PERKINSCOIE

WRAPPING PAPER SERIES

Could a Vendor’s Lax Info Security Ruin Your Holiday Sales?

Seven Preventative Steps for Retailers

Many of the largest retailer data security breaches have been caused or enabled by the acts or omissions of retailers’ vendors, such as the widely publicized incident at Target Corporation. Several such breaches occurred through the use of phishing emails or direct malware attacks on their vendors and exposed retailers to millions of dollars in stolen information, credit monitoring costs, credit card replacement fees and class action lawsuits.

Large retailers often have thousands of vendor relationships, some of which are tightly integrated with the retailers’ businesses. Contracts with vendors, and particularly agreements entered into years ago, may not include clearly defined information-security obligations and standards. Additionally, a vendor’s access to a retailer’s networks and systems may not be subject to clearly articulated policies and procedures.

It can be daunting to look at the list of vendors and contemplate the task of implementing enterprise-wide data security changes. However, understanding that this will be an iterative and ongoing effort will help reduce the burden on your entity’s operations. In order to mitigate the risks of a vendor-related data breach, you should consider the following practical and proactive approach to your vendors’ data security practices.

Take Advantage of Your Compliance with PCI DSS

With respect to cardholder data, your organization should already be in compliance with the Payment Card Industry Data Security Standards (PCI DSS). Requirement 12.8.5 of the PCI DSS requires merchants to track which PCI DSS requirements the merchant will enforce and which the vendor will enforce. This mapping must be performed for each vendor that possesses, stores, processes or transmits cardholder information.

Your organization’s compliance efforts for PCI DSS can serve as a model to improve your vendor security and information management practices. By categorizing your organization’s data and then applying a similar approach to the sensitive systems and information that your vendors possess, store, process or transmit, you are then able to mitigate the exposure of your organization to risk from your vendors’ security gaps. Below we have suggested steps to establish a vendor information security program, which are similar to the steps your organization used for PCI DSS compliance.

Steps to Implement a Vendor Information Security Management Program

Step 1 Organizational Buy-In

Although the legal department has a key role to play, managing the risks associated with vendor information security is not just a legal issue. It is important to identify and involve additional key organizational stakeholders, such as management, IT and procurement, to aid and participate in the process. Without the buy-in and participation of the key stakeholders in your organization, any effort to establish a comprehensive solution is unlikely to be successful.

Step 2 Classification of Data

A logical first action to protect your organization's data is to classify each type of data that your organization possesses, stores, processes or transmits based upon its sensitivity.

You should establish a tier-based hierarchy to define the categories and criteria your organization will use to classify data. The data classifications should be easy for every employee to understand.

For example, you could establish a four-tier system. The highest tier should include your most critical and sensitive information—the kind that could materially impact the organization if disclosed, such as sensitive personally identifiable information and key financial information. The next tier should include data that is still sensitive and could negatively affect the organization if disclosed, such as vendor contracts and non-regulated personnel records. The next tier would include data that is not particularly sensitive but is still not meant for public disclosure. The final tier would consist of data that may be disclosed publicly without harm to the organization.

Step 3 Establishment of Policies and Procedures for Each Tier of Data

Once you have classified your data into tiers based upon its sensitivity, you can establish policies and procedures that instruct your personnel and vendors on how you expect them to handle and manage your information and to access your organization's systems. Obviously this will be a significant cross-functional effort, but your organization is likely to already have information security policies that can be expanded or adapted based upon the data categorizations.

Threshold Authorizations. Based on the data classifications, you can establish a threshold authorization process that would require escalation to a decision-maker for approval of higher-exposure matters. More substantively, these processes may include a standard security assessment questionnaire or a penetration test, if warranted, based on the information that a particular vendor can access. You may also consider implementing and routinely conducting a due-diligence review of all vendors, as well as prospective vendors, who will have access to data in the highest tier(s).

Internal Access Controls. During this process, you should work with your IT and security professionals to ensure that your organization has implemented and/or strengthened internal access controls and validations to restrict internal accessibility to this critical and sensitive data. Several well-known security breaches have occurred by initial access to vendor systems followed by broader access to merchant systems. Fortifying internal access controls and systems can limit harm in the event of unauthorized access through a vendor system.

Security Contract Terms. Based upon the policies and procedures, you should develop standard contract terms on security obligations. Such terms can include the following: compliance with corporate policies; system access requirements; a written security program; indemnity provisions; security reviews (SSAE 16 SOC audit if warranted); breach notification; and the return or destruction of your data upon termination. Additionally, requiring a vendor to flow down these obligations to subcontractors with access to your systems or data can help ensure stronger protection for your organization.

Cost Considerations. As you develop these new requirements, it will be important to consider the costs to the vendor of complying with them. While it is tempting to go for gold-standard security, some security requirements can be extremely expensive to implement. Such requirements will make it difficult to get vendors to accept the requirements. As you develop policies and procedures, we recommend that you work closely with your IT security personnel to identify security requirements and safeguards that are likely to be extremely costly. Consider whether there are lower cost but equally effective alternatives.

Step 4 Data Mapping

After you have completed the data classification, you should identify which vendors have access to which systems and the type and scope of access they have, including the various classes of data. In order to do that, you will need to understand how data flows through your organization, and where it is stored. This can be a significant effort, but if you do not know what data you have and where it is going, you cannot address the risks to that data.

This step may include reviewing access rights, vendor contracts and even internal audits to determine what is happening in practice. While the contract may state one thing, it is important to *verify* actual practices. The results of this exercise should yield a roster of vendors categorized according to the class of information they collect, store, process or transmit on your behalf. Consider that one vendor may have access to multiple tiers of data. Remember that cloud services providers are also vendors and should be analyzed and subject to the policies and procedures you develop. Once you have mapped out which tiers of data each vendor has access to, you will begin prioritizing your risk mitigation process.

Step 5 Vendor Prioritization

Begin your risk mitigation effort by focusing on those vendors who have access to the highest tier of data. A small number of vendors may have a large amount of your most sensitive data, and addressing these first can greatly limit your organization's potential exposure. You may even want to limit your initial focus to these vendors to keep the effort manageable.

Step 6 Make Your Naughty List (Noncompliant) and Your Nice List (Compliant)

As you begin this step, start with the presumption that all of your vendors are on the "naughty list," until you can verify and approve of a particular vendor's data security controls and practices. Until you review your vendor relationships with data security in mind, every vendor could present vulnerabilities.

New Vendors. Apply your new policies and contract terms to all new vendors. This is your maximum point of leverage for addressing data security. But be sure to have an exception policy or alternative internal safeguards if the vendor refuses your data security terms. It can be beneficial to build long-lasting relationships with vendors, and it is important to "get off on the right foot."

By setting the tone early in the relationship, you can reinforce your expectation of adherence to data security policies. One way of communicating this to prospective/new vendors is to make it a two-way street. Both the retailer and the vendor will suffer harms (e.g., reputational harm, enforcement actions, fines, class actions, etc.), but by aligning interests to a commitment of sound data security practices, both parties can significantly reduce their risk of exposure.

Existing Vendors. For current vendors, consider making it clear that your organization is undergoing an enterprise-wide change to data security practices to proactively address the threat of data breaches, which includes coordinating with your vendors.

Start with the highest-risk vendors that you identified in your risk assessment. Data security is an important issue to both vendors and your organization, so try to work collaboratively with vendors to update controls and procedures to conform to your policies. Additionally, you should update existing vendor contracts to reflect the new policies and procedures as soon as possible, which may not be until renewal.

While existing vendors may be hesitant to take on additional obligations, especially as onerous as some data security obligations, you should try updating contracts using incentives, such as paying vendors faster or extending the contract term. Additionally, you should have fallback positions for safeguards that are too costly to implement.

Once vendors' practices and controls are compliant with your established policies and processes, and their contracts have been updated, they can be moved to the compliant, "nice list." Remember that although a vendor may be on the "nice list" on day one, it does not mean it will always be compliant. Your policies should include periodic evaluations of vendors to ensure compliance as the data environment, regulatory framework and your policies evolve.

Step 7 Iterate to Move Forward

Make progress by repeating Step 5 and Step 6 for each tier of data until completion. This systematic approach of first classifying the sensitivity of the data, then identifying which vendors have access to that data, and finally mitigating the risk in regards to each vendor will help you establish a comprehensive vendor security management program, one step at time, while mitigating your largest potential exposures as quickly as possible.

It is important to understand that a vendor security management program is not a one-time effort. Your organization should periodically evaluate vendor compliance and promptly remedy noncompliance, whether that is by penalties or termination. Of course, new vendors will come on board, and the services offered by vendors will change. This is where the authorization process developed in Step 3 will become critical.

While establishing a comprehensive vendor security management can be an overwhelming task for a large retailer, it is possible to minimize the pain by prioritizing your vendors and making the implementation of the program an iterative process.

Contacts

Dean W. Harvey | Partner
DHarvey@perkinscoie.com
DALLAS
+1.214.965.7731

Matthew Cin | Associate
MCin@perkinscoie.com
DALLAS
+1.214.965.7718

Jordon De La Cruz | Associate
JDeLaCruz@perkinscoie.com
DALLAS
+1.469.801.2330

Related Services

- Retail & Consumer Products
- Technology Transactions & Privacy
- Privacy & Security

Some jurisdictions in which Perkins Coie LLP practices law may require that this communication be designated as Advertising Materials.