nccgroup

Shutterstock Royalty-free stock photo ID: 1646694625

Apr 21, 2020 06:40 BST

The location’s changed but the rules haven’t: Maintaining cardholder data security standards while remote

Where organisations provide contact centre services, the move to remote working has posed particular challenges to both ensuring that the right tools are available and managing the risks associated with agents who will be handling cardholder data.

Organisations that currently comply with standards such as the Payment Card Industry Data Security Standard (PCI DSS) may now find themselves needing to enable a new form of working that may never have been within their

existing compliance scope.

With due consideration organisations can, with care, enable remote workers and take steps to help minimise the risk this introduces.

We've outlined some of the key considerations below to help you navigate this change:

- Evaluate the additional risks associated with enabling remote working for your staff, based on the ways that your staff may process, transmit or store cardholder data.
- Contact your Acquirer if you are a Merchant and discuss the situation with them.
- Make sure you educate your staff on additional security requirements and controls you will be asking them to undertake when working from home.
- Transmission of cardholder data may be over open, public networks so give consideration as to how you will ensure the protection of cardholder data in transit.
- Access to cardholder data needs to be limited to only those with a genuine business need. So perhaps further restrict or limit the number of staff who will be in contact with cardholder data when working remotely. Also check that the access rights you have in place are still reasonable in these new circumstances.
- The physical environment in which your staff will be working will be completely different from your controlled contact centre sites. Give consideration to who else may be in the property where the remote workers are based and what controls you would require of your staff in order to ensure no one else can access, view or overhear cardholder data.
- Equipment that enables staff to access systems should be secured in the same manner as any other device that would operate in a compliant environment. For example can you maintain patching and anti-malware services on equipment you issue to staff? Can you ensure that any wireless network in the property is appropriately secured?
- Consider how to ensure authentication is implemented to make use of multi-factor authentication.
- Consider how you can prevent remote workers from copying, moving or storing cardholder data locally.
- If you can implement, or perhaps expand the use of, technology

solutions where your staff do not have to hear or process cardholder data (such as DTMF suppression payment gateway providers) then give these consideration.

- Consider how you manage the incorporation of new technologies into the process to ensure that security restrictions remain suitable. If, for example, you didn't allow receipt of cardholder data via a chat window before, then you still shouldn't be doing so now.
- Ensure you maintain the levels of logging and monitoring of systems you deploy remotely that you do for on premise systems.
- Moving to remote and home working would be considered a "significant change". Make sure you review the impact of this on all PCI DSS requirements that must be reviewed on "significant change".
- If you are a Service Provider, review the contracts and the wording of any agreements you have in place with your customers. There may be prohibitions on home/remote agent working or restrictions on location that need to be discussed with your customers.

All of these issues and more need to be considered. The PCI Security Standards Council recognises the impact this can have and has published a recent article that refers to guidance to help organisations.

The "Protecting Telephone Based Payments" information supplement published by the PCI SSC is also a valuable source of information

Here at NCC Group our PCI DSS QSAs can advise and assist you with evaluating your own particular challenges in support of enabling your workers to operate safely from home while minimising the risk to cardholder data.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750