Voice Communications Compliance and Security in the Era of Cloud Computing

Table of Contents:

Background

The cloud has changed nearly every aspect of modern computing. While many of the benefits for its adopters are significant - lower cost, faster and more elastic deployments, and increased speed to market - new concerns about compliance, security, and business continuity have been raised. Appropriately understanding compliance considerations, risk posture, and cloud security mechanisms is a perpetually-evolving subdomain working on multiple fronts - technology, policy, and law - towards the goals of protecting data, applications, and infrastructure of cloud computing environments.

The world of telecommunications, while based on models that are often significantly older than some of the paradigms in web technologies, has undergone many of the same transformations. Built on the business model and technology advancements of web technology, the telecommunications marketplace has undergone a massive trend to cloud-based telephony and Voice over Internet Protocol (VoIP), in a number of forms. VoIP began as an unregulated, fluid technology that has quickly turned into a replacement service for not only the Private Branch Exchange (PBX) and landline phone systems, but also the traditional Incumbent Local Exchange Carrier (ILEC) and Competitive Local Exchange Carrier (CLEC) service providers.

The growing maturity of public cloud-based telephony demands an increase in regulation, compliance, and certification standards. Previously, federal regulatory agencies maintained a "light-touch" approach to VoIP regulation but as cloud-based telephony emerged as a popular alternative to wireline services, federal and industry regulations have augmented policies to encompass VoIP in conjunction with PBX [1].

As state and federal standards solidify, transparency in VoIP service providers' ability to meet compliance and regulatory standards is required. As the space has matured, and regulations have been clarified, many cloud-based providers offer internal security frameworks developed in conjunction with and aiming toward alignment with federal and industry regulatory standards.

This summary serves to provide a comprehensive guide to the regulatory requirements of interconnected VoIP telephony for service providers to ensure compliance and conformity with best practices, FluentStream's particular role in partnering with our customers, industry, and regulatory partners in developing practical and efficacious standards, and providing an outline of what customers need to apply safety and compliance standards to VoIP technology solutions.

I. Industry and Government Standards for Compliance and Security

There are a number of standards bodies - both within industry and various governmental entities - that define, regulate, and police the security standards for the information and communications technology industry. These standards extend beyond general IT cybersecurity and encompass country, regional, and industry efforts to ensure the security and reliability of many services, including Voice over IP. All qualified Enterprise VoIP services providers should develop technology, services, and protocols that are in compliance with these standards.

Security and Freedom through Encryption (SAFE) Act

Under this legislation, any form of encryption is permitted for use, fostering the protection of classified information for all US citizens[8].

How FluentStream Helps: FluentStream uses the highest, military grade Advanced Encryption Standard (AES) encryption technology for all of our Internet-transit traffic. Our online identities are all validated by an external trusted root certificate authority that provides validation not only of our security but of our identity and the legitimacy of our business entity.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA compliance requires healthcare organizations to put mechanisms in place that control access to patient data. This act mandates industry-wide standards for the protection of health care, insurance, and billing information, and any other medical processes as they relate to personal health information (PHI) [2]. Compliance measures must be continuously verified throughout the communication lifecycle as policy adapts over time. This places responsibility on the service provider, business subcontractors, and customers.

How FluentStream Helps: FluentStream supports all efforts to comply with HIPAA In the event that our customers are covered entities, FluentStream will sign a Business Associate Agreement (BAA) with any HIPAA covered entity to ensure all HIPAA regulations are met. In our standard Terms of Service, we include an addendum indicating our responsibilities under HIPAA, including the commitment to the BAA. Under this contract we protect Personal Health Information (PHI) in accordance with HIPAA guidelines by encrypting all transmissions using 256 bit Advanced Encryption System (AES) cipher technology over TLS/SSL between all server-nodes and audit logging of all system events. In addition to encryption, FluentStream provides

audit logging of the events in the system to ensure medical practices, doctor's offices, hospitals and other healthcare entities can have assurance all patient care information, including electronic patient records, across all platforms FluentStream supports - voice, text, fax, chat - are transmitted and stored with the industry best of security and privacy standards.

The Health Information Technology for Economic and Clinical Health Act (HITECH)

Originally enacted to promote the adoption and meaningful use of health information technology, HITECH was passed to strengthen the enforcement of HIPAA at the civil and criminal levels and encourage healthcare providers to adopt private and secure information technology [3].

How FluentStream Helps: With increased enforcement actions under HITECH, FluentStream helps organizations ensure compliance for the data security of including electronic health records (EHRs) and private and secure electronic health information exchange. [7] Providing attestation, records of systems access, and immutable logs are important to compliance in this framework.

The Payment Card Industry Data Security Standard (PCI-DSS)

This policy sets the global technical and operational standards for all financial and cardholder data shared through applications or devices [4].

How FluentStream Helps: All internet-traffic, including traffic holding financial information, is encrypted using military-grade technologies. Additionally, the ability to audit and monitor all account activity provides transparency into company-wide transactions that involve PII and credit card information. Additionally, FluentStream does not locally hold information within the scope of PCI-DSS inside our systems. An outside, certified PCI-DSS 3.1 certified payment provider for storage of PII and other sensitive information such as credit cards.

Gramm-Leach-Bliley Act (GLBA)

GLBA sets the standards for all financial institutions that manage private information of individuals, including the regulation of the management, disclosure, and protection of customer information while providing transparency into information-sharing practices [5].

How FluentStream Helps: From insurance sales and underwriting to tax planning and preparation providers and investment advisory services, or any company that handle customers' nonpublic personal information (NPI) - credit card numbers, bank account information, social security numbers, the FluentStream Encryption protocols adhere to all GLBA compliance measures. We treat all our customer's information as confidential.

Customer Proprietary Network Information (CPNI)

CPNI is the information a service provider collects from subscribers in order to provide the appropriate services and billing. This information includes inbound/outbound call records, features utilized such as voicemail or call forwarding, phone numbers, and more. Federal standards restrict the disclosure and accessibility of this information to authorized personnel under the following circumstances: with customer approval, by law enforcement, and in the provision of customer services from which the information is derived [6].

How FluentStream Helps: FluentStream, along with all other VoIP service providers, are mandated to file annual reports that certify compliance with commission rules protecting all CPNI. In addition, if there are account changes, data security breaches, or suspicious behavior customers will be notified immediately. This includes password changes, the utilization of a forgotten password retrieval mechanism, account information updates, and more. VoIP services providers are not permitted to use, augment, or share CPNI without the consent of the customer [12].

E-911

In the United States and Canada, all customer-made emergency services 911 calls and Automatic Number Identification (ANI) must be transmitted to the customer's designated Public Safety Answering Point (PSAP). Customers must provide their service provider with their registered location information at the start of service [1].

How FluentStream Helps: For our United States and Canada customers, E-911 associates your device with a physical location to guarantee that emergency calls are directed to the appropriate Public Safety Access Point and routed to the necessary emergency services. By ensuring your numbers and locations are registered to the appropriate databases, the Public Safety Access Point will have the appropriate information to dispatch emergency services, should they be required.

II. Information Privacy and Data Security in Hosted Cloud-Based Telephony

Due to the distributed nature of cloud-based technology and the shared responsibility of data security, safety concerns are a top priority for those interested in adopting hosted cloud technology. The actual and perceived risks for data in the cloud occur in three primary environments: internal, external, and physical. Internal security encompasses reliability of service, data availability, in-house data security, and data destruction. External risk includes hacking, eavesdropping, and failure to segregate private information. Finally, physical security includes data center infrastructure and storage of information.

Redundant Tier IV datacenters with provider diversity ensure **continuity of service** and geographic isolation of independent computing elements **prevent systemic failure**.

Internal Security

Availability

The primary concerns of a customer using cloud-based technology are often the accessibility of data and reliability of service. A key metric to note when auditing VoIP service providers is the five nines, meaning 99.999% service uptime. Adherence to this standard is designed to prove the provider protects access to data and services, no matter the circumstance, and even through many forms of catastrophic failure.

FluentStream uses a number of failover tools that ensure service never goes out, regardless of natural disasters or unforeseen outage occurrences. Should a failover occur, redundant Tier IV datacenters with provider diversity ensure continuity of service and geographic isolation of independent computing elements prevent systemic failure. Additionally, FluentSteam's flexible failover of voice communications include automatic call rerouting to additional SIP destinations, as noted in the Service Level Agreement, including access to Toll Free SMS/800 database routing.

FluentStream services offer an innate suite of

security protocols and architecture plans based on industry best practices. Service providers allocate special attention to security throughout the lifecycle of products and services; implemented in the design, development, and application of technology.

In-house data confidentiality and classification standards

Using the FluentCloud Web Portal, administrators can monitor and manage user access granular permission levels via the Role Management application. With the ability to classify different roles on the front-end system and in Application Programming Interface (APIs), administrators can implement and enforce security protocols to protect data confidentiality, based on company policy or classification standards. Permissions can be assigned to predetermined roles or individual users, via the discretion of the administrator.

Track, monitor, and audit data accessibility

Consumers are advised to select software and infrastructure that allows a defined hierarchy of information privileges to prevent internal information breaches. By providing definitive roles tied to unique permissions, you can completely control the access and manipulation of front-end information. This includes the ability to augment user permission levels, phone extension controls, management of login credentials, and the ability to block inbound/outbound numbers on a user, group, or universal level.

Data Destruction

VoIP data management services include: data acquisition, sustainability, deployment, and destruction processes. This allows clients to comply with all internal corporate responsibility objectives while maintaining federal security standards.

Customers have the ability to destroy both "in motion" and "at rest" data through the tools provided by the FluentStream management tools. Except where required by law, FluentStream uses best-in-class algorithms and full deep data scrubbing of deleted data in our systems, to ensure that data is not preserved when it has been asked to be deleted. We can, when requested, deep delete files stored on our systems to ensure recoverability, even by sophisticated forensic tools, is difficult to impossible.

External Security

Firewalls

Firewalls are designed to prohibit unauthorized access to private network information via proxy servers, packet filtering, Intrusion Detection Systems (IDS), and more [9]. FluentStream technology, among others, allows for packet filtering that controls information transmission based on the source or destination IP as well as the Differentiated Services Control Protocol (DSCP). This allows network and security administrators to apply policies that support a defense in depth approach and to provide attribution for voice ingress and egress paths in the network environment.

Encryption

The value, integrity, and confidentiality of customer data is of primary concern. Media communications and voice over IP can be encrypted via Secure Real-Time Transport Protocol (SRTP) which adds confidentiality and authentication protocol to the RTP payload. This is utilized in conjunction with packet header compression so that quality of service is never compromised when bandwidth is scarce. It also allows for replay protection which ensures multimedia data cannot be manipulated [10].

Segregation of data in the cloud

The transmission of all customer and provider data is continually monitored for inconsistencies or failures. This ensures data is securely segregated from other customer environments and inaccessible to Cloud Security Provider (CSP) personnel. Supporting Session Initiation Protocol (SIP), Transport Layer Security (TLS), and ZRTP and SRTP signaling for call and media transmission, your information can be secured throughout the entire communication lifecycle [10].

FluentStream's comprehensive data-security technologies include: intrusion-detection systems, fraud analytics, system hardening, vulnerability scans, and system logs. FluentStream provides authentication platforms and identify verification protocols that ensure a user can never access data outside of their own network. Finally, our geographically-dispersed, redundant data centers ensure 99.99% uptime and are systematically monitored and upgraded to ensure confidence in service longevity. Your data is available to you, and only you, 24x7x365.

Physical Security

Data center infrastructure and security

Company data stores are accessible solely by FluentStream employees, contractors, and/or agents who are on a need-to-know basis and bound by a confidentiality non-disclosure agreement with FluentStream Technologies. Physical servers are protected in biometrically authenticated environments and monitored continuously. All electronic and physical access is logged.

Storage of customer data

When data is "at rest" it is encrypted and stored within a cloud service to provide data asset security and compliance with security standards, such as HIPAA and PCI-DSS. All FluentStream customer information is stored on a computer system located in a controlled facility with limited, secured access. Where possible, data at rest is encrypted at the volume level and within the operating system's filesystem.

III. Joint Governance of Safety, Risk, and Compliance

Information security is a shared responsibility between a service provider and subscriber, contingent on provider diligence and the subscriber's willingness to intelligently participate in the partnership. There are a number of policies, processes, and technology that are key to optimizing security and compliance that should be considered when considering service providers.

Written policy documentation between the provider and subscriber which outline measurable objectives, designation of responsibilities, and consequences for violation is the key framework to ensuring information security for both parties. Voice over IP service providers have a unique set of responsibilities that include network controls, data security, and safety infrastructure. Subscribers' responsibilities include end user policy management and dissemination, password integrity, limiting internal access to information, and the mindful use of technology. These actions when followed accordingly work in concert to provide confidence in security, privacy, and compliance.

Service Provider Responsibility

The primary function of a service provider is to provide and to help integrate a suite of redundant network controls including firewall protection, encryption, access controls, and maintenance procedures. By offering redundant and complementary protective measures providers produce a comprehensive security plan for combatting external unauthorized attacks on private or personally identifiable information.

Maintaining information privacy in cloud-based infrastructure is done through virtual local area networks (VLAN) which provide a scalable solution to network segmentation and management. Layer 2 VLAN segregation supports network separation into multiple subnets that use unique broadcast domains. This provides a means for segregating sensitive infrastructure and creating a collection of isolated networks within a single data center. This means solely the authorized users are able to "see" servers and associated devices. Furthermore, this provides defense against packet-sniffing and system attacks. [11]

"Written policy documentation between the **provider** and **subscriber** which outline measurable objectives, designation of responsibilities, and consequences for violation is the **key framework** to ensuring information security for both parties."

Service Subscriber Responsibility

The key responsibility of a subscriber is to intelligently utilize cloud-based technology and take a number of steps to facilitate cybersecurity and information privacy. This extends across multiple layers of use.

Subscribers can take a number of actions to solidify in-house information security. First, restrict administrator privileges to a few trusted members and utilize strong passwords and PINs, including a reliable mechanism to systematically update them over time. Additionally, administrators should attempt to avoid known voice phishing attacks and scams and block malicious numbers of unwanted inbound calls to restrict unwanted communications that can serve as an attack conduit.

IV. Strategy for the Future

As cloud computing and VoIP telephony continues to replace antiquated infrastructure and technologies, more industry and federal standards will adapt to encompass this technology. To ensure continued compliance and security, cloud-based technology will remain adaptable to changing policy, fostering continued trust and confidence in VoIP users.

There are a number of different protocols, technologies, and infrastructures in place to provide comprehensive security for data hosted in cloud-based systems. It is FluentStream Technologies' policy to maintain best in class support for these security and compliance efforts and to partner with customers in the designing and developing best-in-class service and support in the Voice over IP industry. Please contact FluentStream with questions about compliance efforts or for assistance in aligning your organization's needs for telephony compliance with solutions in the market.

References:

1. The Common Law Group, comp. “Interconnected VoIP Regulatory Compliance Manual.” The Common Law Group (n.d.): n. pag. The Common Law Group. 01 Aug. 2011. Web. 01 Apr. 2016.

2. “HIPAA.” What Is HIPAA. California Department of Health Care Services, n.d. Web. 19 Apr. 2016. <http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx>.

3. Office for Civil Rights. “HITECH Act Enforcement Interim Final Rule.” U.S. Department of Health & Human Services. N.p., 28 Oct. 2009. Web. 1 Apr. 2016. <http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html>.

4. Security Standards Council. “PCI Security.” PCI. N.p., n.d. Web. 1 Apr. 2016. <https://www.pcisecuritystandards.org/pci_security/>.

5. Rouse, Margaret. “What Is Gramm-Leach-Bliley Act (GLBA)? - Definition from WhatIs.com.” SearchCIO. WhatIs.com, n.d. Web. 19 Apr. 2016. <http://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act>.

6. Federal Communications Commission. “Protecting Your Telephone Calling Records.” Federal Communications Commission. N.p., 17 May 2011. Web. 19 Apr. 2016. <https://www.fcc.gov/consumers/guides/protecting-your-telephone-calling-records>.

7. HealthIT.gov. Health IT Rules and Regulations. N.p., n.d. Web. 19 Apr. 2016. <https://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations>.

8. Watkins, Michael, and Kevin Wallace. “Chapter 1: Understanding Network Security Principles.” Network World. Network World, 23 Apr. 2009. Web. 19 Apr. 2016. <http://www.networkworld.com/article/2268110/lan-wan/chapter-1--understanding-network-security-principles.html?page=2>.

9.“Indiana University Indiana University Indiana University.” What Is a Firewall? Indiana University, 18 Nov. 2013. Web. 19 Apr. 2016. <https://kb.iu.edu/d/aoru>.

10. Ghaffar, Ahmar. “Internet Telephony Feature Article: How Secure Is VoIP?” Internet Telephony Feature Article: How Secure Is VoIP? N.p., n.d. Web. 19 Apr. 2016. <http://www.tmcnet.com/voip/1104/FeatureSecurity.htm>.

11. Olzak, Tom. “VLAN Network Segmentation and Security- Chapter 5 - InfoSec Resources.” InfoSec Resources VLAN Network Segmentation and Security Chapter 5 Comments. N.p., 18 Apr. 2012. Web. 19 Apr. 2016. <http://resources.infosecinstitute.com/vlan-network-chapter-5/>.

12. Federal Communications Commission. “PUBLIC NOTICE.” FCC Enforcement Advisory 35.2 (1980): 50. FCC. 9 Feb. 2015. Web. 1 Apr. 2016. <www.fcc.gov>.