How to Respond to the Inevitable Cyber-Attack

johnreedstark
CONSULTING, LLC

CRYPSIS™
RESPOND • PREVENT

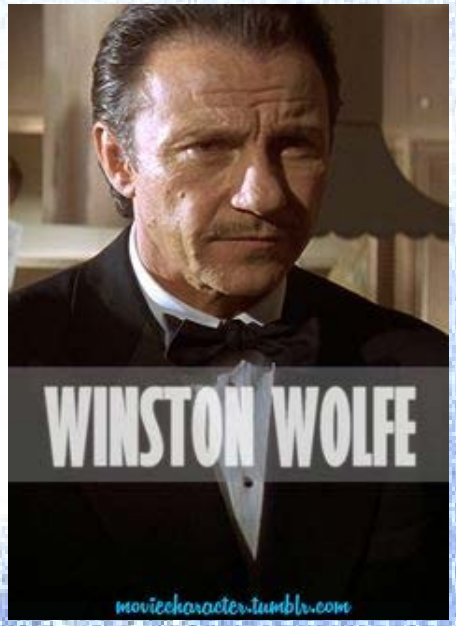
CPE Credits

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.

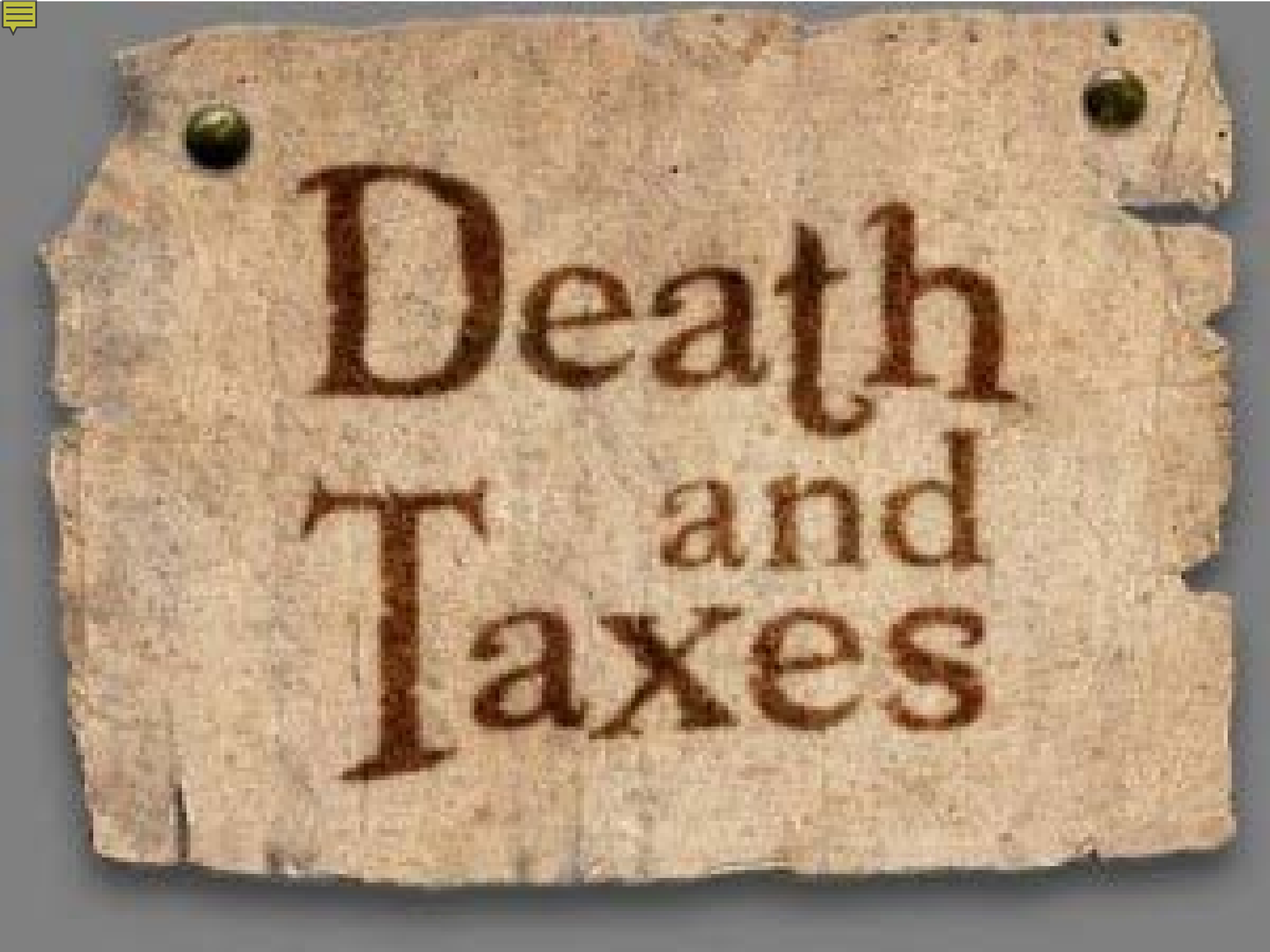
High Tech Plumber



Roadmap

Initial Thoughts

Data Breach Workflows


Death
and
Taxes


Paradigm shift

WHERE TECHNOLOGICAL INFRASTRUCTURE HAS EXPANDED DRAMATICALLY

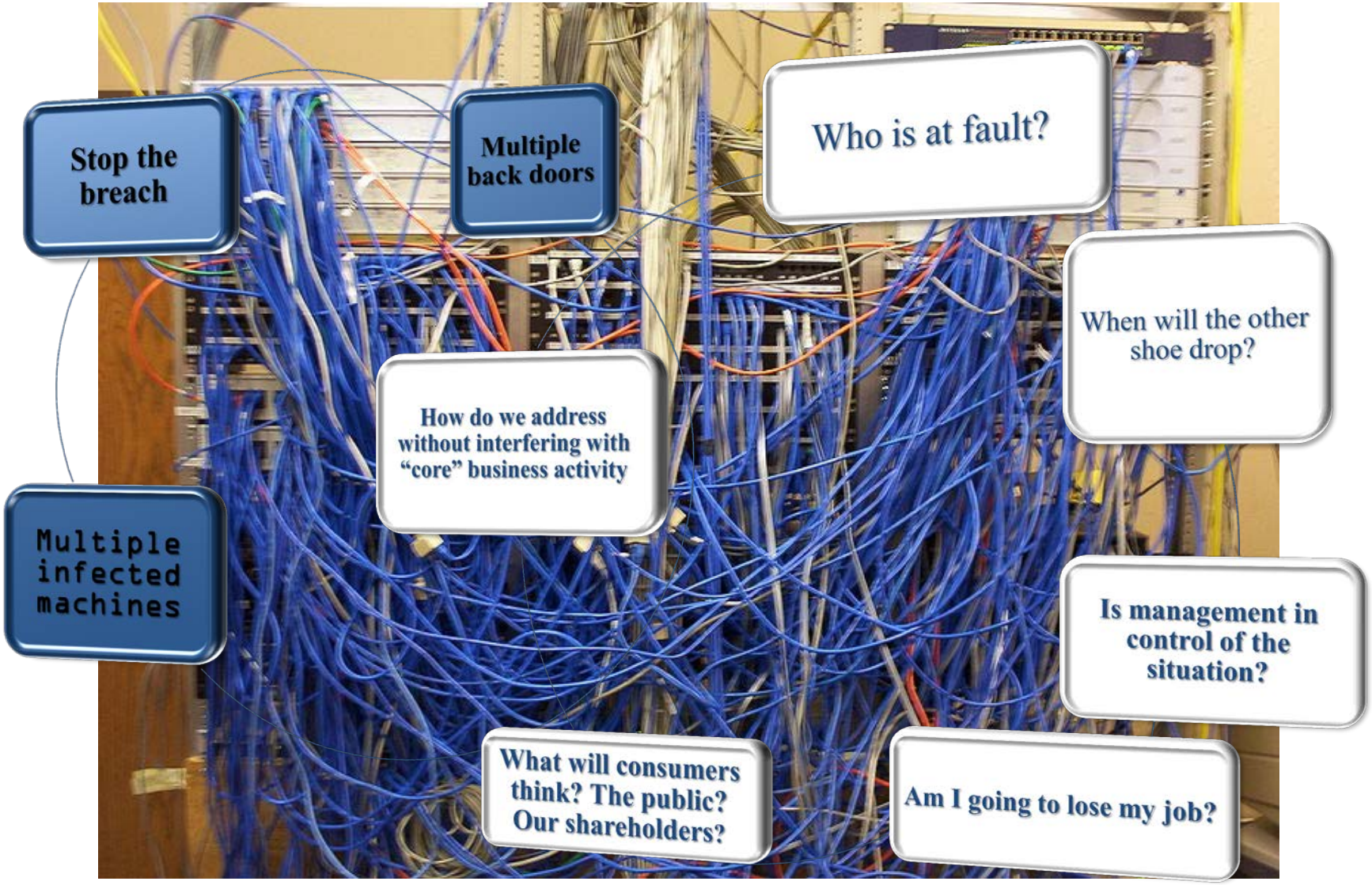
WHERE DATA-POINTS RESIDE ON MULTIPLE PLATFORMS

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

IR Sequence of Events

- Recon
- Attack Vector
- Vulnerability Exploitation
- Lateral Movement
- Exfiltration
- Persistence

TYPICAL DAY ONE STATE-OF-PLAY




SIRI

Data Breach Workflow Overview

Stop Breach

Preservation

Malware Scan

Find Artifacts

Deconstruct Malware

Determine What Was Taken

Remediation

#1

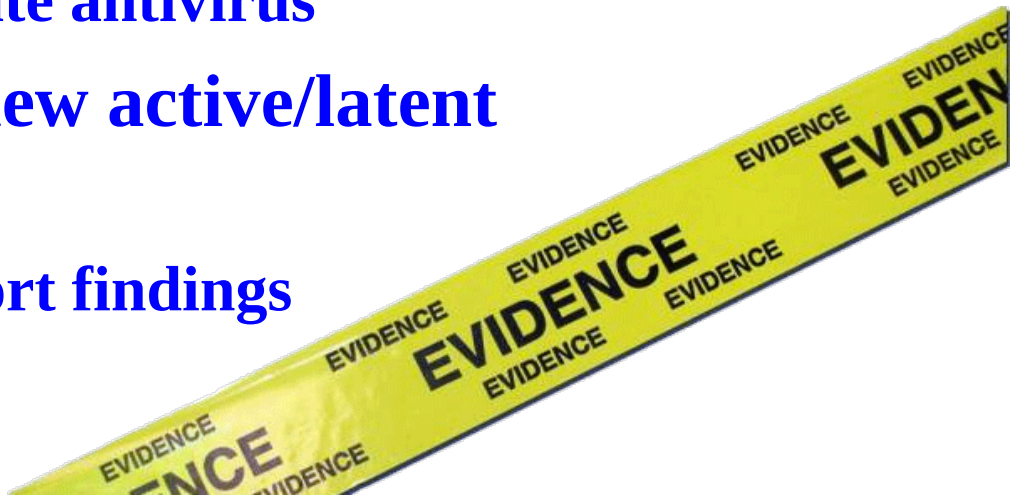
PRESERVE, ETC.

- ASSEMBLE TEAM, DISTRIBUTE LIST OF RESPONSIBILITIES
- UNHOOK INFECTED MACHINES
- CALL OUTSIDE EXPERTS TO FORENSICALLY IMAGE
- PULL NEEDED BACKUPS OUT OF ROTATION AND INSERT CLEAN AND PATCHED MACHINES
- SAVE OFF LOG FILES, KEYCARD DATA AND SURVEILLANCE TAPES
- START REAL-TIME NETWORK PACKET CAPTURE
- FORCE ADMINISTRATOR AND USER PASSWORD CHANGE

PRESERVATION CHALLENGES

COORDINATING IT AND PRESERVATION ACTIVITY

- **IT needs to secure data environment**
  - **Pull network connection, save backups and logs, prepare clean "builds," force password change, update antivirus**
- **Forensics needs to review active/latent data**
  - **Image servers and report findings**

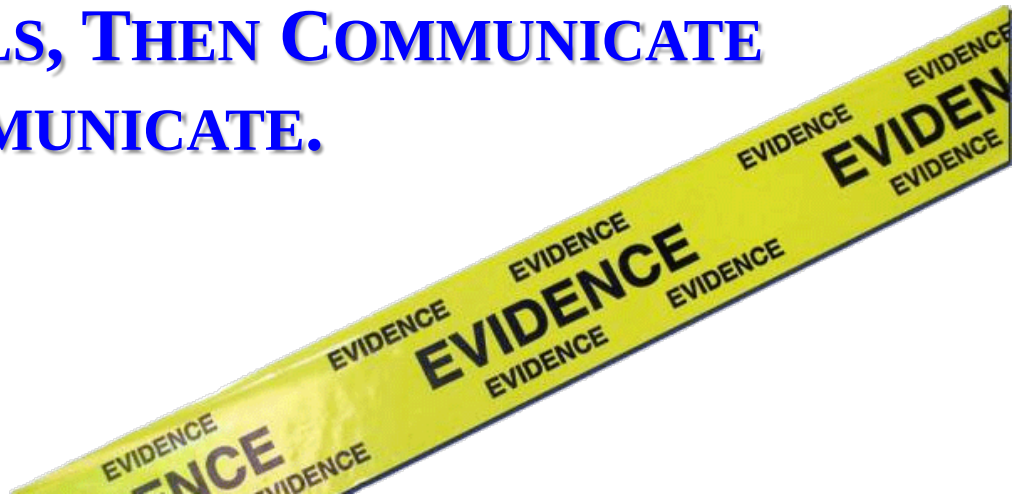


2 DIGITAL FORENSIC ANALYSIS

COORDINATION CHALLENGES

COORDINATING IT AND FORENSIC ACTIVITY

- IT NEEDS TO SECURE DATA ENVIRONMENT
- FORENSICS NEEDS TO REVIEW AND ANALYZE DATA
- BUT CORE BUSINESS ACTIVITY MUST CONTINUE
- ESTABLISH PROTOCOLS, THEN COMMUNICATE COMMUNICATE, COMMUNICATE.



3 LOGGING ANALYSIS

4

Malware Reverse Engineering

5

SURVEILLANCE

6 Remediation Efforts

data breach protections do not detect quickly enough, or act nimbly enough, to counter today's sophisticated and clandestine data breaches.

Yet, so many companies remain unwilling to recalibrate cyber-security into a more effective arche-

John Reed Stark

are important cyber-security measures. But everyone knows that already. Let's focus on what everyone does not already know.

Ever Heard of EDRs?

Recently, a wave of dedicated incident response solutions known as "endpoint detection and response" or "EDR" tools have come into being. Typically installed within a swath of IT equipment including domain controllers, database

down, and a range of other risk-related analytics. Purchasing cyber-insurance is much different, however, because no standard policies exist and the cyber-insurance market remains in its infancy, leading many companies to forego available policies and rely upon their more traditional policies of general liability and property. This is backwards thinking.

Instead, management should undertake an approach towards its insurance calculus based more upon data breach re-

Conventional cyber-security fortification and defense measures need to make way for EDRs; otherwise companies risk a sluggish, incomplete and piecemeal data breach investigation.

that somebody screwed up and left a door unlocked. This only further fuels the fire that breached companies must redouble fortification and detection. That might be true, but the reality is that companies, above all else, should pivot their attention and focus to data breach response."

In other words, when companies trying to prevent data breaches rely too much

activity on endpoints and servers, EDR

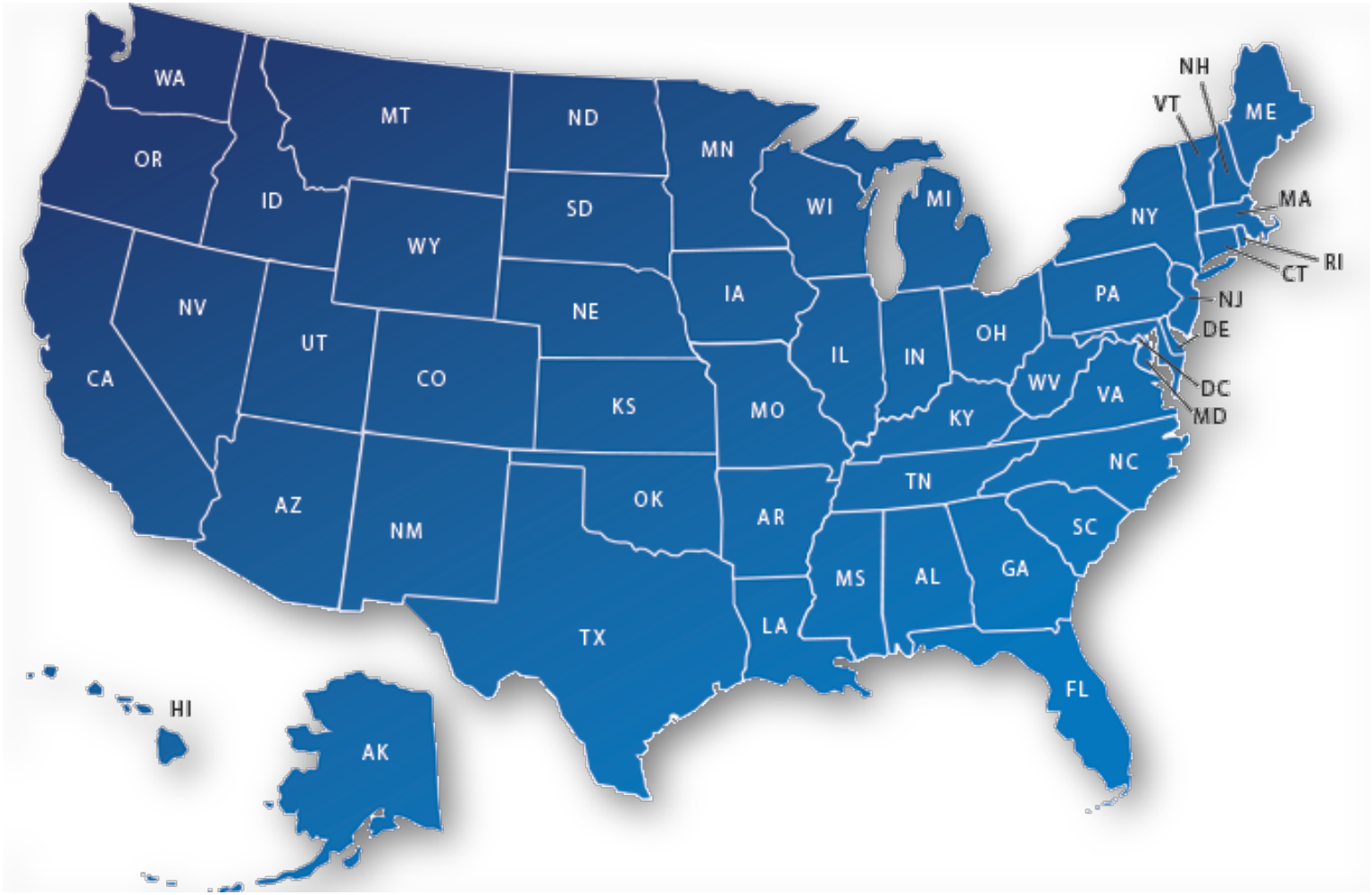
a company can then collaborate with its

Conventional cyber-security fortification and defense measures need to make way for EDRs; otherwise companies risk a sluggish, incomplete and piecemeal data breach investigation.

7 EXFILTRATION ANALYSIS

8

State Regulatory Compliance



9

Federal Regulatory Compliance

PCI COMPLIANCE

Interfacing with Brands

- Contractually bound to hire an investigator "PFI"
- Careful!!! The investigator will be beholden to the brand or regulatory agency – not your company!

Remember the Big Picture

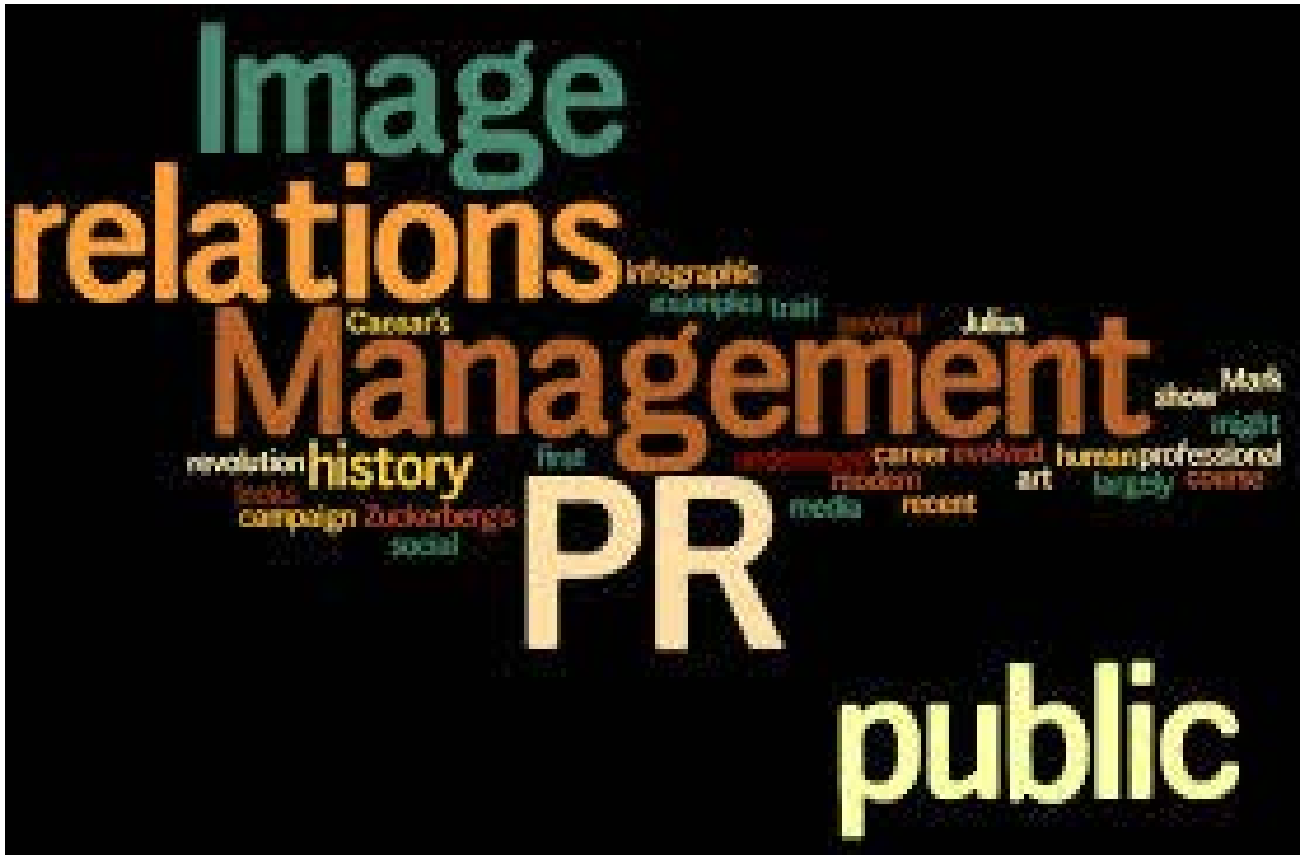
- Often First Outsider To Look At Company's Response
- PFI Report Likely Not Privileged
- Positions Taken Might Impact Other Workflows

11

Law Enforcement Liaison

12

PUBLIC/CONGRESSIONAL RELATIONS



13

CONSTITUENCY NOTIFICATIONS

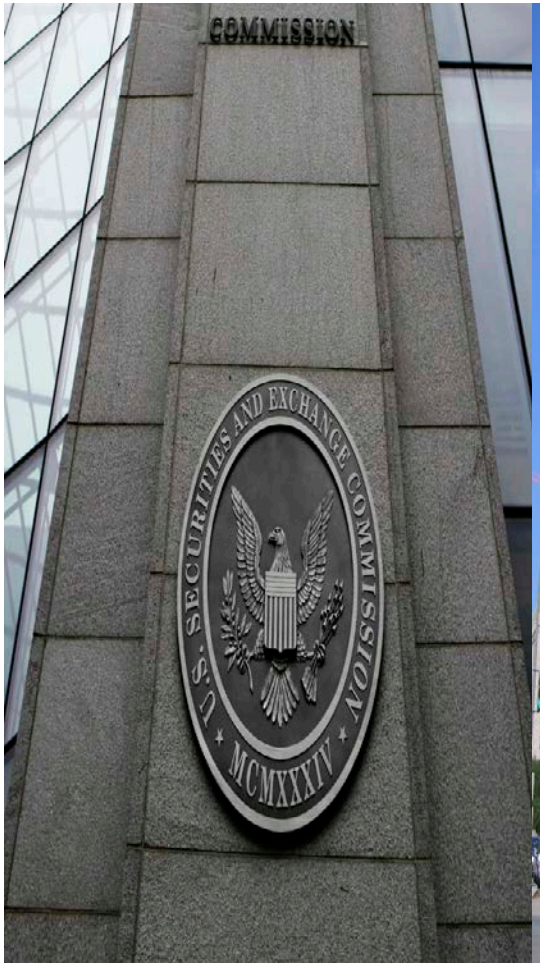
CONSTITUENCY NOTIFICATION: PARTNERS

Constituency Notification: Insurance Carrier

Constituency Notification: Board of Directors

CONSTITUENCY NOTIFICATION: 3RD PARTY VENDORS

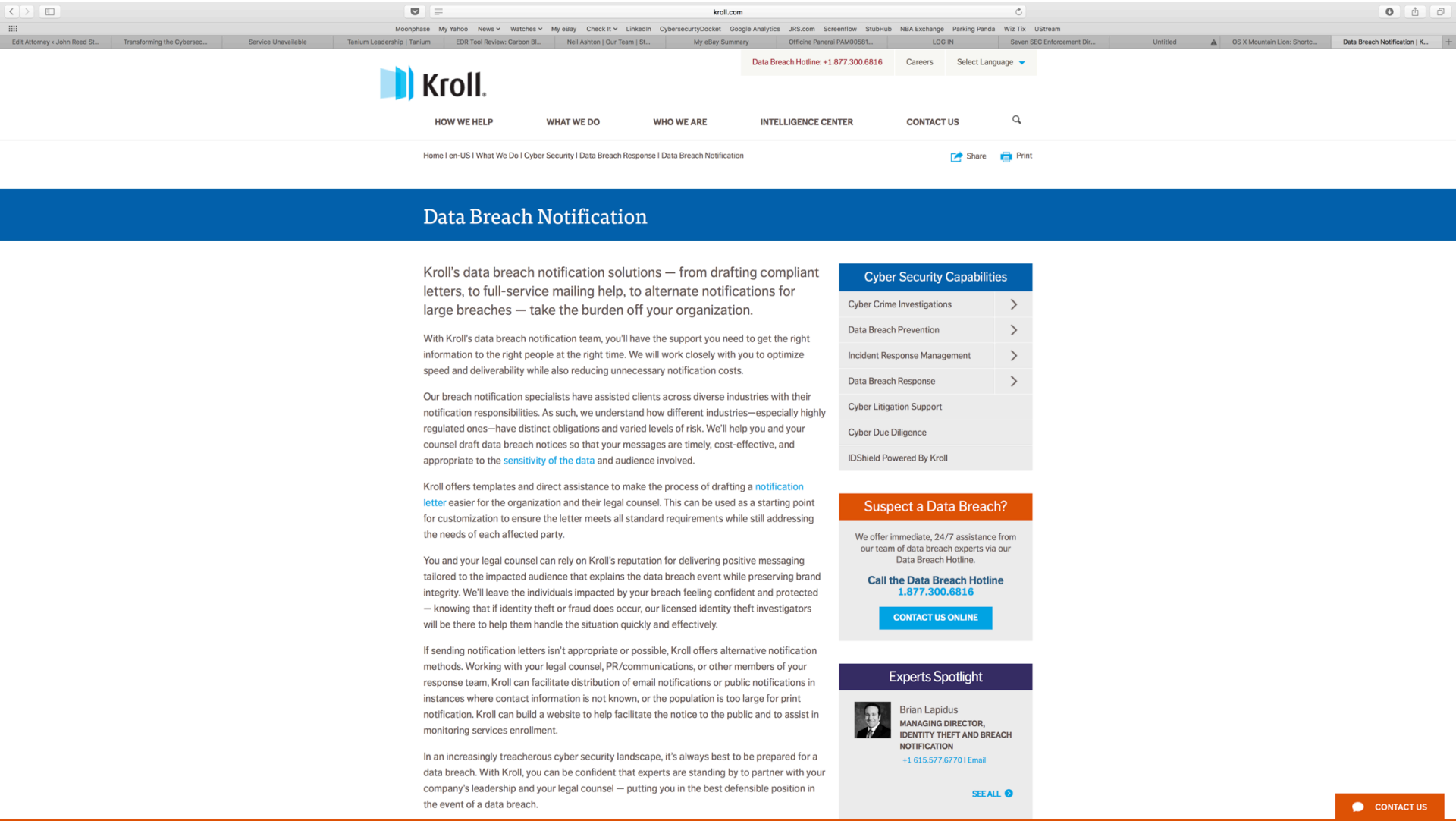
CONSTITUENCY NOTIFICATION: GOVERNMENT



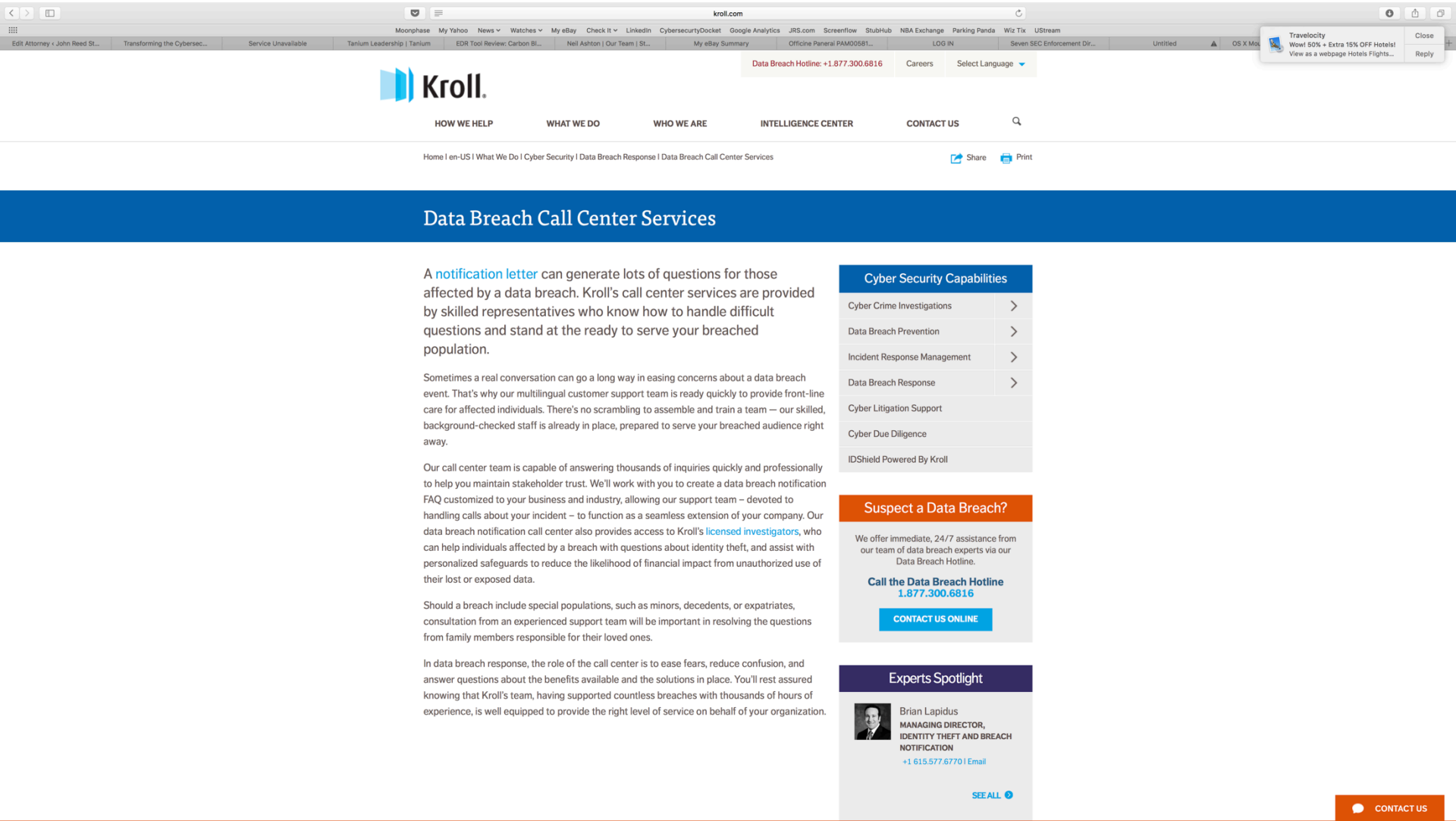
National Association of Attorneys General

Constituency Notification: Employees

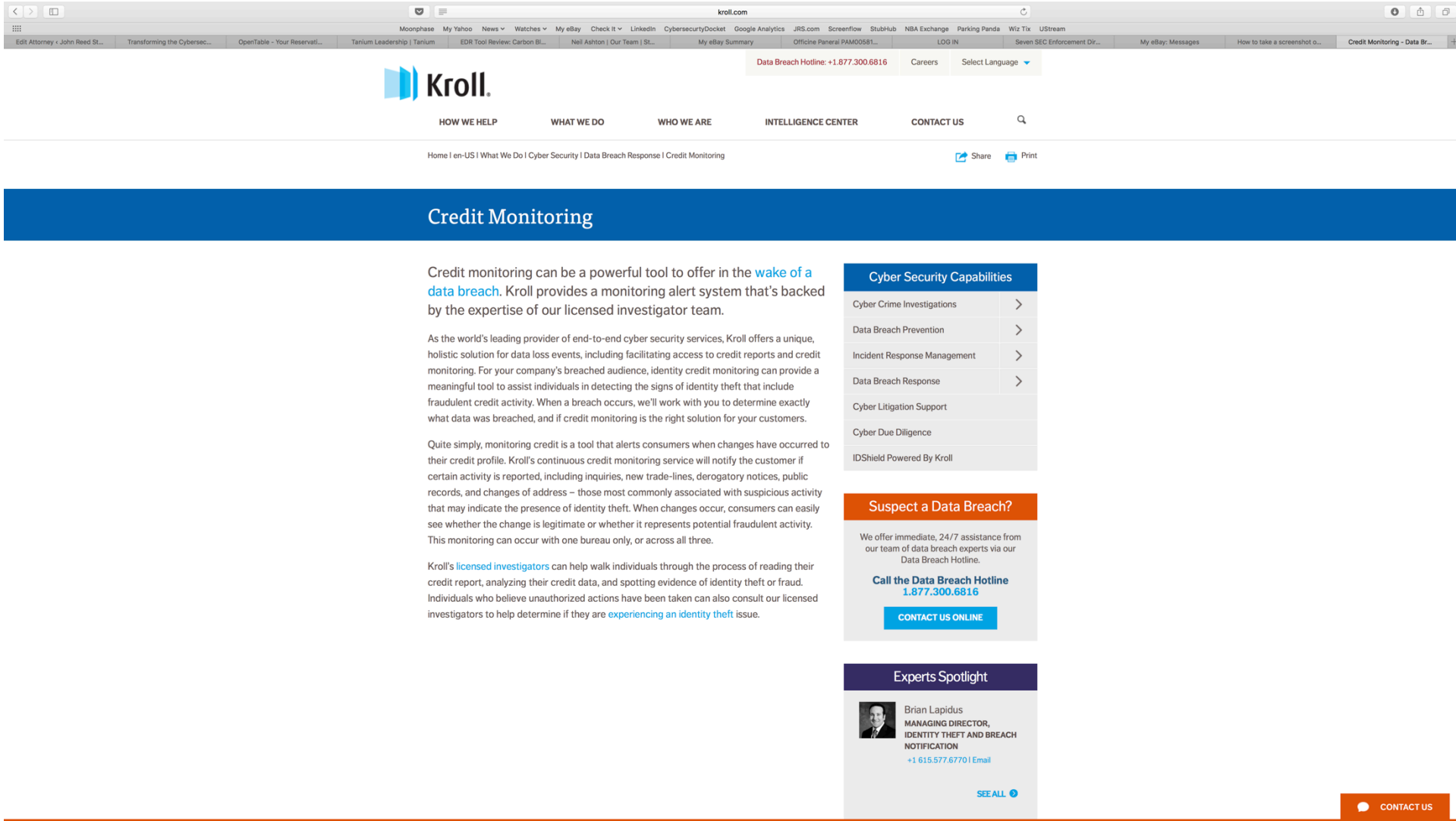
Constituency Notification: Customers



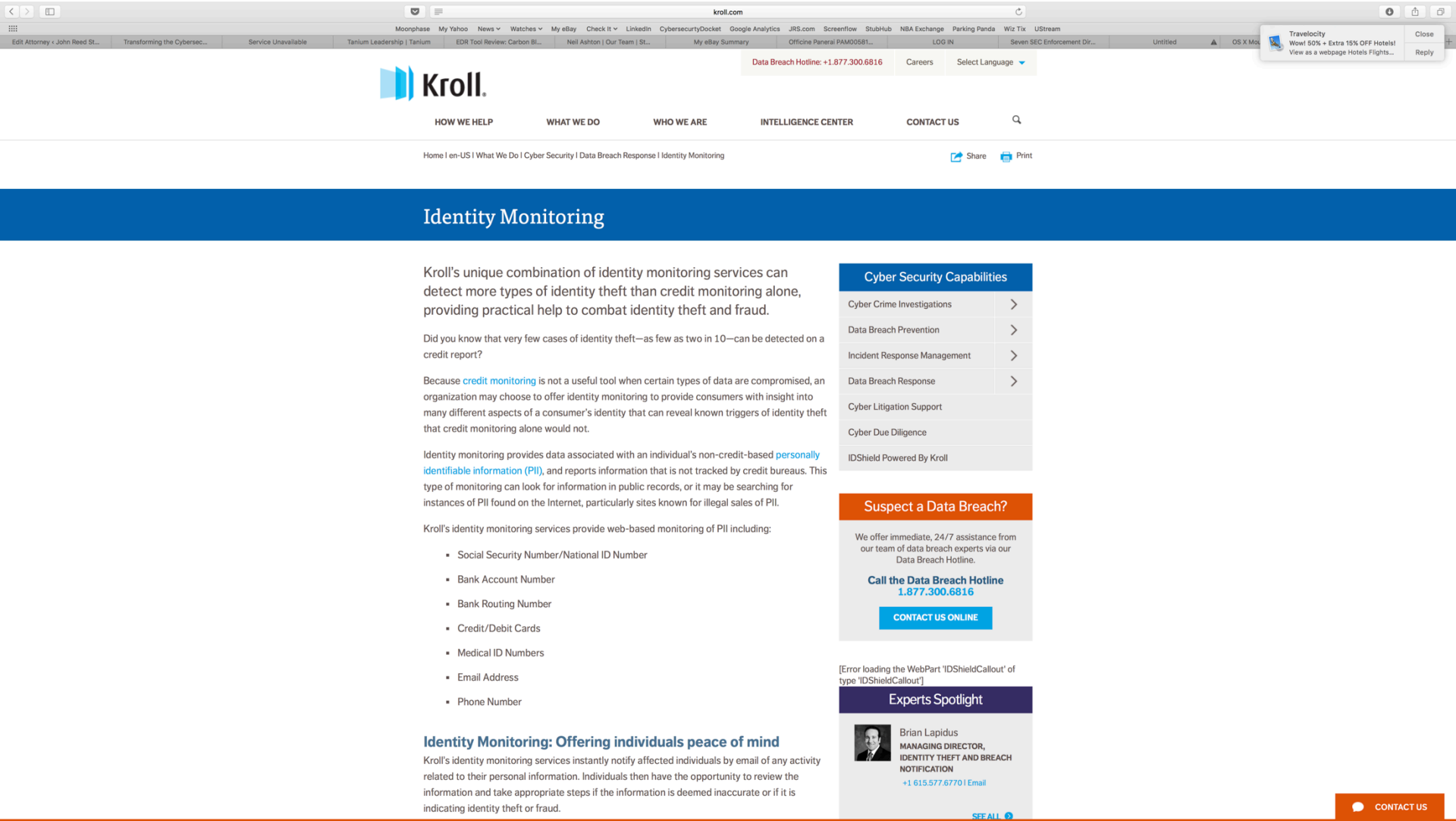
Constituency Notification: Call Center



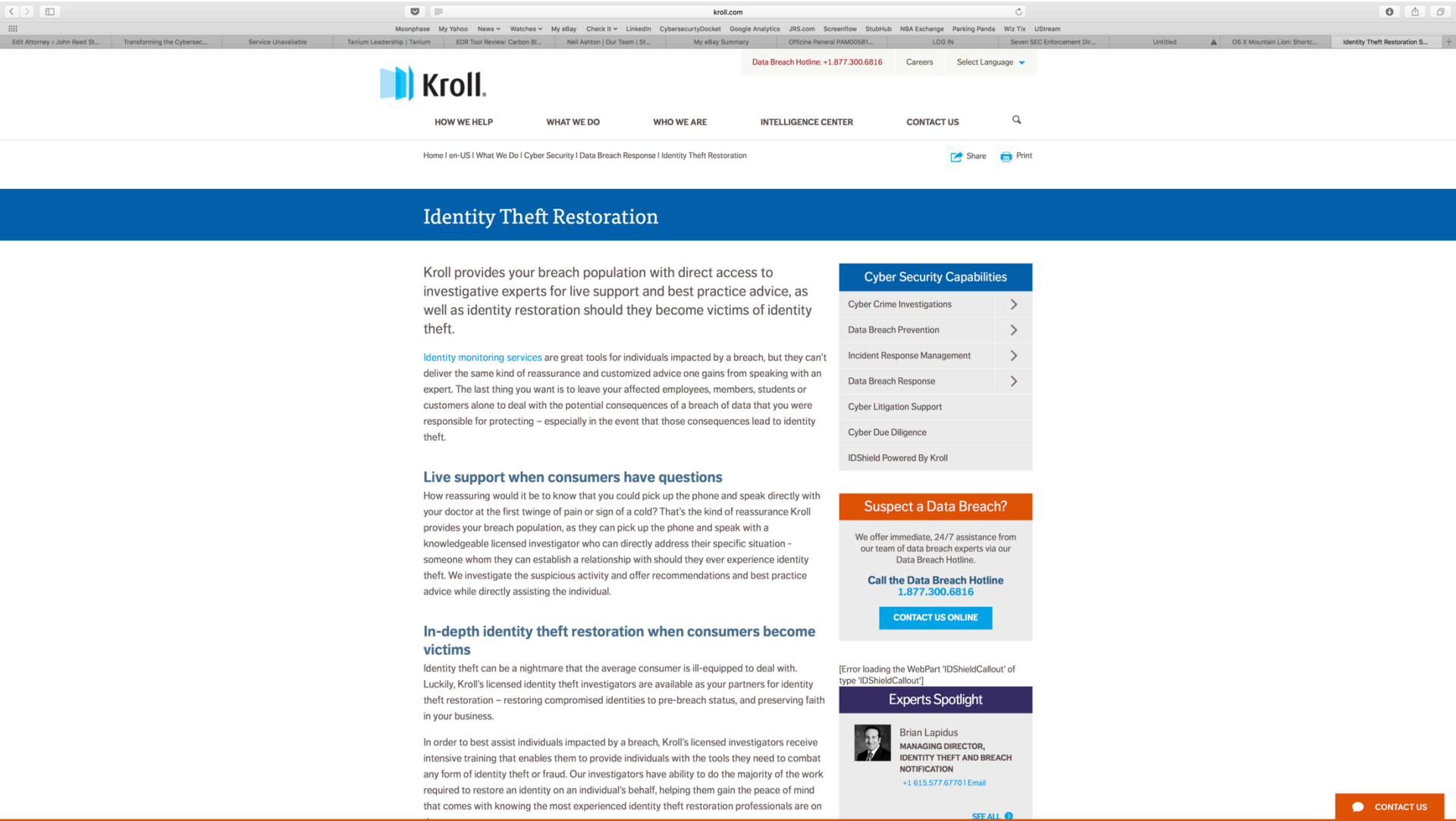
Constituency Notification: Credit Monitoring



Constituency Notification: Identity Monitoring



Constituency Notification: ID Theft Restoration




O
P
[
Q
&
A
?
/

johnreedstark
CONSULTING, LLC

CRYPSIS™
RESPOND • PREVENT