PCI-DSS Compliance Ask the Experts Video Transcript

Robert Ramsay, Director and SOC Reporting Practice Leader

Zachary Riggs, Senior Assurance Associate

Kat Jenkins, Marketing Director

February 2021

Kat Jenkins (00:09):

Hi, and welcome to Barnes Denning Ask the Experts, I'm Kat Jenkins, marketing director. And today SOC reporting practice leader and director Robert Ramsay talks with senior assurance associate Zachary Riggs about PCI-DSS compliance. Robert and Zachary, thanks for joining us.

Robert Ramsay (00:27):

Thank you, Kat. I appreciate you setting this up for us, great to talk with you today. Yeah, we're excited to talk a little bit about the payment card industry data security standards. There's a few kind of high level things that it means to our clients. And then a little bit of history. The industry wanted to self-regulate a little bit so that government didn't come in and impose regulation on them. And so back in 2004, the payment card industry data security standards were born and they gave guidelines and guidance for those processing credit cards.

Robert Ramsay (01:05):

And it's really, throughout the US, it's become a de minimus kind of baseline for data security in a lot of places. And here in Ohio, there's actually... Our security laws give small businesses credit for being compliant as if they're doing reasonable best practices, which is really nice. And it is a baseline for data security. It's super-thorough, it's very precise on cardholder data. But in general, for an environment to be protected following these standards is a really great place to start though. Zachary, do you mind talking us through those kinds of goals and requirements that come from PCI?

Zachary Riggs (01:47):

Yeah, absolutely. So PCI, it's one of the more popular data regulation standards, and I thought I would just kind of go over the main six goals of it. It's pretty robust, but at a high level, the first one is really just building and maintaining a secure network. And this is dealing with firewall management, strong passwords, not using default passwords. The second one is protecting the actual cardholder data. And a lot of this requirement is around encryption and dealing with wireless networks, making sure it's private, not public. The third one is when you get into your vulnerability management program and that's

dealing with having proper antivirus, not being able to disable it and making sure you're pushing out the right patches to all the machines on your network.

Zachary Riggs (02:36):

The fourth is dealing with access control, and that can be logical access. Logical access in the PCI standards are dealing with user IDs, passwords, making sure no terminated employees still have access or logins. And then the other part of access controls, physical access. If you're storing any credit card data on pieces of paper in the office. The fifth is dealing with monitoring and testing your network. This gets into any type of logging tools or IDS tools and kind of doing log reviews. The six goal is really an information security policy, and that gets into formal documentation and having your standards written out. And for everybody that interacts with cardholder data at your company, that they understand what their responsibilities are.

Robert Ramsay (03:31):

Hey, thanks Zachary, that's a great overview. And that does kind of inform, so it is a broad background or baseline for a lot of security and we use it to help our small business clients. We use it as a data security checkup against the data security standards from PCI. We also help them if they're accepting credit cards, and this applies to small businesses and a lot of not-for-profits, we help them with their self-assessment questionnaires so we can help them be compliant on the scale where they're at, given their volume of transactions. We do that quite often and I think it's very helpful so they can let their owners or their board know that yes, we're doing best practices, we're being compliant, we're dotting our I's and crossing our T's. And they come out of that with some data security advice, some really good documentation on their environment and some quality training for their people, occasionally some reduced fees as well for their credit card processing.

Robert Ramsay (04:31):

And then finally, for larger enterprises in the B2B space, so companies that are serving other companies with software or processing services, we do system and organizational control, or SOC work. And we do that with PCI and it's nice to combine the two so that they save time and money. They're both IT audits and so there's a lot of work that can be done efficiently by doing them together. Zachary, you're on this every day. Can you help me with some updates, some new trends in PCI, what you're seeing?

Zachary Riggs (05:03):

Yeah, absolutely. I thought a interesting trend was, especially in the era of 2020 with the big push to remote work, Verizon comes out with a 2020 payment security report every year. And this year they found out that only 28 percent of businesses were able to remain PCI compliant during the full 12 months. And that was almost a 10 percent drop from 2019. And they interviewed some IT managers at a

high level and found that their biggest reasoning for not being able to keep with their compliance was constricted budgets for this year, especially, and just limited time and resources. So I always think PCI, a main benefit of going through the compliance is it's kind of a kickstarter for a better business model around cybersecurity, so I think that's one of the best ways to use PCI for your company as a strategic planning guideline.

Robert Ramsay (06:06):

That is a great way to think about it. And that's interesting how it's trending over time. Perhaps as we wrap up, I'll just kind of share some of the benefits we see our clients getting from going through this process and making sure they're compliant. Sometimes they're able to lower their cyber insurance costs by letting their insurance carriers know that yes, we're compliant, we check it every year and we verify that compliance. They can sometimes reduce their premiums by doing that. And then there are a whole host of benefits from just good cyber health that we've said comes from this as a baseline, more reliable operations. People are more comfortable and confident going to work knowing that things will be processing and operating as expected. I mentioned sometimes we can identify places where lowering credit card processing fees can happen, which is a super nice, really nice bonus, a tangible, measurable benefit.

Robert Ramsay (07:02):

And then having an environment and a culture of compliance and good governance just sends a good signal to employees, customers, vendors, and all those related in operations. If you can be more predictable, the owners and the employees, everyone involved will sleep better and be more confident in knowing that they're safe and secure. Kat, those were the things we wanted to share today. Do you think there's anything else we need to cover?

Kat Jenkins (07:31):

I think you got it. Great information as always Robert and Zachary, thanks for being here. If you have a question about PCI-DSS compliance, or you'd like to set up a conversation, you can visit us barnesdenning.com. We'll see you next time on Ask the Experts.