has quickly become the fastest growing practice area at law firms and consulting firms – and is geared specifically for the legal and compliance professionals who have emerged as critical players during a data breach response.

This year's conference will take place on Tuesday, April 4, 2017, in the elegant setting of the Mayflower Hotel in Washington, D.C. Our stellar faculty of attorneys and experts specializing in data breach response will discuss the most important and timely data breach response topics, including:

- Why legal professionals involved in an incident response must become the quarterback of all workflow and how to handle this important responsibility;
- The legal and compliance aftermath of a data breach, including governmental investigations and litigation, as well as the almost endless list of potential civil liabilities after a cyber-attack;
- In plain English, the kinds of artifacts, remnants and fragments available in the aftermath of a data breach, and how, armed with the information gathered during forensic analysis, legal and compliance professionals can manage efforts to detect and mitigate the damage of a data breach.

Details

When: Tuesday, April 4, 2017

7:00 am - 8:00 am (breakfast & registration)

8:00 am - 5:00 pm (followed by cocktail party)

Where: Mayflower Hotel

1127 Connecticut Ave, NW

Washington, D.C. 20036

CLE Credit: 6.0 hours approved in PA (and in NY/reciprocal states) and VA (pending)

The CISO 50



Cybersecurity Docket's
inaugural "CISO 50" will be
announced at Incident Response Forum 2017!

Corporate Sponsors





info@johnreedstark.com

