2019 PCI Compliance Annual Plan

January

Start the year strong by taking note of when your annual PCI compliance assessment will be due as well as ensuring that your monthly vulnerability scanning program is running smoothly. Now is also a good time to list all third parties and vendors that interact with or influence the security of your company's or your customers' payment card data. Include a column that indicates each service provider's state of compliance.

February

Identify all the places that payment card data is stored, processed and/or transmitted within your environment. Make sure you have the appropriate security controls in each location where a system would interact with that data. Perform a formal risk assessment against your company's business objectives for the year and review your security policies to ensure they are sufficient to cover your risks.

March

Reduce your breach risk by reviewing or creating your company's security awareness training program. Security awareness training is a must for your employees, especially those who interact with payment card data. We recommend that your program is formal, ongoing and comprehensive so that all staff understand your company's security policies as well as data security essentials and best practices.

April

Review your firewall's inbound and outbound network rules. Chances are someone will get into your systems, so prevent them from getting data out of the network by setting up alarms and other methods of intrusion detection. Lock down your network traffic to only those ports and services that are required. If possible, lock it down to the destination networks and hosts as well.

May

Review and test your company's incident response plan (IRP). If you don't have an IRP in place, gather together your organization's key stakeholders to develop one. This plan should seek to identify the risks your company and its data may face, and put in place specific procedures to be followed in the event that one of those risks becomes a reality.

June

Free space for Annual Validation - This open block is here to swap with the month in which your business's annual PCI Compliance validation takes place.

July

Access management is important to strong security. Review your sensitive assets, vendor accounts, unused accounts, remote access accounts, employee accounts, physical access, application accounts, etc., and make sure that all related permissions are current and the level of privileges are justified. If it's not required, remove the access. Accounts that are not used should be disabled or deleted.

August

A comprehensive penetration test should be performed against all entry points into your systems, as well as places where sensitive data is stored. Penetration testing goes much further than vulnerability scanning, because it goes beyond the automated process of looking for basic vulnerabilities. Merchants are required to have a pen test annually and service providers must also validate segmentation controls every 6 months.

September

This is the month to remediate all critical, high and medium-level vulnerabilities discovered in last month's penetration test. Doing so will strengthen your security posture well in advance of the holiday cybercrime spike. Once you have completed remediation, a follow-up test is highly recommended to ensure that nothing was missed and no new vulnerabilities were created in the process.

October

By October, most organizations are well underway with the budgeting process for the next calendar year. If your company's fiscal year is not based on the traditional calendar year, feel free to swap this box with the month when you are typically planning your budget. When considering your budget for the next fiscal year, be sure to give some thought to the ROI advantages of managed security services over in-house resources.

November

The holiday season is here! If you're a brick-and-mortar retailer, that means it's time to review physical security with your store teams. This includes how to spot the telltale signs that a payment-related device has been tampered with, as well as what to do if a shopper leaves their credit card behind. In addition, don't forget to review and tighten your processes for securing all physical points of entry to your store/office space.

December

Congratulations! You made it through an entire year of "business as usual" PCI compliance—and in doing so, you have established a baseline that will make next year run considerably smoother. What's more, following this year's plan has already significantly strengthened your business's security posture.

Now, let's bring on 2020...