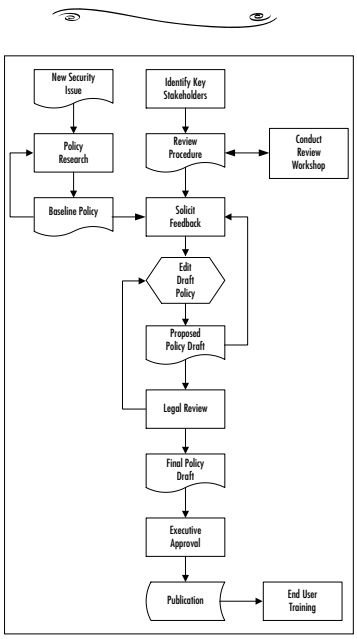
Learn How to Produce a Security Policy

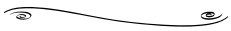


Chapter 5 Answers All Your Questions About Implementing a Secure Site

Q: How do I know if I am logging too much or too little information on my systems?

A: Log the information you feel that you need to make good decisions. If you have problems sifting through the logs to locate issues and you have had proper training, then you need to eliminate the log entries that you do not use to make decisions or keep those log entries and use an automated tool to select only the entries you are interested in. You are logging too little information if you do not have a picture of your systems' operations and your users' behaviors.

Complete Coverage of Third Party Merchants' POS Systems.



ICVERIFY's features include the following:

- Importing credit card transaction data from other PC applications, such as spreadsheets or databases.
- Offline group mode to submit a batch of transactions at one time for authorization.
- Support for Address Verification Systems (AVSs), Retail AVSs, CVV2s, and CVC2s to help reduce fraud due to stolen or fraudulent cards.
- Data import analysis of files for errors before import.

Tools & Traps, Security Alerts, and Damage & Defense Sidebars Make Sure You Don't Miss a Thing:

Tools & Traps…Gauge Your Threat Level with a Honeypot

A honeypot (in an information security context) is a system that is designed to be broken into. Setting up a honeypot will give you an opportunity to study tactics of attackers and possibly pick up a new attack or two along the way. Naturally, the attacker shouldn't be aware that he has broken into a honeypot, and he should think that he's gotten into an ordinary machine with no special monitoring. In fact, a honeypot machine typically has extensive monitoring in place around it, either on the machine itself or via the network. In order for the honeypot to be effective, as much information as possible must be collected about the attacker.

Chapter 8 Answers All Your Questions About Disaster Recovery Planning:

Q: How does e-commerce insurance pay out benefits when I incur a loss?

A: Types of insurance payout provisions are "Pay on Behalf" versus "Indemnification." Pay on Behalf takes care of expenses as they are incurred by the insured and works a bit like homeowner's insurance. If the policy covers your defense in a lawsuit, the legal fees will be paid as they are incurred. Indemnification reimburses the insured for covered expenses already incurred and works a bit like traditional health insurance. You pay for the covered expense and then apply for reimbursement from the insurer. Most insurance offerings for e-commerce are of the "Pay on Behalf" variety.

Q: What's the difference between a password and a passphrase?

A: A passphrase has spaces in it and is made up of multiple words. "ex&mpl3" is a password and "4 sc0re & s3v3n ye4r5 @go" is a passphrase.

Understand Load Balancing and Security

For the most part, load balancers don't change security much, and in fact some can enhance it by acting as limited firewalls. However, in a few cases, security may be impacted.

Obviously the load balancer itself may have security problems—most products do. Attacks against the management interface or address of the load balancer may occur. In this sense, it's much like any system on your network, which might be compromised and give an attacker better leverage for other attacks. If an attacker manages to gain administrative control over your load balancer, they might be able to cause a "virtual defacement" by redirecting your Web traffic to a page of their choosing.

Maintain a Chain of Custody List

- Who was in custody (possession) of the evidence?
- Where was the evidence?
- What security measures are in place at that location?
- What items of evidence existed at that time?