Engineering a Culture of Security Consciousness in Customer Service

FROST & SULLIVAN

A Frost & Sullivan White Paper Excerpt

Michael DeSalles, Principal Analyst

INTRODUCTION AND PURPOSE

Today's customers are more concerned than ever about how companies use their data and track their activities online. While security has traditionally been viewed as the responsibility of the IT organization, progressive companies have built a separate Security Practice to stave off the onslaught of internal and external threats. Battling agent turnover and improving the overall customer experience, continue to be top priorities in contact centers across the globe. However, no one can deny the mission-critical nature of stringent *security and privacy policies*, as a key benchmark for best-in-class contact center performance.

This analyst viewpoint is written for the community of professionals interested in understanding the unique challenges faced in contact centers, globally. This may include, but is not limited to:

- Customer service directors, strategists and operations managers
- IT managers and directors
- Contact center solution providers: hardware, software & services
- Enterprises looking to outsource customer care
- Consultants
- Government entities

The white paper excerpt will provide insights into the background, trends and context for creating the next generation contact center Security Consciousness and Culture; one where there is a rich set of policies, processes and tools to protect clients and their customers. It is not intended to provide technical recommendations, but rather include enterprise security considerations for complete customer experience management. This paper discusses the importance of having a holistic view of contact center security.

JUST HOW COMPLEX IS CONTACT CENTER SECURITY?

Current Threat Landscape

Let's be honest: Agent fraud, within captive or outsourced contact centers, represents the most significant threat. One of the primary information security threats related to contact centers, occurs when employees conduct unauthorized access to private and confidential data without a business need to access that data. For example, one of the most common fraud practices is for an agent to change a customer's postal address with the intent to place a new order for a warranty replacement item. The dishonest agent then ships the product to an accomplice or to their own address.

Think about it. One can point to several obvious sources of contact center 'insider' entry points:

a. Agents, supervisors, quality analysts, account managers and other employees
b. Contractors (Maintenance teams, catering & food vendors, janitorial crews, construction workers)
c. Third-party suppliers of computer equipment/software and office equipment
d. Telephony providers and electrical sub-contractors
e. Visitors (Clients, prospects, analysts, press corps, consultants)

Business Continuity & Disaster Recovery (BC/DR)

Common threat-sources include:

a. **Natural Threats**. Floods, earthquakes, fires, tornados, landslides, hurricanes, avalanches, typhoons, electrical storms and other such events
b. **Human Threats**. Workplace violence, terrorist acts, arson, unintentional acts (e.g. IT-related outages) or deliberate actions and unauthorized access
c. **Environmental Threats.** Long-term power failures, pollution, chemical and hazardous materials leakage

Facility and Building Controls

Here is a partial list of rigorous facilities controls that Frost and Sullivan analysts have observed, firsthand, in contact center sites across the globe:

- Written Security policies and building access procedures including signage and posters on security
- All visitors must be logged and admitted through reception
- ID-badge system for all employees and visitors
- Badge sharing and piggy back entry is prohibited
- Card-key, biometric, or similar entry locks
- 24x7 onsite security guards
- Individual lockers to enforce a clean desk policy
- Video surveillance and motion sensors for entrances, interior doors, equipment cages, and critical equipment locations within the building

PROTECTING CUSTOMER AND EMPLOYEE DATA

A Culture of Safety and Protection

Criminal organizations make it their business to launch large-scale attacks to steal from bank accounts & credit cards, upload employee information and get their hands on social security numbers in order to perpetrate identity theft. Current research points to the fact that the majority of fraud attacks involve at least one 'point person' working on the inside.

As pointed out beforehand, this is especially true in contact center environments- replete with large populations, high turnover and agent access to confidential customer information. Therefore, it becomes imperative that there is an institutional security culture baked into the DNA of an organization.

FRAUD PREVENTION

Certifications Are Not Enough!

Consider this: Security certifications are certainly very important. In and of themselves, they aren't comprehensive enough to prevent and detect call center fraud. Every day, agents make a conscious decision to either commit fraud or behave honestly. If we accept

the fact that a high percentage of fraud occurs from within, then organizations must consistently and responsibly:

1. Authenticate the identity of the agent-something the person 'knows' and 'is'

2. Track agent activity with technology across multiple sites and geographies

Using information the agent "knows" in combination with verifying who they "are," provides a much more secure environment in the enterprise.

Frost & Sullivan believes that a truly effective contact center security program is proactive in not only understanding the current threat environment, but also detecting the kind of fraud that insiders will commit in the future.

SECURITY CONSIDERATIONS

Security Questions Every Enterprise MUST ASK a Potential Partner

When it comes to contact center security, Frost & Sullivan believes that there are a number of critical areas that must be examined when considering a partner for outsourcing customer care; be it service, acquisitions, tech support or sales. Listed below are a number of broad and important considerations:

- ✓ **Leadership Support and Reputation:**
  How does the CEO support security with a system of internal controls and security measures to ensure the privacy of your critical customer data? Is there a council or executive body that governs security worldwide?

  What is the security track record of this provider with companies like yours? Will they provide other reference able clients who can give an honest assessment of the history of security performance?

- ✓ **Security Organization and Management:**
  Does the company have a separate security organization (not part of IT) that reports directly to a C-level executive? What is the experience and background of security

executives?

Does the company offer security Service Level Agreements (SLAs) to its clients? Does the company conduct employee background checks, criminal checks, financial checks and integrity checks?

- ✓ **Fraud Risk Assessment:**
  Can the company perform a comprehensive vulnerability assessment analysis of your company's applications and processes? This process typically generates a list of fraud "opportunities". Can the company create remediation efforts to eliminate those opportunities in agent recruiting, training and daily operations? Are there insider-threat detection procedures currently in-place to reduce risk, cost and complexity?

- ✓ **Certifications:**
  Does the company employ a team of CISSP certified information security experts and fraud risk analysts? Is the company in full compliance with the strictest security standards (IPAA, PCI-DSS PCI DSS ISO 27001/2, HITRUST,HIPAA, SSAE16 specifically SOC1 type II and SOC2 type II and other internationally recognized standards) across industry verticals? How often are independent audits conducted?

- ✓ **Global Scale:**
  Does the prospective partner have an extensive **global** security practice dedicated solely to security? Can the organization, with specific policies, ensure consistent compliance with statutory and regulatory requirements not only in U.S. domestic markets, but also near-shore and off-shore geographies? Is the company able to provide customized technology solutions to meet your company's specific requirements?

- ✓ **Technology:**
  Has the company developed special processes, tools and platforms designed to make the contact center environment more secure? Which specific future technology enhancements for client security will the company put in place in 2-5 years?

  Which technology firms does the company partner with? Does the company utilize a data loss prevention (DLP) system and an Intrusion Detection System(IDS)? Does it own a proprietary, patented security technology for client programs?

- ✓ **Security Analytics:**
  Can the partner bring end-to-end security analytics and behavior analysis to play in detecting and thwarting attacks and insider fraud?
- ✓ **Fraud Hotline:**
  Has the service provider set up an internal Fraud Hotline at each site that allows employees to report suspected fraudulent activity?

The Final Word

Make no mistake. Contact center security is complicated, multi-faceted and difficult to manage across multiple sites, countries and regions. It takes C-level support and millions in resources and investments. It certainly is challenging, but not impossible, to build a security-conscious culture within the entire organization; reinforcing customer trust, reducing agent churn and uncovering gaps that may put client intellectual property at risk.

Building daily awareness with employees is a fraud deterrent in and of itself. Reminding agents that protecting the organization from fraud, also makes a good case for long-term employment and job security. Making anti-fraud operational best practices part of your company's DNA goes a long way in supporting and embracing security as not only 'the right thing to do', but also a competitive advantage for the future.

References

1. The Harvard Business Review, " The Danger from Within" David M. Upton and Sadie Creese From the September 2014 Issue.
2. "Cyberhunting: A Critical Component of Enterprise Security", published by Techtarget and sponsored by Infocyte.

To receive a complementary full copy of this exclusive Frost & Sullivan white paper, please contact the author at Michael.DeSalles@frost.com.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages almost 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi/NCR
Detroit
Dubai
Frankfurt
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Mexico City
Miami
Milan
Mumbai
Moscow
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw
Washington, DC

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400,
San Antonio, Texas 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SW1W 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041