## CHAPTER 27

**Retail**

Once seemingly immune to information assurance woes, retail organizations are now front-page news for the massive breaches they have experienced. Retail breaches are more complicated than may first appear. While the retailer is certainly part of the breach, there are other parties involved that assume part of the overall risk. The credit card providers, credit card processors, the Payment Card Industry Data Security Standard (PCI-DSS) industry, the customers, and the technology providers all have a hand in ensuring that appropriate information assurance is protecting the business and the customers.

**Overview of the Information Assurance Approach**

The MSR information assurance model involves five essential services: confidentiality, integrity, availability, authentication, and nonrepudiation. When applied to the retail industry, these overarching concerns become apparent immediately.

• **Confidentiality** Customers have an expectation of privacy when it comes to their personal information and their credit and debit card information. While many credit cards protect users from fraudulent charges, most debit cards have a limit of exposure and hold the customer liable for losses beyond that amount; in many cases, timely notification of theft or loss is required to mitigate customer losses. In some cases, this amount can be as little as $500. Retailers maintain several types of information that have privacy and confidentiality requirements, such as credit card information, debit card information, bank account information, personally identifiable information, shopping habits (as part of shopping clubs), and surveillance information.

• **Integrity** Retailers rely on accurate, thorough, and timely information regarding marketing, sales, competition, pricing, and logistics. In increasingly competitive markets, retailers must perform not only in the showroom of the store but also in the marketing department, the shipping department, the pricing department, and the customer satisfaction survey. Inaccurate financial records, shipping records, and even customer records can result in the loss of revenue and customers.

• **Availability** If a point-of-sale (POS) system is not operational, a sale cannot be made in many of today’s high-tech retail operations. With the increased use of credit cards and the decline of cash-based transactions, retailers are relying on a resilient infrastructure now more than ever to ensure transactions can take place in near real time.

• **Authentication** Authentication has become a hot topic with many retailers because numerous breaches have now been traced to authentication issues related to internal systems and external providers using remote access systems to gain access to a retailer’s stock, as well as environmental and sales systems.

• **Nonrepudiation** In retail, nonrepudiation is critical for staying in business. A retailer must be able to prove when a transaction took place, who was involved in the transaction, and what was traded. Failures of nonrepudiation lead to the retailer giving refunds when no refund is due, not being able to defend itself in court if needed, and not having reliable audit logs when trying to determine whether an insider is stealing from the company.

Now that a basic outline of a retailer has been created, a risk assessment and mitigation approach can be crafted. Retailers are often focused on their core mission of selling products, but they must be willing to understand the risk they have accumulated through the natural progression of technology in retail. Retailers cannot afford to ignore information assurance because the results can be truly catastrophic for their business. The retail industry uses several terms specific to retail business objectives. The following list provides an overview of commonly used terms:

• **POS** The point-of-sale system is the interface between the cashier (or the self-checkout line) and the numerous back-end systems of the organization. It is typically designed to handle cash, checks, credit card, and social services transactions. Additionally, it is linked to numerous back-office services such as inventory systems and customer information capture systems.

• **Customer information capture systems** These systems capture information about customers for marketing, promotions, and business intelligence. They are often used with customer loyalty programs and bonus cards.

• **Inventory information capture systems** Inventory information systems keep track of a retailer’s inventory and the amount of supplies on hand at a given moment. They are integrated into the POS system so as inventory is sold, the back-office people know whether they need to start ordering more inventory. Alternatively, if a product is not selling well, the inventory system can display the lead time for inventory turnover, which may prompt a sale or reduction in price.

• **Workforce management systems** Workforce management systems are designed to provide the basic operational automation for the retailer’s workforce such as time and attendance, work schedule, and leave.

• **Supply chain management systems** These systems are featured at large retailers and serve to model the logistics process for efficient shipping and supplier relationships.

• **Business intelligence** Business intelligence (BI) is used to find statistical significant events such as triggers or correlations in buyer behavior and business operations. BI typically takes data from throughout the organization to find patterns, trends, and causation.

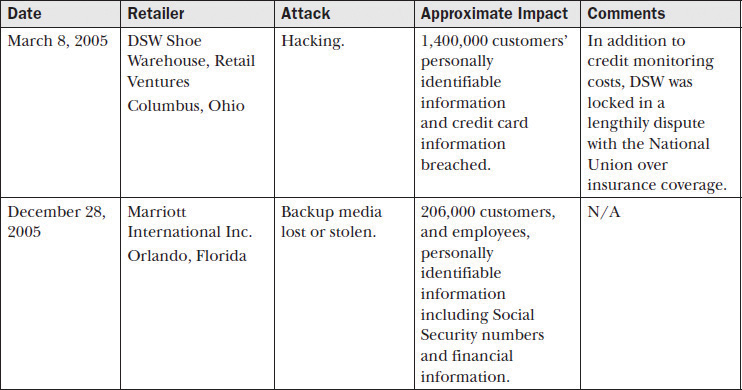
• **PCI-DSS** The Payment Card Industry Data Security Standard is an agreement about baseline security among major credit card providers. It is mandatory for retailers who want to accept the most commonly issued credit cards. PCI-DSS mandates operational, managerial, and technical controls. PCI-DSS is often criticized as insufficient for true security. Since it is a baseline, it establishes a minimum starting point from which an organization builds the rest of its security program through the use of effective risk management.

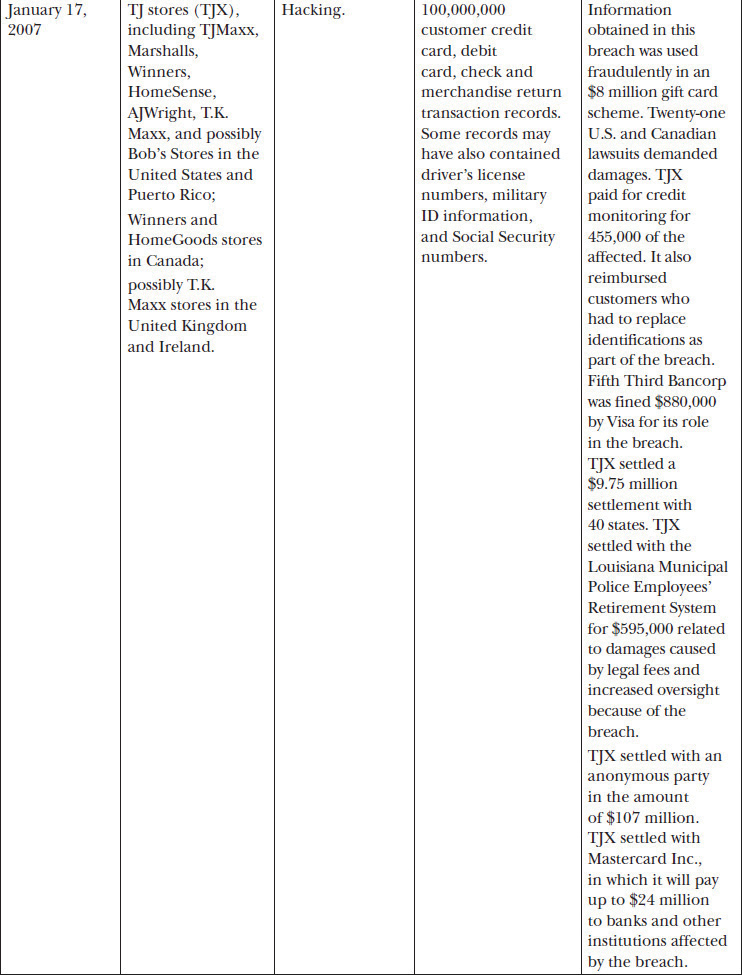
• **EMV** This stands for Europay, Mastercard, and Visa. This is a global standard for the interoperation of “chip and pin” credit cards. These cards contain a microprocessor that allows for the real-time authentication of a customer through the use of a PIN. It is common outside the United States.

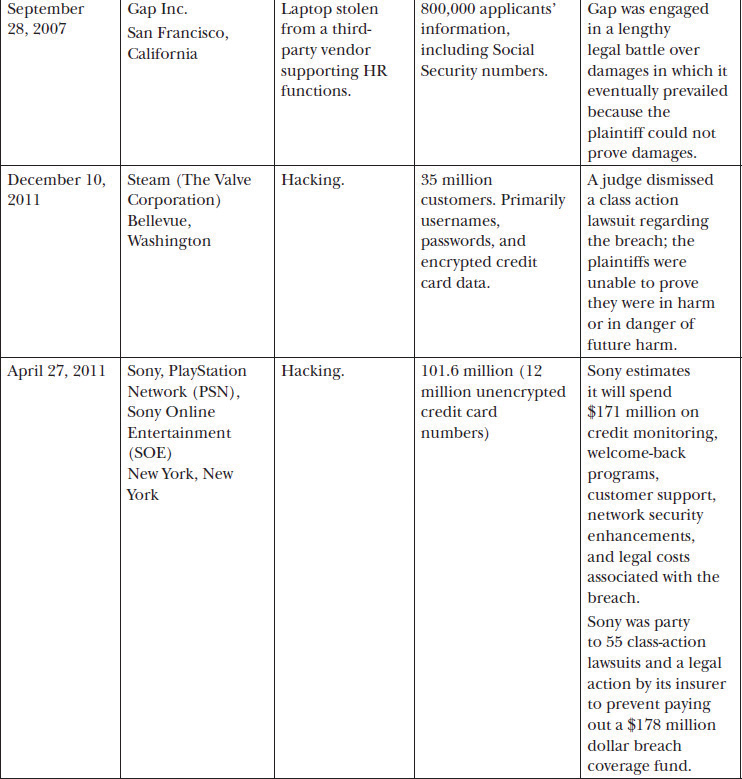
**Information Assurance Management**

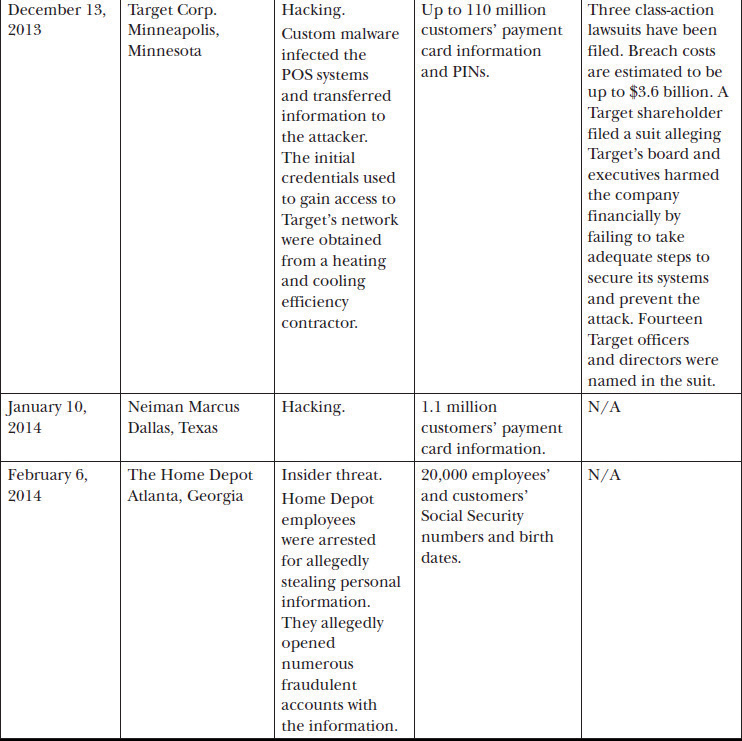
image

The retail industry has been affected by several high-profile security breaches in the past year. You need only to skim the recent news to understand the retail market is a prime target. [Table 27-1](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch27.html#ch27tab1) lists selected breaches by retailer with cause and affected individuals based on information from [privacyrights.org](http://www.privacyrights.org/), a breach reporting clearinghouse.









**Table 27-1** Overview of Retail Breaches

Clearly, the selected examples in [Table 27-1](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch27.html#ch27tab1) demonstrate that the retail industry is not immune to the devastating impact of poorly implemented information assurance. Many retailers face the same adversaries and challenges as the retailers in the table. Through the development of an information assurance program with executive sponsorship, organizations can avoid or greatly reduce the impacts of a breach or worse. As noted throughout this book, information assurance management must address several aspects of an organization outside of information technology. Personnel, the management approach, and careful consideration of regulations must all be carefully accounted for in an information assurance program.

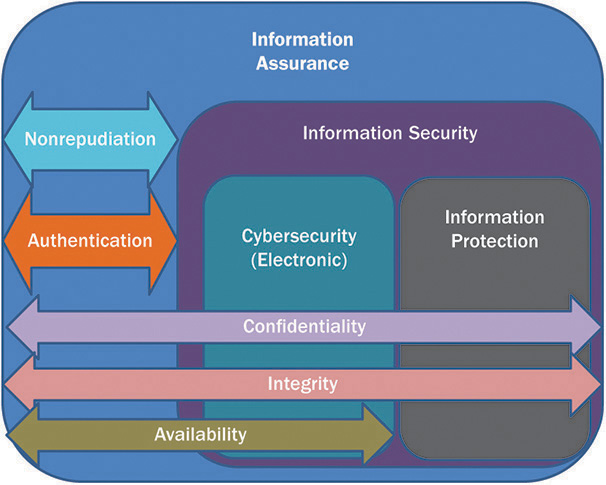
**Personnel**

Retail organizations should consider hiring blended information assurance professionals. An example would be an MBA with an SSCP, CISM, CISSP, or CSSLP certification. This combination of skills is necessary to ensure the person has a working knowledge of business and can apply information assurance controls to the appropriate areas while speaking the language of business impact to the senior executives. While often difficult to find, many educational organizations and professionals have seen this need and developed curriculums around blended information assurance professionals.

**Management Approach**

Retail organizations should employ a top-down approach for information assurance. Senior leadership must set the tone at the top and inform the entire workforce that information assurance is a priority for the organization and for the organization’s customers. A strong information assurance program should be established with clear authority for information system monitoring and incident response. (See [Chapters 20](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch20.html#ch20) and [22](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch22.html#ch22) for more information about incident response and monitoring.)

Management must also ensure their information assurance approach aligns with their IT strategies and encompasses the whole organization, not just traditional IT. Many large retailers maintain full cybersecurity intelligence teams, yet these organizations are the same ones being attacked successfully. In many cases, the reasons revolve around the narrowness of cybersecurity. In [Chapter 3](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch3.html#ch3), information assurance was compared and contrasted with several related subdisciplines including cybersecurity.



[Figure 3-2](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch3.html#ch3fig2) helps explain the difference between information assurance and cybersecurity. An organization that focuses only on cybersecurity is vulnerable to a host of serious threats including, but not limited to, equipment theft, third-party credential misuse, shadow IT, cloud computing blind spots, intellectual property theft by employees, and portable media (including paper records) loss.

Management should have a vested interest in ensuring the due diligence and due care of the organization. As noted in the Target entry of [Table 27-1](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch27.html#ch27tab1), the Target board of directors and senior management were named in a lawsuit by a shareholder. Management must understand they can be held accountable for their actions and their lack of action.

**Regulations and Legal Requirements**

The most commonly cited regulation surrounding retail operations is the Payment Card Industry Data Security Standard (PCI-DSS). Retail organizations must be aware they are now subject to many more regulations than before due to the growing practices of collecting customers’ personally identifiable information and using the information for marketing, business intelligence, and customer loyalty programs. Retailers involved in the medical field including pharmacies must also be aware of medial laws and regulations such as HIPAA in the United States and the Data Protection Act in the United Kingdom. For a list of international privacy laws and regulations retailers must consider, see Appendix F.

**PCI-DSS**

PCI-DSS is a continuous approach similar to the Plan-Do-Check-Act approach outlined in [Chapter 6](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch6.html#ch6) of this book. PCI-DSS prescribes an Assess-Remediate-Report life cycle.

• **Assess** Assessment involves identifying cardholder data, understanding IT assets processing, storing or transmitting cardholder data, and assessing business processes to discover vulnerabilities.

• **Remediate** Remediation involves fixing and resolving weaknesses discovered during the assessment phase. Not storing cardholder information unless absolutely necessary is a commonly highlighted mitigation.

• **Reporting** To remain compliant with PCI-DSS, organizations are required to report status to acquiring banks and card brands the merchant chooses to do business with.

PCI-DSS requires mandatory security controls no matter the size of the organization. In summary, PCI-DSS requires the following:

• Install and maintain a firewall and router configuration to protect cardholder data.

• Do not use vendor-supplied defaults for system passwords and other security parameters.

• Protect stored cardholder data.

• Encrypt transmission of cardholder data across open, public networks.

• Use and regularly update antivirus software or programs.

• Develop and maintain secure systems and applications.

• Restrict access to cardholder data by business need to know.

• Assign a unique ID to each person with computer access.

• Restrict physical access to cardholder data.

• Track and monitor all access to network resources and cardholder data.

• Regularly test security systems and processes.

• Maintain a policy that addresses information security for all personnel.

While these 12 areas may seem simple, they are anything but. Entire books have been written on several of the subjects, such as “develop and maintain secure systems and applications.” Another area that may seem simple is encryption; however, database encryption, session encryption, and full disk encryption for a laptop are very different from one another but are all required for protecting cardholder information throughout its life cycle.

To be PCI-DSS compliant, organizations must use a qualified security assessor (QSA) to perform their assessment. A QSA is certified by the PCI Security Standards Council to perform compliance verification assessments onsite. The QSA handles the Assess portion of the PCI-DSS cycle. Organizations are responsible for choosing a QSA who has a solid understanding of their business, IT infrastructure, cloud use, and culture. PCI-DSS also requires organizations to use an approved scanning vendor (ASV). These are firms that are certified to determine whether a customer is compliant with the PCI-DSS external vulnerability scanning requirement.

Organizations can greatly reduce their scoping and size of network through the use of network segmentation. Network segmentation isolates cardholder data from the rest of the network through physical and logical controls. For example, common business practice may state that having every service and device on the same network will ease management complexity and allow for greater reuse of common services. However, the entire network is now in scope for assessment and also attack from a practical perspective. This could mean an attacker will leverage a different service on the network such as a heating and ventilation efficiency appliance to steal credentials and then launch an attack against other systems processing or storing cardholder information.

**Privacy Laws**

As noted previously, Appendix F describes the vast majority of privacy laws available around the world and the majority of states in the United States. In addition to PCI-DSS, retail organizations must be aware of what legal requirements they may be required to fulfill should a breach of customers’ personally identifiable information occur. The good news is that many laws have a safe harbor provision for organizations that have conducted due care and due diligence measures such as encrypting cardholder information at rest and in transit.

Most privacy laws require the organization ultimately accountable for the information (the retail organization) to notify the customer of the breach and, in cases of moderate or high risk breaches, offer credit monitoring services for a certain duration. While there is a monetary cost of providing notification and monitoring, the real pinch may come from certain laws that require fines to be paid to regulators such as the U.S. Department of Health and Human Services for HIPAA violations.

**Information Assurance Risk Management**

The need for information assurance should be crystal clear in the retail space. PCI-DSS provides a good starting point for many organizations but should not be solely relied on as sufficient protection in today’s threat environment. In February 2014, South Korea KB Kookmin Bank, Lotte Card, and NH Nonghyup Card were fined res_300_Image million and banned from issuing new credit cards for three months because of a data breach. The breach contained information for more than 20 million people (about 40 percent of South Korea’s population) that was sold to marketing firms. Allegedly, an IT contractor working for a credit rating firm stole the information. The South Korean Financial Supervisory Commission (FSC) said the three firms ran afoul of due diligence and due care by not preventing leakage of customer information. Several executives resigned or offered to step down over the issue. Managing information assurance risk requires organizations to thoroughly understand their environments, assets, threats, vulnerabilities, and how best to assess their risk.

**Assets**

Retailers should consider all aspects of customer information and organizational assets to be protected. If the organization collected it, there must be value in keeping it. If not, the organization should determine a secure way to destroy the information. An adversary can’t steal or exfiltrate what isn’t there. As PCI-DSS notes, the information assurance requirements follow data in all its forms through any system or media.

Assets should be categorized or classified according to their impact to the organization. Credit card information and personally identifiable information should be categorized as moderately or highly important to the organization. The systems that process, transmit, or store sensitive information must be identified and inventoried as part of an asset validation process. Account for all data flows or interconnections. In addition, keep track of which partners are receiving information that your organization has ultimate responsibility for.

**Threats**

Retailers are mired with numerous threats. In addition to the traditional threats of hackers operating across the wire, retailers must also have a high level of interaction with the public and therefore must prize availability and customer friendliness over other concerns. Recent events have shown retailers suffer most from external hackers gaining access to card information and insider threats that have access to the data and plan on using it for fraud or personal gain.

Hackers find vulnerabilities in information systems and attempt to leverage them to gain control of systems containing sensitive information. However, organizations must understand that all systems are a target. Even if attackers cannot gain access to the target system, they will find other systems connected to it and attempt to compromise those so they can then move “laterally” through the organization.

Insider threats are based on employees and contractors who either intentionally or unintentionally put information and operations at risk through their actions or negligence. An insider threat may be the honest employee who left his laptop in the car and the car got stolen, or it may be the corrupt senior official planning on spending her retirement in a new country with a new identity and a pile of ill-gotten cash.

As if hackers and insider threats were not enough, retail must also worry about natural disasters such as hurricanes, earthquakes, and floods if they are to remain viable. The U.S. Federal Emergency Management Agency (FEMA) estimates that 40 percent of businesses do not reopen after a disaster. Of those that do open, 25 percent fail within one year. Retail operations face formidable threats from several sources; only a robust approach to information assurance with an associated program can help organizations survive. You can find more information regarding threats in [Chapter 4](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch4.html#ch4).

**Vulnerabilities**

When retailers talk about vulnerabilities, they are often focused on shrinkage or product loss because of theft or destruction. They may also discuss vulnerabilities in terms of their market and associated strategy to remain relevant in a growing environment of international competition. Retail organizations must pay the same attention to vulnerabilities in their information assurance posture.

Vulnerabilities must always be viewed through the three lenses of people, processes, and technology. All three areas must be assessed to determine where weaknesses actually exist in the enterprise.

Technical vulnerabilities are often the first discussed when the topic of vulnerability management comes up. Many organizations believe if they patch their systems and do a vulnerability scan once a month, they are in good shape. This is a good start but far from sufficient. Technical vulnerabilities can also exist in business partners. Is the information assurance team part of all procurement actions that involves the processing, storing, or transmitting of the organization’s information? Is the information assurance team part of all discussions where systems are to be interconnected to share information? Organizations must remember that their requirement to protect cardholder information extends to anywhere that information goes on the organization’s behalf. Is the organization aware of the technical vulnerabilities of their partners and what risk they may be accepting and not telling the organization? Organizations need to understand their vulnerably surface extends far beyond “in-house” IT to partners, volunteers, and anyone who holds information the organization is ultimately responsible for.

An organization’s processes and operations are just as ripe for exploitation as its IT systems. Consider a billing system that prints out customer information for review during marketing meetings. After the meetings, the administrative assistant collects the information and simply deposits the information into the recycling bin. A resourceful industrial spy comes by the office once a week or so and rifles through the recycling bin and collects substantial information about the organization’s performance and customers. Not a single element of IT or technology was involved in this vulnerability. The vulnerability present was completely based on the operating procedures of the organization. If the organization had adopted media-handling protocols that included marking and secure destruction requirements, the information would have been marked sensitive and then been shredded after the meeting.

As pointed out prior, people can be an organization’s greatest asset (in fact, they are arguably the only asset an organization has that doesn’t always depreciate over time), and they can be one of the greatest risks. Hiring individuals with conflicts of interest, backgrounds that could lead to extortion or blackmail, and those with general trust issues can harm an organization more than any technical breach or operational blunder. A massive fortress is worthless if one of the guards is willing to unlock the door in the middle of the night for an enemy.

**Risk Assessment**

To handle the combination of threats and vulnerabilities, retail organizations must adopt risk assessment procedures that not only assess risk from a mandatory compliance perspective but also from an organizational risk perspective. The board of directors should consider bringing in outside assessors or auditors to confirm the information assurance program has sufficient authority to provide visibility into risk and mitigate it where possible.

While many retail organizations will be required to use a QSA as part of their PCI-DSS assessment, they should carefully consider the credentials of the organization they choose. Not all assessors understand the business or mission of the organization. While any organization can run a vulnerability scan, an understanding of assets and mission must be present to determine risk to an organization. The impact of a vulnerability changes from one organization to another and sometimes within the same organization. The vulnerability on a test server with no information on it may be low risk, while the same vulnerability on a production server with cardholder information may be high risk. If the assessor doesn’t understand the difference between the systems and how they support the organization, the risk assessment will be inherently flawed.

When choosing an assessor, organizations should demand to see past work and also interview the assessor to determine how much about the retail organization they actually know. Additionally, asking the assessor how they plan on gathering initial information about the organization will help understand their assessment approach. Are they simply asking for a network map, a range of IP addresses, and any machines they can’t take down? If so, they may not be best suited to give an honest risk assessment. Questions about data flows, business operations, business partners, data interconnections, and business impact assessments should be referred to a more qualified assessor.

**Risk Mitigation**

Once risk is identified, it must be mitigated, transferred, accepted, or avoided. Retail organizations must attempt to mitigate as much risk as possible through a proactive information assurance program. Information assurance controls implemented during the design and requirements phases of implementation are crucial in preventing information breaches.

**Policy, Procedures, Standards, and Guidance**

Retail organizations must ensure that sufficient standards, policy, and guidance exist to protect the organization against allegations of negligence and ignorance. Policies should cover the mandatory regulations covering privacy and PCI-DSS compliance in addition to any industry- or economy-specific requirements.

Retail organizations should develop standards for the encryption used to protect cardholder information and sensitive information throughout the organization. In addition to establishing a key escrow policy, standards should specify approved tools and technologies acceptable to process, store, or transmit sensitive information. Only the CISO or other qualified individual should approve deviations from the standard.

Procedures for handling sensitive information must be developed. These should include not only digital information but also physical information such as paper and portable media. The procedures should reference the correct standards for encryption, destruction, and retention. Additionally, incident response procedures should establish clear reporting instructions for any member of the organization to report suspicious activity or confirmed incidents.

Guidance for the organization should include who to contact in the information assurance program when engaging in a data transfer outside of the organization or who to contact when determining procurement requirements for a new system or a new location.

**Human Resources**

As noted in the February 6 Home Depot breach shown in [Table 27-1](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch27.html#ch27tab1), insider threats should be a considerable concern in retail. From an attacker’s perspective, gaining physical access to the POS system or customer information is the first step in figuring out ways to siphon it out and use it for identity theft or fraudulent actions. While retailers must ensure they control workforce costs, they must also have assurances the workforce is trustworthy.

As part of a mature information assurance program, the retailer’s workforce positions should be categorized according to risk and access to information. The information assurance team should assist in determining which positions are deemed critical in terms of trustworthiness. Retail organizations should consider background investigations for individuals who have administrative access to systems (including contractors) and also those who may have access to large amounts of customer data. Separation of duties is also an option for organizations large enough to support splitting tasks and duties among several people to force collusion in the event of fraud. For more information about information assurance integration in human resources, please see [Chapter 13](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch13.html#ch13).

Some situations, such as the use of seasonal hires, require a different approach. The cost and expense of performing background checks and separation of duties for temporary workforces may not be worth the effort. In these cases, the organization should increase monitoring of information systems and assets. The organization should consider deploying physical controls such as cameras and badging systems to help determine who was accessing a system at a given time; this provides the service of nonrepudiation. Additionally, all workforce members should be required to take the organization’s information assurance awareness training and sign a rules of behavior and acceptable use agreement prior to gaining access to any information system.

**Certification, Accreditation, and Assurance**

While the concept of certification, accreditation, and the associated measures of assurance are foreign to many industries, the retail industry has familiarity with the PCI-DSS compliance standard. While this is a certification, in practice many retail organizations do not attempt to perform accreditation or authorization of information systems, which involves the acceptance of risk to an organization. While this may seem like an optional step, it is done by default in the organization.

Recall that Target’s board and senior executives were sued as part of the breach. In addition, the Korean executives of the credit card issues resigned or offered to resign. By default, someone in the organization is accepting risk. The question is whether they realize it or not. Senior leaders benefit from operational risk visibility because ignorance is not a defense for due care or due diligence concerns. By implementing a robust information assurance program that drives a certification and accreditation program, retailers can gain greater visibility in their risk postures. As credit card issues begin to slide liability for fraud to retailers, they will need to adopt defensible positions that can provide proof of due diligence and due care. A mature and documented certification and accreditation program can provide a documented approach for due diligence and due care by showing a systemic risk management approach with consistent reporting and mitigation or acceptance of risk.

**Information Assurance: System Development and Acquisition**

As detailed in [Table 27-1](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch27.html#ch27tab1), several breaches have been caused by insecure systems and insecure business partners. As part of their information assurance programs, retailers should include standards for encryption or the adoption of technologies such as chip and pin. Secure system development is also a requirement for PCI-DSS compliance. As systems are developed and moved through their life cycles, the information assurance program should be involved in change management and configuration management to ensure changes to the system do not cause negative impacts to the organization.

To ensure systems are procured and developed with appropriate information assurance, retail organizations should consider integrating an information assurance approval as part of any investment that may process, store, or transmit sensitive information on behalf of the organization. The information assurance program would be responsible for ensuring appropriate controls are in place to protect the organization and the cardholders.

**Physical and Environmental Security Controls**

Retailers typically employ some of the most advanced technologies in their actual retail spaces but may fail to employ the same level of concern for their information systems. Open network ports, open wireless access points, and POS terminals left unattended and unlocked are all opportunities for attackers to gain access to a system. Often, attackers need only one system to use as a pivot point and then start to attack the rest of the system from inside the organization.

Retail organizations must focus on limiting physical access to their POS terminals, wiring closets, and data centers. In situations where limiting access to wiring closets is not possible, the organization must consider stronger technical controls such as network access control and encryption to help ensure attackers cannot exploit an open closet.

Retailers often use security cameras throughout their retail spaces. Retailers must be aware of any legal obligation they have to notify customers they are under surveillance and ensure the monitoring system is operated in accordance with the law. It should go without saying that people have an expectation of privacy in dressing rooms and bathroom facilities, so cameras are never appropriate in these areas.

**Awareness, Training, and Education**

All retail employees should take information assurance awareness training as part of their onboarding, and also routinely throughout the year to ensure they are maintaining a basic awareness of the threat environment and the organizational practices required to secure information. Users who refuse to take the awareness training should be counseled and their access limited until they have completed the training.

Specific training should target managers and mid-level management involved in information technology, program management, and procurement. These individuals should be trained by the information assurance program to recognize when the information assurance team needs to be called in to ensure appropriate information assurance processes, standards, technologies, or requirements are implemented as part of ongoing business, changes, new developments, or procurements.

Education should be reserved for senior members of the information assurance team or those in the organization with a substantial role in managing the risk of the organization. Education is an expensive and long-term endeavor that should be focused on the most strategic elements of the organization.

**Access Control**

Access control is critical for retail operations. Preventing breaches by hacking involves ensuring appropriate access control. As part of an ongoing information assurance assessment program, retail organizations should inventory all administrator-level accounts and determine whether access is still required. Accounts with no owner should be scrutinized and placed under observation. By default, all users of the organization should get only “limited” access accounts to inhibit the installation of malicious software through spear phishing or other methods.

Retail organizations should also consider multifactor authentication for their administrative users and senior executives. Multifactor authentication increases the level of difficulty when brute-force attacks are attempted. Additionally, retail organizations must carefully scrutinize the access they give to outside contractors and vendors. While they should have passed a background investigation or suitability check, they should be given no more access than absolutely required to do their job. Organizations must remember that the third party could lose the credentials to a hacker who could then use them to attack the network and systems of the retailer.

**Continuous Monitoring, Incident Response, and Forensics**

A mature continuous monitoring program must ensure collection of threat and vulnerability information from the network and systems in addition to information collected from managerial and operational assessments. The continuous monitoring must ensure residual risk is identified and delivered to authorizing or accrediting officials for mitigation, transference, avoidance, or acceptance. Many organizations will cite their SIEM as their continuous monitoring solution; however, the SIEM is only as good as the statistics knowledge and business knowledge of those using it. False alarms and numerous nonevents only lessen the credibility of a security operations or cybersecurity intelligence team.

**Business Continuity and Backups**

Most retailers are concerned with availability and integrity of their operations when it comes to business continuity and backups. However, losing an unencrypted backup tape can be just as devastating as having an entire system hacked. As part of the retail organization’s business continuity and backup strategy, the information assurance program must demand that strong encryption and media-handling procedures are followed. If cloud computing providers are used for business continuity or backups, they must also adhere to the same standards and be subject to audits by the retail organization.

**Further Reading**

• Federal Reserve Bank of Atlanta. Into the Breach: Protecting the Integrity of the Payment System, February 10, 2014. <http://portalsandrails.frbatlanta.org/emv/>.

• Financial Fraud Action UK. Fraud the Facts, 2013. [www.financialfraudaction.org.uk/download.asp?file=2772](http://www.financialfraudaction.org.uk/download.asp?file=2772).

• First Data, EMV, and Encryption + Tokenization: A Layered Approach to Security, 2012. [www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF](http://www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF).

• Payment Card Industry (PCI) Data Security Standard, November 2013. <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf>.

• Payment Card Industry (PCI). PCI Point-to-Point Encryption: Solution Requirements and Testing Procedures, July 2013. <https://www.pcisecuritystandards.org/documents/P2PE_Hybrid_v1.1.1.pdf>.

• Payment Card Industry Data Security Standard. PCI DSS Applicability in an EMV Environment, Version 1, October 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_emv.pdf>.

• PCI Security Standards Council. PCI for Small Merchants. <https://www.pcisecuritystandards.org/smb/index.html>.

• Privacy Rights Clearinghouse. Chronology of Data Breaches 2005 – Present. <https://www.privacyrights.org/data-breach>.

• Rosenbush, Steve. Target Warning Shows Limits of Cyber Intelligence. <http://blogs.wsj.com/cio/2014/02/14/target-warning-shows-limits-of-cyber-intelligence/>.

• Wang, Abigail. Smart Chip Credit Cards Wouldn’t Have Saved Target. <http://securitywatch.pcmag.com/internet-crime/320071-smart-chip-credit-cards-wouldn-t-have-saved-target>.

**Critical Thinking Exercises**

1. An executive of a small business is worried about attacks and breaches. He accepts credit cards and has a web presence for ordering and accounting. He currently has all his information systems on a single Internet connection and is worried about hackers. What can the executive do to help mitigate his concerns?

2. A large retailer has just experienced a breach. The CIO has explained to the board of directors that this will never happen again because the credit card issuers are requiring the customers to move to “chip and PIN” technology for their credit cards. Is he right?