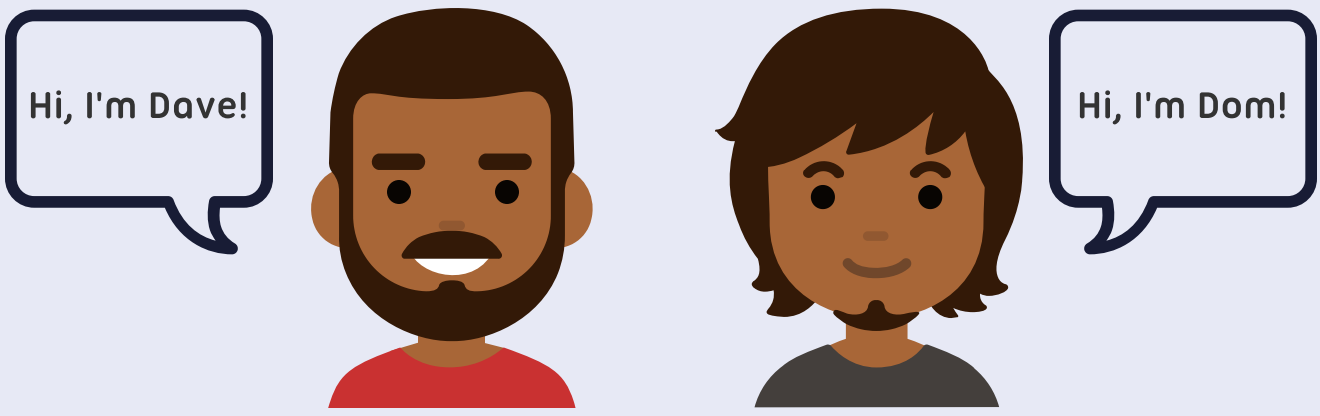
A TALE OF TWINS:
CONTACT CENTER DATA SECURITY CHECKLIST

Meet twins Dave & Dom.



Dave and Dom both lead security efforts at separate contact centers. Dave decided to achieve PCI compliance the hard way. Dom called PCIpal.

Now, Dave is exasperated. His compliance to-do list haunts him in his dreams - and that's when he has time to sleep. Dom, on the other hand, is sitting somewhere under a cabana on the Mediterranean. Thanks to the power of descoping, he knows PCIpal has it covered.

Don't make Dave's mistake.

Descope your contact center environment from the requirements of PCI DSS. Otherwise, you could be facing a growing to-do list like Dave.

	Contact Center Staff (and Back Office Staff) who have access to systems
☐	Lead staff training to ensure staff are aware of the sensitivity of card payments and report anything suspicious
☐	Carry out criminal record checks on staff
☐	Have a clean desk policy, restricting agents to taking notes on a digital computer notepad that is flushed from the computer memory as the agent logs off
☐	Prohibit bags from being allowed on premise
☐	Require mobile phones to be stored in lockers away from the contact center
	Contact Center PC/Desktop
☐	Lock down USB ports on agent PCs
☐	Run anti-virus software on agent PCs
☐	Implement website whitelists – these stop agents from sending sensitive emails containing card data to external website emails (such as Gmails)
☐	Scan for malware – need to especially look out for keyloggers, which are malicious software programs that track and record keystrokes from other computers
	Telephony System
☐	Pause call recordings while card details are taken
☐	Ensure phone systems are in locked and monitored in a secure area
	Network
☐	Encrypt traffic, so sensitive card data is not sent over the contact center network as plaintext packets
☐	Implement Network Segmentation (VLANs/ACLs) to stop sensitive card data from being transmitted across the whole network
☐	Scan email servers and databases for stored card data
	Wi-Fi
☐	Ensure Wi-Fi is protected with strong encryption
☐	Regularly search for 'rogue' Wi-Fi devices
	Contact Center Building
☐	CCTV access systems
☐	Require access card entry into the contact center
☐	Ensure visitors are clearly identified with visitors' badges and escorted at all times

Ready to get descoping so you can sit back and relax like Dom? Contact PCIpal today at info@pcipal.com.