Fit forCommerce™

eCommerce Diligence™ Checklist

Internet Security Best Practices

1. ***Conduct a risk assessment and include more than just your ecommerce site.*** Analyze your site, access to the site, and internal systems that communicate with your site to identify potential intrusion, corruption, and destruction risks. Assign a criticality level to each. High priority components would include systems that, if attacked, would have a major disruption to your business; medium, a moderate effect, and low, a minor effect.

2. ***Create an information security policy.*** Security policies will outline your employees' roles and responsibilities for each system they access. It also defines which systems are off limits. Extending this policy to contractors and suppliers will inform them of the security protocols they must follow.

3. ***Identify ways to secure each system and create.*** Starting with the high priority systems, determine the systems, applications and processes needed to make them secure, being careful not to lock them down, impacting desired business usage.

4. ***Create and manage a vulnerability program.*** Security must be considered across all areas of your organization, not just eCommerce. Internal systems, networks and processes, offsite backups, laptop and VPN access, internet and intranets -- all can be sources of security breaches. Ensure they are current.

5. ***Develop a security team with adequate resources and processes.*** As you consider systems to secure data, you will need to also consider the resources, responsibilities, and processes to use and manage the security systems. Who will manage the systems? Who will monitor and address intrusions?

6. ***Create a security response plan.*** Develop a plan to respond to security violations; a plan to shut down, fix, and restore services; and a post-mortem process to identify ways to prevent security breaches. Ensure your legal team has signed off on this response plan, as 45 out of 50 states now have "Data Breach Laws" and associated penalties.

7. ***Design your security plan to work with your business processes.*** Security is critical to the survival of some businesses. However, so is actually running the business! Make sure that each security measure is planned out to consider the impact to business processes.

8. ***Make sure your network is secure.*** A good starting point in network security is to lock down all access points and only open up the ones needed. Microsoft SQL, FTP, and SSH servers are popular targets for password guessing attacks because of the access that is gained if a valid username/password pair is identified. SQL Injection, Cross-site Scripting, and PHP File Include attacks continue to be the three most popular techniques used for compromising web sites.

9. ***Determine the right level of website content security for you.*** Many times, retailers feel that they must encrypt product data going to their ecommerce site. Why? All of this data is available on the web anyway. Make sure you really think about the pros and cons of securing website data and have a solid rationale or business case for each.

10. ***Hire an outside internet security firm to routinely test your systems.*** There are many firms that help 'certify' your website as secure. These services typically test your network, insure SSL usage, and provide a visible 'seal of approval' to give your customers higher online purchase confidence.

For 1000s of Best Practices and Advice across 100s of topics:
Join eCommerceKnow-How.com!

eCommerce Diligence™ Checklist

Internet Security Key Questions to Ask Providers

Company

1. How long have you been in this business?
2. How many clients do you have? How many clients have you lost, and why?
3. What clients fall into your "sweet spot"?
4. What peripheral or support services do you offer that support your product (e.g., ecommerce, accounting, custom development, training)?

Products/Services

1. Is your solution offered as a consulting service or on-demand solution?

If consulting service:

   a. Please describe your implementation process.
   b. When do you re-evaluate customers' security?

If SAAS/ASP:

   a. Do you have different service tiers?
   b. What do they include?
   c. Do all tiers include maintenance and support?
   d. How often are new features introduced
   e. What can I do if I need a feature you don't have or plan to have soon?

2. What optional services do you provide?
3. How long to implement a basic solution? A sophisticated one?
4. What type of training do you provide?
5. What skills does my organization (or hired third-party) need to implement this platform?
6. What technical support services are available? What is your SLA?
   a. Are there human beings I can reach during business hours?
   b. Is your support team located in the US?
7. Which third-party products or ecommerce platform providers have you worked with?
8. Do you provide insurance against external intrusion and malicious manipulation?
9. What security certifications or legal support does your service include?

Features

1. What key features are included in your solution?
   a. What features are currently missing? Or on your roadmap?
   b. What features does management love? What about shoppers?
2. What is your product's competitive advantage over other services? Why?
   a. Price? Dashboard? Ease of use? Flexibility? Don't say "all of the above".
3. Do you provide website certification? How often do you test your customers' sites?
4. Does your service include helping clients achieve PCI Compliance?
   a. Describe exactly what that means. Do you help clients achieve compliance in all areas, or just those directly under their control?
5. Does your service include network intrusion testing?
6. Does your service include SSL certificate creation, monitoring and replacement?
7. Do you monitor and insure data security?
8. Do you protect your clients' visitors from phishing, scams, ad/spyware or browser hacking? How?
9. Do you have a management console or back-end tools for retailers to manage security and view their security status?
   a. Does it include security alerts, or other notification and correction capabilities?
   b. What else can I manage with it?
   c. Does it include reporting and a dashboard?
      i. Please describe reporting capabilities.
      ii. Please provide a list of standard reports.
   d. Is it web-based, application-based, other?

Pricing

1. Please describe your pricing model.
   a. How do you charge?
   b. Are there different levels?
2. How do you charge for annual support? What about maintenance?
3. Are there any additional fees (e.g., implementation, transaction costs, revenue sharing)?