

EXPERT ADVICE

How E-Commerce Apps Are Putting Your Site at Risk

[Back to Online Version](#)

[E-Mail Article](#)

[Reprints](#)



By Michael D. Peters
E-Commerce Times
10/05/10 5:00 AM PT

Many developers do not overlook security on purpose; it's just that the focus is usually on feature and functionality, not the nuts and bolts of building a secure software application. These technical oversights can leave a relatively easy opening for attackers to leverage. Cross-site scripting or data source injection are the most common attacks -- yet, ironically, among the easiest to prevent.

▼ advertisement

High Demand for Qualified Internet Marketing Professionals!

The MBA/Internet Marketing from U.S. News-ranked Florida Tech adds a powerful credential to your resume. [Advance your career and master Internet marketing with an MBA 100% online.](#)

E-commerce security has never been more top-of-mind for retailers. Security breaches like the one that happened at TJX in 2007 reverberate not only through the media, but also -- more importantly -- through consumer confidence, for years. Even with an aggressive clean-up strategy, an attack can create lasting damage to a retail brand from which sales may never recover.

In the past few years, e-commerce applications have evolved to become more advanced and more intricate in nature. If you were to compare today's applications to a machine, you would find far more moving parts than there were 10 years ago. Adding more moving parts to the machine exponentially increases the associated risks to the retailer.

As developers continue to push the limits of feature and functionality, these slicker, faster applications are prompting retailers concerned with security to ask, "Which applications are leaving my site most vulnerable?"

The simple answer is that they all are. Any application that is human-facing presents opportunities for theft and corruption. However, it's an important distinction to note that "human-facing" is not limited to the dangerous world of cybercriminals beyond the gates. While hackers

certainly pose significant threats to an e-commerce site, trusted internal sources like employees, partners, vendors -- even auditors -- can introduce an even greater risk.

This is why it's important for retailers to take a hard look at any application running on their site to determine both internal and external vulnerabilities to customer data and company information. Then, there are several strategies to decrease the level of risk applications create for a retail organization.

Focused Project Management

Implementing a strong project management methodology is one of the most fundamental ways to increase the security of e-commerce applications. Information security should be a part of the conversation from project inception. It is more logical and economical to build a foundationally sound application than to retrofit an application when something bad happens.

Following is a brief checklist of considerations in the planning stages:

- **Privacy:** the relationship between collection and transmission of data and the expectation of privacy. Privacy concerns exist wherever personally identifiable information is collected and stored in electronic or physical forms.
- **Encryption Technologies:** the process of transforming electronic information using a software cipher to make it unreadable to anyone except those possessing the key.
- **Security Architecture:** describes how the security controls or security countermeasures are positioned, and how they relate to the overall IT architecture while serving the purpose of maintaining the system's quality attributes -- among them confidentiality, integrity and availability.
- **Compliance:** in general, conforming to a rule such as a specification, policy, standard or law.
- **Governance:** overall information management activities used to ensure that critical management information reaching the executive team is sufficiently complete, accurate and timely, providing the control mechanisms to ensure that strategies, directions and instructions from management are carried out systematically and effectively.

At the application development stage, it's crucial to be diligent about segregation of duties. The code can't be created in a vacuum. Review by independent team members will help keep malicious or vulnerable code out of a production environment. The usage of unencrypted customer data is also quite prevalent, and it can be easily used for identity theft purposes, so oversight, data obfuscation and hashing techniques are critical to keeping the data safe.

It's important to bring security to the forefront of preproduction testing. By running security certification evaluations of application development, QA and pre-production environments, a technical team can ferret out any bugs that may pose a risk to the retailer.

Once into production, the strongest security strategy entails routine and ongoing support and vulnerability assessments. The team should be looking at the same checklist of considerations used in the planning stages on an ongoing basis. For example, be sure that the database

administrator isn't exempt from the oversight rules that were put in place. The database administrator poses the single greatest risk in an organization because of the individual's access to customer information and knowledge of internal systems.

Strengthened Technical Capabilities

In the past, hackers were often interested in doing no more than hacking into and defacing a site. That is no longer the case. Today, it is all about profits. Cybercriminals are well funded and going straight for the customer information. This naturally makes applications like the shopping cart, which handles financial information, a greater target than the library application for product information. A poorly written application, regardless of the code it was developed on, opens a site up to potentially devastating vulnerabilities that can very easily be avoided.

For instance, the lack of strong encryption is one of the most straightforward things to remedy. Message digest, symmetric block cipher, or public-key algorithms come in a variety of strengths, depending on the intended application of encryption. While there are dozens of encryption algorithms in the world, it's highly recommended that developers use the strongest and most secure encryption algorithms available. Chances are, your users, clients or customers will not even be aware of the usage of the stronger encryption algorithms.

Oftentimes, for example, a basic security check reveals that the configurable features on the Web server are left unlocked in their full-feature condition, which permits weaker encryption algorithms to be used in addition to the strongest. The e-commerce application is then built on top, thereby allowing similar vulnerabilities that transfer the first vulnerability to the public-facing area of the site. A simple disabling of these vulnerable features goes a long way toward increasing the security of the application.


Many developers do not overlook security on purpose; it's just that the focus is usually on feature and functionality, not the nuts and bolts of building a secure software application. These technical oversights can leave a relatively easy opening for attackers to leverage. Cross-site scripting or data source injection are the most common attacks -- yet, ironically, among the easiest to prevent.

Improved Technical and Business Team Communication

The technical and business teams need to develop a synergy that will support security through the entire organization. The management team has the ability to set the tone from the top down that security is a priority. The technical team in turn has the responsibility to include information security as part of the ongoing strategy.

One of the challenges is that the teams are often speaking different languages. The technical team needs to articulate the technical risks in a way that ties back to business priorities. The team should not only be aware of the risks, but also come armed with solutions to mitigate those risks. It's not enough to come to the table and say, "this could be a problem." Offering concrete solutions with an identified risk gives the business team an actionable plan to support going forward.

On the other hand, as a business leader, it's important to seriously consider the advice of the technical experts. Many of the most significant security risks start small and may sound insignificant, but they can prove to be devastating in the long term. There will always be the demands of delivery and budget, but with the company's reputation and customers' data at risk, it's unwise to gamble and ignore the sage advice of the security and technical professionals.

All of the above being said, e-commerce applications are really no different from any other software applications from a technical or information security perspective. The trifecta approach of governance, technology and vigilance can help mitigate risk and go a long way toward protecting the company's brand and customers. 

Michael D. Peters, MBA, CISSP, CRISC, CISM, CMBA, CCE, is chief information security officer of [CrossView](#), a provider of mobile data intelligence solutions.