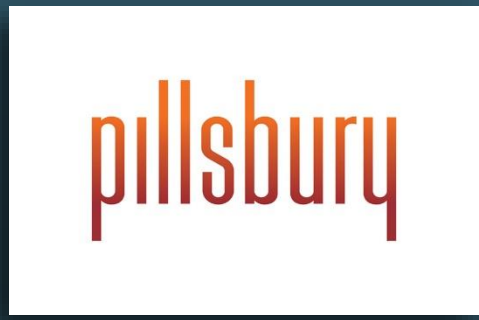
Cybersecurity Compliance, Contract Considerations & Insurance for Cloud Communications Providers

Cloud Communications Alliance - Virtual
January 19, 2022



Cloud Communications Alliance

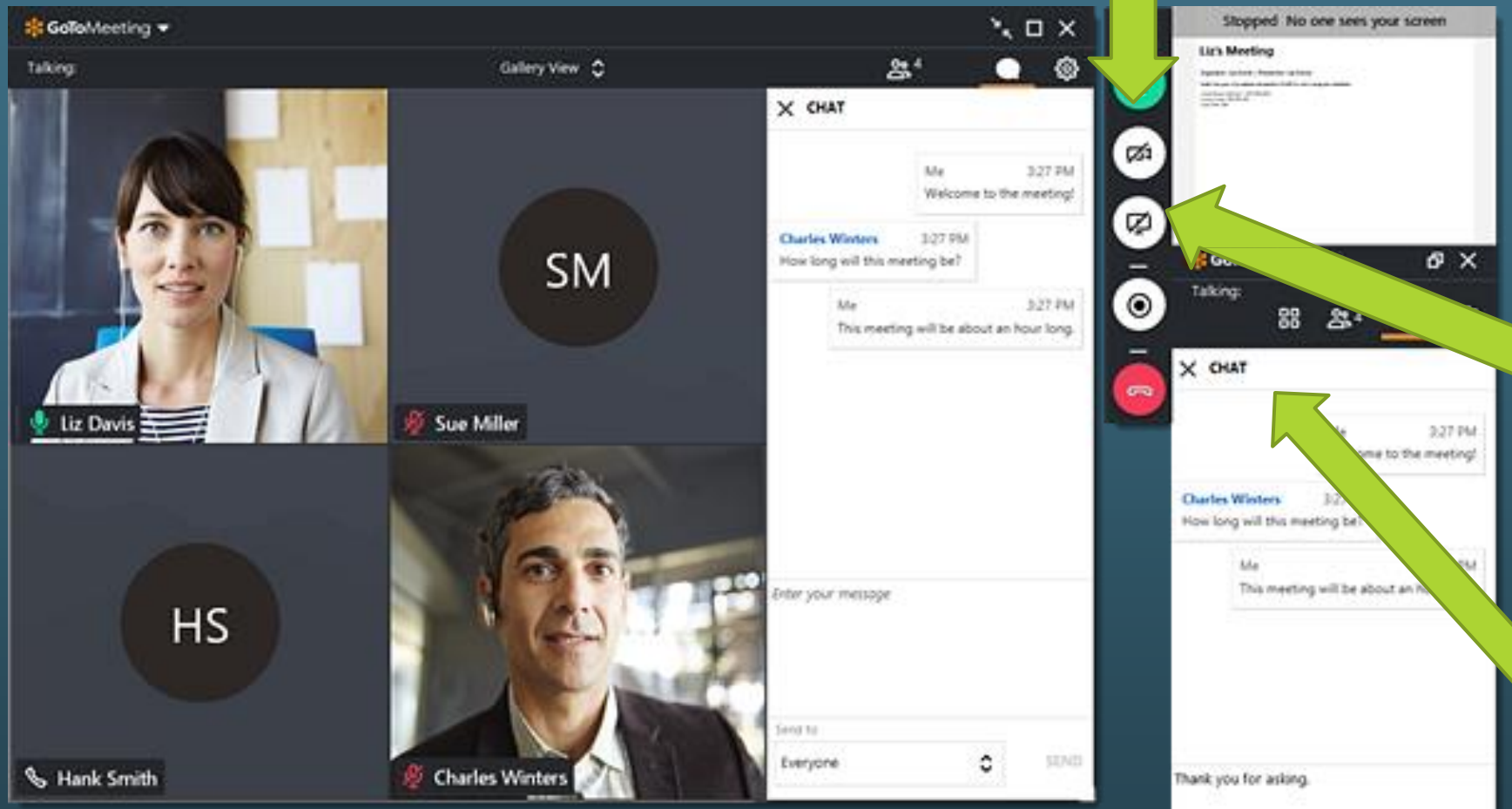
pillsbury


JOIN US AT OUR VIRTUAL MEETING:
Cybersecurity - Compliance, contractual considerations & insurance for Cloud Comms Providers
Cloud Communications Alliance
Featuring:
Pillsbury Winthrop Shaw Pittman LLP
January 19th, 12 PM EST

pillsbury

Cloud Communications Alliance

Mute Button



Camera on/off button

View speaker or all button

Chat/Text questions/comments

pillsbury

BRIAN E. FINCH | Partner
Pillsbury Winthrop Shaw Pittman LLP
Email: brian.finch@pillsburylaw.com
Phone: +1.202.263.8062

Education

J.D., The George Washington University Law School 1999
B.S., Cornell University, 1996

Professional Highlights

•Recognized by *Chambers USA* in Government: Government Relations, by *The Legal 500 U.S.* in its Cybercrime and the Data Protection and Privacy categories and by *Law360* as a "Rising Star" in Privacy Law.
•Received the 2015 Distinguished Legal Writing Award from The Burton Awards.
•Serves as a senior fellow with The George Washington University Center for Cyber and Homeland Security.
•Visiting legal fellow, The Heritage Foundation, Washington, DC.
•Former senior fellow with The George Washington University Center for Cyber and Homeland Security.

Brian Finch, a Pillsbury Public Policy partner with extensive regulatory and government affairs advocacy experience, is a recognized authority on global security and cybersecurity threats. He co-leads Pillsbury's COVID-19 Response team, providing clients with real-time guidance on the implications of the rapidly evolving epidemic.

Based in Washington, DC, Brian provides strategic legal counsel to companies from nearly every industry regarding regulatory issues, cyberattacks, national defense and intelligence policies, and homeland security concerns. He has helped more than 150 clients take advantage of SAFETY Act liability protections following terrorist or cyberattacks and has testified before the U.S. Congress regarding the Act's provisions. Brian advises on risk mitigation tactics, minimizing post-event negative consequences, and litigation strategies. He has also worked with the Departments of Defense and Health and Human Services on a variety of emergency medical preparedness matters, including weapons of mass destruction (WMD) and pandemic preparedness/response issues.

Representative Experience

•Advised and advocated on behalf of a leading cybersecurity company providing real-time threat protection for global enterprises and governments regarding legislative defense authorization and related appropriations.
•Advocated for the American Gas Association, American Public Power Association, National Rural Electric Cooperative Association and others regarding federal cybersecurity solutions to help reduce liability for exposure to cyberattacks.
•Represents automobile manufacturers in the development of cybersecurity best practices.

TAMARA D. BRUNO | Partner
Pillsbury Winthrop Shaw Pittman LLP
Email: tamara.bruno@pillsburylaw.com
Phone: +1.713.276.7608

Education

J.D., Hofstra University School of Law, 2009
B.F.A., New York University, 2005

Professional Highlights

- Insurance MVP, *Law360* 2021
- Recognized, *Chambers USA*, 2017-2021
- Insurance Rising Star, *International Financial Law Review*, 2020
- Member, The American Lawyer Young Lawyer Editorial Board, 2018-2021
- Insurance Rising Star, *Law360,* 2017
- Recognized, *Best Lawyers,* 2021-2022
- Member, *Law360* Insurance Practice Group of the Year, 2020, 2016, 2015

Partner Tamara Bruno leads the Texas section of Pillsbury's Insurance Recovery & Advisory practice, recently named a 2020 "Insurance Practice Group of the Year" by *Law360*, from Houston, though her practice spans the nation.

She advises companies and institutional policyholders on complex and cutting-edge issues involving insurance and risk, and represents clients in high-stakes litigation involving insurance coverage disputes. Her experience spans a wide range of business insurance, including property and casualty coverage and a variety of liability coverages. Her primary focus is on specialized insurance coverages, including Directors & Officers liability, Cyber, Commercial Crime and Professional Liability insurance. Bruno advises and represents policyholders in all industries, including energy, technology, hospitality and consumer products.

Tamara is widely recognized for her work and expertise. She has been recognized by *Best Lawyers*, *Law360* and *Chambers USA* for her notable successes in insurance litigation and was named a *Law 360* MVP in September 2021 and an Insurance Rising Star by the *International Financial Law Review* in their 2020 Americas Rising Star Awards. Additionally, Tamara served on *Law360's* 2020 Insurance Editorial Board and is a member of The American Lawyer's Young Lawyer Editorial Board. She served two terms as an elected council member for the Insurance Law Section of the Texas State Bar and is currently serving her second term on the Board of Directors for the Corporate Counsel section of the Houston Bar Association. She regularly writes and speaks on insurance law topics.

MEIGHAN E. O'REARDON| Partner
Pillsbury Winthrop Shaw Pittman LLP
Email: meighan.oreardon@pillsburylaw.com
Phone: +1.703.625.3984

Education

J.D., George Mason University School of Law, 2007
M.S., The George Washington University, 2003
B.S., Clarkson University, 1998

Professional Highlights

- Named Next Generation Lawyer for Outsourcing through *The Legal 500 U.S. from* 2017-2021
- Recognized, *Chambers USA* for Technology and Outsourcing, 2018-2021
- Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals (IAPP) since 2007

Partner Meighan O'Reardon is an experienced technology and data privacy attorney in Pillsbury Winthrop Shaw Pittman's internationally recognized Global Sourcing and Technology Transactions practice. Meighan's work is specifically focused on structuring, negotiating and managing complex services transactions across multiple industries, most notably in the financial services and healthcare sectors.

Meighan advises clients through all phases of a transaction, from initial bid preparation through contract negotiation, relationship governance and renewals. She has worked on many forms of services and technology agreements including IT infrastructure outsourcings; payroll, accounts payable, human resources, help desk and back office process outsourcings; application development deals; offshore outsourcing arrangements; information technology consulting agreements; teaming and collaboration agreements; software and hardware contracts; and SaaS and Cloud agreements. Meighan also regularly advises on various forms of software licensing and development agreements.

A portion of Meighan's practice is devoted to advising on privacy and cybersecurity issues that arise in commercial services and technology transactions including advising on best practices related to incorporating security compliance requirements into these deals.

The Cybersecurity Environment

pillsbury

The Cybersecurity Environment

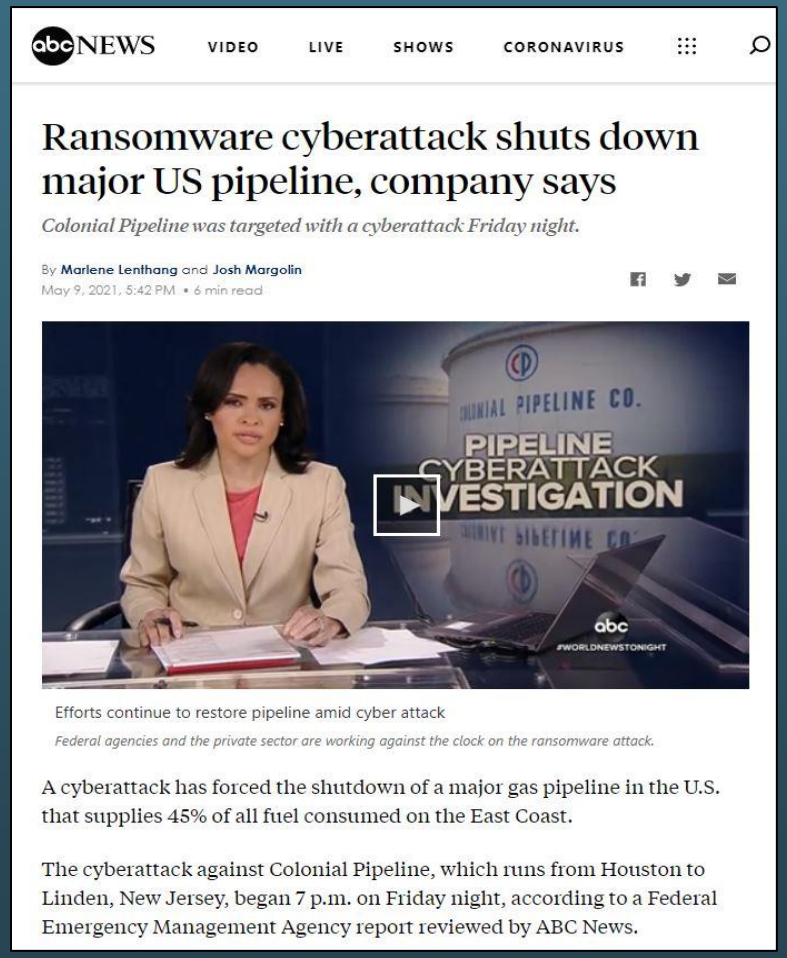
Cybersecurity firms found government-linked hackers from China, Iran, and North Korea attempting to use the Log4j vulnerability to gain access to computer networks.

Researchers have already found over 600,000 attempts to exploit the vulnerability.

December 2021

pillsbury

The Cybersecurity Environment



abc NEWS VIDEO LIVE SHOWS CORONAVIRUS

Ransomware cyberattack shuts down major US pipeline, company says

Colonial Pipeline was targeted with a cyberattack Friday night.

By Marlene Lenthang and Josh Margolin
May 9, 2021, 5:42 PM • 6 min read

Efforts continue to restore pipeline amid cyber attack

Federal agencies and the private sector are working against the clock on the ransomware attack.

A cyberattack has forced the shutdown of a major gas pipeline in the U.S. that supplies 45% of all fuel consumed on the East Coast.

The cyberattack against Colonial Pipeline, which runs from Houston to Linden, New Jersey, began 7 p.m. on Friday night, according to a Federal Emergency Management Agency report reviewed by ABC News.

High profile ransomware attack on Colonial Gas by a DarkSide threat actor affiliate.

45% of all fuel consumed on the East Coast was shut down.

$4.4M was paid.

April 2021

pillsbury

The Cybersecurity Environment

Cloud computing services are a target.

The Russian Foreign Intelligence Service was reported in October 2021 to have launched a campaign targeting cloud service providers. The U.S. also announced in June 2021 that Russia hackers attempted a series of attacks in 2019-2021 targeting users of Microsoft cloud services.

Impacts of outages can be seen from the multiple December 2021 AWS outages.

pillsbury

The Cybersecurity Environment

- The COVID-19 pandemic has exacerbated the prior trend of accelerating cyberattack activity
- 400% increase in attacks since the start of the pandemic (as of August last year)
- Rapid increase in cybersecurity incidents among small to mid-sized businesses

pillsbury

Attacks Continue …

EUROPE POLITICS

Ukraine claims Russia behind cyberattack in ‘hybrid war’

PUBLISHED SUN, JAN 16 2022•1:08 PM EST | UPDATED SUN, JAN 16 2022•7:54 PM EST

AP

SHARE

pillsbury

Cybersecurity Legal Obligations

pillsbury

Increasing Regulation

- Increasing numbers of states expanding the definition of “personal” information:
  - California Consumer Privacy Act
  - NY SHIELD law
- In those states, “personal information” much broader than before
- Biometric data included or otherwise regulated, i.e. Illinois Biometric Information Privacy Act
- Failure to obtain consent, properly protect, or even delete information could lead to claims of privacy violations

pillsbury

Increasing Enforcement

- U.S. Treasury Dept recently issued updated guidance on sanctions risks in making ransomware payments
- Robust cybersecurity and reporting/cooperation with law enforcement considered significant mitigating factors for potential sanctions

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: September 21, 2021

pillsbury

Regulatory Response

- DHS increasing oversight of cybersecurity in wake of ransomware attacks:
  - TSA Pipeline Security Directives
  - Planned regulations coming for aviation, rail
- Legislation pending:
  - Data breach notification for critical infrastructure
  - Ransomware notification legislation also pending
- Software bill of materials, supply chain regulations and more coming.

pillsbury

Increasing Enforcement

- SEC Enforcement Actions:
  - For alleged misrepresentations to investors about a security breach (*e.g.* Pearson plc, $1M fine, August 2021)
  - Failure to adopt cybersecurity measures to protect confidential customer information and comply with policies (*e.g.* eight Cetera broker/advisor firms, $750k fine, August 2021)
- DOJ Civil Cyber-Fraud Initiative (October 2021)
  - Fines for knowingly providing deficient cybersecurity products or services under the False Claims Act

pillsbury

Incorporating Cybersecurity Standards Into Contracts

pillsbury

When Should Cyber Terms be a Priority?

- ***Most all of the time***…regardless of the type of services or technology
- Critical element where a company's systems and/or data are involved
- Contracting Shortfalls
  - Many agreements tend to be more focused on contract terms for incident response rather than prevention
  - Attention is needed on a holistic set of contract terms for prevention and risk mitigation in third party services and technology contracts

pillsbury

Incorporating Cyber into Contract Lifecycle

- Due Diligence
  - Screening and Documenting Vendor Practices
  - Benchmarking against Peers
  - Evaluate Vendor Program and Policies
- Contracting / Onboarding
  - Third-party Training
  - Attestation
  - Contract-based Requirements including Adherence to Company Policies and Standards
- Relationship Status Quo
  - On-going Monitoring and Benchmarking
  - Periodic Risk Assessments (annual)
  - Receipt and Review of Third-Party Audits
- Incident
  - Notice
  - Remediation
  - Audit
- Renewal of Contract
  - Re-assessment
  - Refresh Contract Terms and Requirements
- End of Relationship
  - Return of Data / Removing Access
  - Linkage to Record Retention Requirements
  - Final Attestations

pillsbury

Key Cyber-related Contract Terms

- Confidentiality and Data Protection
- Background Checks and Restricted Personnel
- Disaster Recovery and Business Continuity
- Compliance with Law
- Audit and Incident Reporting
- Cyber Insurance
- Cyber Indemnities
- Limits of Liability
- Security Schedule / Addendum

pillsbury

Best Practices vs. Market-Driven Realities

- Services and technology agreements are not static!
  - Keep agreements current as technologies change and practices evolve
  - Use renewals as a chance to revisit cybersecurity terms
- Use built in contractual mechanisms to “check-up” on your Suppliers’ adherence to cybersecurity terms and practices
  - Audit
  - Governance Provisions
  - Reporting
  - Business Continuity and Disaster Recovery Testing
- Establish standard positions on cyber terms including a Security Addendum
- Challenges – Market-driven realities
  - Cloud/SaaS: Established providers have institutional terms
  - Managed Services/Outsourcing: Greater flexibility but risk tolerance is diminishing

pillsbury

Cyber Insurance Trends

pillsbury

Coverage for Cyber Risks

- Trend towards hardening of the cyber insurance market.
- Impacts include higher premiums and more risk area carve-outs.
- Obtaining dedicated cyber insurance can be a particular challenge if an organization is small/medium sized, does not have existing cyber coverage, handles significant amounts of personal information and/or is in a higher-targeted industry.
- Some companies covering cyber risks through captives.

pillsbury

Insurance for Cyber Risks

- Some courts have found coverage for cyber liability in traditional policies, but that is not to be counted on or obtained without a fight.
- *See, e.g.*, *Landry's Inc. v. The Insurance Co. of the State of PA*, 4 F.4th 366, 367 (5th Cir. Jul. 21, 2021) (requiring insurer to defend suit by payment processing vendor for alleged failure to maintain cybersecurity resulting in stolen consumer data under personal and advertising coverage for publication of material violating a person's right of privacy)

pillsbury

Coverage for Cyber Risks

- Trend away from liberal underwriting and back to more in-depth and complex application questions
- Careful responses needed to broad or technical questions
- Rescission of cyber coverage enforced based on responses to application questions such as:
  - Do you check for security patches to your systems at least weekly and implement them within 30 days?
  - Do you replace factory default settings to ensure your information security systems are securely configured?
  - Do you control and track all changes to your network to ensure it remains secure?

Columbia Casualty Co. v. Cottage Health Systems, No. 2:15-cv-03432 (C.D. Cal. May 31, 2016)

pillsbury

Cyber Policy Terms

	Coverage	Description
1st Party Costs	Business Income/Extra Expense	Reimbursement for loss of income and/or extra expense resulting from an interruption of computer systems due to a network security breach.
	Data Asset Protection	Recovery of costs and expenses to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a computer attack
	Cyber Extortion	The costs of consultants and extortion monies for threats related to interrupting systems and releasing private information
	Breach Response	The costs of complying with the various breach notification laws and regulations, legal expenses, call centers, monitoring, forensic services, and public relations
3rd Party Costs	Privacy Liability	Defense and liability for the failure to prevent unauthorized access, disclosure or collection of confidential information.
	Network Security Liability	Defense and liability for failure of system security to prevent or mitigate a cyber attack.
	Privacy Regulatory Defense	Costs to defend an action or investigation by regulator due to a privacy breach, including indemnification for any fines or penalties assessed
	Media Liability	Defense and liability for online libel, slander, misappropriation of name or likeness, plagiarism, copyright infringement, disparagement, negligence in content

pillsbury

Cyber Policy Terms - Cloud Computing

- Most cyber insurance policies now include coverage for interruption of cloud computing systems operated for insureds.

Shared Computer System means a Computer System, other than an Insured's Computer System, operated for the benefit of an **Insured** by a third party under written contract with an **Insured**, including data hosting, cloud services or computing, co-location, data back-up, data storage, data processing, platforms, software, and infrastructure-as-a-service.

pillsbury

Cyber Policy Terms - Cloud Computing

8. **Infrastructure Outage**

alleging, based upon, arising out of, or attributable to any electrical or mechanical failure or interruption, electrical disturbance, surge, spike, brownout, blackout, or outages to electricity, gas, water, Internet access service provided by the Internet service provider that hosts an **Insured's** website, telecommunications, or other infrastructure. However, this exclusion shall not apply to failures, interruptions, disturbances, or outages of telephone, cable or telecommunications systems, networks, or infrastructure:

a. under an **Insured's** operational control which are a result of a **Network Security Failure**;

b. solely with respect to Insuring Agreement B, which are the result of a **Cyber Incident** impacting a **Shared Computer System**; or

c. solely with respect to Insuring Agreement E, which are the result of a **Cyber Incident**.

pillsbury

Cyber Policy Terms - Cloud Computing

- Most cyber policies also waive subrogation if an insured has previously agreed in writing to waive subrogation.
- Cyber insurance requirements can therefore provide significant protection to cloud computing companies.
- However, they should be realistic for the market.

pillsbury

Cyber Policy Terms

- Key cyber coverage issues for technology services companies include:
  - Definition of technology services - typically defined to include developing/operating computer systems and software
  - Covered business interruption - can be narrowed to not include internal response
  - Definition of privileged information - often focused on consumers and not B2B
- Consider an up-front policy review by coverage counsel

pillsbury

Questions?

Cloud Communications Alliance

pillsbury

Upcoming Virtual Meetings

- March 10 – In Person Event – London –CCA Thought Leadership Breakfast

You can find a complete list of all upcoming meetings at www.cloudcommunications.com

Cloud Communications Alliance

pillsbury

Thank you for joining us today.

Cloud Communications Alliance

pillsbury