TIERED COMMUNICATION SERVICES

MANAGEMENT | INSTALLATION | PROCUREMENT

Where Technology and Security Meet in Hotels

Jonathan Adam, CTO

Jonathan Adam

CTO | Co-Founder, Tiered Communication Services, Inc.

With 17 years of hotel experience and as a founding member and CTO of Tiered Communication Services, Inc., Jonathan focusses on pairing high end development projects with extremely secure advanced technology systems for an unsurpassed guest user experience, driving amazing rates of return to owners. Jonathan holds multiple technology patents, and has also co-founded the ySuite Incubator in Austin and PracTECHal Solutions headquartered in Las Vegas. The ySuite team owns and operates multiple hotels in the Austin area, and utilizing the TCS technology infrastructure, they generate significant amounts of high margin add-on revenue through new hospitality revenue channels.

How Technology Helps Hotels Succeed

Data and Privacy Security in a Covid19 World

- What to watch for with Privacy and Security Data
- How to manage this data the right way
- How Brands help
- Being secure in the room with BYOS
- How secure is your guest network?
- How it all works together

Privacy and Data Security in the Front Office

There is a big difference between securing your data and SECURING your data. Security is more than things like encryption. How is your data secured throughout things like physical access control, employee turnover, third party service workers, and more? Through new temperature readings of guests, are you using a HIPAA compliant service to store this data? Please don’t take on HIPAA compliance yourselves.

Managing Data the Right Way

- Security includes encryption, data access control, physical access control, transmission storage to drive or the cloud, and retention during employee turnover.
- Who has read access? Who has write access? Who has full access to which data? GM and higher should be only people with full access. Input users like the front desk should be able to input only. Supervisory level and higher should have read access to make decisions on data.
- What is your software update policy? Are you maintaining updates on all operating systems, firmwares on hardware (printers, storage drives, etc) and antivirus.
- You should have a minimum of three backups of all of your data, one on site, and two off site in different locations, off site moved at least weekly, and on site backed up to a compliant cloud infrastructure as well.
- Are you following HIPAA compliance on any health related guest data? You HAVE to, even though you are not a medical office, even just a temperature reading is health data.

How Brands Help

As much as some of us see some of the Brands' standards as a pain in the rear, in the case of data protection they have been very proactive. Sourcing approved vendors from their lists ensures you are investing in service providers that have been vetted to provide the right data management processes. This is especially important in a current and post Covid19 economy. Travel will change, and requirements from both a guest and operator perspective will be different, the brands will create standards around this to help protect the operation and the guests. IHG for example has "sold-insert cough here" us all new signage to help us keep guests better informed, and they have chosen a single HIPAA data service provider.

Bring Your Own Service (BYOS)

The new guest trend and the problems it presents

More brands are moving to guests bringing their streaming services with them as the entertainment heart of the room. This is in high demand from the guests, but presents a security nightmare for operators, especially those not following brand standards (or independents without brand guidance). There are several services out there offering the ability for guest devices to cast to room devices, and it's great, however the most important thing to ask a service provider is what is their erasure procedure? Do they interface with the PMS? If not, when are they removing this guest data? What data are they mining from the system for marketing purposes of their own? Can you opt out of their marketing mining? What data do they store on your premises, and what are they doing to protect that data on your network? Even if you are using a third party provider to provide these valuable services to your guests, knowing the answers to these questions are imperative.

How Secure Is Your Guest Network?

Guest network security should be the most important thing on your mind when it comes to data security in your operation. Ask your provider (not your ISP…)

- Are we using Client Isolation?
- Are we using cookies for authentication? If so, are we telling the guests? If not, why aren't we?
- How are we cataloging access data? If a brand central system like IHG's Meraki integration, are we fully brand compliant? (Hint, even though the cost is highly marked up, IHG is actually managing this for you through brand approved vendors)
- If you're using on premise routing (most are), what security layers are being used to isolate guest rooms from each other? What are your whitelisting policies for devices like gaming consoles?
- I know it is a huge Capex cost, but please plan on upgrading your network infrastructure at least every four years. This will help plug security gaps, and also provide network performance your guests want, leading to better OSAT scores. Please don't use off the shelf equipment. None of this gear has functionality needed at an enterprise level, and is not nearly secure enough for your operation.

How It All Works Together

Most of your operations will have two different ISP circuits and two different routed networks. This is great until integration is needed for something from the guest network to the PMS, which ones a “hole” that must be properly secured. Brands have considered and solved this, for independent owners, find a service provider to help you maintain the security integrity of your PMS and guest network.

Data storage compliance is an easy thing to do, as long as you have a plan, a process, and knowledgable help from a service provider. This rings true especially for HIPAA compliance if you are keeping any record related to health of your guests.

Your networks will work seamlessly through APIs to help secure all of your data if you have them setup correctly. Again though, you have to have a plan, process, and procedures for physical and access control of your data. Don’t store your backup drives at the front desk for example. They should be in a room with logged secure access. Have a plan to manage data so that employee turnover can be controlled and access terminated to the data. Things like Google Drive have controls not allowing storage in any folder other than Google Drive for example, so if an employee leaves, access can be removed immediately to the data.

Embrace the cost of a managed IT solutions provider to help manage this and to make sure the things you haven’t thought about are planned for. Applying common sense to this highly technical area can help to remove some of the intimidation factor.