FROST & SULLIVAN

Engineering a Culture of Security Consciousness in the Customer Service Organization

A Frost & Sullivan White Paper

www.frost.com

Michael DeSalles, Principal Analyst

50 Years of Growth, Innovation and Leadership

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 the future of security initiatives in the contact center industry. 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 and services
- Enterprises looking to outsource customer care
- Consultants
- Government entities

The white paper 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 includes enterprise considerations for complete customer experience management and 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 a 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. There is indeed a delicate balancing act that takes place in call centers on a global level. Managers must provide agents with the necessary access, while protecting the security and privacy of customer data. Perpetrators of fraud exploit authorized access for illegitimate and malicious purposes. 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 and 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)

Outside of a malicious attack or theft, carelessness, negligence and ignorance on the part of insiders can also enable cyber-attacks and create vulnerabilities.

The harm done by attacks mounted by outside hackers cannot be discounted, be they foreign governments, individuals or international crime syndicates. Not to mention network intrusions, distributed denial of service (DDOS) attacks, email viruses/worms, spam, and the sale of sensitive information on the Dark Web. However, based on our research and interviews with call center executives, Frost & Sullivan believes that the most pernicious threats often develop from within the organization. According to various estimates, at least 80 million insider attacks occur in the US each year.[1] A significant number of them go unreported because access to confidential data can go undetected.

Business Continuity & Disaster Recovery (BC/DR)

Customer contact centers lie at the center of disaster response, or business continuity/disaster recovery (BC/DR) issues and strategies. They are the "go-to" information hubs in times of calamities and disasters. In a white paper authored by Genesys, it was concluded, "…It is important to note that business continuity differs from disaster recovery, despite the fact that these terms are sometimes used interchangeably. Business continuity is concerned with mitigating risk before a disaster. Disaster recovery refers to the plans and actions to be acted upon once the disaster has occurred."[2] The BC/DR challenges become even more acute when an organization is operating dozens of centers in several countries and delivering language support across multiple geographies.

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 leakages

Exhibit 1.0 shows the results of a recent Frost & Sullivan survey of over 250 IT managers. It revealed that only 31% agreed that their organizations are prepared to handle outages (of any kind) and natural disasters.

Exhibit 1.0: Alignment of IT Strategies and Business Objectives Strongly or Somewhat Agree, North America,

Source: Frost & Sullivan analysis

This low response rate illustrates the strategic challenge of balancing the potential risks and losses associated with disasters against the investments required to effectively deploy a proper business continuity solution.

Facility and Building Controls

Here is a partial list of rigorous facilities controls that Frost & 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

To accommodate the personal needs of agents, the vast majority of contact centers have quiet break areas. In these separate and distinct leisure spaces, employees can stay connected to the Internet, use mobile devices and utilize a wide variety of communication channels for personal use. It is considered an industry best practice.

PROTECTING CUSTOMER AND EMPLOYEE DATA

A Culture of Safety and Protection

Outsourcing clients, in particular, place a great deal of trust in service provider partners—expecting the highest certification levels to protect customer data, employee records, financial information and profiles. Criminal organizations, on the other hand, make it their business to launch large-scale attacks to steal from bank accounts, pinch credit cards, upload employee information and lay their hands on Social Security numbers 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. It is our opinion that engineering a culture of security consciousness begins at the CEO level. The CEO establishes that cyber security is a top priority and will be a competitive differentiator for the company.

> ***"Engineering a culture of security consciousness begins at the CEO level. The CEO establishes that cyber security is a top priority and will be a competitive differentiator for the company."***
> *Frost & Sullivan*

Process and Policy

Frost & Sullivan research shows that top-tier service providers that have a defined security practice or division, autonomous and separate from IT, are in the best position to offer:

A. A comprehensive, ongoing employee security awareness and education program

B. A rigorous security assessment and risk analysis for clients

C. A global team of CISSP-certified information security experts and fraud risk analysts

D. Standardized processes and internal policies to monitor contact center compliance on a federal, state and country-by-country level

E. Proprietary tools to track and "red flag" unauthorized agent access and behaviors

F. Security service-level agreements (SLAs) for clients

G. Demonstrated security best practices with the goal of being the security "center of excellence" leader in the industry

H. The ability to conduct frequent random remote quality checks, with recorded voice and visual images, on every type of call and transaction

I. Innovation, customization and investment in state-of-the-art security technology

J. Full compliance with the strictest security standards across industry verticals, including those set by HIPAA, PCI-DSS and other internationally recognized standards. At a minimum this would include PCI DSS ISO 27001/2, HITRUST, HIPAA, and SSAE16, specifically SOC1 type II and SOC2 type II.

K. A C-level security council to prioritize, track and evaluate global security policies and procedures.

Obviously, today's contact center security environment is more complicated than ever before. Threat risks are morphing and evolving rapidly. We strongly believe that with a comprehensive, holistic approach to contact center security, enterprises can begin to truly protect themselves from brand damage, financial liability and massive losses.

> ***"A truly effective contact center security program is proactive in not only understanding the current threat environment, but also detecting what kind of fraud insiders will commit in the future."***
> *Frost & Sullivan*

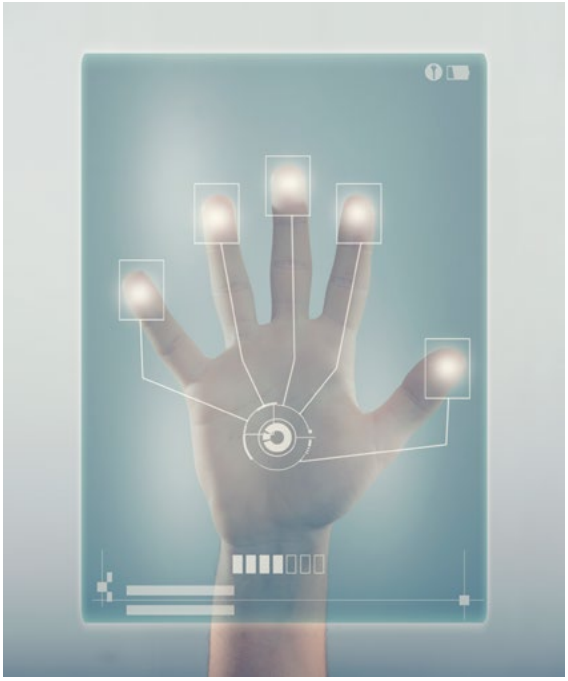
FRAUD PREVENTION

Certifications are Not Enough!

Consider this: Security certifications are certainly important, but 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"
   a. ID card, security token, passwords, retinal pattern recognition
   b. Voiceprint, fingerprint, RFID, biometric identification, keystroke patterns
2. Track agent activity with technology across multiple sites and geographies
   a. Educate continually and document individual compliance
   b. Record 100% of calls and log screen activity
   c. Monitor physical access and egress controls and reports
   d. Use video surveillance CCTV cameras to detect suspected fraud and provide proof for fraud prosecution
   e. Use technology to detect and track non-conformance outliers

Using information the agent "knows" in combination with verifying who they "are" provides a much more secure environment in the enterprise. For example, the ability to compare and verify a voice sample with a video feed of the individual significantly increases the likelihood that the right person is attempting to access a customer account within the context of the transaction.



Agent fraud is the proverbial "bad penny." It shows up in the most unlikely places. In effect, we have to expect and look for agent fraud. An extension of this is now coined "cyber hunting." It means finding malicious activity and vulnerabilities before any harm can be done. These specialized security analysts, or cyber defenders, have to think like attackers and effectively block avenues of attack. It is much more than behavior analytics and anomaly detection.

Andrew Nanson, chief technology officer of Corvid, says, "Hunting is the most effective way of detecting compromise because if organizations hunt instead of sitting back and waiting for something to advertise that an attack is under way, then they are being proactive rather than reactive, potentially reducing the window of opportunity for attackers."[2]

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 it provide other references 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 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 US 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 two to five years?

With which technology firm does the company partner? 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?

Industry Best Practices

The following is a short list of contact center security best practices. This has been provided to Frost & Sullivan courtesy of the certified professionals at SecurityMetrics—a leading provider and innovator in data security and compliance for organizations worldwide (www.securitymetrics.com):

- Each campaign should be segmented from all other campaigns. This includes both the data and VOIP networks. At the very least, any campaign involving credit cards must have its data and VOIP segmented from all other campaigns. In this case, segmentation means that there should be NO access from one campaign to another.

- If at all possible, recording credit card data (account numbers (PAN), CVV numbers, expiration dates) should be avoided. CRM systems can be integrated to call recording servers so that when an agent goes to the field to enter a card number, the recording is stopped and starts again once the agent clicks to another field or page. If it is not possible to stop the voice recording and credit card data is recorded, call recordings must be securely encrypted following the principles in the Payment Card Industry (PCI) Data Security Standard section 3. Access to call recordings containing card data must be on a need-to-know basis. Access to the calls must be recorded in audit logs. Log entries must include an identification of the individual accessing the call recording.

- All unnecessary applications must be removed (or disabled) on the call agent's systems. Agents should not be able to save files (.doc, .xls, .txt, etc.) or use chat, social media, or email *unless* there is a valid business need related to the campaign. If email is required only for corporate use, it should be restricted to corporate email addresses so that the agent cannot email outside addresses.

- Agent Internet use must be limited to only the sites needed for the campaign. Agents should not be able to browse the Internet or use Internet email such as Gmail, etc.

- A strict clean desk policy should be in place. Agents should be required to place all belongings, including electronics (phones, tablets, cameras, etc.), books, notebooks, etc., in lockers prior to entering the call floor. Some call centers have even stricter rules and do not allow private electronics in the facility. Employees are sometimes required to go through metal detectors or are subject to bag checks before entering the facility. Only registered electronics, for example, a company-owned laptop, are allowed. If agents need to write down information during a call, a small white board is the best option. If paper must be used, it should be shredded after the call.

- Agents logging into workstations, CRM systems, and any tool used to collect sensitive data (e.g., credit card data) must use unique account names and passwords so that all actions taken can be traced to an individual.

- A strong software update process must be in place to verify that all applications are being updated and patched against known vulnerabilities. This should be managed by a system that can track the computers and verify software versions. Manually patching software on call center workstations always seems to prove ineffective, and companies often default to updating software "when the customer requests it."

CONCLUSION

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. This is no small feat when considering the fact that the "threat from within" may be actually greater than the harm that outside hackers could inflict on an enterprise.

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 to supporting and embracing security as not only "the right thing to do," but also a competitive advantage for the future.

References

1. Upton, David M. and Creese, Sadie. "The Danger from Within," The Harvard Business Review, September 2014.

2. "Cyberhunting: A Critical Component of Enterprise Security," published by Techtarget and sponsored by Infocyte.

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 more than 40 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.

NEXT STEPS

Schedule a meeting with our global team to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

Visit our **Digital Transformation** web page.

Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

SILICON VALLEY
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

SAN ANTONIO
7550 West Interstate 10
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

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
3211 Scott Blvd
Santa Clara CA, 95054