CASE STUDY

DELIVERING SECURITY AND COMPLIANCE TO LARGE PUBLIC SECTOR ORGANISATIONS

Sadly, data breaches and cyberattacks are becoming common place and are something that every organisation, regardless of its size, needs to be prepared against. It is crucial to make sure that systems and processes are in place to protect customer information and to ensure your organisation complies with the very latest data protection and security compliance guidance and regulations.

For public sector organisations or government departments, they are of course no different, although the reputational damage and financial consequences that a breach may have will be difficult to bear.

Ensuring adequate measures are therefore in place to safeguard data is a must, particularly when you take into consideration the significant amount of personal data these types of organisations hold on members of the public.

IS YOUR ORGANISATION PCI DSS COMPLIANT?

Developing and maintaining good data security procedures and policies is a relentless task. If you are taking credit card payments, the Payment Card Industry Data Security Standard (PCI DSS) is a good place to start the data security journey. PCI DSS also helps organisations stay ahead of the curve when it comes to the continually evolving pressures of handling information privacy.

PCI DSS has been designed to govern the protection and handling of sensitive cardholder data as well as also seeking to reduce payment fraud. While the standard applies to online customer service methods, it also includes more traditional approaches, such as telephone-based contact centres, which are the mainstay of public sector and governmental departments.

WHAT YOU NEED TO CONSIDER AS A PUBLIC SECTOR ORGANISATION

Becoming fully compliant with PCI DSS means dropping the use of compensating controls, a work-around introduced to give organisations an alternative to security requirements that could not be met due to legitimate technological or business constraints.

Research conducted by Verizon shows that the organisations that suffered a breach of security were more likely to be using compensating controls – for example using 'pause and resume' on call recordings when taking payment information over the phone.

PCI DSS version 4.0, to be released during 2021, does away with compensating controls all together, moving instead to a customised validation regime.

Over reliance on compensating controls significantly increases the security risks, potentially leading to fraud and breaches, and therefore organisations continue to face related risks to reputation, revenues and fines.

The first step is to identify how to stop your department or wider organisation being on a hacker's target list. So, whilst strong cyber perimeter defences are needed, it is also important to focus on encrypting your data. Minimise data storage wherever possible, ensuring there is no sensitive data for the hackers to steal in the first place. Descoping technologies can be used for payments handled via a contact centre, and so sensitive payment card data will never enter the enterprise and therefore the risk is removed.

Descoping technologies, if managed via cloud-based solutions such as PCI Pal's Agent Assist, integrate seamlessly with existing premise-based telephony and payment infrastructures. This creates no additional in-house IT burden or systems management headache for already-busy IT staff.

THE SOLUTION

Telephone-based payments are an intrinsic part of the service for public sector and government organisations, and while there are many independent departments, they all need to offer a consistent customer experience as an alternative payment method for those people not wanting to make payments online or by bank transfer.

PCI Pal's Agent Assist solution provides organisations with the ability to efficiently take payments over the phone, by enabling customers to input payment card information via their telephone keypads.

Agent Assist solution not only provides a seamless customer experience but allows contact centre agents' terminals to meet global standards for accessibility. This ensures that agents of all abilities can easily use the Agent Assist solution. These accessibility features include the ability to integrate Dragon dictation speech recognition and screen reading technologies, for example.

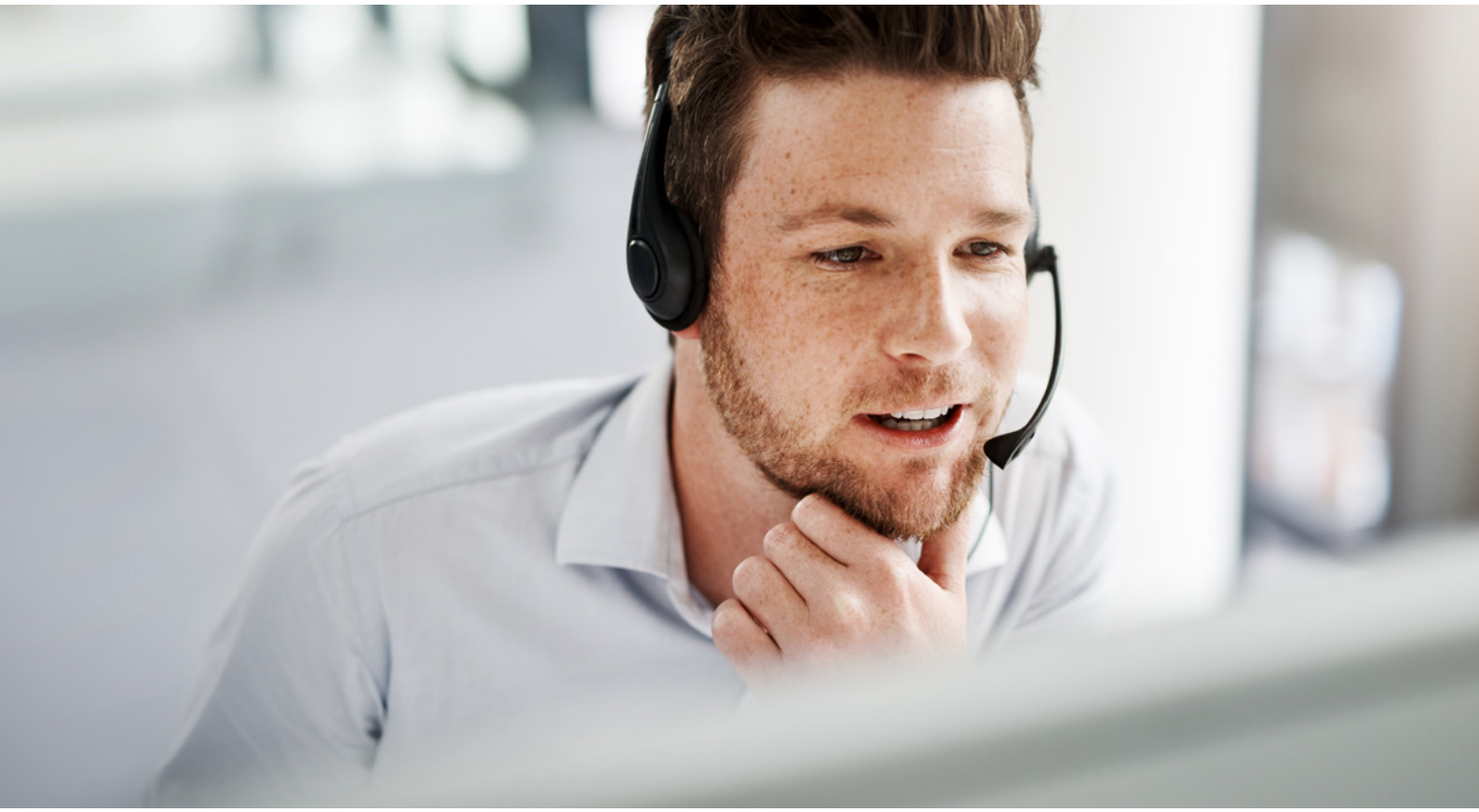
Training is always tailored to suit the organisation – whether it's via an e-learning package or a 'train the trainer' model.

RESULTS DELIVERED

PCI Pal works with a wide range of public sector organisations, including one of the largest contact centres in the UK. The feedback we receive regarding Agent Assist is excellent. Our systems help reduce call handling times and significantly reduce errors when customers provide payment information, as the contact centre agent remains in full two-way conversation during the payment part of the call. Agents simply talk callers through the payment step by step, making it a friendlier experience for customers.

For Public Sector organisations which are very much in the public eye, PCI Pal also puts in place strict SLA agreements to guarantee maximum uptime. The team also maintains contact with all service delivery parties to ensure updates and enhancements are made, as needed.

PCI Pal ultimately safeguards cardholder-not-present payments and PCI DSS requirements are 100% assured, no matter what the size or type of organisation involved.



OUR ACCREDITATIONS

pci WINNER Awards for Excellence 2020

CNP AWARDS 2019 WINNER — BEST PCI COMPLIANCE PROVIDER — JUDGES AND CUSTOMER CHOICE — WWW.CNPAWARDS.COM

COMPLIANCE SOFTWARE SOLUTION PROVIDER OF THE YEAR

London Stock Exchange

PCI Security Standards Council PARTICIPATING ORGANIZATION

ISO 27001 CERTIFICATION EUROPE

QMS ISO 27001 ISO 22301 REGISTERED

QMS ISO 9001 ISO 14001 REGISTERED

GET IN TOUCH

+44 207 030 3770

info@pcipal.com