

Summary 209

Solutions Fast Track 210

Frequently Asked Questions 214

Chapter 4 Designing and Implementing Security Policies 219

Introduction 220

Why Are Security Policies Important to an E-Commerce Site? 220

What Is a Security Policy? 221

Value versus Risk 222

Security versus Services Provided 223

Cost of Security versus Cost of Not Having Security 224

Where Do I Begin? 225

What Elements Should My Security Policy Address? 228

Confidentiality and Personal Privacy Policies 230

Requirements for Authentication 231

Requirements for Protecting Customer Information 236

Privacy Policies 239

Information Integrity Policies 240

Quality Assurance Policies 241

Assuring Information Integrity through Technology 244

Availability of Service Policies 244

Are Prewritten Security Policies Available on the Net? 246

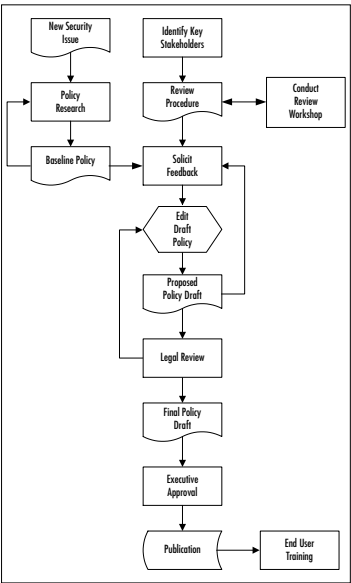
All Organizations Are Different—and So Are Their Policies 246

Example Policies and Frameworks 247

A Word about the Outsourcing of Policy Development 248

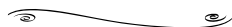
How Do I Use My Security Policy to Implement Technical Solutions? 248

Learn How to Produce a Security Policy



How Do I Inform My Clients of My Security Policies?	251
Building Customer Confidence through Disclosure	252
Security as a Selling Point	253
Summary	254
Solutions Fast Track	255
Frequently Asked Questions	259

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.

Chapter 5 Implementing a Secure E-Commerce Web Site	261
Introduction	262
Introduction to E-Commerce Site Components	262
Implementing Security Zones	264
Introducing the Demilitarized Zone	266
Multiple Needs Equals Multiple Zones	268
Problems with Multi-Zone Networks	271
Understanding Firewalls	272
Exploring Your Firewall Options	272
Designing Your Firewall Rule Set	275
It Starts with a "Deny All" Attitude	276
Common Ports for Common Communications	276
Converting Pseudo-Code to Firewall Rules	278
Protocols and Risks: Making Good Decisions	279
How Do I Know Where to Place My Components?	280
Profiling Systems by Risk	280
Establishing Risk Control Requirements	282
Creating Security Zones through Requirement Grouping	283
Implementing Intrusion Detection	283
What Is Intrusion Detection?	285
Your Choices in Intrusion Detection	286

Network-Based IDS	288
Host-Based IDS	290
Example of a Network-Based IDS	292
Example of a Host-Based IDS	293
Managing and Monitoring the Systems	295
What Kind of Management Tasks Can I Expect to Perform?	295
What Kinds of Monitoring Should I Be Performing?	296
Basic System Monitoring	298
Monitoring Your Security Devices	299
Log File Management	300
Should I Do It Myself or Outsource My Site?	301
Pros and Cons of Outsourcing Your Site	302
Co-Location: One Possible Solution	303
Selecting an Outsource Partner or ASP	303
Summary	305
Solutions Fast Track	305
Frequently Asked Questions	311

Chapter 6 Securing Financial Transactions 313

Introduction	314
Understanding Internet-Based Payment	
Card Systems	315
Credit, Charge, or Debit Cards: What Are the Differences?	315
Point-of-Sale Processing	317
Differences That Charge Cards Bring into the Picture	318
Capture and Settlement	319
Steps in an Internet-Based Payment	
Card Transaction	321
Toxic Data Lives Everywhere!	325
Approaches to Payments via the Internet	326
Options in Commercial Payment Solutions	327
Commerce Server Providers	328
Braving In-house Resources	329

Complete Coverage of Third Party Merchants' POS Systems.

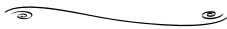
ICVERIFY's features include the following:

- 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.

Secure Payment Processing Environments	331
Additional Server Controls	335
Controls at the Application Layer	336
Understanding Cryptography	337
Methodology	337
Substitution Method	337
Transposition Method	338
Transposition Example	339
The Role of Keys in Cryptosystems	342
Symmetric Keys	342
Asymmetric Keys	342
Principles of Cryptography	343
Understanding Hashing	344
Digesting Data	345
Digital Certificates	348
CCITT X.509	349
Examining E-Commerce Cryptography	351
Hashing Functions	351
Block Ciphers	352
Implementations of PPK Cryptography	352
The SSL Protocol	353
Transport Layer Security (TLS)	355
Pretty Good Privacy (PGP)	356
S/MIME	357
Secure Electronic Transactions (SET)	357
XML Digital Signatures	359
Virtual POS Implementation	362
ICVERIFY	362
Alternative Payment Systems	364
Smart-Card-Based Solutions	365
EMV	365
MONDEX	367
Visa Cash	368
The Common Electronic Purse	
Specification (CEPS)	369
Proxy Card Payments	369
PayPal	370

Amazon Payments	370
Funny Money	371
Beenz	371
Flooz	371
Summary	372
Solutions Fast Track	373
Frequently Asked Questions	379

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 7 Hacking Your Own Site 381

Introduction	382
Anticipating Various Types of Attacks	382
Denial of Service Attacks	382
Information Leakage Attacks	384
File Access Attacks	385
Misinformation Attacks	386
Special File/Database Access Attacks	387
Elevation of Privileges Attacks	388
Performing a Risk Analysis on Your Site	389
Determining Your Assets	390
Why Attackers Might Threaten Your Site and How to Find Them	392
Testing Your Own Site for Vulnerabilities	395
Determining the Test Technique	396
Researching Your Vulnerabilities	399
Mapping Out a Web Server	407
Using Automated Scanning Tools	409
Hiring a Penetration Testing Team	414
Summary	418
Solutions Fast Track	419
Frequently Asked Questions	423

Chapter 8 Disaster Recovery Planning: The Best Defense 425

Introduction	426
What Is Disaster Recovery Planning?	426
Structuring a Disaster Recovery Plan	428
Loss of Data or Trade Secrets	429

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. "example" is a password and "4 score & 3v3n ye4r5 @go" is a passphrase.

Loss of Access to Physical Systems	431
Loss of Personnel or Critical Skill Sets	436
Practicing Compliance with Quality Standards	436
Ensuring Secure Information Backup and Restoration	438
The Need for Backups and Verification	439
An Example Backup Rotation Process	440
Storage Area Networks	442
Protecting Backups of Sensitive Information	443
User Authentication	444
Data Encryption and Controls	445
Key Management	446
Planning for Hardware Failure or Loss of Services	447
The Single Point of Failure Problem	448
ISP Redundancy	449
Network Hardware Redundancy	451
System Hardware Redundancy	451
Expanding the Scope of Your Solutions	453
How Do I Protect against Natural Disasters?	454
Hot Sites: The Alternate Path to Recovery	455
How Do I Choose a Hot Site?	456
Testing the Process	456
Understanding Your Insurance Options	457
Errors and Omissions Coverage	458
Intellectual Property Liability	459
First Party E-Commerce Protection	460
Determining the Coverage You Need	461
Financial Requirements	463
The Delicate Balance: Insurance and the Bottom Line	464
Coverage That May Not Be Needed	464
Summary	466
Solutions Fast Track	467
Frequently Asked Questions	472

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.

Chapter 9 Handling Large Volumes of Network Traffic 475

Introduction	476
What If My Sites Popularity Exceeds My Expectations?	476
Determining the Load on Your Site	478
Determining Router Load	479
Determining Switch Load	483
Determining Load Balancer Load	484
Determining Web Server Load	485
Performance Tuning the Web Server	488
How Do I Manage My Bandwidth Needs?	493
Contracting for Bandwidth	493
Estimating Required Service Levels	496
How Do I Know When I Need More Bandwidth?	497
Obtaining Bandwidth on Demand	498
Introduction to Load Balancing	499
What Is Load Balancing?	500
Changing the Destination MAC Address	501
Modifying the IP Addresses	502
Using a Proxy Server	503
Finding a Custom Software/Clustering Solution	504
Determining Load	504
The Pros and Cons of Load Balancing	505
Load Balancing and Security	505
Summary	509
Solutions Fast Track	510
Frequently Asked Questions	512

Chapter 10 Incident Response, Forensics, and the Law 515

Introduction	516
Why Is an Incident Response Policy Important?	516
Panic or Be Calm: You Decide	516
How Not to Handle an Incident	517

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?

Proper Policy Pays Off	518
Incident Response Policy Recap	524
Establishing an Incident Response Team	525
Setting the Prosecution Boundaries	526
Attackers Crossing the Line	526
Understanding the Chain of Custody	529
Establishing an Incident Response Process	530
Introduction to Forensic Computing	531
Tracking Incidents	538
Resources	542
Legal/Government/Law Enforcement	542
Backup/Forensics	542
Incident Tracking Systems	543
Miscellaneous	544
Summary	545
Solutions Fast Track	546
Frequently Asked Questions	550

Appendix A Cisco Solutions for Content Delivery **553**

Introduction	554
Improving Security Using Cisco LocalDirector	555
LocalDirector Technology Overview	555
LocalDirector Product Overview	556
LocalDirector Security Features	557
Filtering of Access Traffic	557
Using <i>synguard</i> to Protect against SYN Attacks	557
Using Network Address Translation to Hide Real Addresses	559
Restricting Who Is Authorized to Have Telnet Access to the LocalDirector	560
Password Protection	561
Syslog Logging	562
Security Geographically Dispersed Server Farms Using Cisco DistributedDirector	563

DistributedDirector Technology Overview	563
DistributedDirector Product Overview	565
DistributedDirector Security Features	565
Limiting the Source of DRP Queries	565
Authentication between	
DistributedDirector and DRP Agents	566
Password Protection	568
Syslog Logging	570
Improving Security Using the Cisco Content	
Services Switch	570
Content Services Switch Technology	
Overview	571
Content Services Switch Product Overview	572
Content Services Switch Security Features	573
FlowWall Security	573
Using Network Address Translation	
to Hide Real Addresses	574
Firewall Load Balancing	575
Password Protection	576
Disabling Telnet Access	577
Syslog Logging	578
Known Security Vulnerabilities	578
Summary	580
Frequently Asked Questions	581
Appendix B Hack Proofing Your	
E-Commerce Site Fast Track	583
Index	625