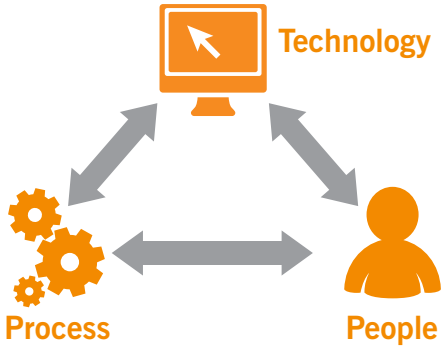
Ensuring Data Protection in the Cloud

inContact®

Different Types of Personally Identifiable Information (PII)

A. Credit card number
B. Social security number (SSN)
C. Passport number
D. Driver's license number
E. Taxpayer identification number
F. Account number
G. Bank account routing number
H. Account pin number
I. Password
J. User ID

Holistic Data Protection Model



The contact center is the world's hub for personally identifiable information. From mobile service providers to pet insurance companies – and everything in between – we are constantly being asked for our social security number, credit card information, passwords, user names, pin codes, routing numbers and so on. As consumers, we want to be sure this sensitive data is protected from misuse – whether intentional or not.

Not only are we constantly providing personal information, there is now a proliferation of virtual contact centers—home-based agents, Software as a Service (SaaS), managed solutions and cloud computing. Today's consumer is left wondering exactly how safe his/her data is.

The good news is that the world of virtualization is actually making our data safer than it was just a few years ago. Cloud computing and cloud contact center service providers earn and keep customers through the virtualization of contact centers and the like, and the very nature of their business makes them hyper-aware of data protection and data privacy safeguards. Cloud contact centers must protect customer data or no organization would trust their customer-facing contact center (and all of the personally identifiable customer information that goes with it) to one of these providers.

Not all cloud providers offer the safeguards businesses need and there are various elements an organization must consider when selecting or re-evaluating the vendors for its contact center. And, they also need to consider how the organization manages policies and procedures with regard to data protection.

THE COMPREHENSIVE DATA PROTECTION APPROACH

The best approach to contact center data protection is with a comprehensive, holistic strategy that permeates both the contact center and its cloud provider. Working together helps ensure your contact center (and your customers' private data) is protected on all fronts.

This type of overarching program should consist of best-of-breed data security and privacy technologies (offered by the cloud/hosted provider), as well as carefully trained staff and best practice governing policies, procedures and training programs (employed by the contact center itself).

Let's take a deeper look into each of these areas:

A. TECHNOLOGY

Customer data (.WAV, JPEG, MPEG etc.) enters an organization from customer interactions but once it is in-house, it can "live" in many different areas, touching many different applications/systems. Starting with the data itself, let us classify it into two parts – call recording and CRM/payment system data, both of which likely contain some sort of sensitive customer data. It is imperative for a contact center to ensure both data types comply with PCI-DSS (Payment Card Industry Data Security Standard) or the organization may face serious consequences.

The call recording data can enter the contact center in two ways – through the company's quality monitoring (selective recording) system or through its 100 percent compliance recording system. This data can be captured as voice-only or voice-plus-screen and stored for days or even years, depending upon its intended purpose – agent training, dispute resolution, compliance, and so on. Some recording systems require the agent to trigger the muting of the interaction while credit card information is given, for example. This leaves the data protection solely up to the agent. Other recording systems circumvent manual triggering by automating the masking and muting of sensitive data. Either way, the approach helps minimize unauthorized exposure to sensitive data.

B. PEOPLE

In addition to the elements above, one of the most effective means of guarding sensitive customer data is to empower a select group of highly trained, skilled and trusted agents to handle all interactions which include the disclosure of sensitive information. These "super agents" can be taught to never put their phone on speaker or to not repeat the social security number, for example, back to the customer verbally. There are obviously many skills and procedures this group would learn to help ensure data protection.

Even with the best team in place, unintentional misuse and human error can occur. However, with this type of highly skilled team in place, the risk of sensitive data exposure is far less.

C. PROCESS

As important as the systems that collect, utilize and store this personally identifiable information are the rules and policies that govern its management. Each contact center must implement, train and enforce strict data protection protocols and mandates. These will vary from organization to organization, but a good example might be that no calls containing credit card information can be used for training purposes. Additionally, only a certain department within the contact center should handle such calls, and no trainees should be allowed to monitor these types of interactions.

The company's policies should also include certain systematic measures to restrict access to sensitive data, whether it is at the

Questions to Ask a Cloud Contact Center Provider

1 Are you a member of the Cloud Security Alliance?

2. Do you have a Chief Security Officer, and if so, what is his/her function?

3. Do you offer a 99.99% SLA guarantee?

4. Do you have documentation of your compliance (if applicable) with PCI, SOX, and CPNI?

5.Do you operate on fully redundant, fault tolerant, carrier-grade networks?

6.How seriously do you embrace the trust principles of security, availability, process integrity, confidentiality and privacy?

time of interaction capture or upon retrieval and playback. For instance, white noise and bleeping sounds can be used to block out sensitive audio, and screen masking can be used to cover up select portions of the agent's screen.

These types of data control measures serve as an additional layer of data protection. However, the best defense is not to store this information at all, unless mandated by regulation.

In March of 2011, the PCI Security Standards Council issued an information supplement called "Protecting Telephone-based Payment Card Data." In this industry directive, it laid out a specific "Decision Process for Voice Recordings" to "…show the process a merchant should follow when assessing the risk of their call center operations…"

With regard to process, there is another element to consider – the physical layout of the contact center. Similar to how data capture and access should be partitioned between authorized and unauthorized agents and departments, so should the cubicles/desks in which these individuals work. It is too easy to (intentionally or accidentally) overhear a neighbor's call, especially in the tightly packed environment in which many contact centers operate. This also holds true for business process outsourcers who serve multiple clients. They may or may not want to put members of the same account team next to each other.

The United States continues to evolve its policies and procedures in the area of the data protection/data privacy.

In February of 2012, the White House issued a proclamation to the country with regard to information privacy. In its "A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" document the Administration announced the formation of a Consumer Privacy Bill of Rights, or a 'blueprint for privacy in the information age.' The White House also states its intent to work with Congress to put the principles of this bill of rights into law.

COMPLIANCE

PCI Compliance, HIPAA and other consumer protection regulations also help protect sensitive customer data. Contact centers that fail to comply risk serious penalties. For example, a major PCI-DSS credit card infraction can cost an organization weeks of downtime, tens of thousands of dollars (or more) in penalties, loss of merchant capabilities, and tremendous data management scrutiny from a PCI-DSS certified forensics security examination team. Add to this the loss of customer trust, and the contact center would have real trouble on its hands.

LIt is imperative that an organization select a cloud contact center provider that has the capabilities necessary to help facilitate such compliance. A provider that could not mask or mute the sensitive portions of the customer call (upon recording the interaction), for example, would not provide the protection needed to maintain PCI Compliance.

HOME-BASED AGENTS

Home-based contact center agents pose a series of challenges as well in terms of data security and protection. These agents are typically entering sensitive customer data into their on-screen application and sending it over the Internet to the company's secure internal servers or directly into the cloud if using a virtual contact center platform. This opens the door to data encryption, data transfer and data storage concerns. As remote employees, these agents do not fall under the direct physical supervisor monitoring that in-office agents do. It is sometimes much easier for home-based agents to accidentally mishandle a social security number which can have serious implications to the customer's personal identity.

Is the Cloud Secure?

The right cloud services provider should have a robust security infrastructure, with these types of security measures in place:

- Security devices at edge of network
- Firewalls with deep packet inspection
- Applications sitting in protective DMZs
- Penetration tests
- Intrusion detection activities
- 24x365 application and network monitoring
- Log file monitoring
- Frequent internal and external vulnerability scans

For these reasons, it is critical that your cloud service provider offer secure data encryption and data transfer measures to ensure all customer data is protected. This includes data privacy considerations at the agent, system and infrastructure level. Do not be afraid to ask your provider for these details.

A TRUST OFFICE

"Trust is the sum of privacy and security," says Jim Cavalieri, SVP & Chief Trust Officer at salesforce.com.

What he is referring to is a tiered approach to data protection. The bottom layer is the "security" layer in which data integrity, availability and confidentiality are considered. The next layer is "privacy," where data security, transfer and use are considered. The top layer is "trust." This is where the notion of a Trust Office comes into play, in which a cloud service provider carefully balances the elements of data reliance and data confidence of the environment as transparently as possible. This openness would give its contact center clients the reassurance they need to put their customer care data in its hands.

Tasked with building a layer of transparency between the service provider's daily operations and the customer's working environment, a Trust Office is an actual department within the service provider's organization. This highly trained data protection team focuses solely on ensuring a high security, high performing and high reliability environment for customers.

The Trust Office can even form a "Trust Site" to openly demonstrate system transparency, sharing performance information, for example, about specific applications and platforms, or about service outages, etc.

WHERE DO YOU BEGIN?

This paper attempts to introduce the notion that personally identifiable information must be protected by organizations at all costs, in both on-premise and cloud contact center environments. The proliferation of cloud computing and cloud contact centers has taken the data privacy issue to yet another level but brings with it significantly increased security measures that actually better protect personally identifiable information.

A cloud contact center also allows the contact center itself to focus solely on just two parts of the data protection triangle – process and people. It can leave the third piece – technology – up to the service provider, who is likely better equipped to implement and enforce the necessary data security and data privacy measures.

Whether you choose to operate in a cloud or on-premise contact center environment, remember that data privacy cannot and should not be taken lightly. The success of your business and your customers' well-being very much depend on it. You must select a service provider that shares your same data protection philosophy and has engineered its business and its offerings accordingly.

To learn more about how to take advantage of a hosted contact center solution that is robust, flexible, and secure, contact us.

CALL 1-866-965-7227

E-MAIL customer.experience@inContact.com

VISIT www.inContact.com

Author:

Tamara Palmer

Internal Control Officer

inContact, Inc.

inContact

7730 S. Union Park Ave.
Suite 500
Salt Lake City, UT 84047

1-866-965-7227

www.inContact.com

inContact®