Security in a Work-at-Home Environment

Teleperformance
each interaction matters

Executive Summary

During the last decade, there has been a remote worker revolution. In the US alone, more than four million people work from home, representing about 3.2 percent of the total workforce.[1]

Given record-low unemployment and a tight job market, the at-home model provides businesses with access to a larger, more diverse labor pool. Contact centers, in particular, have embraced the at-home model and have seen many benefits. In addition to cost savings and increased productivity, companies that have adopted the at-home model report improvements in customer satisfaction and lower employee turnover.

Despite the benefits, concerns about security prevent some businesses from taking advantage of this growing trend. But those concerns are easily addressed with the right strategy and technology.

Growth and Benefits of the WAHA Model

Since the end of the Great Recession in 2009, unemployment has steadily declined. In January 2019, unemployment was at four percent, according to the US Bureau of Labor Statistics. While low unemployment is an indicator of a strong economy, it presents hiring challenges for many businesses. Companies have had to be more creative and flexible in their hiring practices to fill positions. The at-home model has provided a viable solution to record-low unemployment, says contact center outsourcing expert Peter Ryan. The at-home model "opens up a whole segment of the labor force that might not want to work in a brick-and-mortar environment."

WAHA (work-at-home agent) has become an established business model in the United States in the last decade and it's starting to spread globally, says Ryan. A survey of 350 contact center service buyers conducted by Ryan Strategic Advisory found that WAHA ranked in the top five of 20 possible solutions that clients will consider to meet their staffing needs. Companies adopting a WAHA model cite multiple benefits. Topping the list is cost savings. Businesses save on costs associated with owning, leasing, or maintaining office space—an estimated savings of $121 billion per year.[2]

A much larger pool of talent opens up to companies that embrace a work-at-home model, notes Terry Rybolt, Managing Director of Home Agent Deployment for Teleperformance. "The stats are very specific, that being able to recruit on a wider scale allows for a differentiated workforce," he says.

Additionally, remote employees tend to be highly engaged and therefore more productive, says employee engagement and retention expert Vicki Brackett. They are typically a little older and more educated than the average on-site agent. Remote workers value their independence and the flexibility that working from home provides. As a result, companies that adopt the WAHA model are often able to attract and retain a workforce with diversity in experience and skills.

Case studies from Teleperformance speak to the benefits of the WAHA model. Clients consistently report improvements in customer satisfaction (CSAT) and average handle time (AHT) with at-home versus on-site employees. The studies also reveal improved employee retention rates. Lower turnover allows for greater consistency in customer service.

1. Global Workplace Analytics, "2017 State of Telecommuting in the U.S. Employee Workforce," globalworkplaceanalytics.com. ***2.*** Ibid.

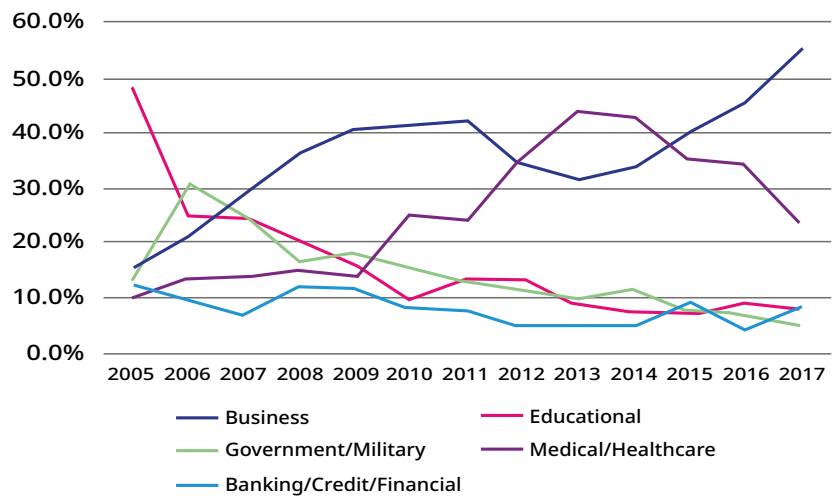
The Concern for Security

"Security is an omnipresent fact of life in today's commercial environment," adds Ryan. By far, fraud is the greatest concern of clients and customers when it comes to online security. People fear having sensitive data such as their social security number, credit card information, or health records stolen and used in nefarious ways.

It's a valid concern given a recent report from the nonprofit Identity Theft Resource Center (ITRC). Its research shows a 45 percent increase in security breaches since 2016.[3] The industry sector with the most breaches was business (see figure 1). "We've seen the number of identified breaches increase as a result of industries moving toward more transparency," said Eva Velasquez, ITRC's president and CEO.

Figure 1: Percent of Breaches by Industry Sector

(Source: Identity Theft Resource Center)



A Comprehensive Strategy to Ensure Security

Concerns about security breaches can be easily addressed with a comprehensive strategy that includes highly trained employees, well-defined processes, stringent policies, proactive management methodologies, and cutting-edge technology. Together, these help establish a company culture that can anticipate and act on potential fraud and data breaches before they happen.

"Home-based agent delivery and the companies providing home-based agents have done an exceptional job addressing security concerns," says Ryan. A good starting point is in having a remote work policy that ensures data security. Proper training, implementation, and stringent enforcement are key.

An effective policy starts with the recruiting process, advises Brackett. Prospective at-home agents should be vetted. Rigorous financial and criminal background checks should be conducted, and references—both personal and professional—should be contacted, she says.

Data security policies and procedures should be made clear to new employees during orientation and through ongoing training. Many companies require all employees—whether on site or at home—to read and sign policy documents. Anytime policies are added or amended, signed documents should be reviewed and updated.

3. Identity Theft Resource Center, "2017 Annual Data Breach Year-End Review," idtheftcenter.org/2017.

The most effective security measures employ these best practices that are reviewed and strictly enforced.

1. Strong passwords with multi-factor authentication (MFA). Password management programs can generate and store unique, complex, and non-hackable passwords. Other effective measures include single sign on (SSO). An additional measure requires passwords to be changed periodically, such as every three to four months.

2. Clean desk policy. All sensitive documents or data are removed or locked away when an employee leaves their workstation. This includes papers on a desk as well as files and programs on a screen. Enforcing this policy with at-home agents requires a commitment to educating employees on security awareness, and complying through regular checks.

3. Encryption, encryption, encryption. Devices, software, and cloud services should have end-to-end encryption to secure data across all devices.

4. Use a dedicated VPN or secure cloud service. Don't allow remote employees to use unsecured public Wi-Fi.

5. Lock down devices. Ensure that all devices employees use or access have the latest firewall, malware, and virus protection and can be wiped remotely or disabled, if necessary. The ability to transfer data, including cutting and pasting, screen prints, or drive mapping are prohibited.

6. Limit access to sensitive information. Provide access to data, files, networks, or applications only as needed.

7. Downloading restrictions. Prohibit the downloading of information, software, apps, and the like from unsecured or unapproved sites.

8. Proactive, real-time monitoring. Invest in tools to monitor agent activity and detect behavior that deviates from the norm, signaling possible fraudulent activity.

Engaged Employees Enhance Protection

In addition to employing best practices, Vicki Brackett emphasizes the importance of employee engagement—especially for at-home agents.

"The employee engagement piece is extremely important. When people value working at home, they are going to protect that. Employees who feel that they have a stake in the company will protect customer data and protect the integrity of the systems," Brackett says.

Teleperformance Provides Unsurpassed Protection

When it comes to security, Teleperformance has the system and tools that can help (see figure 2). Through a holistic approach, Teleperformance identifies and mitigates risks. With a strong people-focused foundation, Teleperformance was the first in the industry to achieve PCI certification, and more recently BCRs certification. Its security culture is second to none. Teleperformance security professionals include Certified Information Systems Security Professional (CISSP), Certified Fraud Examiner (CFE), Certified Information Systems Auditor (CISA), ISO Certified Lead Auditors, and Project Management Professional (PMP) Managers.

Teleperformance adheres to security standards and regulations, including Global Essential Compliance Security Policies (GECSPs). This group of policies governs Teleperformance's approach to security. These policies go several steps beyond standard best practices to include:

- Security Data Analytics
- Clean Desk
- Infrastructure Hardening
- Fraud Hotline Reward and Security Awareness
- Security and Fraud Communication
- Contractual Compliance
- Security Awareness Training
- Login Provisioning and Deprovisioning
- Risk Discovery and Fraud Prevention
- Social Media Confidentiality
- Employee Confidentiality

Figure 2: Teleperformance Security Structures for a Work-at-Home Environment

Our security structures are designed to address the main security concerns for a work-at-home environment and mitigate the most common data breaches and fraud situations.

HIGHLY SECURE ACCESS CONTROLS
End Point Inspection provided by Citrix Netscalers; validates PC firewall configuration, security settings, and antivirus scans.

COMMUNICATION
Dedicated VPN appliances ensure encrypted data path from agent's PC to virtual machine in data center. Citrix Netscaler uses an ICA proxy with no data path except local agent-accessed ICA protocol for virtual environment entrance.

NO DATA STORED LOCALLY
Data remains within data center and connections made from virtual machine that boots from "read only" hard drive with "redirected smart menus" and no local or mapped storage. Reboot to default state after each connection.

NOISE CONTROL
Agents are required to sign a zero noise tolerance form and supervisors monitor for any infractions to certify that the agent is alone in their work space at home. All infractions are reported to HR.

TWO-FACTOR AUTHENTICATION
Required authentication factors. Agents are issued unique identifiers, strong passwords, and duo-issued controls.

LOCK DOWN DEVICES
Citrix remote desktop strategy ensures encrypted connection to virtual desktop in a secure data center. It prevents local data transfers, cut and paste, screen prints, drive mapping, etc. Entire screen is taken over by virtual machine.

CLEAN DESK ENFORCED
Policy reviewed during recruiting, orientation, and training that requires agents to sign a document stating they understand policies and expect frequent supervisor reviews.

A Proactive Approach

Teleperformance embraces a proactive approach to ensuring the security of client data and systems. A key feature of Teleperformance's security program is a comprehensive risk assessment. The assessment is a non-intrusive, non-biased service that identifies possible privacy/fraud risks and noncompliant criterions in client programs. Teleperformance's assessment includes a custom risk mitigation and reduction plan, as well as an assessment status follow-up meeting.

Teleperformance also offers specific training that focuses on PCI requirements, as well as other GECSPs, explains Rybolt. Teleperformance's operational supervisors reinforce key policies, such as clean desk, every day in team huddles, which are documented in Teleperformance's TOPS compliance process. As a rule, the company emphasizes proactive security awareness.

"Teleperformance has added innovation to contact center security that often surpasses the client's internal security controls for fraud prevention and early detection," attests Michael DeSalles, industry analyst from Frost & Sullivan. In short, for companies that absolutely require the highest degree of data and customer information security, Teleperformance is indisputably the industry leader."

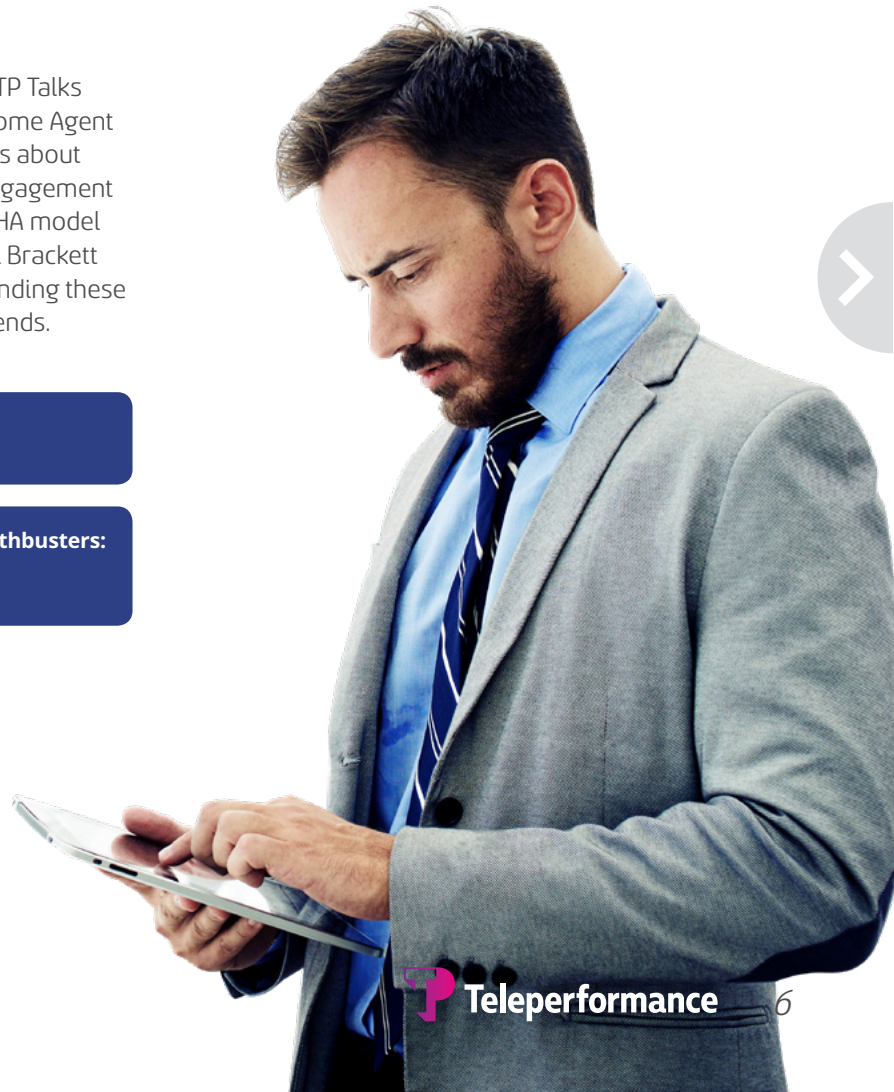
Closing Thoughts

Concerns surrounding security and data protection need not prevent companies from embracing the home-agent model as a viable solution to contact center staffing. Highly trained agents and state-of-the-art technology combined with best practices will go a long way in ensuring security for your business and customers.

To learn more, watch the webcast series TP Talks "Home Agent Mythbusters: Debunking Home Agent Myths." This webcast focuses on concerns about security, loss of control, and employee engagement that have slowed the adoption of the WAHA model for contact centers. Industry experts Vicki Brackett and Peter Ryan debunk the myths surrounding these concerns and share best practices and trends.

TP Talks Webcast Series Library
tinyurl.com/tp-talks-webinar-platform

TP Talks Webcast Series "Home Agent Mythbusters: Debunking Home Agent Myths"
tinyurl.com/home-agent-mythbusters



About Teleperformance

Worldwide Leader in Omnichannel Customer Experience

We are the worldwide leader in outsourced omnichannel customer experience management. Teleperformance connects the biggest and most respected brands on the planet with their customers by providing customer care, technical support, customer acquisition, digital solutions, analytics, back-office and other specialized services to ensure consistently positive customer interactions.

Teleperformance
each interaction matters

For more information:
teleperformance.com

Follow us:

/teleperformanceglobal
@teleperformance
/teleperformance
blog.teleperformance.com
/company/teleperformance
@teleperformance_group