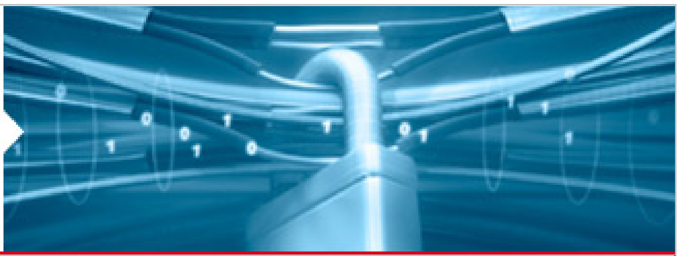
PERKINS COIE
COUNSEL TO GREAT COMPANIES



Data Security Initial Assessment Checklist for Retail Counsel

ASSESSMENT QUESTIONS	REASONS TO ASK
1. Does your organization have a written data security policy?	A written data security policy (or policies) is the foundation of a successful data security program. A policy should be used to address the three components of data security: (1) people, through training, (2) process, through procedures developed to comply with the policy; and (3) technology, by establishing minimum standards to be met. A policy provides a basis both for training employees to avoid breaches, and for holding accountable any employees who either negligently or maliciously violate the policy. From a legal compliance perspective, a data security policy provides written proof of compliance efforts and makes compliance auditable. According to the Ponemon Institute, the absence of a data protection security policy is a factor in the losses arising from data security breaches. The report is available here.
2. Is the policy part of a comprehensive program or just an IT policy?	An effective security program must be supported by senior management and must apply across organizational boundaries. IT policies may not reach all business processes.
3. Is there any sort of audit or verification to confirm compliance?	It is important to confirm that the security policy is actually being followed.
4. Is the policy(ies) updated at least annually?	As your organization changes (e.g. offering new products/services), and threats change, your policy(ies) need to be updated. Policies that do not reflect current operations or defend against current threats are of little value.
5. Do you have an information security officer or other senior individual responsible for overseeing data security throughout the entire organization?	Having an information security officer demonstrates to all employees that management is committed to and supports the security program. Additionally, appointing an officer to oversee security across the entire organization provides a single point of accountability, an organization- wide point of escalation on data security issues, and an enterprise view of data security to company's management.

6. Does your organization's POS permit remote access?	Target's POS was apparently hacked by individuals who were able to access it from the vendor billing system. This is not surprising. According to Verizon, the POS intrusion is the second most popular type of hacking attack on retailers. View Verizon's report here. Retailers should address this significant threat by restricting remote access to the POS as much as possible, and by strengthening authentication and verification procedures.
7. Are your e-commerce applications on a separate network from your other systems?	The most common attack on retailers is the denial of service attack. View Verizon's report here. Moving these systems to a separate network and server farm can improve security and help to resist denial of service attacks.
8. What types of personally identifiable information (PII) is your organization collecting?	In order to understand what regulatory mandates apply to your organization, you need to understand what PII is being collected. Additionally, while cardholder data justifiably is a focus of data security, general PII is the most stolen data. The Target breach follows this trend, with 40 million cards compromised, but the PII of 70 million customers taken.
9. How does PII come into the enterprise? Where is PII being stored? How is it being used?	If you want to protect PII, you need to understand where it comes from, how it is used where it is stored, with whom it is being shared, and how it is being disposed of.
10. Is PII encrypted at rest and in transmission?	While encryption alone will not meet your organization's legal compliance obligations, if your organization's PII is encrypted at rest and during transmission it dramatically reduces the risk of data security breaches.
11. Is PII being stored on mobile devices? Is it encrypted?	Theft of mobile devices with PII is on the rise. If your organization permits access to PII from mobile devices, it should consider encrypting all such data and registering and installing remote wiping software on all such mobile devices.
12. Is PII being stored in the cloud?	If your organization is storing PII in the cloud, it is important to confirm that adequate safeguards are in place to protect it. You may want to pick the top five cloud or SaaS providers (or whatever sample set is reasonable for your organization) who are storing PII and review the terms of the contracts to see if they are consistent and adequately protect the PII.

13. Does your organization have a standard security assessment questionnaire for vendors?	It appears that the Target data security breach occurred through a vendor's billing and invoicing system when that vendor was hacked in a phishing attack. Any vendor either accessing your organization's network(s) or hosting data should be evaluated prior to contract to determine if it has adequate security measures in place. Due diligence on such vendors can be initiated by requiring such vendors to fill out a security assessment questionnaire before entering into a contract. Such a questionnaire should among other things require the vendor to describe its network scan and penetration test regimen.
14. Does your organization have standard data security terms for vendors with access to network(s) and/or hosting PII?	A standard set of terms enables your organization to ensure that each vendor is establishing consistent safeguards to protect your PII. Your organization should consider safeguards such as requiring penetration testing, establishing minimum security standards, and requiring SOC audits by an independent third party to confirm that the controls are being followed. Your organization should also consider the impact of key risk allocation terms (e.g. limitation of liability, indemnity and, breach notification) in the event of a data security breach, and establish standard clauses for agreements involving the sharing of sensitive data.
15. Does your organization include network monitoring for networks transmitting PII?	Network monitoring is critical to detecting attacks. Once an attack is detected, it can be blocked.
16. Who is responsible for addressing alerts and blocking attacks?	Target paid a third party to provide network-monitoring services. It has been alleged that this third party provided alerts that an attack was occurring, but no action was taken. If true, this is an example of one component of security (technology) working, but failures in the other components (people and process) leading to a disastrous security breach.
17. Do you have an information technology disaster recovery plan (IT DRP)?	Part of data security is protecting the integrity of your organization's data in the event of a security breach or other emergency. This can be accomplished through the creation of a disaster recovery plan and infrastructure. Such a plan should establish recovery time objectives and recovery point objectives for all-important systems in the organization.

18. Do you have a written security incident policy?	No security program is perfect. In the event that your organization suffers a data security breach, it is important to be prepared to manage the breach. A written security incident response plan establishes the procedures to follow in the event of a breach report in order to mitigate the effects of the breach and minimize its impact on the organization. It should include clear tasks and allocated responsibilities. Organizations that do not have security incident response plans tend to react much more slowly to breaches than those that do. Delays can be costly.
19. Is the security incident policy tested?	It is important to actually work through the security incident response policy as if a breach had occurred. This will help you to identify any ambiguities or weaknesses before an actual breach.
20. Are you PCI DSS certified?	If your organization is not PCI DSS certified, and it accepts payment cards, it is risking data breaches and significant liability.
21. Does your organization use compensating controls for PCI DSS?	If your organization is relying on compensating controls, it is important to periodically re-evaluate whether these controls continue to be justified in light of the potential risk as technology and threats change over time.