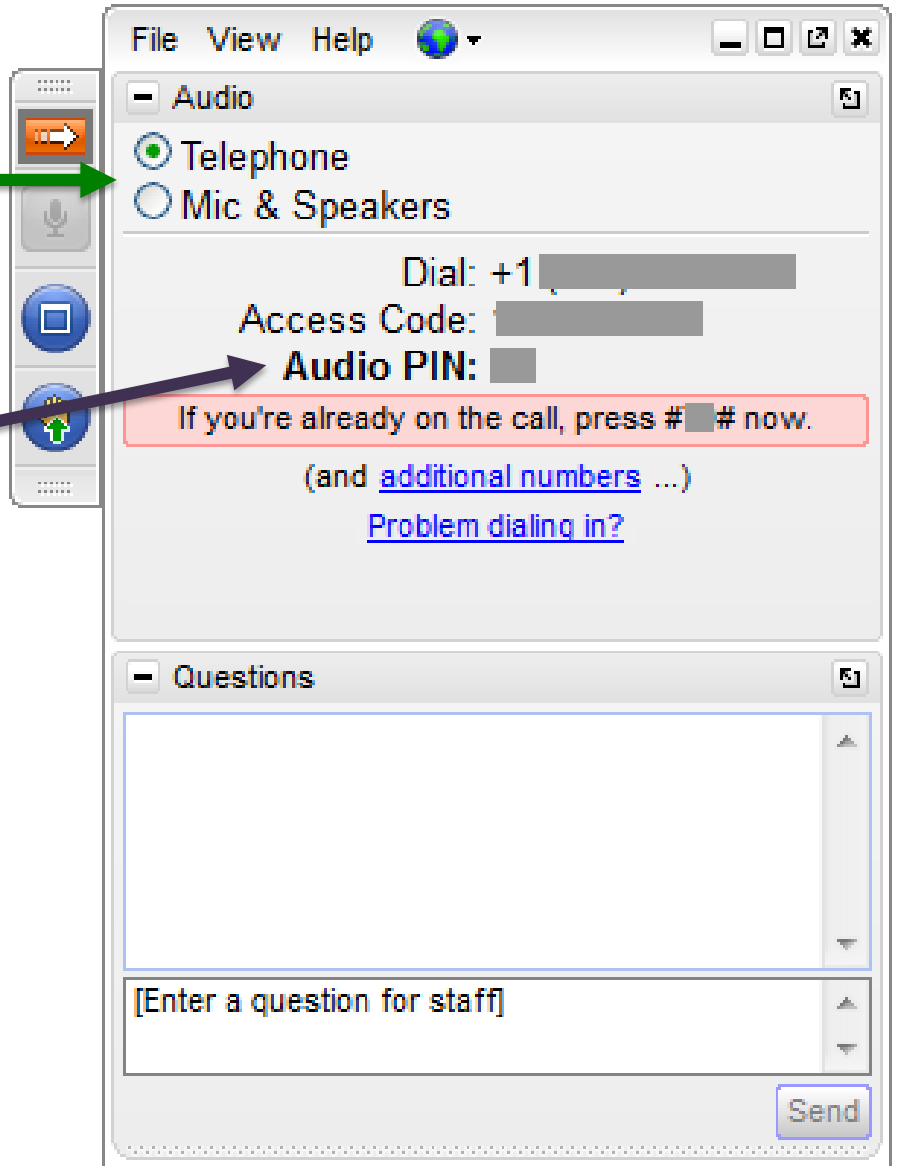
Welcome

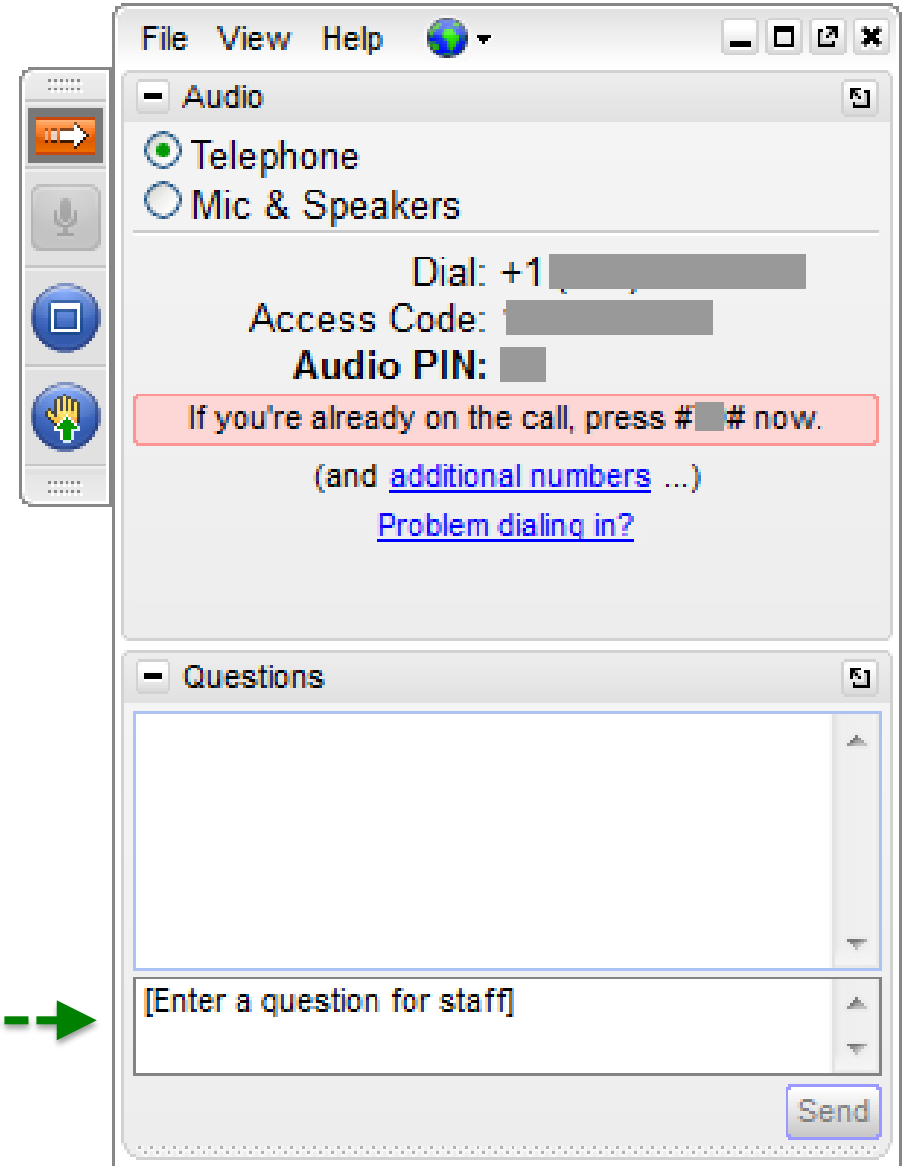
Please dial-in, or use your mic & speakers

Enter your Audio PIN, if you dial in.

All lines are muted.



How to Ask a Question



Type and send

About WaterISAC

- Physical Security
- Cyber Security
- Emergency Management

Alerts via E-Mail
Secure Portal
Pro Update Newsletter

WaterISAC BASIC
- Free

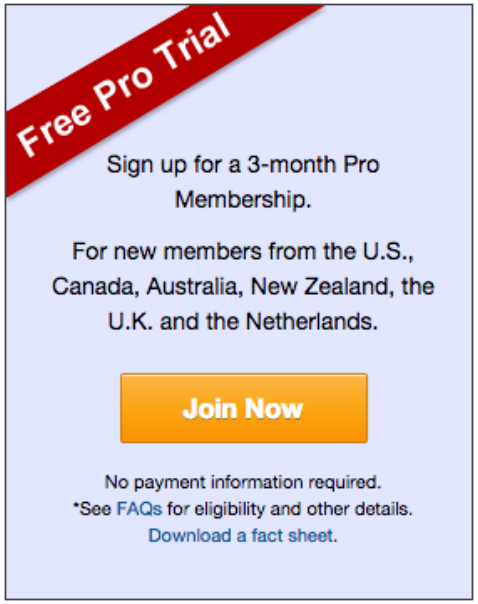
WaterISAC PRO
- Annual Fee
- 3-Month Trial

4,000+

PUBLICATIONS
AND TOOLS IN THE
WATERISAC LIBRARY

Clearinghouse of public, private and proprietary information (Unclassified and FOUO)

Contaminant Databases



www.waterisac.org

American Water Works Association · Association of Metropolitan Water Agencies · ASDWA · NAWC · NACWA · NRWA · Water Research Foundation · Water Environment Federation · WERF

Panelists

Steven Bonafonte, Pullman and Comley, LLC

Jim Grooms, Brown and Brown of New York, Inc.

Bob Bregman, International Risk Management Institute, Inc.

Slides and recording will be posted by Friday.

Water Sector (PCI)

Cybersecurity and Legal Issues

PULLMAN &COMLEY LLC
ATTORNEYS

Pulling Together. Succeeding Together.

Steven J. Bonafonte

Water ISAC Briefing – 11 Dec 2014

Legal Briefs for Today….

PULLMAN &COMLEY LLC
ATTORNEYS

- Current Legal Landscape
- Aftermath of a Breach
- Legal Side of Avoidance

PULLMAN &COMLEY LLC
ATTORNEYS

CURRENT LEGAL LANDSCAPE

Cybersecurity vs. Privacy

PULLMAN &COMLEY LLC
ATTORNEYS

- Privacy Law is different than Cybersecurity Law. This is important to realize, even though both operate in conjunction with each other.

- Privacy law typically deals with how an entity collects and uses personally identifiable information (PII) and also the transparency behind consent to use an marketing.

- Some “Privacy” laws, however, have security components that trigger a duty to protect the information using “reasonable” means or other technologies.

Cybersecurity vs. Privacy

PULLMAN &COMLEY LLC
ATTORNEYS

- Data Breach Reporting Statutes – (States) and those Federal rules that govern certain types of protected information (e.g., HIPAA – Health Information) may have both Privacy and Security components.

- Generally, encryption is a good mechanism to provide safe harbor and avoid triggering the data breach reporting monster.

- Establishing robust policies and procedures for the protection of sensitive information – and more importantly, following these procedures – is essential to the defense of any organization facing a data breach investigation.

Cybersecurity - Bush Administration Efforts:

PULLMAN &COMLEY LLC ATTORNEYS

On January 8, 2008, President Bush issued National Security Presidential Directive 54 – Homeland Security Presidential Directive 23 concerning Cybersecurity Policy.

Unfortunately, President Bush's directive was classified "Top Secret." Thus, it was not until 2010 that his successor revealed that those directives were comprised of a dozen initiatives, including:

- Consolidating external access points to federal systems;
- Cybersecurity education and awareness; and,
- Mitigating risks to the global supply chain for information technology.

Cybersecurity: Obama Administration Efforts

PULLMAN &COMLEY LLC ATTORNEYS

Executive Order 13636, Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21, which:

- Requires information sharing and collaboration between the public and private sectors,
- Mandates the development of a process for identifying and protecting critical infrastructure,
- Requires regulatory agencies to assess and address risks, and, perhaps most significantly to today's topic,
- Requires NIST to lead in developing cybersecurity standards and best practices for protecting critical infrastructure.

Fun NIST Facts:

PULLMAN &COMLEY LLC
ATTORNEYS

The National Institute of Standards and Technology ("NIST")

- Established by Congress in 1901 -- with a budget of $40,000 – and known as the National Bureau of Standards until 1988.
- NIST has been responsible for developing national standards for everything from anti-freeze to radio weather broadcasting.
- NIST's Boulder, CO facility houses the atomic clock which is source of our nation's official time.

NIST Cybersecurity & Privacy

PULLMAN &COMLEY LLC
ATTORNEYS

- On February 12, 2014, NIST released its first version of its Framework for Improving Critical Infrastructure Cybersecurity as ordered by the President in his Executive Order (13636)

- The President's executive order charged NIST with creating a "voluntary Cybersecurity Framework that provides a 'prioritized, flexible, repeatable, performance-based, and cost-effective approach' for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk."

NIST….

PULLMAN &COMLEY LLC
ATTORNEYS

- This Framework provides a reference to Critical Infrastructure operators to follow – and also references third party standards as benchmark guidance (e.g., ISO 27000, NIST SP 800)
- Specifically acknowledges critical infrastructure sectors of **Water Systems** and **Dams**
- Also, includes an appendix (B) on protecting Privacy Data (PII) which has been revised.

NIST Standards…

PULLMAN &COMLEY LLC
ATTORNEYS

- The Framework is intended to be used by entities to review and assess not only core systems (networks, ERM, and operations systems) but also Industrial Control Systems (ICS) such as SCADA.

- Regulatory Agencies will be required to review whether they can/should issue regulations that will require organizations to implement the Framework.

NIST….

PULLMAN &COMLEY LLC
ATTORNEYS

- State regulators also have expressed an interest in adopting the Framework as part of their regulatory mandates.

- The Connecticut utility regulator (PURA), for example, recently released a 31-page report on Cybersecurity and public utilities and issued (this year) a RFP for cybersecurity consultant services in anticipation of issuing regulations and/or audits of utility self-assessments.

NIST….

PULLMAN &COMLEY LLC
ATTORNEYS

- While the Executive Order described the framework as a “voluntary” program, observers believe that it will evolve to a regulatory requirement and/or will be tied to various “incentives” as described by the White House.

- Proposed Incentives include: Rate Recovery for Price-Regulated Industries; Liability Limitation and Federal Grant Funding.

NIST….

PULLMAN &COMLEY LLC
ATTORNEYS

Immediate Advice:

Critical Infrastructure Entities should become very familiar with the NIST Framework and strongly consider conducting a full review of cybersecurity practices against the NIST risk assessment modules

Consider engaging third party cybersecurity consultants for security testing via legal counsel to create additional protections (Attorney/Client Communication and Attorney Work-Product) to shield against exposure in potential litigation or regulatory actions.

PULLMAN &COMLEY LLC
ATTORNEYS

AFTERMATH OF A BREACH

Probably more a question of "when," and not "if."

PULLMAN &COMLEY LLC
ATTORNEYS

Ponemon–IBM 2014 Cost of Data Breach Study:

The probability of a material data breach over the next 2 years involving 10,000 records or more is nearly 19 percent.

This likelihood varies by industry.

- For public sector organizations, the probability is 23.8%.
- For energy and utility companies, the probability is 7.5 percent.

Consequences and Frequency

PULLMAN &COMLEY LLC
ATTORNEYS

- Data breaches are on the increase in frequency, size and severity.
- Breach can happen in seconds, but take months to discover.
- The average cost to a company from a data breach has increased to $5.9 million -- on average, that's more than $200 per record.
- The cost per record varies by industry – Healthcare is $326/record.
- Data loss or exfiltration from malicious attacks costs approximately $246 per record on average.
- Companies report that they are losing more customers (abnormal churn) following a data breach.

Breach Response Plan

PULLMAN &COMLEY LLC
ATTORNEYS

- Do you have a robust data breach response plan (or one at all)?
- What is your mechanism for continuous monitoring (Detection)?
- What is your mechanism for response?
- To what level have you drilled with your legal and communications staff regarding how you will deal with public impact?
- Do you have an awareness of your contractual obligations – and more importantly – the contractual obligations of your suppliers/vendors should a cybersecurity incident take place?

Response…

PULLMAN &COMLEY LLC
ATTORNEYS

- HIPAA, GLB (some), California State Data Breach Laws….
- Who OWNS the response when there is a Data Breach?
- Who is on your team? Who is not? Who should be?
- What is the best way to defend you after you failed to prevent a data loss? (Oops or circle the wagons)
- CAUSE(s): Human error? Lack of compliance? Lack of preventative investment in technology?
- Important to engage quickly and with team of specialists that deal with these issues – litigation is increasing and plaintiff's lawyers are becoming very creative at getting past hurdles of damages

What NOT to do…

PULLMAN &COMLEY LLC
ATTORNEYS

- Don't ignore the issue. If you think nobody will find out, you are risking serious regulatory, legal and financial/reputational harm.

- Don't try and investigate the matter internally or yourself. If you suspect an infiltration, you should immediately trigger your "response team" under the attorney-client privilege.

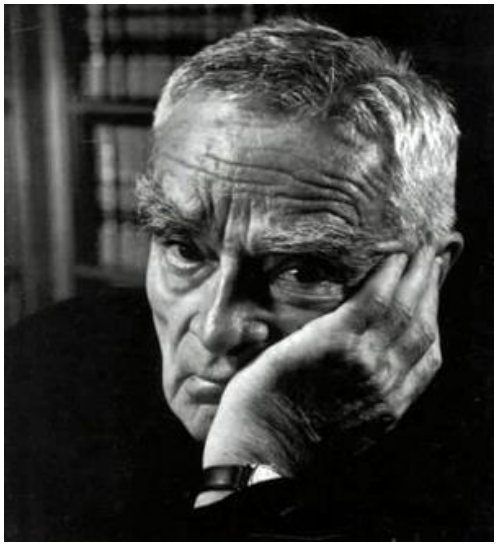
PULLMAN &COMLEY LLC
ATTORNEYS

LEGAL SIDE OF AVOIDANCE

Analyzing Cybersecurity Breaches as Torts

PULLMAN &COMLEY LLC
ATTORNEYS

Lessons learned from Judge Learned Hand and tugboats and barges that break loose in the middle of the night:



Where something goes wrong and, God forbid, there is no clearly defined standard of care governing the situation, some Judge will create one.

The "calculus of negligence."

PULLMAN &COMLEY LLC
ATTORNEYS

In re Eastern Transportation Co. (T. J. Hooper), 60 F.2d 737 (2d Cir.), cert. den., 287 U.S. 662 (1932).

United States, et al., vs. Carroll Towing Co., et al., 159 F.2d 169 (2d Cir. 1947).

Two otherwise forgettable cases – one about a tugboat that went down without a radio and the other about the sinking of an unmanned barge loaded with flour in New York harbor -- that are now famous for Judge Hand's articulation of the cost-benefit analysis for determining negligence and assigning liability, expressed algebraically as whether $B \geq PL$ or $B < PL$.

The Discretion of the Court in Evaluating Risk vs. Utility

PULLMAN &COMLEY LLC
ATTORNEYS

- The “Hand Formula” balances the burden and cost of taking adequate precautions against magnitude and gravity of the potential loss multiplied by the probability of the occurrence of such loss.
- In the absence of clearly articulated “best practices” Judge Hand’s risk vs. utility framework has been offered as a means of determining liability for companies suffering from less than optimum cybersecurity.
- It is an appealing formula, however, each of its components is subjectively determined – affording great discretion to judges and leaving room for a great deal of uncertainty and a wide range of outcomes.

Contractual and Legal Liability

PULLMAN &COMLEY LLC
ATTORNEYS

- So, what is the “Standard of Care” in order to protect against a negligence case in cybersecurity matters?

- This is a moving target – and the NIST Framework may ultimately create a floor for minimum diligence and “duty of care” of critical infrastructure operators (despite disclaiming use as such)

- For example, if a Water Company had a critical cyber event which caused interruption in service such that there was resulting harm and damages to its customers, litigation may ensue.

Legal Liability….

PULLMAN &COMLEY LLC
ATTORNEYS

- Would certain defenses that might afford the utility with immunity from suit/liability apply in such a case?

- The law is evolving – and the plaintiff's bar is paying a great deal of attention in how to craft claims (class actions or large tort business interruption claims) against utilities that fail to take appropriate measures to avoid service interruption.

- One of the proposed potential benefits of adopting and integrating the NIST Framework into core operations may be that it provides utilities with additional protections (safe harbor) from liability to third parties resulting from a cyber event.

Legal Liability…

PULLMAN &COMLEY LLC
ATTORNEYS

- For publicly traded utilities, derivative shareholder suits are also a possibility.
- These suits may allege breach of fiduciary duty and gross mismanagement (among other things) in that officers and directors failed to exercise their requisite standard of care.
- Failing to meet cybersecurity industry standards could rise to the level of this breach of duty.

Class Actions and Fiduciary Duties

PULLMAN &COMLEY LLC
ATTORNEYS

- It remains too early to tell how effective these class actions will be at shaping law and policy in this area.
- One recent case filed against the executives with Wyndham Hotels following 3 separate attacks by Russian-based hackers alleged these theories -- *Palkon v. Holmes*, Case No. 2-14-cv-01234-SRC (D.N.J.) -- but it was dismissed earlier this month by the court.
- However, *Kulla v. Steinhafel*, Case No. 0-14-cv-00203-SRN (D. Minn.) a shareholder derivative action filed against Target Corporation executives following that company's infamous data breach is still winding its way through the court.

(You may recognize the name [Gregg] Steinhafel as that of the 35-year "lifer" and former CEO of Target Corporation, who stepped down within months of that company's infamous data breach.)

Prevention: Know Your Contracts…

PULLMAN &COMLEY LLC
ATTORNEYS

- Do you know YOUR legal exposures for the acts of your suppliers and consultants?
- Have you effectively negotiated terms into your service contracts that will help protect you from liability to third parties should your service providers have a failure that causes you to be unable to deliver services?
- What diligence have YOU taken to inquire as to the business continuity abilities of your third party service providers and how can you protect (or transfer these risks) to third parties – either contractually or via insurance.

Contracts…

PULLMAN &COMLEY LLC
ATTORNEYS

- Where is the information?
- What are the warranties/indemnifications?
  - Security/Privacy; NIST-based compliance?
  - Change in control (if service provider goes bankrupt, where will your information go?)
- What is the CBA of reduced infrastructure and maintenance costs (including increased efficiency) balanced with the external spend and the legal/business risk accepted in the agreement.

Risk Transfer/ Cyber Insurance….

PULLMAN &COMLEY LLC
ATTORNEYS

- What is it?
- Do I need it? If so, how much?
- How do I (can I) negotiate terms and conditions, exclusions and pre-conditions?
- After looking at all the exclusions, what does it <u>really</u> cover?

Contact Information

PULLMAN &COMLEY LLC
ATTORNEYS

Steven J. Bonafonte

Pullman & Comley, LLC
90 State House Square
Hartford, CT 06103

Tel: 860.424.4333

sbonafonte@pullcom.com

PULLMAN
&COMLEY LLC
ATTORNEYS

Pulling Together. Succeeding Together.

Brokering Cyber & Privacy Insurance Policies

Jim Grooms, Vice President Commercial Lines

Brown & Brown Empire State

(315) 474-3374 ext. 267

jgrooms@bbempirestate.com

Brown & Brown
EMPIRE STATE℠

Current Environment:

"2014 – Year of the Data Breach"

- Greater threat of Cyber loss than Property loss
- 1 in 5 small business organizations were targeted with attacks in 2013 (Symantec 2014 Internet Security Threat Report)
- 60 Minutes (11/30/14) comments by Dave DeWalt, CEO of FireEye

  - 97% of all businesses have been breached

  -229 days from time of infection to discovery

Brown & Brown
EMPIRE STATE℠

Tips to Risk Managers:

- The penetration rate for Cyber & Privacy insurance is still relatively low. In fact, according to a recent estimate, the coverage is purchased by only 25 to 35 percent of all companies (see "Making Sense of Cyber Insurance," Property Casualty 360.com, January 13, 2014).
- An Ernest & Young study found that fully one-third of corporate chief technology officers (CIO's) confessed to not knowing for sure if they had insurance to cover cyber events, and, more alarmingly, another third believed they had cyber insurance coverage – and were wrong. (Ernst & Young, 2003 Global Information Security Survey)

Brown & Brown
EMPIRE STATE℠

Tips to Risk Managers – Continued:

- **<u>It's Not Just Your Employer's Survival That's on the Line – It's Yours!</u>**
  If your company's systems are breached, and you haven't at least obtained a quotation for Cyber & Privacy coverage, don't let the door hit you on the way out.
- **<u>Sell the nonindemnification Aspects of the Coverage to Sr. Management</u>**
  Reimbursement from an insurer is only half the story (or maybe even less)
- **<u>No Matter How Much Opposition: Undergo the Application Process</u>**
  Even if the "deciders" reject the opportunity to buy coverage - at least YOU will be covered!

Brown & Brown
EMPIRE STATE℠

Historic Analogy:

- Similar to Employment Practices Liability 15-20 years ago
    - Growing number of carriers with various coverage forms
    - Coverage forms expanding and premium stabilization
    - More events / claims = more reactive coverage purchases
- As specialized cyber coverage becomes more available, CGL, property and crime insurers' policy forms will increasingly restrict the extent of cyber coverage they provide
- Data breaches are not considered "bodily injury" or "property damage" so they don't trigger coverage under CGL forms
- Data breaches don't involve "physical damage" and thus don't trigger coverage under crime or property insurance forms

Brown & Brown
EMPIRE STATE℠

Issues:

- A Doolittle study concluded 95% of U.S. CFO's are not involved in the management of their company's information security risks.

- Cyber Risk is thought of as an IT issue only and this "technology-only" approach cannot operate successfully. These organizations are blind to the financial dimensions of cyber risk management and, accordingly, will neither be empowered to properly analyze cyber risk and its management nor properly appreciate the true costs of funding the required solutions.

Brown & Brown
EMPIRE STATE℠

Issues – Continued.:

- Management will not get a handle on the problem until they appreciate cybersecurity as a strategic and economic issue as much as an operational/technical one.

- Cyber policy is a new expense item (premium) not in current budgets.

- D&O policy issue – potential for exclusion of coverage for not purchasing cyber insurance if the company suffers a data breach.

Brown & Brown
EMPIRE STATE℠

Process:

- Requires full management team to be involved
- Typically must have support from the Board of Directors
- Requires detailed application answering questions on the size and scope of the operations; management of privacy exposures; computer systems controls; and prior claims and circumstances.

Brown & Brown
EMPIRE STATE℠

Process - Benefits of the Application :

- Compels a business to comprehensively (and honestly) assess its risks and vulnerabilities
- Assists in quantifying potential losses (which will help in selecting limits!) because apps ask about: #'s of customer records, sales volumes, locations, etc.
- Focuses senior management's attention on the importance of cybersecurity. Remember: a Sr. Executive must SIGN the application!
- Increases support for having an independent audit - without which a business will never receive an objective assessment of its cybersecurity program.

Brown & Brown
EMPIRE STATE℠

Process - The Need for Cyber Audits:

- Insurers don't generally require them as a condition of providing coverage - but they do encourage them
- Insurers will be happy to recommend providers - yet another benefit of the application process - assuring that you will receive a competent evaluation
- BUT audits are not submitted with coverage applications, to avoid the findings of the audit being discoverable in the event of a loss
- Expect internal resistance to an audit from your company's IT department, but this is one battle a risk manager should be able to win
- If there is a weakness or problem in your company's protection systems, better to find out during an audit than after a data breach!

Brown & Brown
EMPIRE STATE℠

Process - Continued

- **Cyber Privacy Policy** – helpful to obtain the most favorable quote
- Selecting Limits and Deductibles - no easy answers
  - Broker's knowledge and experience can be helpful
  - Large National firms have extensive data bases to assist In making such decisions
  - Business Interruption Worksheets can be an effective tool in estimating potential time-element losses

Brown & Brown
EMPIRE STATE℠

Process – Continued:

Key Factors in selecting Limits & Deductibles:

1. Business Type
2. Business size (revenues, # of customers, # of transactions)
3. Number of Electronic Records
4. Geographic location
5. “Other” miscellaneous factors
6. Cash position a key to making deductible/retention choices

- Market coverage to a number of carriers
- Prepare spreadsheet comparing quotes for coverage, exclusions and premium
- Present marketing results to management / board

Brown & Brown
EMPIRE STATE℠

Cyber & Privacy Insurance: The 7 Key Coverages

Bob Bregman, CPCU, MLIS, RPLU
Senior Research Analyst
International Risk Management Institute, Inc.
(972) 687–9351; Bob.B@IRMI.com

WHAT IS "CYBER & PRIVACY INSURANCE"?

Cyber & Privacy Insurance is a term used to describe the type of insurance written to cover losses resulting from data breaches

WHAT IS A DATA BREACH?

A data breach is an incident in which sensitive, protected, secure, or confidential data is intentionally or unintentionally:

- **stolen,**
- **copied,**
- **transmitted,**
- **viewed, or**
- **used**

in an unauthorized or unlawful way.

A DATA BREACH INVOLVING THE 7 KEY CYBER & PRIVACY COVERAGES

A hacker gains access to a water supplier's computer system, allowing him to obtain the names, addresses, social security #'s, and credit card #'s of 100,000 customers (i.e., "personally identifiable information" or "PII"). A class action lawsuit is later filed by 10,000 of the customers against the water supplier. State and federal regulators also bring legal actions against the supplier, resulting in the imposition of fines and penalties against the organization. As a result of the breach, the supplier is unable to provide water to its customers for 10 days. During the forensic investigation of the breach, the supplier discovers that its entire electronic customer database is missing. The hacker then notifies the supplier that unless it pays him $10 million, he will unleash a spam attack against its website that will render the site permanently inoperable.

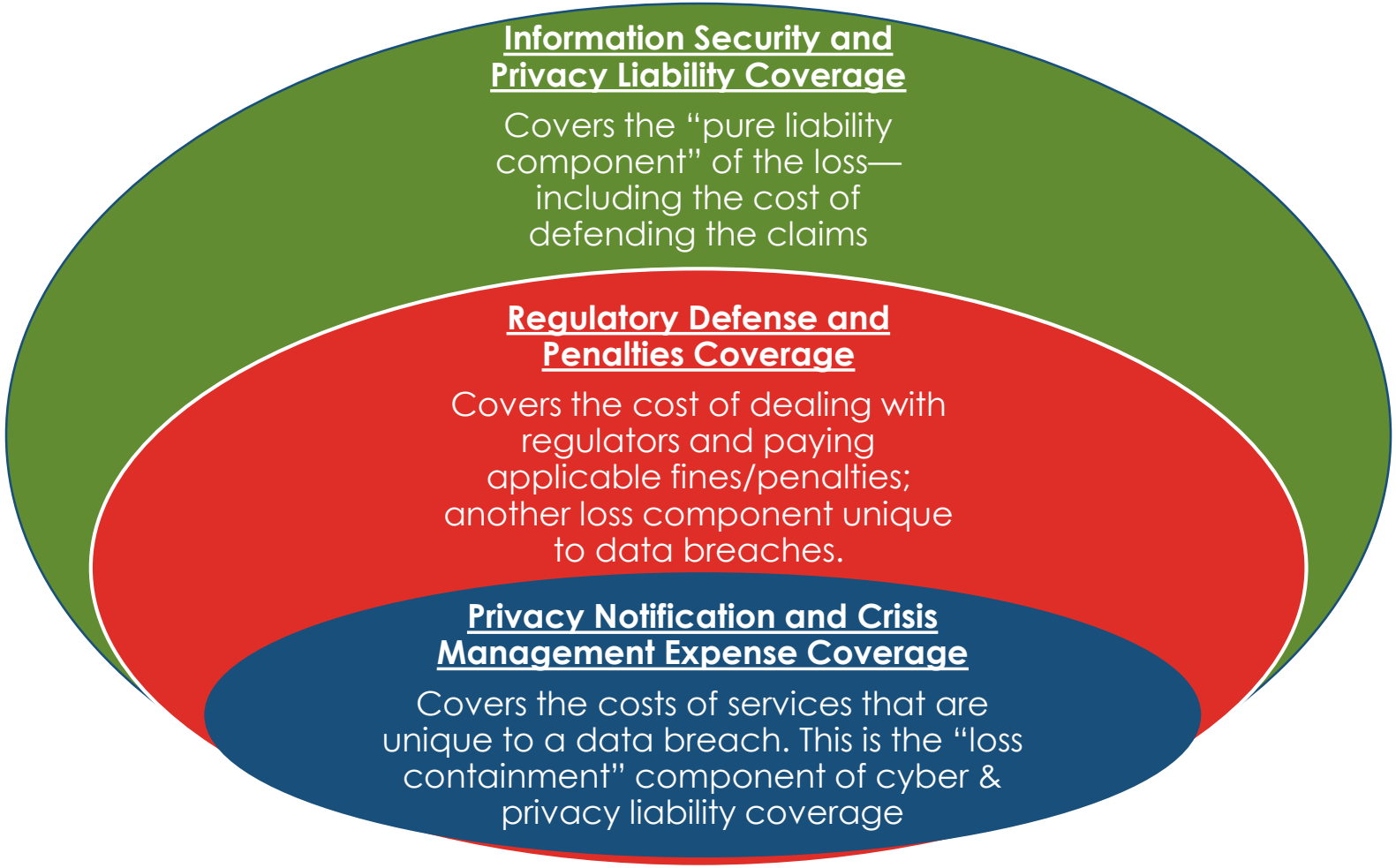
THE 7 KEY COVERAGES THAT RESPOND TO THE DATA BREACH

Liability Coverages	1. Privacy Notification and Crisis Management Expense 2. Regulatory Defense and Penalties 3. Information Security & Privacy Liability
Time Element Coverages	4. Business Interruption 5. Extra Expense
Theft of Property Coverages	6. Data Assets 7. Cyber Extortion

IMPORTANT POINTS ABOUT THE 7 KEY COVERAGES

- À la carte approach: each of the 7 coverages must be purchased separately
- Each coverage is written with a separate limit and a separate deductible
- Policy also contains an "annual aggregate" limit per policy term (i.e., the most the policy will pay out under all coverages, combined)
- Not all insurers offer "time element" or "theft of property" coverages

CONCEPTUALIZING THE 3 LIABILITY COVERAGES



PRIVACY NOTIFICATION AND CRISIS MANAGEMENT EXPENSE: LOSS CONTAINMENT COVERAGE

Covers the direct expenses required to:

- Hire a forensics expert to determine the cause of the breach, suggest measures to secure the site, and offer advice on how to prevent future breaches
- Engage a PR agency to assist the insured in dealing with the crisis
- Set up a post-breach call center
- Notify individuals whose personal information has been compromised
- Monitor customers' credit (usually for 1 year)
- Pay costs needed to "restore" stolen identity (e.g., costs to notify banks and credit card companies)

PRIVACY NOTIFICATION AND CRISIS MANAGEMENT EXPENSE COVERAGE: KEY POINTS

- This coverage affords the insured access to the insurer's cadre of experts who can provide the hands-on know-how to help an insured work through a data breach. This is sometimes referred to as "breach coaching."

- Immediately after a data breach, an insured will benefit immensely by having an insurance company partner with expertise in handling such matters. Responding to a data breach cannot be a "learn by doing" project.

- If an organization is able to purchase just ONE of the seven insuring agreements—this is the single most important one to buy.

REGULATORY DEFENSE AND PENALTIES COVERAGE: REGULATORY "HEADACHE" COVERAGE

Covers the costs of dealing with regulatory agencies that oversee state and federal data breach laws and regulations, including:

- Costs of hiring attorneys to deal with regulators during investigations. This is especially valuable when multiple sets of regulators (state and federal) are involved.
- Costs of fines and penalties that are levied against the insured as a result of the breach.
- "Regulatory Defense" means that only the legal costs of dealing with regulators—not customers/claimants—are covered by this insuring agreement.

INFORMATION SECURITY AND PRIVACY LIABILITY: TRADITIONAL LIABILITY COVERAGE

Covers the insured's liability for damages from a data breach, including:

- Liability for loss, theft, or unauthorized disclosure of personal information in the insured's care, custody, and control
- Defense costs associated with all of the above items

INFORMATION SECURITY AND PRIVACY LIABILITY COVERAGE: KEY POINTS

- This is the true "liability" coverage element of a cyber & privacy policy
- Pays actual liability losses (i.e., settlements and judgments) sustained by various claimants (UNLIKE the first two insuring agreements)
- Contrast with Privacy Notification and Crisis Management Coverage, which pays without admission of liability (e.g., "medical payments" coverage under a homeowners/personal auto policy)
- Pays actual defense costs required to defend claims alleging loss by claimants (but NOT legal costs required to deal with regulators)

TIME ELEMENT LOSS COVERAGES: BUSINESS INTERRUPTION AND EXTRA EXPENSE

Business Interruption (BI): covers loss of income incurred during the "period of recovery" resulting from an "electronic disruption."

Extra Expense (EE): covers additional costs required to expedite recovery after a "disruption," such as overtime labor, express parts shipping, hiring special experts

TIME ELEMENT COVERAGES: KEY POINTS

- Standard property insurance won't cover data breach-related BI or EE loss because the policies require physical damage to trigger a covered loss
- Both BI and EE coverage are triggered ONLY by an "electronic disruption" (as defined by the policy) but NOT by other types of physical damage, such as fire, windstorm, flood, etc., as under standard property insurance policies
- Under some policies, EE coverage applies only if the extra expense reduces the business interruption loss
- Both BI and EE coverages are usually (but not always) subject to a "time" deductible (rather than a "dollar" deductible) before coverage applies, typically 24, 48, or 72 hours

TIME ELEMENT COVERAGES: COMPLICATIONS, CAVEATS, AND A RECOMMENDATION

- Many insurers do not offer cyber-related time element or theft of property coverages because, philosophically, they view cyber & privacy insurance as a liability coverage ONLY. Others offer these but by endorsement—*not* within their standard policy form.
- Under some forms, a covered "computer system disruption" MUST involve data theft; under others, this is not required (e.g., can be introduction of a virus).
- Some insurers "bundle" BI and EE under a single insuring agreement; others separate them; still others offer BI but not EE.
- A recommendation: if insured has purchased BI coverage, insurer has added incentive to handle the privacy notification and crisis management aspects of a data breach MORE EXPEDITIOUSLY! So consider buying BI coverage for that reason.

THEFT OF PROPERTY COVERAGE: LOSS OF DATA ASSETS

Covers the cost of restoring and recovering the data lost from the "failure of an insured's computer system"

- Coverage usually does not apply when loss of data assets is caused by intentional employee acts
- No coverage for upgrading software or other programs during the post-breach restoration process
- No coverage for the cost of research to recover lost data (only provides coverage for "electronic" recovery methods)
- Insurer must (usually) preapprove costs for all expenditures

CYBER EXTORTION COVERAGE: RESPONDING TO ELECTRONIC RANSOM DEMANDS

What's Covered:

(1) Monies paid to meet the extortion demands

(2) Monies paid to computer security experts to advise insured on how to prevent future extortion attempts

(3) Cost of expert assistance to deal/negotiate with cyber extortionists (perhaps more important than #1 and #2)

RECAP:
HOW THE 7 KEY COVERAGES RESPONDED TO THE DATA BREACH

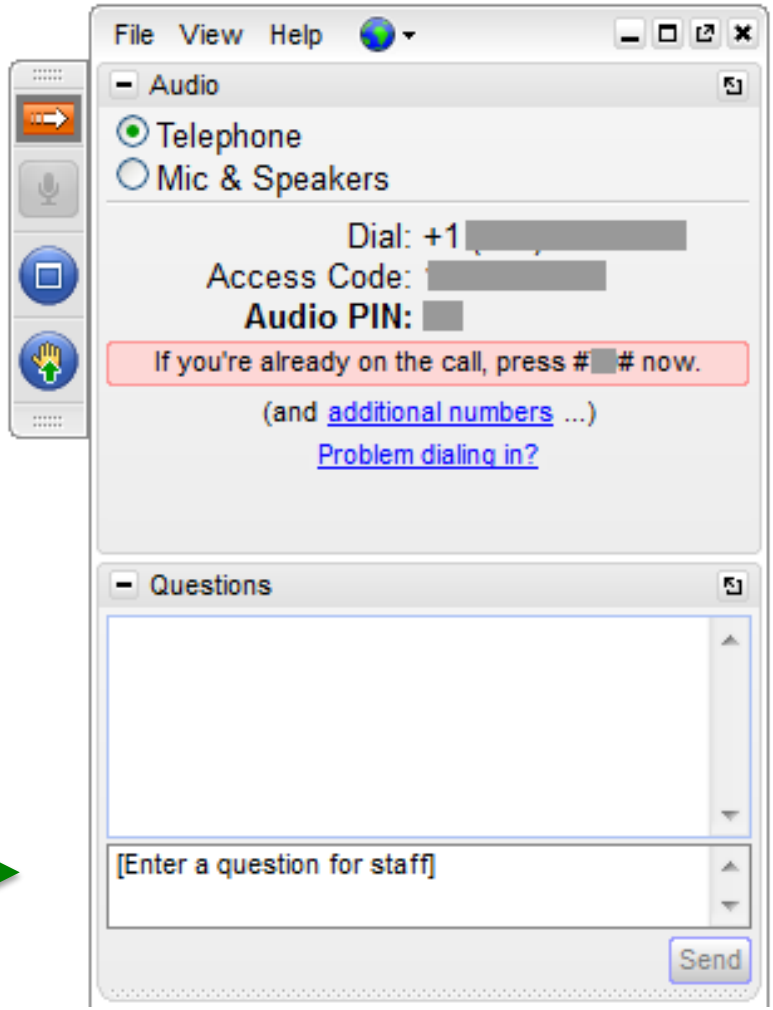
Coverage Type	Payment
• Privacy Notification & Crisis Management Expense	Covered costs of (a) forensics expert, (b) PR agency, (c) call center, (d) customer and bank notification, (e) credit monitoring
• Regulatory Defense & Penalties	Paid legal costs to deal with state and federal regulators, plus fines & penalties the regulators assessed
• Information Security & Privacy Liability	Covered costs of class action and individual settlements/judgments, plus defense costs

RECAP:
HOW THE 7 COVERAGES RESPONDED TO THE DATA BREACH *(continued)*

Coverage Type	Payment
• Business Interruption	Covered income lost during 10-day shutdown
• Extra Expense	Paid added costs to expedite resumption of operations
• Data Assets	Paid computer expert to recover lost customer data
• Cyber Extortion	Covered (a) ransom demand, (b) cost of negotiator, (c) cost to "ransom-proof" website

Questions?

Type and send



Thank You

WaterISAC Contact Information:

1-866-H2O-ISAC

Charles Egli
Lead Analyst
egli@waterisac.org

Michael Arceneaux
Managing Director
arceneaux@waterisac.org

WaterISAC