nccgroup

Shutterstock: photo ID: 1035162001

Apr 02, 2020 14:47 BST

Why your PCI assessment might be different this year

Let's say you're a merchant or service provider and it's time for your annual Payment Card Industry (PCI) assessment. You have been through this before and assume you know what to expect. However, during your current assessment, you may find yourself in a situation where you or your Qualified Security Assessor (QSA) are coming across new findings. As unwelcome a surprise as this is, it's not uncommon. There are several reasons why this can happen.

Industry trends shift along with the cybersecurity landscape.

The PCI-DSS (Data Security Standard) is widely perceived to be among the most prescriptive compliance frameworks out there. Either you have each control in place as they are mandated or you are not in compliance. There are several PCI controls which are sometimes the subject of intense discussion during PCI assessments and require some consideration for the industry you are in and the infrastructure you have implemented.

For example, Requirement 5.1.2 of the PCI DSS states: "For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software."

According to the PCI SSC's guidance: "Typically, mainframes, mid-range computers (such as AS/400) and similar systems may not currently be commonly targeted or affected by malware. However, industry trends for malicious software can change quickly, so it is important for organizations to be aware of new malware that might affect their systems…"

Historically, there have been cases where both QSAs and organizations have stated that Unix/Linux-based system infrastructure are not required to have anti-malware solutions deployed as they are not vulnerable to this type of attack.

A quick Google search of compromised systems from 2019 yields results proving just the opposite. Hence, it is crucial to remain up to date on the cybersecurity landscape to better understand the risks and threats that are relevant to your organization.

It is yet to be seen whether this requirement will change with PCI DSS version 4 (due most likely sometime in 2021), but at least until then this continues to be one instance of a PCI requirement that is at the mercy of your QSA's interpretation: will they choose to accept the justification that Macs or Unix/Linux systems are not commonly affected by malware based on how they are implemented and used?

Let's also consider the current situation with COVID-19. In the event of extenuating circumstances (such as the ongoing global pandemic), the PCI SSC has given guidance on remote assessments in lieu of the routine onsite audits. There is a risk, though, that over-use of remote assessments by some

QSA companies may lead to undetected risks that surface in your 2021 PCI assessment. A remote assessment may need prior approval from the entity you report to and will need to comply with any payment brand requirements.

PCI's approach to sampling may lead to overlooking issues.

Assume you are a retail environment with about 100 stores. Under the DSS approach to sampling, your QSA will visit a representative sample of stores (assume 10 stores). In prior years, the QSA may find that all 10 stores are compliant with applicable requirements: employees have been trained, POI devices are inspected daily, POS systems are updated, back-of-house cameras are in place, and there are no local stored instances of manual cardholder data. During the current year, a different QSA performs the assessment and chooses a sample of 10 different stores then discovers material findings: employees are unaware of inspection methods, POS systems are unpatched, and the back-of-house POS server is not appropriately secured.

In another example, your previous QSA inspected a sample of 20 Windows servers and determined the configuration settings are adequate. This year, your current QSA has selected a sample of 20 different servers and found inconsistencies in patching, anti-virus deployment, and password complexity settings.

To best avoid issues related to sampling, it is imperative that companies undergoing PCI assessments ensure that all in-scope systems are maintained consistent with configuration standards and aligned to PCI requirements.

Have you properly defined your PCI scope?

It is difficult to assess the unknown. It is up to the merchant or service provider to define the PCI scope. Every organization subject to PCI should as a first step carefully detail all cardholder data flows within their organization, regardless of the volume of each process. The next step is to review processes and technology using the applicable PCI criteria to any system that "stores, processes or transmits cardholder data, is connected to, or can impact the security of cardholder data."

On the other hand, QSAs must be sure to ask detailed questions about scope to understand all of the working components of the CDE. "Scope creep" (as it is often referred to) is one of the leading causes of PCI assessments spiralling out of control and may also result in significant delays. Some of the most common examples of scope creep may include processes and systems not

treated as “in scope”, like: call centers that were not considered; warehouses storing manual card receipts; support services where companies fax, scan or email sensitive data; or, systems that can impact the security of the CDE.

The PCI standards may have introduced additional requirements since your previous audit.

Surprises are almost never a good thing in the world of cyber security and compliance. PCI version 3.2 had many controls that were listed as best practices and became mandatory requirements after January 31, 2018. If the assessment took place after this date against PCI DSS version 3.2.1,), and you had previously marked these controls as “Not Applicable,” this may have caught you off guard.

Ultimately, the onus is on the assessed entity to stay informed requirement changes. They are responsible for meeting any changes to the PCI DSS or new interpretations described in the Security Standards Council FAQ. If you or your team are responsible for PCI compliance, it is recommended you subscribe to the PCI SSC’s mailing list and watch for changes or new interpretations on PCI requirements. This will allow time to prepare ahead of any upcoming PCI assessment. You may want to consider having periodic meetings with the compliance team and across departments to communicate these changes and develop a roadmap as necessary.

The human factor in compliance assessments cannot be ignored.

PCI assessments are document-intensive and occur within a tight timeframe. There are hundreds of policies, procedures, standards, and evidence artifacts that are required to be reviewed and assessed by, sometimes, a single assessor. The assessor might not have noticed a document was missing a date, or that the group policy setting on a Windows system was misconfigured, or that a store was missing in an external vulnerability scan. Although inexcusable, this is a reality that could result in a finding that was missed in prior years.

To avoid these common pitfalls in PCI compliance, assessed entities should keep PCI initiatives in mind throughout the year and get prepared early, as opposed to making it a focus shortly before the annual assessment begins. Companies are strongly advised to have detailed scoping discussions with their QSAs well before the start of the actual assessment.

Finally, keep in mind the old adage: compliance is not security, but security will lead to compliance. Establishing a culture and standard for security throughout the organization, as opposed to just the PCI environment will help ensure fewer surprises, even amidst the dynamic, ever-changing cyber security landscape.

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