



THE STATE OF DATA SECURITY IN CONTACT CENTRES

Analysis by

semafone
securing data • protecting reputations

Contents

Introduction	3
Executive Summary	4
Data Collection and Customer Interaction	8
Pause and Resume	8
Reading Numbers Aloud	9
Using Interactive Voice Response (IVR) Systems	9
Sharing Data Through an Online Chat Window	9
Entering Data into the Telephone Keypad	9
Breach Attempts & the Threat Landscape	10
Insider Threats	10
Unnecessary Access to Data	11
Unauthorised Access to and Sharing of Data	12
Outsider Threats	14
Small Numbers Add Up to Big Risks	15
Handling Breach Attempts	16
What Data is Most at Risk?	17
Geographical Variations	18
The European Threat Landscape: Where the Contact Centre Risks Lie	20
Industry Findings	24
Security Measures: How are Contact Centres Currently Protecting Customers' Data?	27
The Drawbacks of These Security Measures	28
How Contact Centres Can Secure Customer Data & Reduce Risk	29
Descope the Contact Centre: They Can't Hack Data You Don't Hold	31
DTMF Masking Technology	31
Problems Solved by Descoping	32
Conclusion	33

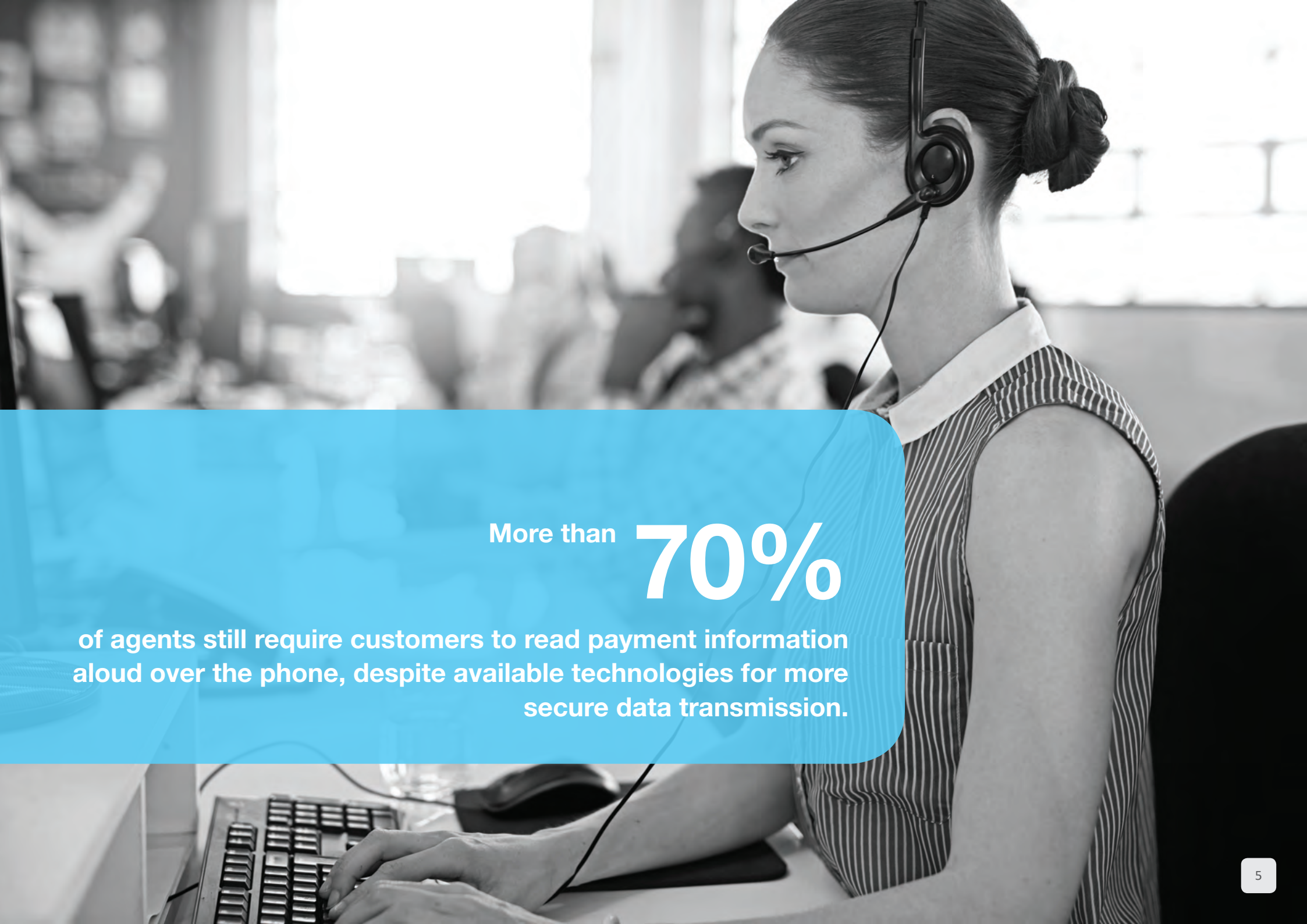
EXECUTIVE SUMMARY

This survey shows that a concerning number of contact centres continue to rely on outdated, risky practices for customer interaction, data collection and fraud prevention. For example, more than 70% of agents still require customers to read payment information aloud over the phone, despite available technologies for more secure data transmission. At the same time, a disconcerting number of agents have been approached directly by company insiders and/or outsiders to share customer information.

Survey findings emphasise the urgency for contact centres to secure all sensitive data and reduce the risk of brand-damaging data breaches. Current security measures, such as the use of clean rooms (no writing utensils, paper, phones or bags) and checkpoints for agents are not enough. While there is reason to believe that not all agents have fraudulent intentions, it is important to understand that it takes just one malicious person – coupled with poor data security – to send an organisation into a downward spiral.

Recommended solutions for mitigating contact centre security risks include: more robust incident management policies; proper access controls for computer systems; tokenisation technologies that replace data with a meaningless equivalent; and dual-tone multi-frequency (DTMF) masking technologies that shield data from agents as customers enter it into their telephone keypads.

However, the best way to protect customer information, deter fraud and safeguard a company's reputation is to remove sensitive data completely from the contact centre environment.

A black and white photograph of a woman in a call center. She is wearing a headset with a microphone and is looking down at a keyboard. The background is blurred, showing other people in the office. A blue semi-transparent box is overlaid on the left side of the image, containing white text.

More than **70%**

of agents still require customers to read payment information aloud over the phone, despite available technologies for more secure data transmission.

Key statistical findings from this survey include:

Contact centres still rely on outdated and risky data collection and customer interaction practices.

72%

of agents who collect credit or debit card information over the phone said they still require customers to read payment card numbers out loud, despite the readily available technologies that secure voice transactions

30%

of agents reported that they have access to customers' payment card information on file even when they're not on the phone with the customer

Agents are experiencing and witnessing breach attempts from both insiders and outsiders, yet many do nothing to mitigate the risks.

7%

of agents admitted that someone *inside* their organisation had asked them to access or share customers' payment card information or other sensitive data

4%

said the same about someone *outside* their organisation

9%

said they personally know someone who has unlawfully accessed or shared customers' payment card information

42%

of agents who were approached said they did not report the situation

Contact centres aren't doing enough to protect customer data.

26%

of agents said they work in a contact centre “clean room,” which prohibits personal items and recording devices of any kind

38%

of agents are not allowed paper or pens at their work station

31%

of agents are not allowed personal items or bags at their work station

28%

of agents are required to pass through a security check before entering or leaving work

Industry and geographical trends are apparent.

0

European agents reported instances of outsiders approaching agents to share information – likely reflective of Europe's stricter governance rules

35%

of agents in the Business Process Outsourcing (BPO) industry have access to customer information when they aren't on the phone with them; and **11%** said an insider had approached them to share customer information

50%

of agents in Central and South America have access to customer data when they aren't on the phone with the customer. These regions also had the highest number of requests to share data

The above findings point to increased risks due to outsourcing and offshoring, making strong data security even more important for contact centres with such business models.

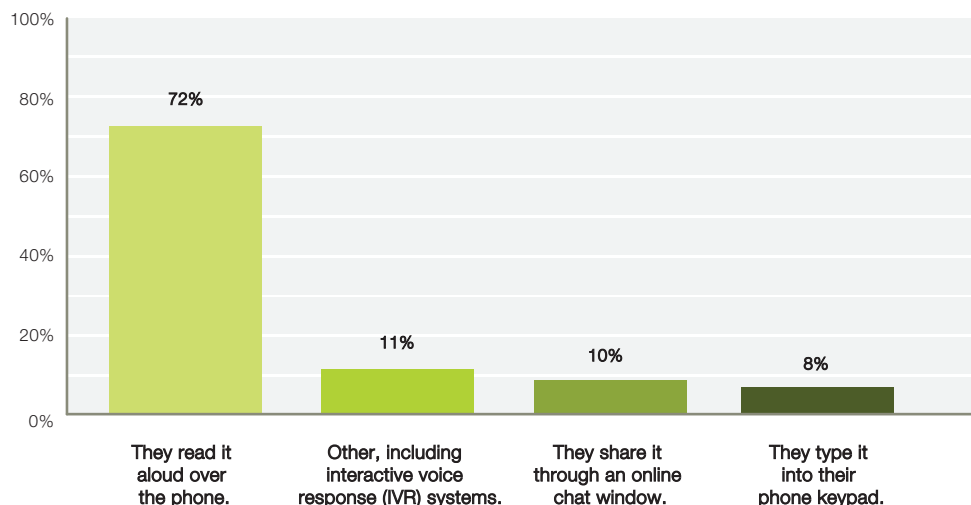
Data Collection and Customer Interaction

In response to this survey:

- **55%** of agents said that customers share credit or debit card information with them over the phone
- **36%** said that customers share that information via the Internet

Yet, some of the methods used by contact centres to gather customers' PII raise even greater concerns.

Figure 1. **How does the customer share their payment card information with you?**



Pause and Resume

When customers read their card numbers aloud, it creates additional challenges for organisations that record calls for legal, regulatory or quality assurance reasons. For example, the Payment Card Industry Data Security Standard (PCI DSS)¹, which provides guidelines for securing payment card data, prohibits the recording of sensitive authentication data (SAD), such as three-digit security codes, including CID, CVC2 and CVV2.

Many contact centres use a practice called “pause and resume” or “stop/start” to manually or automatically block payment card data from call recordings.

However, these practices create gaps in an organisation's data management strategy:

1. If an agent forgets to pause the call, SAD and other PII may be inadvertently captured, putting the call recording back in scope for compliance purposes and leaving the information vulnerable should there be a data breach.
2. If an agent forgets to resume the call recording, vital information may be excluded that is needed to solve transaction disputes or support quality control.
3. With an incomplete call recording, a company may not be able to demonstrate compliance with industry or state/government regulations.

¹ “PCI Security Standards Council Document Library,” Payment Card Industry Security Standards Council (PCI SSC): https://www.pcisecuritystandards.org/document_library



Reading Numbers Aloud

72% of agents who collect credit/debit card information over the phone said their companies still require customers to read payment card numbers aloud (Figure 1). This poses numerous security and compliance risks, as the information is exposed to the agent on the line, as well as nearby eavesdroppers. The information could easily be copied down for fraudulent use.



Sharing Data Through an Online Chat Window

10% of agents said they capture customer information through a chat window. Although data is not verbalised in these cases, many of the same challenges experienced with live caller-agent engagements exist:

1. The contact centre agent is still exposed to sensitive data through the chat window.
2. The merchant must prevent the storage of data on the desktop computer, CRM system and the webserver that hosts the chat application in order to secure the payment.
3. The contact centre must implement an efficient, accepted and appropriate method to encrypt the payment session within the chat engagement.

The problem lies in the fact that basic chat functionality is just an “instant messenger” program that was not designed for encryption. While there are chat applications that offer secure connections, extra data protection measures are required, such as pre-exchanged passwords and security keys.



Using Interactive Voice Response (IVR) Systems

11% of agents said that they use “other” methods of collecting payments, including interactive voice response (IVR) systems. These automated telephony systems interact with callers to shield PII from agents, but they create their own set of issues. Without an agent on the line, customers often don’t know how to correct miskeyed information, which can result in ended calls before the transaction is complete. This poor customer experience can impact important contact centre metrics like first contact resolution (FCR) and average handling time (AHT). Additionally, by having the customer hang up prematurely, the organisation loses a potential sale.



Entering Data into the Telephone Keypad

8% of agents said customers provide information by typing it into their phone keypad. This approach may involve using dual-tone multi-frequency (DTMF) masking secure payment technologies. DTMF masking solutions allow customers to directly enter payment card numbers into their keypad. Neither the agent on the line nor anyone listening to the call recording can decipher the numbers, as the DTMF (keypad) tones are masked with flat tones, and PII or payment card data never enters the contact centre IT infrastructure.

Breach Attempts & The Threat Landscape

While contact centre data security threats come in many shapes and sizes, most can be categorised as “insider” or “outsider” threats. The survey indicated that both types of threats are prevalent in the contact centre, and that a concerning number of agents have been involved in some way.

Insider Threats

Company insiders account for approximately

50%

of security incidents², and more than

7,700

insider incidents (277 with confirmed data disclosures) were reported in 2016 alone.³



Suspect 1: Opportunistic Oscar, The Tempted Temp

The situation: To accommodate high-volume periods like Christmas or sale days, contact centres frequently hire temporary or seasonal employees. These staffers can pose an added insider fraud risk, whether due to lax employee screening practices or a lack of loyalty to the employer.

The crime: Oscar lands a temporary position in a retail contact centre to make some extra money during the holiday season. After taking a few calls, he realises that customers are reading him their credit card numbers without hesitation. Thinking no one will notice, Oscar starts writing down callers' card numbers and is even successful in obtaining some CVVs

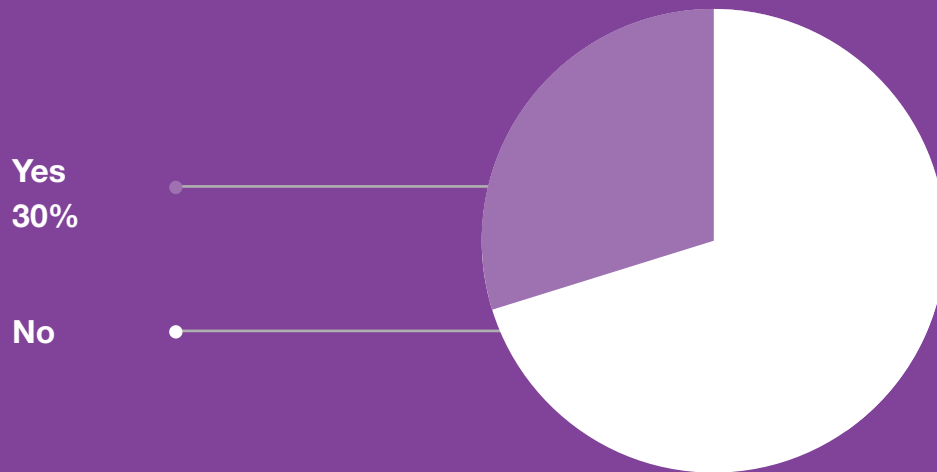
and expiry dates. As a temporary employee with no loyalty to the company, he thinks he has very little to lose. Oscar goes home with his newfound information and begins his online shopping spree.

The lesson: Whether or not Oscar gets caught, this situation demonstrates that it can take just one agent to jeopardise customer data. It also shows the importance of investing in more thorough data security processes – for example, shielding payment information and other PII from agents. Relying on recruitment protocols to weed the “good” agents out from the “bad” is not enough, especially when it comes to temporary employees.

² “World’s oldest hacking profession doesn’t rely on internet,” by Maggie Overfelt, CNBC, May 13, 2016: <http://www.cnbc.com/2016/05/13/a-surprising-source-of-hackers-and-costly-data-breaches.html>

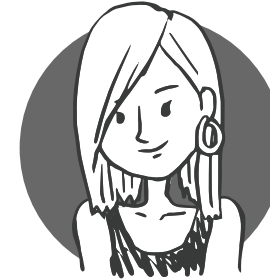
³ “2017 Data Breach Investigations Report,” Verizon: <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

Figure 2. Do you have access to customers' payment card information on file even when you're not on the phone with the customer?



Unnecessary Access to Data

30% of agents said they have access to customers' payment card information on file even when they're not on the phone with the customer (Figure 2). This means that customer information is not only available to "rogue" agents for malicious use, but is also susceptible to a data breach due to accidental or negligent behavior. For example, an agent may open a phishing email or plug in a thumb drive that's infected with a Trojan. Or, an agent could forget to log out of his or her desktop, leaving sensitive information exposed to prying eyes.



Suspect 2: Unfortunate Ursula, The Credulous Clicker

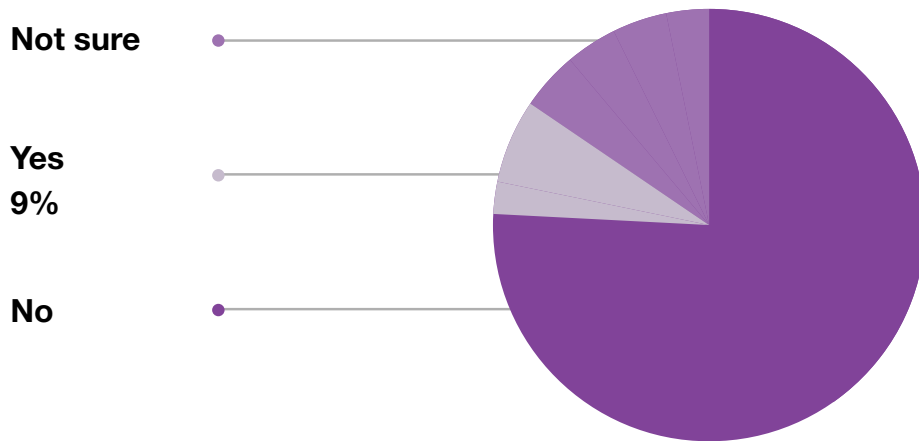
The situation: Not all fraudsters are malicious. Even the most trustworthy employee can accidentally expose sensitive customer data, especially if the data resides within the contact centre environment.

The crime: Ursula, a diligent customer service representative, is responding to customer emails, resolving complaints, answering questions and facilitating account changes. She comes across an email from a customer claiming to have received a damaged product, including a photo in an attached file as evidence of the damage. Ursula clicks on the attachment, which installs a malicious worm that spreads across the contact centre's

IT network, stealing customers' data. Once the virus infection is detected, the company makes front page news for suffering a major data breach. In the coming weeks, the company's stock prices drop and customers take their business elsewhere.

The lesson: To prevent the damage caused by a well-intentioned employee who falls victim to a targeted outsider attack, businesses must properly train their staff on the dangers of phishing and social engineering tactics. Contact centres should educate their employees on what to look for and what to do in such a situation. A combination of staff training and removing sensitive data from business infrastructure is crucial.

Figure 3. Do you personally know anyone in your industry who has accessed or shared customers' payment card information when they're not supposed to?



The survey findings highlight many illicit behaviors that are contributing to the increasing insider threats posed to organisations.

Unauthorised Access to and Sharing of Data

9%

of contact centre agents surveyed said they personally know someone in their industry who has accessed or shared customers' payment card information without authorisation (Figure 3). Similarly, **7%** said they had been asked by someone inside their organisation to access or share customers' payment card information or other sensitive data (Figure 4). **2%** said that they had been offered a payment to share this information.



Suspect 3: Disgruntled Daisy, The Vengeful Victim

The situation: Although an agent may not be the mastermind behind a fraud operation, there are others inside the contact centre's organisation who may have malicious intentions. The catalyst for a data breach can come down to three simple things: a disgruntled employee, an accomplice with access to customer data and a bribe.

The crime: Daisy has worked at a contact centre for 10 years and is dissatisfied with management. While she no longer directly works with customers, she has many colleagues who are employed as agents. Daisy offers to pay one of her colleagues £100 in exchange

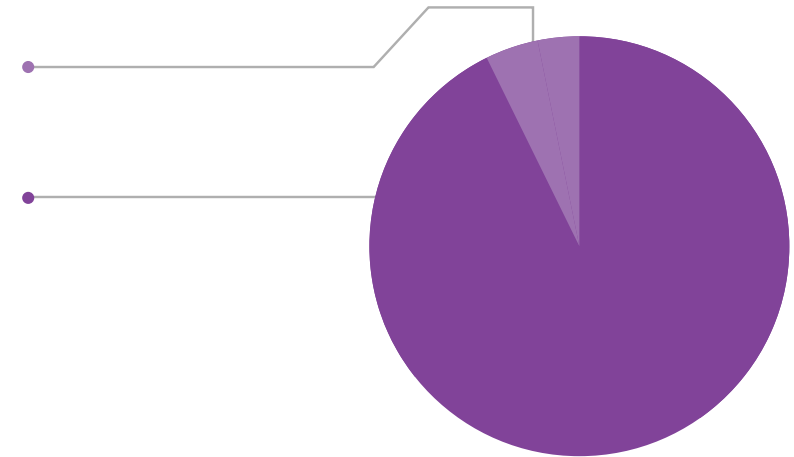
for customer payment card data. She justifies her fraudulent activity as compensation for her years of being underpaid and underappreciated. From her perspective, the theft won't hurt anyone, as most customers have fraud insurance.

The lesson: One angry employee can put all customers in danger of identity theft and fraud. Companies must keep PII out of the contact centre environment if they are to also keep it out of the hands of malicious insiders.

Figure 4. **Has anyone inside your organisation ever asked you to access or share customers' payment card information or other sensitive data?**

Yes
7%

No



Despite these alarming findings, it is important to note that most contact centre agents are actually good, honest and trustworthy people. The adage, “good guys must be right every time, but the bad guys only need to be right once,” applies here.

With poor data security, it takes just one successful hacker or fraudster to offset the positive work of a typical agent.

Outsider Threats

Rogue agents and malicious insiders are not the only ones putting customer data at risk. Research shows that outsider security threats have increased by as much as 300%⁴.

Figure 5. **Has anyone outside your organisation ever asked you to access or share customers' payment card information or other sensitive data?**



4% of agents confirmed that someone outside the organisation had asked them to access or share customers' payment card information or other sensitive data (Figure 5). In addition, **2%** said they had been offered a payment to share or to allow an outsider to access this information.

Although **4%** is a relatively low figure, it is likely that there is a significant number of incidents that go unreported or unnoticed. The use of social engineering tactics makes it particularly difficult to detect attempts to manipulate agents into providing customer information. In fact, **60%** of enterprises⁵ fell victim to at least one targeted social engineering attack in 2016, and financial accounts were breached in **17%** of those attacks.



Suspect 4: Scheming Steve, The Secret Cyber-man

The situation: Employees aren't the only ones who expose or access sensitive data, whether maliciously or accidentally. Contractors, IT support and other third parties who regularly come in contact with agent desktops also pose an often-overlooked risk.

The crime: Steve is an IT contractor who is learning how to hack into IT systems for fun. His intent is mostly harmless. However, one of Steve's clients is a contact center for a bank. Realising how much personal information the contact center holds, Steve decides to put his hacking skills to the test. While fixing an agent's computer, Steve discretely inserts a keyboard, video and mouse (KVM) switch into

the back of the machine. These unassuming devices allow users to control multiple computers remotely. From his home computer, Steve can now hack into the contact center's network and access customer accounts. With this information at his fingertips, he could easily steal thousands of pounds.

The lesson: Any data stored within the contact center infrastructure is vulnerable, and hackers will take advantage of every opportunity to access this data illegally. The most effective way to protect this data is to ensure it's not stored in the first place.

⁴ "Malicious outsider data breaches up nearly 300%," by Bob Violino, Information Week, March 30, 2017: <https://www.information-management.com/news/malicious-outsider-data-breaches-up-nearly-300>

⁵ "60% of enterprises were victims of social engineering attacks in 2016," by Roi Perez, SC Magazine UK, November 30, 2017: <https://www.scmagazineuk.com/60-of-enterprises-were-victims-of-social-engineering-attacks-in-2016/article/576060/>

Small Numbers Add Up to Big Risks

While the aforementioned statistics are seemingly small numbers, when applied to the larger contact centre agent population globally, the risk is significant.

Consider this: there are approximately 2.2 million contact centre agents in the U.S. alone⁶. Based on the survey findings, it is possible that close to 150,000 active agents in the U.S. have been asked to share sensitive customer and payment data by others within their company; and more than 85,000 agents may have been approached by an outsider to share information.

Moreover, the damage resulting from a successful breach can be devastating. The average consolidated total cost of a single data breach is £2.5 million, according to IBM's 2017 Cost of a Data Breach Study⁷. This figure takes into account more than just financial losses and customer compensation, but also the reputational damage, legal fees, auditing services and more.

The average consolidated total cost of a single data breach is £2.5 million, according to IBM's 2017 Cost of a Data Breach Study.⁷

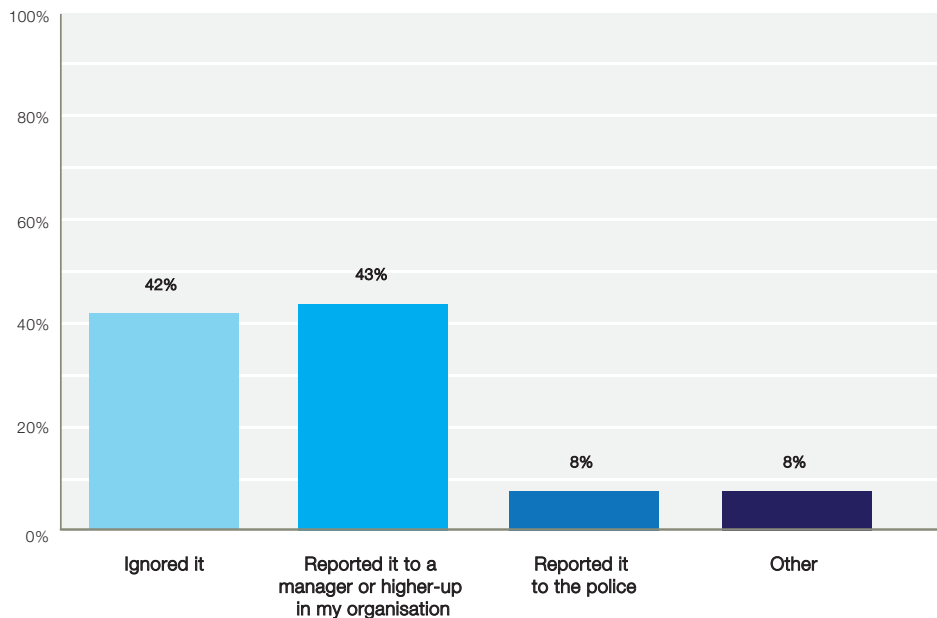
⁶ "How Big is the U.S. Call Center Industry Compared to India and The Philippines?" by King White, Site Selection Group, February 17, 2015: <https://info.siteselectiongroup.com/blog/how-big-is-the-us-call-center-industry-compared-to-india-and-philippines>

⁷ "2017 Cost of Data Breach Study," IBM: <https://www.ibm.com/security/data-breach/>

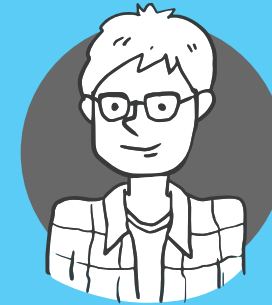
Handling Breach Attempts

Of agents who have been asked to share data, only **43%** notified a manager or supervisor of the situation and **8%** reported the attempt to the police (Figure 6).

Figure 6. **If you experienced a potential breach by an insider and/or outsider, what did you do about the situation?**



Alarming, **42%** said they did not report the incident, indicating that a sizeable number of data breach attempts go unnoticed by an organisation.



Suspect 5: Conniving Carl, The Contract Cleaner

The situation: When sensitive data is stored in the contact centre, it is susceptible to being stolen by anyone who has easy access to the IT system – even someone as unassuming as a maintenance operative or a cleaning crew.

The crime: Three times a week, Carl works as a janitor at a large corporate building where he has unrestricted access to every floor and office. One of the tenants is a contact centre and Carl learns that the computer system stores large amounts of customer information. While cleaning the office, Carl slips a thumb drive containing malware into several computers. Over the course

of the next week, the malware captures detailed information of all customer transactions, including payment card numbers. Carl returns the following week to remove and collect the thumb drives, which have gone completely unnoticed.

The lesson: Third parties with access to the contact centre pose significant risks when sensitive data is available. Removing the data from the business and IT environment can avoid this risk and protect customers' information.

What Data is Most at Risk?

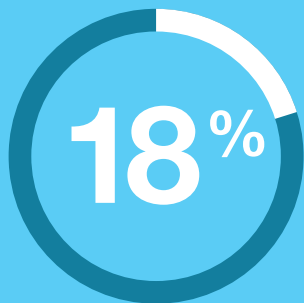
Of the agents who had been approached by someone inside or outside their organisation to share customer information:



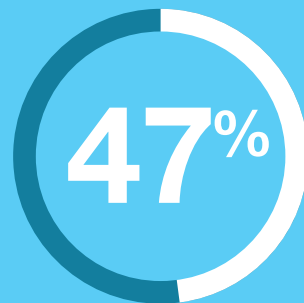
were asked for payment card data



were asked for medical/health records

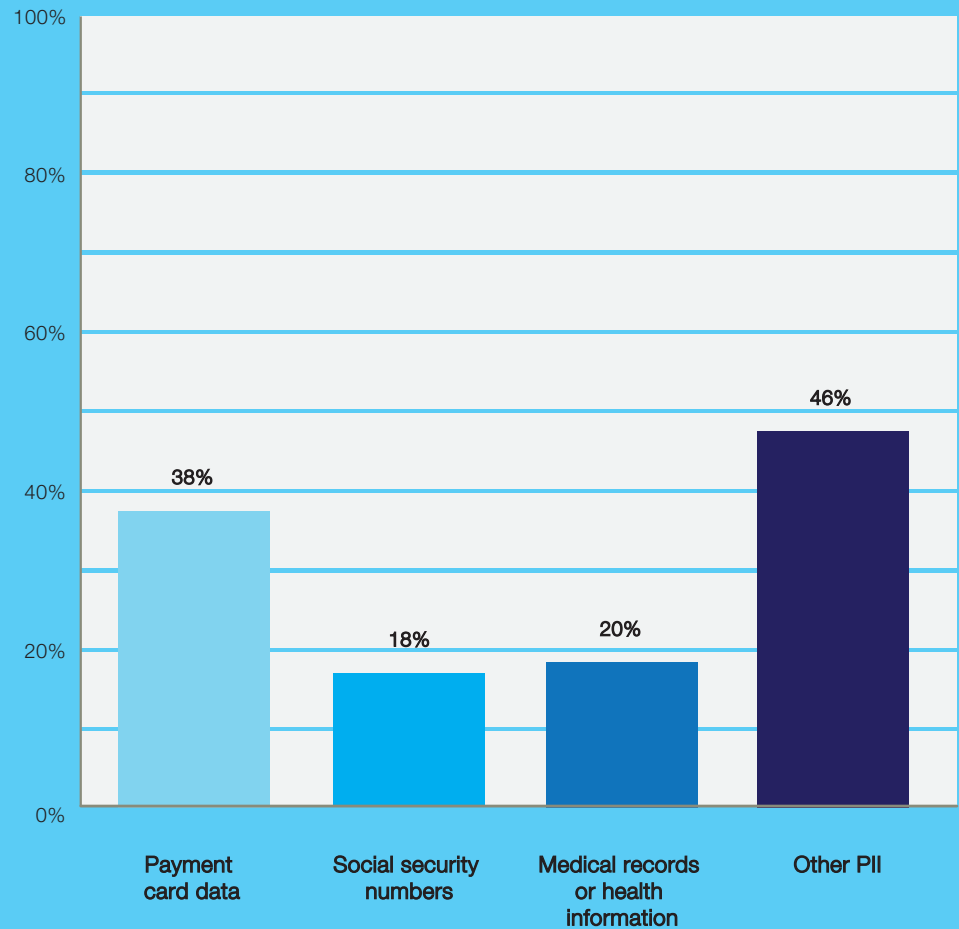


were asked for SSNs



said they were asked for "Other PII," which includes customer names, contact information, etc. (Figure 7)

Figure 7. What type of information were you asked to access or share?



Geographical Variations

The survey gathered responses from contact centre agents around the world. Participant breakdown is as follows (Figure 8).

Figure 8. Which region do you live in?

North America 40%

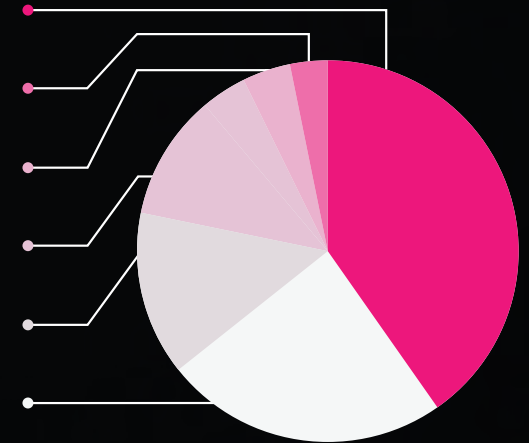
South America 3%

Central America 4%

Europe 14%

Africa 14%

Asia/ Pacific Islands 24%



Some Significant Geographical Statistics Emerged:



North America had the highest percentage of agents whose customers provide payment card information and SSNs over the phone **(70%)**. It also showed the third-highest percentage of agents who have access to customer information when they are not on the phone with them **(31%)**.



In Central America and South America, **50%** of agents said they had access to customer SSN or payment card information when they aren't on the phone with the customer. This is a matter of concern, given that the agents in these areas also had the highest number of requests from both insiders and outsiders to share customer data. Central America also had the highest percentage of agents who were offered a monetary bribe to share sensitive data **(10%)**.



Asia reported a high threat level and ranked third in percentage of agents approached by insiders and outsiders to share customer information **(13%)**. However, only **35%** of agents in Asia said they take customer payment information over the phone.



Europe emerged with the least apparent risk, however, **16%** of agents still reported having access to sensitive information even when not on the phone with the customer.

The European Threat Landscape: Where the Contact Centre Risks Lie

The report findings indicate that Europe is ahead of the rest of the world when it comes to protecting against contact centre data security threats. However, in the face of an increasingly complex regulatory landscape, organisations across the continent will be required to implement even more rigorous data security frameworks in order to comply with not only the PCI DSS, but also impending regulations such as the EU GDPR. The new European law will carry with it some of the largest fines of any data protection legislation - stipulating a financial penalty of €20 million or **4%** of global turnover - whichever is higher - for companies who fall foul of the regulation.

With such significant focus placed on securing citizens' private data, it follows that any company that suffers a data breach will also bear a bigger public backlash, and more serious damage to company reputation. The EU GDPR will also impose strict data breach reporting times, requiring companies to declare breaches within 72 hours, which means organisations will be unable to hide from the widespread negative publicity that comes with failing to secure customer data.





Looking at Europe as a whole, the region doesn't handle SSNs, which in the US are often used to steal a customer's identity. What's more, some parts of Europe - for example Germany and Sweden – use pay-by-bank methods and, as such, don't require card numbers to complete transactions. However, British consumers are conversely heavily reliant on payment cards; as of 2016, there were 51.5 million debit card holders and 32.3 million credit card holders in the UK⁸. The total volume of card payments is predicted to increase substantially over the next decade to 21.9 billion, with the total value of card payments projected to reach £942 billion⁸. As mail order/telephone order (MOTO) currently

represent almost 10 per cent of the value of all card transactions⁸, the need to secure consumers' sensitive data in the contact centre is even more apparent. This is especially true considering the report findings, which highlighted that 16 per cent of agents still have access to sensitive information even when not on the phone with customers. Payment card fraud is also rising dramatically in the UK; 2016 was the fifth consecutive year of increased losses, seeing £618 million in fraudulent card transactions⁹. It's clear that contact centres cannot afford to be complacent when it comes to securing customers' sensitive card data.

⁸ "UK Card Card Payments 2017", 31 December 2016, http://www.theukcardsassociation.org.uk/wm_documents/UK%20Card%20Payments%202017%20%20website%20FINAL_.pdf

⁹ "Fraud the Facts 2017: The Definitive Overview of Payment Industry Fraud", 2017, https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf

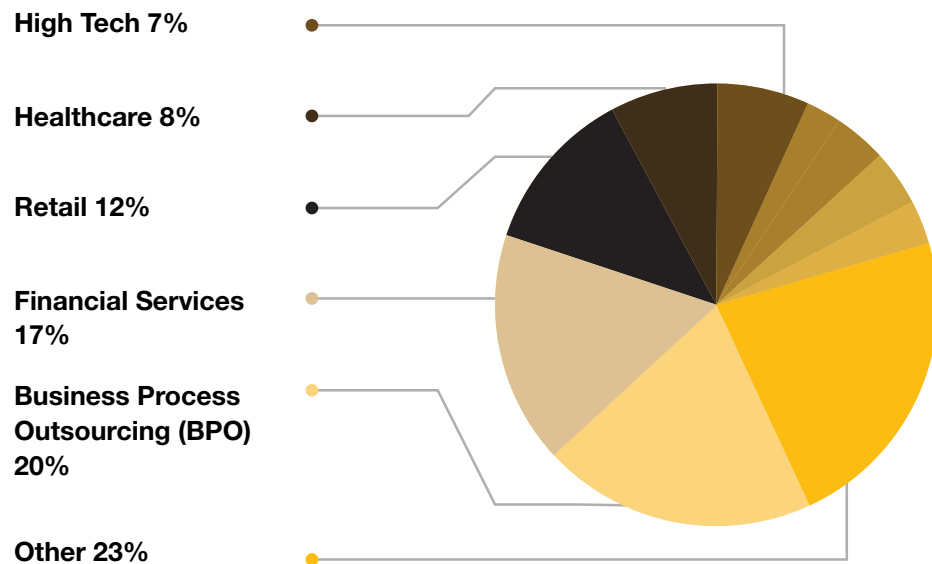


The use of **risky, outdated**
contact centre practices
– including having **customers read**
payment card numbers aloud
– is common around the world.

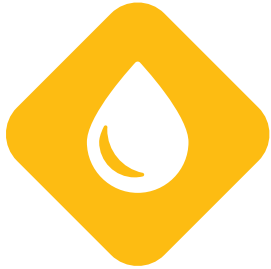
Industry Findings

In addition to a geographically diverse group of participants, this survey generated responses from contact centres in many different industries (Figure 9).

Figure 9. **What industry is your company in?**



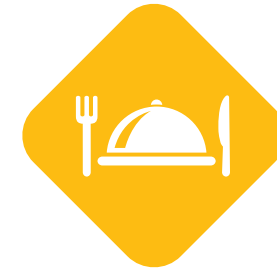
Key Findings by Industry:



The Utilities industry not only had the highest percentage (**75%**) of customers providing credit/debit card information over the phone, but also had the highest percentage of agents (**11%**) who said they personally knew someone who had unlawfully accessed customer information.



Business Process Outsourcing (BPO) was another industry with high percentages across the board. More than **35%** of agents said they have access to customer information when they aren't on the phone with them; **11%** said an insider had approached them to share customer information; **3%** had been offered a bribe; and **10%** said they personally knew someone who had unlawfully accessed sensitive data.



In the Hospitality industry, **42%** of agents said they have access to customer information when they are not on the phone; and more than **10%** of those agents had been approached by an outsider to share this information.



Despite the Healthcare industry ranking second in number of 2016 data breaches,¹⁰ it was the only industry in this survey whose agents did not say an outsider had attempted to obtain customer information from them.



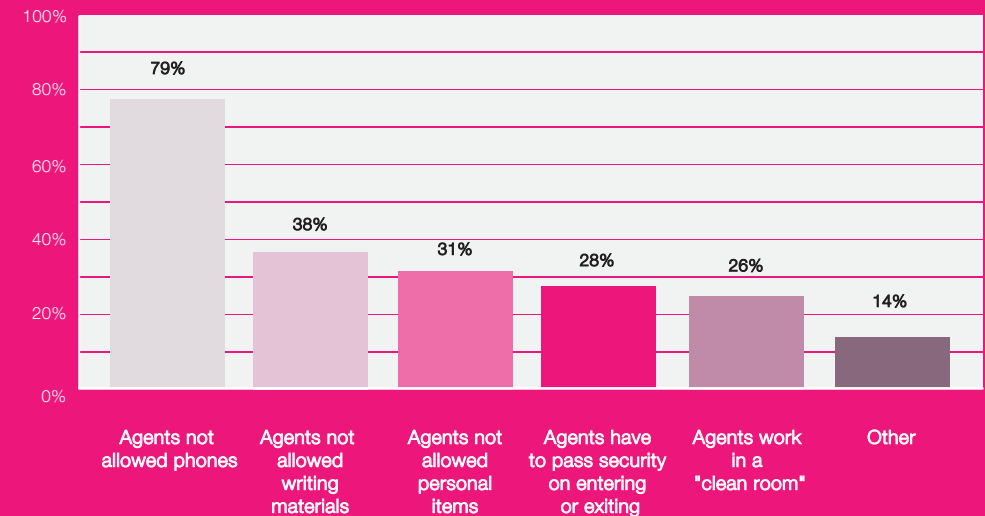
Agents in Government had the second-highest percentage of agents approached by insiders to share customer information (**9%**) and third-highest approached by outsiders (**5%**).

¹⁰ "The ITRC 2016 Data Breach Report," Identity Theft Resource Center: http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf

Security Measures: How are Contact Centres Currently Protecting Customers' Data?

To conclude this survey, participants were asked about the types of security controls their organisation has in place to prevent contact centre agents from taking customer data (Figure 10).

Figure 10. What type of security controls does your organisation have in place to prevent contact centre agents from taking customer data?



The most common security method encountered was prohibiting of cell phones at agents' work stations **(79%)**, followed by:

- Banning agents from having writing materials **(38%)**
- Barring personal items/bags **(31%)**
- Requiring agents to pass through a security scanner or checkpoint upon entering or leaving **(28%)**
- Working in a contact centre "clean room," which forbids personal items and recording devices of any kind, as well as requiring strict security checks **(26%)**

With a turnover rate of more than 20 per cent for agents in the UK,¹² retaining employees is already a challenge for contact centres.

The Drawbacks of These Security Measures

Draconian measures to control the actions of contact centre employees can be effective for protecting sensitive data, but can also negatively impact employee morale. In fact, they can raise operational costs and lead to increased staff turnover. Furthermore, if customer payment information is read out loud, agents are still able to hear it and are sometimes required to enter it into a computer. The information may also end up on a call recording, whether intentionally, as the result of human error, or due to a failure in the pause and resume system. Regardless of workspace restrictions, sensitive customer data still touches various CRM systems and desktop applications.

¹² "The UK Contact Centre HR & Operational Benchmarking Report 2016/17" by ContactBabel, September 2016, <http://www.contactbabel.com/pdfs/jan2017/UK-HROB-Marketing-v3.pdf>

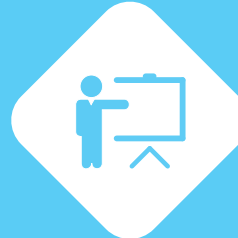
How Contact Centres Can Secure Customer Data & Reduce Risk

It is impossible to predict and prevent every potential breach, but there are a number of steps contact centres can take to reduce risk and keep customer data safe. The following best practices will help mitigate many of the risks unveiled in the survey findings – including the use of outdated data collection practices, agent exposure to sensitive data, insider and outsider breach attempts and the use of draconian security measures:



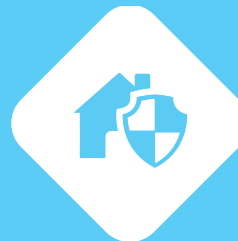
1. Treat all data as toxic

With cybercriminals and fraudsters seeking a wide range of data (from credit card numbers, to birth dates) contact centres must treat all PII as toxic. The more information that is vulnerable in the case of a breach, the easier it will be for a criminal to steal a customer's identity, drain their bank account, access their private medical records and more. For the victim, resolving an incident of identity theft is especially distressing, expensive and time consuming.



2. Properly train (and vet) employees

Contact centres should take time to properly train and educate agents on the very real dangers of insider- and outsider-caused data breaches. For instance, they should create awareness surrounding social engineering tactics and advise agents to report suspicious activity to a supervisor. Also, hiring “good people” is not enough. Conducting thorough background checks, even for temporary employees, is a valuable step.



3. Implement an incident management policy

Contact centres should have an incident management policy and/or process in place, preferably as part of an Information Security Management System. It is wise to prepare for a worst-case scenario and have a documented Incident Response Plan that is tested at least annually.



&%?!^*
"£:@\$&

4. Fight social engineering with tokenisation

Humans aren't error proof, so contact centres should use technology to assist in the event of a social engineering attack. One ideal method is to use tokenisation to replace data with a meaningless equivalent. Even if a breach is successful, the available data will be of zero value to the cybercriminal.



5. Enforce the principle of least privilege

When possible, use the principle of least privilege on computer systems. This will give employees the minimum level of access required to perform their job function at the appropriate time. So, if the agent doesn't need to view customer credit card data when a phone transaction isn't taking place, for example, they shouldn't have access.



6. Authenticate the user to authenticate the agent

This simple approach essentially prevents agents from having access to customer data until the agent has received the right data from the user. This means that until the caller has been successfully identified using the appropriate secure authentication approach, access to detailed PII is denied.

While incident management plans and employee training sessions are great, they only go so far.

Descope the Contact Centre: They Can't Hack Data You Don't Hold

While incident management plans and employee training sessions are great, they only go so far. The crux of the situation is that sensitive data is being exposed to agents, held in various business systems and captured on call recordings – just waiting to be compromised. The only way to truly reduce risks is to remove sensitive data from the contact centre environment, completely. After all, they can't hack data you don't hold. But, how?

DTMF Masking Technology

Using dual-tone multi-frequency (DTMF) masking technology is one of the most effective ways for contact centres to de-scope their environment (or, to significantly reduce the number of applicable PCI DSS controls). Such technologies allow customers to enter payment card information and other PII directly into the telephone keypad. DTMF tones are masked with flat tones, so the agent on the line, the call recordings and any eavesdroppers are unable to decipher the numbers. The agent can remain in full conversation with the customer throughout the call, assisting with any issues and completing wrap-up tasks, thus enhancing the customer experience, and even improving first contact resolution (FCR) and reducing average handling time (AHT). Once information is entered into the telephone keypad, it is sent straight to the appropriate third party (like a payment processor), bypassing the contact centre's infrastructure altogether.



Problems Solved by Descoping

By descoping the contact centre environment, organisations can solve the challenges underscored by the survey results. Descoping enables the following:



Agents are no longer exposed to sensitive data, nor do they have access to customer PII when they are not on the phone with them. This reduces risks associated with “rogue” employees and social engineering tactics. Moreover, when approached by insiders or outsiders to share customer information, agents are unable to oblige.



PCI DSS compliance is dramatically simplified, allowing organisations to cut costs and focus on business as usual (BAU).



Customers do not need to read their card numbers aloud and have full control over inputting their data.



There is no need for clean rooms or excessively stringent security measures that jeopardise employee morale. A better working environment means happier, more productive employees and reduced turnover, which can translate to a better bottom line.



Sensitive data is not stored in the contact centre infrastructure, rendering hacking attempts (by both insiders and outsiders) useless.

About SemaFone

SemaFone is your contact centre data security and compliance expert. We work closely with enterprises around the world to remove sensitive data from IT and business networks – protecting your customers and your company reputation, while simplifying compliance with regulations like the Payment Card Industry Data Security Standard (PCI DSS). Our award-winning, patented data capture method allows contact centre agents and customer service representatives (CSRs) to securely capture personal information including payment card data, bank account details over the phone using dual-tone multi-frequency (DTMF) masking technology. Unlike interactive voice response (IVR) systems, agents remain in full voice communication with the caller as they enter their numbers into their phone keypad, ensuring a positive customer experience.

By conducting this survey of more than 500 global agents, we hope to raise awareness about the risks inside and outside today's contact centres – a part of virtually every business – and create a greater sense of urgency among the contact centre community for securing their data...and securing it *now*.



0845 543 0822



info@semafone.com



www.semafone.com



@semafone



Google+



LinkedIn



Pannell House, Park Street, Guildford, Surrey, GU1 4HN

