Debunking Security Concerns with Hosted Call Centers

TABLE OF CONTENTS

Executive Summary
The Changing Call Center Landscape
Identifying and Mitigating Security Risks
a. Data
b. Applications
c. Disaster Recovery and Business Continuity
d. Control and Compliance
Qualifying Hosted Call Center Providers
Conclusion
Security Is Serious Business with inContact

inContact®

This paper examines current economic and business trends impacting the contact center market. It provides guidance and recommendations for contact centers looking for an alternative to on-premises contact handling solutions.

EXECUTIVE SUMMARY

The call center landscape is experiencing significant changes, both in the business model itself and its underlying technology. The ability to access telephony and applications over the Internet has increased the flexibility of the call center workforce, introducing a new trend: the work-at-home agent. Driven by a greater need for both flexibility and cost control, hosted call center solutions, also known as hosted call centers, are seeing double-digit growth rates. Hosted call centers provide a number of business benefits, improved business agility, decreased capital expenditures, and lower total cost of ownership (TCO).

While research shows a steady increase in the number of companies moving to cloud-based services, many business leaders are questioning the ability of the provider to ensure adequate security. The risks, both real and perceived, are present at many levels, and each solution provider differs in its approach to security. This paper discusses the different layers requiring security, how security should be addressed in each layer, and how to select a qualified hosted call center provider.

> The number of hosted call centers is expected to grow 375% between 2008 and 2015.
>
> Frost & Sullivan[1]

THE CHANGING CALL CENTER LANDSCAPE

Today's call centers are not what they used to be. Changes in technology, the economy, and consumer expectations are creating opportunities for call centers to offer new services, while reducing costs. Call center executives are embracing a multisourcing approach, adding outsourced agents to meet changing demands and better manage costs. In-house call center agents are being supplemented with remote experts and work-at-home agents. To support this new trend, many call center executives are welcoming a move to hosted call centers. In fact, Frost & Sullivan says the compound annual growth rate for hosted call centers is expected to grow from nearly $400 million in 2008 to $1.5 billion by 2015[1].

Hosted call centers work very well when using outsourced agents. Outsourced agents include those located onshore, offshore, in remote offices and even at home. Frost & Sullivan believes that the work-at-home agent model could become the industry norm in the coming years[2]. Call centers are increasingly adopting a work-at-home model to access desired skill sets, reduce agent turnover, and achieve cost savings. Industry statistics have calculated a decreased cost of $25,000 per at-home employee compared to a traditional call center agent[3]. However, remote locations and disparate technical environments mean the IT costs and complexities can be enormous.

Additionally, call centers struggle to adjust to seasonal call volumes, which create a need for temporary capacity—both in on-premise and remote locations. Retailers experience spikes around holidays and financial companies experience spikes that coincide with fiscal time periods. Building the technical infrastructure to meet peak demands is inefficient, as the additional capacity goes unused the majority of the time.

Call center executives are now exploring hosted call center options that are based on the cloud services model. With a cloud-based model, the technology management and ownership is outsourced to the provider and the user pays for the service on-demand. Cloud-based services enable organizations to rapidly and affordably scale up or down as their business needs dictate.

Cloud-based services are gaining acceptance as an effective business strategy for call centers. No longer do companies need to invest in costly hardware and software or pay for expensive IT resources to provide daily administration and manage upgrades. Hosted call centers using the cloud-services model reduce CAPEX investments, reduce overhead costs, and offer “pay-as-you-go” for more predictable monthly costs. Gartner predicts that between 2008 and 2013, cloud-based services will grow at a compound annual growth rate of 59.5%. In fact, with more of the IT environment moving to the cloud, Gartner also predicts that as soon as 2012, 20% of businesses will own no IT assets[4].

With the significant cost savings, reduced IT complexity, and easy scalability, it’s easy to believe the Gartner 2012 estimate. However, IT and business leaders still have a major hurdle with cloud-based services: security. While many companies are ready to reap the benefits of cloud services, a study by TheInfoPro, an independent research network and leading supplier of market intelligence for the information technology industry, says 72% still have concerns about security in a cloud environment[5]. Given the mission-critical nature of the call center and its data, this concern is understandable.

IDENTIFYING AND MITIGATING SECURITY RISKS

Security risks are present in all aspects of the call center business, regardless of function or location. While the security risks in a cloud environment are similar to the corporate environment, control over those risks is quite different. However, every hosted call center has different levels of controls, so it’s wise to take extra care when evaluating providers.

Evaluating security practices begins with understanding the risks that occur at many different levels, including the data level, application level, and physical level. Providers need to offer protection for sensitive customer data, such as credit cards or SSNs, and help their clients meet compliance regulations, such as PCI. Applications must be protected from intrusion and hacking that could seriously compromise the center’s functionality. And, the hosted call center must employ physical security, including personnel, disaster recovery plans, and redundancy.

Gartner predicts that between 2008 and 2013, cloud-based services will grow at a compound annual growth rate of 59.5%. In fact, with more of the IT environment moving to the cloud, Gartner also predicts that as soon as 2010, 20% of businesses wil own no IT assets.[4]

Each level has its own mitigation strategies as well. Within each level, a variety of different mitigation tactics rely on both technologies and processes. Areas where risk needs to be addressed include data security, control and compliance, applications, and disaster recovery and business continuity. What follows is a brief discussion of how leading hosted call center providers mitigate the risks.

DATA SECURITY

The number one concern with cloud-based services is the security of the exchanged data. Given the amount of customer documentation done by call center agents with chat screens, e-mail, and call notes, this concern is understandable. As the work-at-home agent model grows, so does the concern around access to customer records, credit card numbers, and social security numbers. Fortunately, the leading hosted call center providers do not store customer data unless required by their clients. Using custom scripts or special tools, the providers help companies limit desktop functionality, including disabling copy, paste, and print functions. Scripts are also used to obscure certain data fields from view, such as fields for credit card information and social security numbers. And, while hosted call center providers do not store customer data, they help facilitate security by encrypting communications.

Best Practices

- Store customer data only when absolutely necessary and provide encryption when transmitting customer data.
- Use encryption, access controls, and filtering to ensure data in multi-tenant systems is protected from unauthorized access.
- Maintain a database of client ID and information that is used to validate that only the appropriate users can access that client's data.
- Use a Session Border Controller to authenticate phone calls over a VoIP network. This reduces the risk of fraudulent or unauthorized calls through the cloud provider's network.
- Leverage Virtual Private Networks (VPNs) to provide extra security for any data that is transported across the Internet.
- Implement intrusion detection systems to provide alerts when there are attempts to access the network in an unauthorized manner.
- Offer a secure FTP option for data transfers between the provider's site and the customer's site.

The second biggest concern, also related to data, is multi-tenancy, or sharing a provider's hardware and software among multiple clients. Some are apprehensive that one client may somehow be able to access another client's data or that one client will pass along a virus or cause a system malfunction accidentally. Because these concerns are valid in theory, providers go to great lengths to prevent them, designing and testing systems to prevent data leakage and system issues.

CONTROL AND COMPLIANCE

Companies today have a great responsibility to manage and protect their data. Several new compliance regulations were put in place in the last several years, requiring companies to use protective measures to track and guard corporate and customer information. With company data moving into an offsite, hosted environment, business leaders may expect the hosted call center provider to take over the responsibility for compliance, though in reality, the corporation is ultimately responsible.

Best Practices

- Use a role-based security model within each business unit that allows customers to control what security rights they grant to each of their users.
- Design security to include strong password policies, such as unique passwords and GUIDs, especially in the case of multi-tenancy.
- Employ outside security vendors to scan the provider's network on a quarterly basis looking for vulnerabilities that could result in a breach of security.
- Have published maintenance windows and change-control policies and procedures in place.
- Comply with PCI, Safe Harbor, Section 404 (SOX), SAS70, FCC (CPNI), and other FTC regulations.
- Physically secure data centers by card key access, iometric scans, and video surveillance.
- Ensure antivirus software is maintained and updated through a regular process on all corporate and production machines.

A provider must meet its own compliance regulations. In addition, many providers offer services that help facilitate compliance for customers, so that nothing it does will make customers noncompliant. Leading providers broadly offer change control, strict hiring and personnel policies, identity access management, and overall security. Some have even established customized controls based on the type of industry or business the customer is in.

APPLICATION SECURITY

Given that, with hosted call centers, agents are accessing applications that reside outside of the corporate walls, extra steps must be taken to ensure these critical applications are safe and secure. As with any application, it is subject to damage, either intentionally or by accident. Call center application intrusion could impact critical areas such as call routing, credit card authorizations—even the on-hold music and messages. And, though web and thin clients are the preferred access tools, connecting across the public Internet can expose applications to potential hackers.

Best Practices

- Employ a thin client or browser-based application at the agent workstation.
- Use SSL encryption to secure all data communications between the agent's thin client application and the hosted call center's.
- Make sure access to the applications and their administration is role based.
- Create and enforce policies that define how access and transmission to internal company systems, such as CRM, are handled, and whether any data is stored.
- Offer a flexible platform to allow customization to fit the security needs of the client.

Leading hosted call center providers assure that strong protective measures are in place. The most advanced providers offer multiple access options, like both web client and desktop. Financial service call centers, for example, employ some of the tightest security measures, not allowing agents a browser connection to the Internet. Additionally, many customers require the call center applications to integrate with their on-premise CRM systems. Top providers work with customers to identify information to be shared, who should have access, and how to handle calls in the event the CRM system does not function as expected.

DISASTER RECOVERY AND BUSINESS CONTINUITY

The ability to continue business in the event of a disaster also ranks as a major security concern, especially for call center executives. If an outage occurs, plans must be in place for calls in process. Can calls continue without interruption or is there an opportunity for the system to redial dropped customer calls? Decisions also need to be made about whether active session screen information is lost or kept alive through redundancy. Adding this additional functionality can be expensive and complex for call centers to implement and manage internally.

Hosted call center providers must offer their clients assurance through a comprehensive disaster recovery plan. This plan must minimize impact through fault tolerance and redundancy, both in systems and geographic locations. Leading providers offer an environment where equipment failure is undetectable, with no dropped calls or lost information. They also offer multiple, redundant locations in different geographic regions, as well as up to double capacity to support sudden spikes in demand.

Best Practices

- Maintain two or more fully redundant data centers located in geographically diverse locations.
- Contract with multiple Tier 1 ISP vendors to provide high-speed interfaces with BGP peering employed across multiple BGP peering routers to ensure high Internet connectivity, reliability, and recovery.
- Deploy carrier-grade, fully redundant hardware at all sites.
- Maintain a redundant system architecture that allows services to continue operating in the event of component failures.
- Replicate and back up all customer data between two separate data centers to ensure rapid data recovery and survivability.
- Use redundant protected power systems with battery and generator backup to ensure reliable, protected power for all servers and network equipment.

HOW TO QUALIFY HOSTED CALL CENTER PROVIDERS

Not all hosted call center providers are the same. They vary not just in the features they offer, but also in the approach to security. Also, every call center has different security needs. It's imperative that call center leaders carefully scrutinize each provider and make sure their individual needs can be met before committing to a contract for services.

Securing services in a cloud-based environment requires a layered approach that includes physical security, application security, and data security, including compliance. Providers should be able to describe how they handle security for each layer. The more detail a potential vendor provides, the more likely its security measures are robust.

At the highest level, providers should be vetted based on the financial health of the company and its personnel policies. Take time to research available public information about the longevity of the company, financial history (if available), relationships with partners, and the types of customers served. Ask for customer references and discuss their level of satisfaction. Also ask about personnel hiring and management policies. Staff should have passed background checks, identity-access management practices should be in place, and the provider should conduct regular internal audits.

Leading hosted call center providers have comprehensive disaster recovery plans that provide redundancy both in the technical infrastructure and geographic location. The plan should guarantee "up-time" or availability statistics that approach 100%. It should also document the process to follow in the event of a disruption, addressing the various types of potential events. Communication and notification processes should be included. Together, the provider and the client work together to create a service level agreement that meets the client's needs. Some of the questions to ask potential providers include:

- Who has access to data and how are they vetted?
- What data security technologies—such as DLP or encryption—are used, especially in the case of multi-tenancy?
- Is the data completely deleted when the user deletes it from the application?
- How many copies of the user's data are kept and where is it stored?
- What is the vendor's privacy policy?
- How are investigations and audits handled on shared infrastructure?
- Are tested encryption methods used in the case of multi-tenancy?
- Is the provider designing systems so they can scale?
- What are the providers' change-control polices and review process?
- How quickly can the provider recover from a disaster?
- What customer information is stored? Are any chat sessions and e-mails stored?

> The reality is that a well-engineered hosting environment will have deeper security infrastructure in place than many SMBs could afford on their own.
>
> Frost & Sullivan[1]

CONCLUSION

Security will always be a primary concern for business leaders. Now, with the introduction of cloud-based services, that concern grows even larger. Hosted call center providers that rely on cloud-based services must be very diligent in addressing security, even surpassing the client's ability to secure its on-premise environment. Fortunately, many hosted call center providers have stepped up to the plate and offer features such as 24/7 monitoring, fail-over ACD, redundant data centers, and ongoing intrusion detection.

However, each provider has a different approach to security. It's important that call center executives fully understand the potential risks and how they are addressed before selecting a provider. Executives need to be completely confident that their call center function is just as secure—if not more secure—in a hosted environment than it is in the on-site environment.

Economic, social, and technological changes continue to shape the call center industry. Hosted call center solutions offer enormous benefits over on-premise solutions, including scalability on demand, flexibility to access from any location, lower IT administration overhead, and reduced capital expenses (CAPEX). The benefits of a hosted call center are too great to ignore and successful call center executives are the ones who thoroughly research potential providers until finding the provider that offers security measures above and beyond the call center's needs.

SECURITY IS SERIOUS BUSINESS WITH INCONTACT

inContact offers a state-of-the-art, hosted contact handling and agent optimization platform. Since 2001, inContact has provided call centers with connectivity and agent management tools to be successful. Its cloud-based technology includes a full-featured Automated Call Distributor (ACD) with skills-based routing, Interactive Voice Response (IVR) with speech recognition, and Computer Telephony Integration (CTI). inContact is publicly traded on NASDAQ and corporate financial information is at www.incontact.com.

inContact takes client security seriously. The skilled technical team, with many years experience in network operation centers (NOC), maintains the highest levels of security at every layer—data, applications, and physical security. Some of the security highlights include:

- Fully redundant hardware, software, and system architecture with battery and generator backup
- Two geographically dispersed, carrier-grade data centers in Los Angeles andDallas, physically secured by key access, biometric scans, and video surveillance
- Any customer data stored is backed up and replicated in real time
- Industry-leading security technology protects transmission of data and VoIP calls over the Internet, as well as preventing unauthorized access and malicious intrusion
- Security methods that are specially designed for multi-tenancy
- Compliance with PCI, Safe Harbor, Section 404 (SOX), FCC (CPNI), and other FTC regulations
- Security demonstrated through Independent SAS 70 audit verification
- Voice-recording encryption and secure storage for client retrieval

Because inContact feels so strongly about providing confidence and gaining trust with clients, it's created the hosted contact center industry's first Trust Office. The inContact Trust Office mission is to improve the transparency around security, compliance, and general operations. If the Trust Office believes inContact can do a better job supporting customers in these areas, it works within the organization to develop the actions to produce that improvement.

The bottom line: inContact wants its clients to experience the full benefits of a hosted contact center solution with even greater trust and security than an on-premise solution.

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

inContact

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

1-866-965-7227

www.inContact.com

inContact®

[1] Frost & Sullivan: Strong Industry Growth in Hosted Contact Center Market in North America Despite Economic Meltdown, Frost & Sullivan, November 6, 2009 http://www.frost.com/prod/servlet/press-release.pag?Src=RSS&docid=184389860

[2] "The New Mantra: The Agent is King", Frost & Sullivan

[3] International Telework Association and Council (ITAC)

[4] Gartner's Top Predictions for IT Organizations and Users, 2010 and Beyond: A New Balance, Gartner, Inc., December 2009

[5] TheInfoPro's 2010 Information Security Study Reveals Budget Changes, Cloud Concerns, Potential Consolidation, TheInfoPro, February 25, 2010, http://security.tekrati.com/research/10755/