Vigilance in a Work-Everywhere World

Offering an integrated approach—from professional agents to hardened infrastructure to locked-down data.

Protecting data and privacy needs to be a state of mind—before it can become the state of the business.

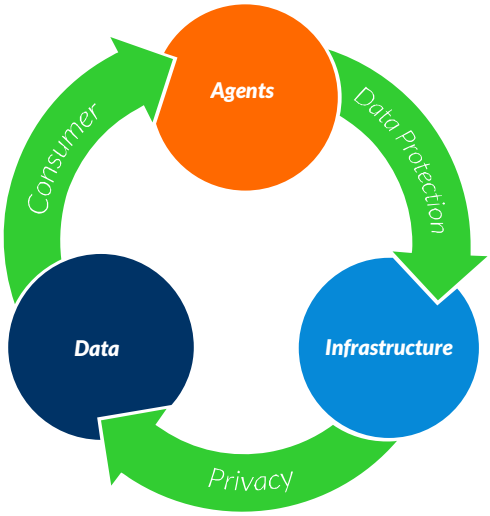
With almost 20 years in contact center services, we know the security issues facing organizations today:

- Breaches are accelerating across all industries, with retail and public sector being especially vulnerable.
- Attacks or mishaps are increasing in scope and scale, with fallout for companies not taking precautions.
- Even as more breaches occur, there are still organizations that only pay lip service to data security.

Enterprise or industry-specific, we factor in these issues to safeguard your operations and customers by:

- Creating a security-minded culture from the get-go
- Leveraging agents who specialize in at-home work
- Securing agents' home operations and technology
- Ensuring digital security—wherever business is done
- Monitoring agent performance—at all touchpoints

PCI DSS – Level 1 Compliant *Report On Compliance* ***(ROC)***	*Health Insurance Portability and Accountability Act* ***(HIPAA)***	***Going beyond certifications to protect data and privacy***
Payment Card Industry Data Security Standard (PCI DSS) Completing our last audit on June 25, 2014. All parts of our platforms and operations are Level 1 certified for credit-card transactions, covering: security management, network architecture, software design and development, storage and transmission, and remote-access policies. We do quarterly vulnerability scans of our systems. PCI COMPLIANT LEVEL1	Adherence in accordance with **HIPAA Security at §164.308 (a)(4)** and **HIPAA Privacy Rule at §164.508**. We have all of the appropriate policies and procedures in place to secure protected health information (PHI) transmitted over communications networks. HIPAA compliant	Industry standards certainly have their place. They are, however, the price of admission to safeguard data and privacy. That's why at Working Solutions we invest in common-sense security measures, such as **data masking**, to further ensure consumer protection and privacy. Data Masking



Protecting data and privacy

Digital threats are escalating for enterprises and individuals alike.

At Working Solutions, we know how to protect data and privacy for your business and customers—from agents to infrastructure to data.

We interlock all three to create a continuous cycle of integrated security.

Agents

We rigorously monitor agents adhering to strict administrative processes and physical security standards.

Administrative controls include Ethics and security training and awareness, clean-desk policy, business associate agreements and confidentiality agreements for HIPAA compliance.

We do background and drug screening, follow clinical content guidelines and conduct quality monitoring. To them, we add audit logs, system access reports and data breach notification.

Risk management processes are in place, with periodic security evaluations and annual audits. They track data breaches and security incident reporting for HIPAA compliance. Security incident reporting also is part of managing risk for payment cards.

In both instances, the work is done by a third party, which ***provides audit results to clients***.

Physical security standards include password-protected, confidential files—as well as procedures for receipt and removal of hardware and software, and clean separation between host machine and virtual desktop environment (VDI).

Beyond these measures, we disable local print capability, and copy-and-paste and print-screen functionality. Email distribution and Internet access are limited.

We also prohibit and restrict individual remote workstation local storage, backups and use VDI-based network drive.

Infrastructure

Working Solutions offers a multichannel contact center application suite of services.

Residing in a hardened environment, these services provide peace of mind for clients and their customers.

This work encompasses ***disaster recovery, redundancy and failover***.

It takes in multiple data centers, robust network infrastructure, and system security plans for all applications and hardware and software configuration management.

Integrated network security includes firewalls, redundant technology and intrusion detection—regularly tested with penetration attempt, and quarterly vulnerability scans of our systems.

Data

Working Solutions ensures technical standards are met for data protection, ranging from PCI DSS Level 1 security for payment card transactions to HIPAA compliance for healthcare.

Our work adheres to documented and auditable policies, procedures and processes to ***protect physical data***—as well as encryption and monitoring for data in transit.

At-rest data is inactive, stored in any digital form. Included are authentication policies and procedures, access and audit controls, and data integrity verification and validation controls.

In-transit data is sent via the Internet or private network. Included are encryption capabilities and data masking, alarm features for abnormal activities or conditions, and flow-through assurance of data transmission.

Best Prepare: "Something Wicked This Way Comes"

Identity theft is a multibillion-dollar industry, with its own perverted profit and loss.

Headlines chronicle widespread crimes done by hackers—with data breaches affecting FORTUNE 500 companies, mid-sized to small organizations and untold consumers worldwide.

CBS News reported that an identity fraud occurred in America every two seconds in 2013. The U.S. Justice Department's statistics bureau states **more than 16 million Americans** experienced identity theft in 2012, according to its last report. The U.S. price tag alone was $24.7 billion.

Shakespeare had it right: "Something wicked this way comes."

Best prepare now.

Ask About "The Fundamental Five"

Nothing is more personal than your identity. Unless, of course, if you're a business—and it's your customers' data and privacy.

PII, or personally identifiable information, needs protection by those entrusted with it. To ensure that trust, do your due diligence before working with a contact services provider.

Ask "the fundamental five"—common-sense questions that should be commonplace security. Does the provider:

- Build and run a secure network?
- Provide a vulnerability management program?
- Implement strong access control measures?
- Monitor and test networks—routinely?
- Maintain an information security policy?

They're basic to run a safe, secure operation. You—and your customers—deserve to know.

Experts Report: "Better Get Home"

Home-based agents beat their brick- and-mortar counterparts every time, according to industry analyst Frost & Sullivan and the FBI. How so?

The quick list:

- College educated—84% vs. 35%
- More experienced—15 years vs. 5
- Disaster resistant—calls in when others call out

And, just the facts: Home-based agents are less likely to commit theft, forgery or fraud.

Ongoing Security: Upfront Beats Catch-up

Today, we continue to elevate home-based security—exploring practices such as intermittently videotaping agents while working at home.

We also are piloting additional measures to continually sharpen our security. They include:

- Masking data for identify protection
- Introducing new pinpoint security devices
- Rolling out a virtual desktop—controlled out of a data center

Digital threats are escalating for organizations and consumers alike.

At Working Solutions, we know how to protect data and privacy for your business and customers—believing upfront trumps catch-up every time.

Data Masking

Making Common-Sense Security Commonplace

When it comes to data protection, common-sense security isn't always commonplace.

Sad but statistically true—with identifies being compromised and crimes compounding daily.

There are assured ways to protect privacy, however. One of them is called data masking or scrambling, which blocks or Xs out confidential information. Hard to steal someone's ID if it can't be seen. Right?

With increasing security threats, data masking should be standard practice, but it's not the industry norm. Yet, such security is a proven way to safely conduct business. Here's why:

1. Apps can be written to block out selected data. Normally, a consumer's Social Security or credit card numbers are masked, eliminating the potential for theft. Stricter restrictions can hide deeper levels of data.
2. Data masking goes beyond any clear-desk policy. With no content to copy, it even eliminates breaches such as "finger-nailing," where a brick-and-mortar call center agent reportedly copied consumer data onto her cuticles to steal it.
3. As more security breaches occur and regulations intensify, data masking is proactive and practical— with can't-see/can't-steal applications to ensure privacy protection.

At Working Solutions, we know what it takes to safeguard data, with almost 20 years of protecting information for clients and their customers across many industries. Today, our X-ID™ technology can help stop identity theft before it starts. It's simple, yet effective.

Given the times, it's wise to build in security that goes beyond industry standards. It's all part of taking a holistic enterprise approach. Masking keeps data safe and secure. In this case, not seeing is believing—and that's a benefit for businesses and consumers.