

Business Interruption Coverage for Cyber-Related Losses: Terms and Exclusions, Interplay With Other Policies

THURSDAY, JULY 19, 2018

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Mary E. Borja, Partner, **Wiley Rein**, Washington, D.C.

Mark E. Miller, Co-Founder, **Miller Friel**, Washington, D.C.

Eric B. Stern, Partner, **Kaufman Dolowich Voluck**, Woodbury, N.Y.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1.**

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-927-5568** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

BUSINESS INTERRUPTION COVERAGE FOR CYBER-RELATED LOSSES

MILLER | FRIEL
PLLC

1200 New Hampshire Avenue, NW, Suite 800, Washington, DC 20036
373 Park Avenue South, 6th Floor, New York, New York 10016

Stafford
Webinars

July 19, 2018

THE PROBLEM: CYBER ATTACKS



❖ **Understanding past cyber attacks helps us understand risks to be insured.**

- **Yahoo**
- **Target**
- **Anthem**
- **Sony**

THE PROBLEM: CYBER ATTACKS

- ❖ **Yahoo (2013 to 2014)**
 - ❖ 1 Billion user accounts breached
 - ❖ Forged cookies permitted outsiders to log on to users email accounts



THE PROBLEM: CYBER ATTACKS

- ❖ **Yahoo (continued)**
 - ❖ Names, DOB, Emails, possibly Security Questions and Passwords were compromised – raises issues of password sharing, content in emails themselves
 - ❖ Investigations: SEC Investigation
 - ❖ Lawsuits: US Lawsuits for “gross negligence.” UK lawsuits for breaching “Data Protection Act”
 - ❖ Renegotiated Verizon Deal at a \$350 million loss
 - ❖ All because Russian hackers targeted them (DOJ charges)

THE PROBLEM: CYBER ATTACKS

- ❖ **Target (2013)**
 - ❖ 40 million debit and credit card numbers stolen; 70 million customers implicated
 - ❖ HVAC provider clicked on email, hackers infiltrated Target's internal network



THE PROBLEM: CYBER ATTACKS

- ❖ **Target (continued)**
 - ❖ **Lawsuits:** Consumer lawsuits; Bank lawsuits; state AG lawsuits
 - ❖ Credit card company claims
 - ❖ Reported Expenses – In excess of \$290 Million (\$240 million for refunding fraudulent charges)
 - ❖ Massive financial losses (46 percent drop in income for 4th Quarter, 2013)

THE PROBLEM: CYBER ATTACKS

- ❖ **Anthem (2015)**
 - ❖ Customer data base breached; 69 to 80 million impacted by breach
 - ❖ Personal information, including social security numbers, stolen



THE PROBLEM: CYBER ATTACKS

- ❖ **Anthem (continued)**
 - ❖ **Lawsuits**: more than 50 class action lawsuits; state AG lawsuits
 - ❖ **Investigations**: NAIC investigation; HHS citation
 - ❖ **Reported Losses Billions.**
 - ❖ **Source for breach not identified. Reportedly no impact on membership.**
 - ❖ **BI losses not disclosed**

THE PROBLEM: CYBER ATTACKS

- ❖ Sony (2011)
 - ❖ Play Station network targeted
 - ❖ Personal and credit card information taken
 - ❖ 102 million people impacted



THE PROBLEM: CYBER ATTACKS

- ❖ **Sony (continued)**
 - ❖ Reported losses: \$171 million (but reports vary widely) (includes estimates of future lost profits).
 - ❖ Gaming system interrupted
 - ❖ 65 class action lawsuits

THE PROBLEM: CYBER ATTACKS

❖ Summary:

❖ Average costs of data breach is \$4 million (IMB)

❖ What makes up losses:

- ❖ Government Investigations (regulatory fines and penalties)
- ❖ Lawsuit defense and settlement costs
- ❖ Credit Card Reimbursements (PCI risks)
- ❖ Notification and remediation costs
- ❖ Forensic Investigations
- ❖ Interruption of business, lost business, and financial losses

POTENTIAL SOLUTION: CYBER INSURANCE

❖ Opportunity for Insurance Companies



- ❖ **\$2.5 billion written premiums today, expected to increase to \$7.5 billion by 2010 (PWC)**
- ❖ **Growing at nearly a 28 percent compound annual growth rate (Business Insurance)**

POTENTIAL SOLUTION: CYBER INSURANCE

- ❖ **Opportunity for Insurance Companies**
 - ❖ **Lloyd's of London stated that cyber insurance sales would save the organization**
 - ❖ **Since the first cyber insurance policy was introduced in 1997, we have seen a feeding frenzy of marketing and sales, like no other we have seen in insurance**
 - ❖ **“the [insurance] industry needs to sell the problem first, before discussing coverage” (Advisen)**
 - ❖ **“News of cyber related loss” was the top driver for growth in cyber insurance marketplace (Advisen)**
 - ❖ **That feeding frenzy also includes lawyers**

POTENTIAL SOLUTION: CYBER INSURANCE

- ❖ **Cyber insurance is the “Wild Wild West” of insurance**



- ❖ **Unlike other kinds of insurance, cyber insurance is unregulated**

CYBER INSURANCE COVERAGE AND EXCLUSIONS

❖ Stand Alone Cyber Insurance Policies

❖ Scope of coverage

❖ Third-Party

❖ First Party

CYBER INSURANCE COVERAGE AND EXCLUSIONS

- ❖ Scope of coverage: First-Party
 - ❖ Costs of responding to cyber breach
 - ❖ Costs of notification; Credit monitoring for customers; Public relations / crisis management
 - ❖ Contingent Business interruption (Loss of data at third party location causes business interruption for insured)
 - ❖ Data recovery costs
 - ❖ First-Party Cyber extortion expense
 - ❖ Theft of goods, services or money over the internet
 - ❖ Network business interruption

NETWORK BUSINESS INTERRUPTION LIMITATIONS TO COVERAGE / EXCLUSIONS

❖ Exclusions / Limitations to Coverage:

1. Scope of Coverage
2. Time limitations
3. Fraud exclusion
4. Profit or advantage exclusion
5. Prior notice exclusion
6. Conditions to coverage

NETWORK BUSINESS INTERRUPTION LIMITATIONS TO COVERAGE / EXCLUSIONS

1. Scope of Coverage – Review Carefully

“’Security Failure’” means a failure or violation of the security of a Computer System. . . .”

- ❖ Better policies cover computer systems owned by Insured and cloud computing scenarios

NETWORK BUSINESS INTERRUPTION LIMITATIONS TO COVERAGE / EXCLUSIONS

2. Time limitations

- ❖ Coverage for loss of Net Income is limited in time
- ❖ 120 days
- ❖ Typically not adequate; need at least one to two years, plus additional time pursuant to extended period of indemnity coverage

NETWORK BUSINESS INTERRUPTION LIMITATIONS TO COVERAGE / EXCLUSIONS

3. Fraud exclusion

“arising out of, based upon or attributable to any dishonest, fraudulent, criminal or malicious act, error or omission, or any intentional or knowing violation of the law”

- ❖ any dishonest act?
- ❖ any dishonest error or omission?
- ❖ Any knowing violation of the law?

Inconsistent with consumer privacy laws: GDPR, data disposal laws, privacy laws, etc.

NETWORK BUSINESS INTERRUPTION LIMITATIONS TO COVERAGE / EXCLUSIONS

4. Profit or advantage exclusion

“for any profit or advantage to which any
Insured is not legally entitled”

- ❖ Insures may argue: “you violated consumer protection laws, and you have no right to recover BI losses because of your wrongdoing . . . You were not legally entitled to those profits.”
- ❖ Exclusion does not play well with consumer protection laws
- ❖ Exclusion has no place in BI coverage grant

NETWORK BUSINESS INTERRUPTION LIMITATIONS TO COVERAGE / EXCLUSIONS

5. Prior notice exclusion and related acts provision

Prior Notice Exclusion: “arising out of, based upon or attributable to any Security Failure or Related Act thereto which has been reported, or in any circumstances of which notice has been given”

- ❖ **Ok – just be careful not to report issues too soon?**
- ❖ **But, Network Interruption Coverage applies only to a “Security Failure first occurring during the Policy Period. . . .”**

NETWORK BUSINESS INTERRUPTION LIMITATIONS TO COVERAGE / EXCLUSIONS

5. Prior notice exclusion and related acts provision (cont.)

“Related Acts” means all First Party Events and Third Party Events which are the same, related or continuous and all First Party Events and Third Party Events which arise from a common nucleus of facts. All Related Acts shall be considered to have occurred at the time the first such Related Act occurred.”

❖ Recipe for disaster

NETWORK BUSINESS INTERRUPTION LIMITATIONS TO COVERAGE / EXCLUSIONS

6. Conditions to Coverage

- ❖ Proof of loss within 90 days – Impossible
- ❖ Submit to an examination under oath – problematic and unnecessary
- ❖ Submit to appraisal – can't decide legal issues
- ❖ ADR provisions – never favorable to policyholders

CONTACT INFORMATION

Mark E. Miller
Direct: (202) 760-3161
millerm@millerfriel.com



KAUFMAN DOLOWICH VOLUCK

ATTORNEYS AT LAW

Business Interruption Coverage for Cyber Related Losses

Eric Stern, Esq.
Partner
estern@kdvlaw.com
516-283-8703

Andrew Lipkowitz, Esq.
Associate
alipkowitz@kdvlaw.com
516-283-8728

135 Crossways Park Drive, Suite 201
Woodbury, New York 11797

KDVLAW.COM

Telephone: 516.681.1100
Fax: 516.681.1101

Background on Standard Business Interruption Coverage



Commercial Property Policy

- The standard Commercial Property Policy form provides coverage for “actual loss of Business Income” sustained due to the “necessary suspension of your operations during the period of restoration.”
- Suspension of operations must be caused by “direct physical loss of or damage to property.”
- Policy only provides coverage for what would have been earned had Insured resumed operations as quickly as possible.

Commercial Property Policy

- Business Income definition includes net income after taxes that would have been earned.
- Plus continuing normal operating expenses, including payroll.



Commercial Property Policy

- Business Interruption Coverage is triggered after a waiting period and runs for a set period from date of loss or the actual time to repair, rebuild or replace the property.
- BI coverage may be triggered by direct physical loss of by damage to “electronic media and records.”
- Electronic media and records includes “electronic data processing” including films, tapes, discs, drums or cells.

Do Cyber-Related Losses Constitute “Physical Loss” Under a Commercial Property Policy?



Background on the Issue

- Commercial Property Policies only cover loss caused by “direct physical loss or damage.”
- Courts have reached different conclusions on whether cyber-losses constitute “physical loss.”

Am. Guarantee v. Ingram

2000 U.S. Dist. LEXIS 7299 (D. Ariz. 2000)

- Insured's computer systems were rendered inoperable as a result of a power outage.
- Insured sought coverage for business interruption and related losses.
- Court held that "physical damage" is not limited to physical destruction or harm but includes "lack of access, loss of use, and loss of functionality."

Am. Guarantee v. Ingram

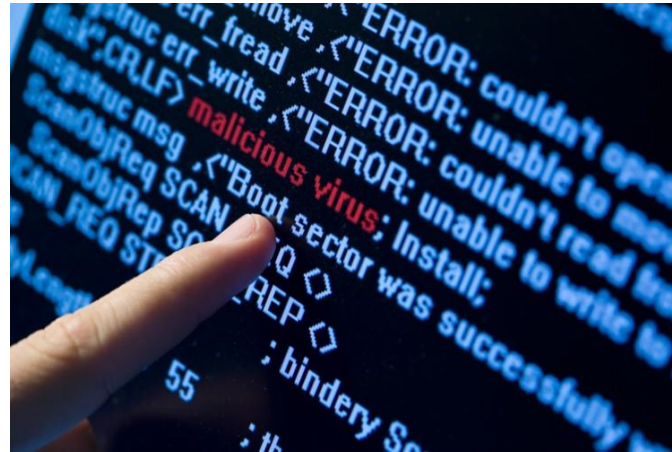
- There was no tangible, physical damage.
- The Court looked to definition of computer crimes in state and federal statutes, noting that these statutes reflect the determination by lawmakers that “when a computer’s data is unavailable, there is damage.”
- Court further held that the computer system physically lost programming information and configurations necessary for them to function.

Lambrecht v. State Farm Lloyds

119 S.W.3d 16 (Tex. App. 2003)

- Hacker installed a virus on insured's computer systems forcing insured to replace its server and purchase a new operating system triggering a BI and property damage claim.
- Insurer argued that loss of information on an insured's computer system was not "physical loss" because the computer data did not exist in tangible form.

Lambrecht v. State Farm Lloyds



- Court rejected Insurer's argument, holding that BI coverage was afforded as the insured's computer server falls within definition of covered "electronic media and records."
- The Court found that the hard-drive and disks were physically damaged because they could not longer hold or store information

Ward General v. Employers Fire

7 Cal. Rptr. 3d 844 (Cal. Ct. App. 2003)

- The insured was updating its computer data when the operator inadvertently pressed the “delete” key on the keyboard , wiping out critical data.
- The insured sought coverage income lost during the recovery period.
- The trial court found that the losses were not covered and the appellate court affirmed.
- Court reasoned that the policy only covered physical damage to property, and that the loss was not physical because the lost information was not tangible.

Covered Cyber Losses

- *NMS Services, Inc. v. The Hartford*, 62 Fed. Appx. 511 (4th Cir. 2003): Court held that there was coverage under a business property policy for an insured's loss of business and costs to restore records lost when a former employee hacked into the insured's network. Concurring opinion held that rearrangement of atoms or molecules of a disk or tape is a 'physical' change.
- *Southeast Mental Health Center Inc. v. Pacific Ins. Co. Ltd.*, 439 F. Supp. 2d 831 (W.D. Tenn. 2006): Insured proved necessary direct physical loss where the insured's pharmacy computer data was corrupted due to a power outage.

Uncovered Cyber Losses

- *Am. Online v. St. Paul Mercury Ins.*, 207 F. Supp. 2d 459 (E. D. Va. 2002): Court held that CGL Policy did not cover costs to defend AOL against lawsuits alleging that AOL software damaged customers' computers because such lawsuits did not involve "physical damage" to "tangible property."
- *Seagate v. St. Paul Fire*, 11 F. Supp. 2d 1150 (N.D. Ca. 1998): Insured sought coverage under a CGL policy for lawsuit based on damage to consumer's computer data caused by defective disk drives sold by the insured. Court held that there was no coverage because the alleged damage to data was not physical damage to tangible property.

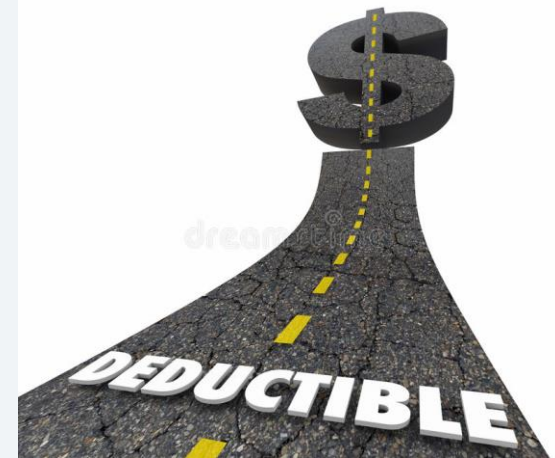
Summing Up

- If there is physical damage caused as part of the cyber-loss, then there is probably coverage.
- Absent real-world physical damage, whether there is coverage is left up to the Court's interpretation of the policy to overlook or broadly interpret the "tangible property" requirement.

Deductibles & Retentions for Cyber Related Losses

Deductibles & Retentions

- Business interruption coverages are typically subject to a time-based deductible.
- Commercial Property policies typically contain a BI “waiting period” of 72 hours before coverage is triggered.



Waiting Period

- A standard waiting period to trigger Business Interruption coverage on a Commercial Property Policy may not adequately address a cyber-loss
- Repair of physical property covered under a Commercial Property Policy takes a longer period of time than repair of cyber-damage.
- Losses over short periods of disruption of a traditional property damage loss are typically smaller than cyber-related losses.

Waiting Period

- The DDOS attack on October 21, 2016 caused many websites to be down for only 2-3 hours.
- According to web-analytics firm Neustar, the average Business Interruption loss from a DDOS attack is \$250,000 per hour.
- According to Forbes, the interruption of Amazon's website for 30 minutes in 2013 resulted in Business Interruption loss of approximately \$2 million.

Waiting Periods

- Even assuming coverage under a Commercial Property Policy for a cyber-loss, a Waiting Period of 72 Hours (or even 24 hours) may be too long to trigger coverage for a cyber-event



Unlike Commercial Property Policies, Cyber-Coverage Forms

- Reimburse income loss, interruption expenses and other expenses incurred during a “period of restoration.”
- Provide coverage for expenses caused by “total or partial interruption,” degradation in service or failure of computer system.
- Reimburse costs incurred during a period of recovery from a security breach or privacy breach.

Conclusions

- Standard Commercial Property Policies may provide coverage for cyber-related losses, but leaves insureds at the mercy of Court and subject to conditions that are not commensurate with cyber-losses.
- To ensure coverage for cyber-losses, insureds should purchase a cyber-specific policy.

Questions & Answers



Eric Stern, Esq.
Partner
estern@kdvlaw.com
516-283-8703



Andrew Lipkowitz, Esq.
Associate
alipkowitz@kdvlaw.com
516-283-8728



KAUFMAN DOLOWICH VOLUCK

ATTORNEYS AT LAW

135 Crossways Park Drive, Suite 201
Woodbury, New York 11797

KDVLAW.COM

Telephone: 516.681.1100
Fax: 516.681.1101



Cyber Policies – BI and CBI Coverages

Mary E. Borja

Wiley Rein LLP
mborja@wileyrein.com

202.719.4252



Mary E. Borja, Esq.

Mary Borja is a partner in the insurance and litigation practices at Wiley Rein LLP in Washington, D.C. She has extensive experience in insurance coverage disputes involving professional liability, commercial general liability, cyber, and crime insurance. Ms. Borja represents insurers in coverage litigation at both the trial and appellate levels before federal and state courts, as well as in arbitrations, across the country. Ms. Borja also defends complex or high exposure malpractice claims against lawyers and other professionals.

Ms. Borja is a frequent speaker on insurance coverage issues and litigation strategy. She has served as Co-Chair of the ABA Insurance Coverage Litigation Committee CLE Seminar, the Professional Liability Subcommittee, and the Construction Subcommittee, and she is a Fellow in the American College of Coverage and Extracontractual Counsel. Ms. Borja received her law degree from the University of Miami School of Law, *magna cum laude*, and her undergraduate degree from the Johns Hopkins University.

Cyber Policies



Cyber Policies

- Cyber coverage can be endorsed onto a property policy or GL policy or written as a standalone policy, depending on the insurer
- Regardless of form, insured must prove covered cause of loss
 - must link cyber event and claimed business interruption
 - need to quantify the amount of lost revenue

Cyber Policies

- Coverage grant for cyber event, even within single policy, may be afforded by a single insuring agreement or determined by multiple insuring agreements and endorsements
- Terms used are not defined uniformly among insurers

Cyber Policies – No Uniform Definitions

Cyber-attack means the transmission of fraudulent or unauthorized Data that is designed to modify, alter, damage, destroy, delete, record or transmit information within a System without authorization, including Data that is self-replicating or self-propagating and is designed to contaminate other computer programs or legitimate computer Data, consume computer resources or in some fashion usurp the normal operation of a System.

Cyber Policies – No Uniform Definitions

“Enterprise Security Event” means any of the following:

1. Accidental release, unauthorized disclosure, theft, or loss of Protected Personal Information by the Insured or Service Contractor;
2. Unauthorized access to or unauthorized use of Protected Data on the Insured’s Computer System that directly results in theft, alteration, destruction, deletion, corruption or damage of Protected Data;
3. Transmitting or receiving Malicious Code via the Insured’s Computer System; or
4. Unauthorized access to or unauthorized use of the Insured’s Computer System that directly results in denial or disruption of access of authorized parties.

Cyber Policies – No Uniform Definitions

Computer Crime and Computer Attacks. An act, mistake, negligent error or omission in the operation of your computer system or handling of your digital assets by your employee, or by a BPO service provider or outsourced IT service provider, that fails to prevent or hinder any of the following attacks which was intended to maliciously cause harm to your computer system:

1. Denial of service;
2. Malicious code;
3. Unauthorized access; or
4. Unauthorized use.



Business Interruption and Cyber Events

- Cyber events increasingly causing BI across all industries – manufacturers, construction companies, banks, health care providers, etc.
- BI loss does not have to result from a “hack” or social engineering, it may result from routine technical failures or human error

Business Interruption and Cyber Events

- Coverage triggers for BI not uniform across cyber policies
- Determine what caused event
- Review insuring agreement and coverage extensions:
 - Is BI coverage triggered by non-malicious acts?
 - By power interruption?
 - By failures of security?

Business Interruption and Cyber Events

- Period of indemnity
 - Extended Period of Indemnity – may pay continued loss after the service is restored up to the time when the business recovers
- Period of interruption before coverage is triggered
 - When does the period begin
 - In cyber policy, usually measured in hours
 - Is a monetary deductible preferred
- Sublimits

Business Interruption and Cyber Events

- Crisis management expenses
- Breach notification costs, credit monitoring, call center services, forensic investigations, public relations
- Who picks counsel, vendors
- Consequences for failure to notify insurer promptly of breach

Liability Coverage for Cyber Event

- Cyber event may give rise to liability claims
- Liability arising from loss of confidential data
- Coverage for acts of third parties such as vendors
- Data in care, custody or control of third parties such as data storage center, cloud provider

Regulatory Coverage for Cyber Event

- Insured may be subject to federal and state regulatory regimes in multiple jurisdictions
 - Where does the insured do business or have customers



Regulatory Coverage for Cyber Event

- Costs of obligations to state and federal regulatory agencies that enforce data breach laws and regulations
- Regulatory investigation costs, attorneys fees, and regulatory fines and penalties
- Some cyber policies pay defense expenses and regulatory fines where allowable by law

Remediation Coverage

- First party costs for replacing, recreating, restoring, and repairing damaged or destroyed programs, software or electronic data
- Amounts for restoring reputation or brand name
 - How are they calculated



PCI Coverage Under Cyber Policies

- PCI-DSS provides baseline of technical and operational requirements designed to protect cardholder data
- Cyber policy may have coverage for PCI-DSS Liability
 - may cover amounts for PCI demands for assessments, including fines and penalties for non-compliance with PCI Data Security Standards



Cyber Policies and CBI Coverage

- CBI - coverage for losses when a third party service provider cannot operate because of a cyber incident
- Cyber insurers starting to extend CBI to system failure triggers and higher limits
- Potential aggregation
 - Supply chain and CBI may have concentrated risk, such as a major internet or cloud service provider or a security flaw in a widely used software product

Infrastructure Attacks - Network



- *E.g.*, WannaCry - massive ransomware cyber-attack infected over 100,000 computers in more than 150 countries.

- Microsoft vulnerability weaponized by NSA; leaked by hackers. Many companies failed to install patch.
- WannaCry sought Bitcoin ransom payments or encrypted files would be deleted and all non-backed up data would be permanently lost.

Infrastructure Attacks – Conventional Infrastructure

- *E.g.*, in 2017 hackers gained “operational access” at some US power firms: control of interfaces engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses.



FINAL THOUGHTS

Q&A

To ask a question from your touchtone phone, press *1.
To exit the queue, press *1 again.

You may also use the Chat function to ask questions, or email questions to insurancelaw@straffordpub.com

CLE CODE: TLEIVI

Tell us how we did!

Look for our 'Thank You' email (which you should receive within 24 hours) for details and a link to the program survey and attendance attestation.

Not A Passholder Yet?

Try the CLE Individual Annual Pass

- Get all your CLE credits for one low price with the Strafford CLE Individual Annual Pass.
- Attend unlimited live webinars in any of our legal practice areas where we produce over 600 advanced live webinars each year.
- Plus you get unlimited access to hundreds of recorded webinars.

Simply respond to the email you will receive after the program.