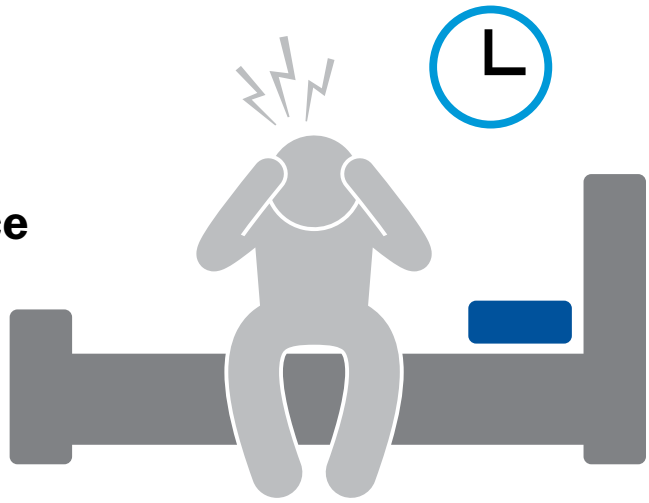
WHAT KEEPS *YOU* UP AT NIGHT?

"Contact centers face a growing array of compliance requirements, rules and regulations for handling sensitive data."

Contact Center Pipeline

WHAT KEEPS *YOU* UP AT NIGHT?

Tackle fraud prevention, compliance and security to rest easy.



BY Lori Bocklund, Strategic Contact

"Bad guys" seem to be lurking around every corner these days. They steal customer information and break into networks and systems. At the same time, contact centers face a growing array of compliance requirements, rules and regulations for handling sensitive data. It's no surprise that contact center professionals in both operations and IT have increased risk of insomnia worrying about the things that could go wrong for their centers and how to keep things going right.

Fortunately, there are a variety of technology tools that can help you reduce risks and manage staff to meet the demands in all areas. While there might not be one single strategy for a good night's sleep, we'll provide some key things to factor into your thinking on three important fronts: fraud prevention, compliance and security. As the saying goes, "Hope is not a strategy!"

FIGURE 1: Acronym Bingo

THESE ARE REALLY ACRONYMS WE PULLED FROM RFPS AND PROPOSALS!

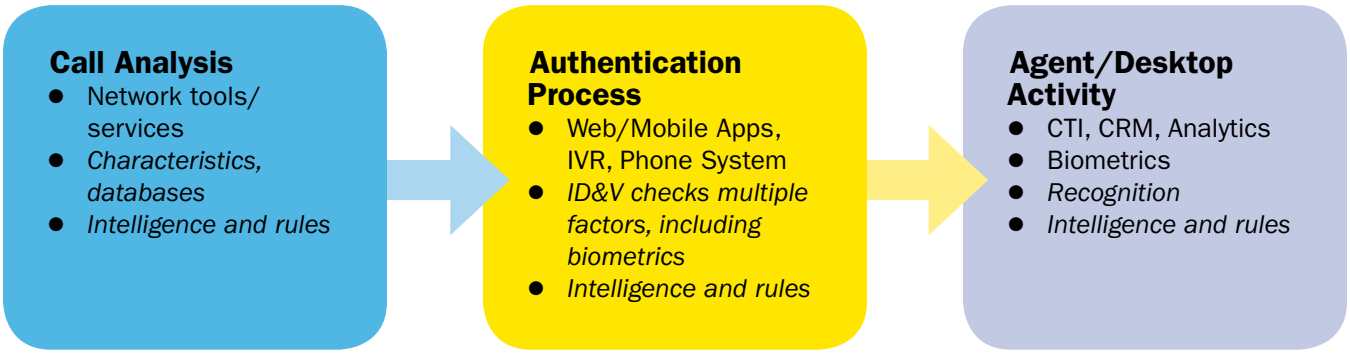
B	I	N	G	O
SSAE16	IDS/IPS	SIEM	HIPAA	CIS
AES	SRTP	FedRAMP	SHA-512	SSL/TLS
DDOS	PCI DSS	NOTHING IS FREE SPACE!	IPSEC	DOS
ISO 9001	PBKDF2	SCAP	CSP	SBC
ISAE	PCI	SOC (1/2/3)	HTTPS	SAS70

Beyond Hope… Collaborative Action

As you sidle up to the planning table, you'll face a land of protocols, standards, certifications and audits. FIGURE 1 shows relevant acronyms we pulled from client requirements documents and vendor proposals. Don't feel alone exclaiming, "Yikes!" It can feel like gibberish only experts can understand. You won't need to learn to speak the language, but you'll use it to set guideposts of what to look for from your vendors and as mechanisms for IT to deliver peace of mind.

All these acronyms highlight the need to turn to specialists. In this era when everyone wants to move fast (think cloud solutions!), you need to take your time and involve the right players in *deep* discussions. Planning and action mean you need to work with your vendors under a "trust but verify" approach. Involve the right subject-matter experts in your IT department (including risk, security, etc.) and view them as key partners in the process.

FIGURE 2: Fraud Prevention in the Call Flow



Frog Prevention? No, Fraud Prevention

Discover Card's advertisements about "Frog Protection" got us all laughing about identity theft, but it's certainly no joke. Whether you are a financial institution protecting people's money and identities or are defending against fraudulent parties trying to pretend they are your customers, you have to approach authentication with caution. At the same time, you don't want the identification and verification process to be overly burdensome on your customers or your staff.

The first goal is to keep low-risk scenarios simple, quick and easy so you can spend time on the potentially problematic contacts. (See "It's [Time for] a New Day in Authentication and Routing," May 2016). Don't just rely on the traditional method of **knowledge-based** authentication loaded with time-consuming and potentially irritating—and not necessarily infallible—questions. Use multifactor authentication, applied intelligently using (lots of) data—both internal and external. Use **possession** (e.g., mobile device) and **inherence** through things like biometrics (e.g., thumbprint, voiceprint, facial recognition, retina scans). Add layers for self-service that protect access to information while also avoiding unnecessary diversions that compromise self-service success rates and associated costs and the customer experience.

Cross-channel fraud prevention ties in initial activity for someone logged into the web, mobile app or IVR. An already authenticated customer moves seamlessly and both the customer and the agent know everything is A-OK. A suspect customer from failed logins flags on the source of the call (e.g., spoofed number), or evidence of repeated attempts to access the IVR can trigger workflows customized to the risk level. Intelligent routing sends the tricky ones to specially trained agents who then rely on technology to guide them through the proper steps. These scenarios use network information, account access history, length of IVR sessions and more to build smarts into the process.

FIGURE 2 outlines a variety of technologies that can play a role in helping to reduce your risks and smooth the process for all involved. The common themes of data, intelligence and rules stand out. Network tools or services work on the front end to evaluate characteristics of contacts and their origin, leveraging databases with defined business rules or even artificial intelligence. Predictive analytics define the probability of fraud, which can then be used in the smart routing and agent guidance described. The various self-service tools can have rules on account access, based on changes, number of failed attempts and multifactor authentication that is not just about what you know (logins, passwords) but what you have (e.g., mobile phone to receive a code via text) or who you are through biometrics.

> Recording and storage are hot buttons for PCI that the center must consider.

Good old CTI can pop screens with flags or codes about authentication success or warnings, and CRM scripts can guide an agent through the right steps. Biometrics can kick in during the conversation as well, again tying in to provide more guidance at the desktop.

Analytics after the fact can help to bolster databases of risk factors, and biometrics success can be further boosted by passive enrollment from customer conversations. Alerting and notification tied to analysis of activity can inform customers or risk teams.

Becoming Compliant

Compliance has been a priority for many companies for many years because of requirements from PCI and HIPAA, among others. Some of those other acronyms we saw come from vertical-specific compliance requirements (e.g., banking), some are tied to data centers, while others come from "accounting rules" that also engulf information control. In spite of the high importance, centers have not always been fully compliant. With the increasing pressure and risk, it's time to get it right, because close doesn't count!

Compliance is an area where experts are required to dive into all aspects, many of which are not in the center's control. IT and vendors play a role in ensuring proper access control and management (e.g., logins and their use, password rules and triggers for change). Recording and storage are hot buttons for PCI that the center must consider. Recognize the products themselves may not be "compliant"—rather, they enable you to be

Don't Forget Certification, Testing and Audits

Certification, testing and audits should be part of your "good night's sleep" strategy and can play a key role in ensuring success on any of these three elements.

FRAUD PREVENTION:
Employ services that try to penetrate your network and systems to compromise sensitive account data, "phish" for information and access accounts. They won't make changes to accounts, of course, but they will let you know if someone could!

COMPLIANCE:
Use third parties to implement and validate compliance. Include relevant certifications specific to your vertical market or functions, the regulations that apply to your business, or that apply to the technology delivered. And hold your vendors similarly accountable.

SECURITY:
Certifications are common for many elements here, so identify which ones apply and to whom, and make sure they are in place and stay up to date.

Testing may include a variety of elements, such as vulnerability assessment, penetration testing, risk assessment and recovery. Develop these as part of your overall plans and ensure they are done on a routine schedule that continues to assure that your company and customers are protected.

compliant. Define requirement and have vendors show how they help you achieve them.

Here are the biggest hot buttons contact centers need to consider regarding compliance:

- **LOGINS:** Centers have many systems to log in and out of, often with fast timeouts impacting handle times and potentially customer and agent satisfaction. Single sign-on solutions can address these issues and ensure compliance across a variety of systems. They can be standalone or incorporated into things like Unified Agent Desktop (UAD) or CRM applications.
- **RECORDING:** Centers need to block recording of key information such as the three digits on the back of the credit card. Vendors offer a variety of options. Don't fall for the manual ones that rely on an agent to turn recording on and off at their desktop—both because it won't pass an audit and it creates risk. Look for integrations that are based on where the cursor is on screen, within an application or browser. Another option is to move the capture of sensitive information to an IVR, masking the information from agents. And don't forget to look at controls over who can access the recordings, how they are managed, the networks they travel on, etc.
- **STORAGE:** Storage policies must address retention and disposal. A full policy considers backups as well as recovery of data. For too long, many centers have put off developing full business continuity/disaster recovery plans. A push for compliance creates another reason to prioritize it!
- **ENCRYPTION:** Encryption has a role in recording and storage, for data "at rest" and "in transit." It may apply to the interactions themselves (voice conversations as well as other channels—e.g., emails, chat sessions, text messages) and to data about those interactions. Many different protocols have encryption built in—e.g., AES, SRTP, IPSEC, SSL/TLS, etc. (SEE FIGURE 1). Another hot button is management of encryption keys—an area your IT experts and vendors should explore together.
- **SECURITY:** This one, while it can be part of compliance, is worthy of a section of its own, so let's go there next.

Security on Many Fronts

Security is a rather broad term. Let's look at some specific things about security—all of which involve your IT department and associated specialties, and can be particularly important for cloud solutions. High reliance on the vendor and their partners for security demands that you ask LOTS of questions when evaluating a cloud provider. Don't move fast and trust without verifying!

The first aspect to address is access to physical spaces: Who has access to what? How is that access managed and tracked? The best scenarios employ biometrics, multifactor authentication and audited logs, backed up with strictly defined and enforced policies.

You must consider access to systems and networks, and all associated elements (e.g., servers, routers). Firewalls, DMZs and SBCs, along with secure data connections using HTTPS, SSL or other protocols—along with the all-important logins—can control access across networks and play a role in thwarting the bad guys.

Login access should be on a need-to-know basis, with role-based permissions. As noted in the discussion about compliance, careful management of logins and passwords, and access to recordings (interactions) and data about the interactions must all be considered. Part of security is also keeping track of who did what, so logging and event management tools must be considered as well (e.g., history of access, triggers for issues). Data storage and access are also part of security and are addressed above in the compliance section.

Make sure you address all aspects of data centers—whether your own, or those of cloud vendors, third parties or platform as a service providers (e.g., Amazon Web Services [AWS] or alternatives from others such as Google, Microsoft, IBM and Oracle, etc.). And don't forget the network. Explore certifications, audits and testing (SEE THE SIDEBAR) and make sure that your agreements and SLAs hold vendors accountable for ongoing security commitments.

Cloud vendors expect this kind of scrutiny. Some show their expertise and focus on this area on their website information, including many of the acronyms floating around FIGURE 1. They may have a "trust office" that shows

they have someone with assigned responsibilities and accountability. So don't be shy about getting them to tell you all about their policies, protocols and safeguards.

Rest Easy

Centers can play a big role in compromising or protecting the company and customers. Everyone is handling sensitive data and needs to protect it. Nobody wants to be on the front page of *The Wall Street Journal* (big issue!) or endure the ire of customers or senior execs (relatively small issue). You have a responsibility to put strategy and plans in place to minimize risks, and there are a variety of technologies to help. Take the time to plan, carefully select solutions, and work collaboratively with IT experts and vendor partners to ensure that you can rest easy.

Lori Bocklund is Founder and President of Strategic Contact. (lori@strategiccontact.com)

CONNECT WITH PIPELINE

 @SusanHash • @CCPipeline

 youtube.com/ccPipeline

 linkd.in/17M5rKM

About Contact Center Pipeline

Contact Center Pipeline is a monthly instructional journal focused on driving business success through effective contact center direction and decisions. Each issue contains informative articles, case studies, best practices, research and coverage of trends that impact the customer experience. Our writers and contributors are well-known industry experts with a unique understanding of how to optimize resources and maximize the value the organization provides to its customers.

To learn more, visit: www.contactcenterpipeline.com

 Download complete issues, articles, white papers, and more at http://bit.ly/14bq01k

PIPELINE PUBLISHING GROUP, INC. PO Box 3467, Annapolis, MD 21403 • (443) 909-6951 • info@contactcenterpipeline.com