A COMPLETE SOLUTION FOR CYBERSECURITY & CYBERDEFENSE

Information Systems Security & Assurance Curriculum

www.issaseries.com
At Jones & Bartlett Learning, our commitment to creating high-quality print and online learning solutions is revolutionizing how instructors teach and how students and professionals learn. We develop educational programs and services that improve learning outcomes and enhance student achievement by combining authoritative content written by respected authors with innovative, proven, and engaging technology applications that meet the diverse needs of today’s instructors, students, and professionals. Our experienced Account Specialists will work with you to match our titles and technology learning solutions to your unique curriculum.

Contact Your Account Specialist and Experience the Difference Today!

- Quality Content
- Cutting-Edge Technology
- Custom and Curriculum Solutions
- Student and Educator Support
- Superior Customer Service

Stay Connected

Facebook: www.facebook.com/jonesbartlettlearning
Twitter: @JBLearning
Blog: blogs.jblearning.com

Click Here to Learn More
A Leader in CyberSecurity & CyberDefense Education

As the number of cyberattacks increases, so does the need for qualified cybersecurity professionals. To help meet this need, Jones & Bartlett Learning has developed the first comprehensive program solution designed to prepare students for success in IT Security, Cybersecurity, Information Assurance, and Information Systems Security. This innovative curriculum, developed by certified IT professionals, combines first-of-its-kind technology, student-friendly texts, and complete instructor support to facilitate seamless implementation, ensure improved student outcomes, and increased retention rates.

The Jones & Bartlett Learning Information Systems Security & Assurance Curriculum (ISSA Series) works with cutting-edge technology and software to deliver hands-on, experiential learning that provides authorized CompTIA Approved quality content.

We urge you to explore the many teaching and learning options that the ISSA Series provides, and welcome your thoughts, feedback and ideas for new content coverage.

Christopher Will,
Sr. VP, Curriculum Solutions
Publisher, Information Systems Security & Assurance Series
cwill@Jblearning.com

Technical Support

With dedicated technical support, you can feel confident that you and your students have the help you need when you need it, including a full service help desk with knowledgeable technicians ready to troubleshoot any lab step.

For added convenience, a Common Tasks document is included with all Virtual Security Cloud Labs, allowing you to troubleshoot on your own.

Table of Contents

- Virtual Security Cloud Labs 5-11
- Interactive Cybersecurity Game Environment 12-13
- Fundamentals of Communications and Networking 14-15
- Fundamentals of Information Systems Security 16-17
- Legal Issues in Information Security 18-19
- Managing Risk in Information Systems 20-21
- Security Policies and Implementation Issues 22-23
- Auditing IT Infrastructures for Compliance 24-25
- Access Control, Authentication, and Public Key Infrastructure 26-27
- Security Strategies in Windows Platforms and Applications 28-29
- Security Strategies in Linux Platforms and Applications 30-31
- Network Security, Firewalls, and VPNs 32-33
- Hacker Techniques, Tools, and Incident Handling 34-35
- Internet Security: How to Defend Against Attackers on the Web 36-37
- System Forensics, Investigation, and Response 38-39
- Cyberwarfare: Information Operations in a Connected World 40-41
- Wireless and Mobile Device Security 42-43
- ISSA Student Survey Result 44-46
- Also Available in Cybersecurity 47

View This Catalog Online and On the Go!

To view this catalog online and on your mobile device, visit www.issaseries.com.
Account Specialists

CAREER & PROPRIETARY SCHOOLS:
For more information on implementing the ISSA series in your institution, please email careered@jblearning.com.

COLLEGES, UNIVERSITIES, & HIGH SCHOOLS:
Kirstie Mason
1-800-832-0034 ext. 8182 | kmason@jblearning.com
DE, MA, NH, NY, TX
Aaron Fatato
1-800-832-0034 ext. 8239 | afatato@jblearning.com
AR, AZ, CO, CT, GA, HI, ID, IL, IN, KS, KY, LA, MD, ND, NE, NM, NV, OK, PA, SD, TN, VA
Amanda Chagnon DeCoste
1-800-832-0034 ext. 8122 | achagnon@jblearning.com
AK, AL, CA, DC, FL, IA, ME, MI, MN, MO, MS, MT, NC, NJ, OH, OR, RI, SC, UT, VT, WA, WI, WV, WY

BUSINESS DEVELOPMENT & SALES:
Meghan McCauley
Director of Business Development & Sales
1-978-460-4382 | mmccauley@jblearning.com

CANADA:
Nelson Education, Ltd
1120 Birchmount Road | Toronto, Ontario M1K5G4 | Canada
Phone (416) 752-9448|(800) 268-2222
Fax (416) 752-8101|(800) 430-4445
For orders: nelson.orderdesk@nelson.com
For all other inquiries: nelson.her@nelson.com

WHOLESALE, TRADE, & RETAIL:
Lisa Papa, Executive Director Retail Trade Sales
lpapa@jblearning.com
Office: 1-518-250-5231
Mobile: 1-978-460-3666

For the Latest Information on the ISSA Series, Visit: www.ISSASeries.com
THE Best Price
ON YOUR PRINT & DIGITAL COURSE MATERIALS

Buy Direct and Receive the Lowest Price on Your Course Material

For Students, Ordering Textbooks and Digital Courseware Directly from Jones & Bartlett Learning is as easy as 1-2-3

1. Visit www.shopJBLearning.com
2. Enter the Product Code/ISBN in the Search Field
3. Add to Cart and Proceed to Check Out

Students using www.ShopJBLearning.com will receive preferred pricing and all in stock orders will ship within 24-48 hours!

Questions? Contact Us Today at: JBLSupport@shopJBLearning.com or 1-877-420-1732.
Toolwire and Jones & Bartlett Learning Win Gold Medal for Security Training and Education

PLEASANTON, CA and BURLINGTON, MA—Toolwire and Jones & Bartlett Learning announced that Info Security Products Guide, the industry’s leading information security research and advisory guide, has named their Virtual Security Cloud Labs winner of the 2013 Global Excellence Awards in the “Security Training and Educational Programs” category. These prestigious global awards recognize security and IT vendors with advanced, ground-breaking products and solutions that are helping raise the bar in all areas of security and technologies.

Jones & Bartlett Learning Virtual Security Cloud Labs, powered by Toolwire, provide a first-of-its-kind learning environment for Information Technology (IT) security training. This “virtual sandbox” learning environment provides instant, unscheduled access to 65 labs from the convenience of a web-browser and allows students to practice “white hat” hacking on an actual IT infrastructure. Reproducing complex real-world challenges, these labs enable students to learn by completing actual “hacking” exercises and then prepare students with the skills to protect digital assets against these types of activities.

For learning institutions, these fail-safe practice labs keep learning self-contained so that student activities are isolated in a safe environment and do not put a learning institution’s assets at risk. For instructors, these labs, part of the Jones & Bartlett Learning comprehensive twelve-title Information Systems Security & Assurance Curriculum, are an easy-to-use blended learning solution.

For students, the labs are mapped to popular industry certifications such as CompTIA Security+, SSCP, 8570.01 Directive, NSA (4011 and 4013 government standings), and NIST Standards (800 series). Providing up to 200 hours of hands-on experience, while students are still in school, enables those who want to sit for these certifications to get ahead of the game.

“We are extremely honored to receive this industry recognition from the Info Security Products Guide.” commented Cameron D. Crowe, Toolwire’s Executive Vice President. “Toolwire has developed and hosted hands-on learning environments for Information Technology training for over 15 years. Through our partnership with Jones & Bartlett Learning, we have created a unique cybersecurity solution that has already been very well received by institutions of Higher Education. A must have for all college and security professionals, these practical training environments could become an industry standard in the next few years.”

“We work tirelessly to develop the highest quality content—both print and online—so this acknowledgement is extremely rewarding. More importantly, it means educators have a high-quality, CNSS-approved, ISSA coursework offering to train and prepare information systems security professionals.” said Christopher Will, Senior Vice President of Custom and Curriculum Solutions at Jones & Bartlett Learning.

ABOUT INFO SECURITY PRODUCTS GUIDE AWARDS
SVUS Awards organized by Silicon Valley Communications are conferred in four annual award programs: The Info Security’s Global Excellence Awards, The IT Industry’s Hot Companies and Best Products Awards, The Golden Bridge Business and Innovation Awards, and Consumer Products Guide’s Best Choice Awards. These premier awards honor organizations of all types and sizes from all over the world including people behind them, the products, performance, PR and marketing.

To learn more, visit www.svusawards.com.
The new **Virtual Security Cloud Lab 2.0** environment includes the following operating system and software.

**Featured Operating Systems:**
- Windows 2012 R2 (64 bit)
- Debian v7 (x64 bit)
- CentOS 6.4 (x64 bit)
- FreeBSD (x64 bit)

**Legacy Operating Systems:**
- Windows XP (Legacy)
- Windows Vista (Legacy and against Microsoft licensing to virtualized)
- Windows 7 (Microsoft does not allow virtualization for Desktop as Service)
- Windows 8 (Microsoft does not allow virtualization for Desktop as Service)
- Ubuntu 10.10 (Legacy)
- Debian 5 (Legacy)

**Virtual Security Cloud Labs 2.0 Software includes:**

<table>
<thead>
<tr>
<th>Software Name</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader</td>
<td>Microsoft Internet Information Services</td>
</tr>
<tr>
<td>Aircrack-ng</td>
<td>Microsoft Users and Computers</td>
</tr>
<tr>
<td>Apache</td>
<td>Microsoft Windows Active Directory</td>
</tr>
<tr>
<td>Avast</td>
<td>Microsoft Windows Defender</td>
</tr>
<tr>
<td>AVG</td>
<td>Microsoft Windows Event Viewer</td>
</tr>
<tr>
<td>BackTrack</td>
<td>Microsoft Windows Firewall</td>
</tr>
<tr>
<td>Basic Analysis and Security Engine (BASE)</td>
<td>Microsoft Windows Network Policy Server (NPS)</td>
</tr>
<tr>
<td>Bmon</td>
<td>Microsoft Windows Picture and Fax Viewer</td>
</tr>
<tr>
<td>Chrootkit</td>
<td>Microsoft Windows Security Configuration Wizard</td>
</tr>
<tr>
<td>ClamAV</td>
<td>Microsoft Windows Security Essentials</td>
</tr>
<tr>
<td>Damn Vulnerable Web Application (DVWA)</td>
<td>Microsoft Windows Server Backup</td>
</tr>
<tr>
<td>Device Manager Viewer (DevManView)</td>
<td>MyLastSearch</td>
</tr>
<tr>
<td>DVWA</td>
<td>MySQL</td>
</tr>
<tr>
<td>EICAR</td>
<td>Nessus</td>
</tr>
<tr>
<td>FavoritesView</td>
<td>Netwitness Investigator</td>
</tr>
<tr>
<td>FileZilla (FileZilla Server and FileZilla Client)</td>
<td>OpenOffice</td>
</tr>
<tr>
<td>Firefox</td>
<td>P2 Commander</td>
</tr>
<tr>
<td>FreeNX</td>
<td>PHP</td>
</tr>
<tr>
<td>GNU</td>
<td>Pkstat</td>
</tr>
<tr>
<td>GnuPG (GNU Privacy Guard (GnuPG)</td>
<td>Process Explorer</td>
</tr>
<tr>
<td>GPG (GPG4Win)</td>
<td>PuTTY</td>
</tr>
<tr>
<td>Gufw</td>
<td>Python</td>
</tr>
<tr>
<td>Helix</td>
<td>Rats Source Code Auditing Tool</td>
</tr>
<tr>
<td>Icacls.exe</td>
<td>Rootkit Hunter</td>
</tr>
<tr>
<td>IECacheView</td>
<td>Sam Spade Freeware Utility</td>
</tr>
<tr>
<td>IECookiesView</td>
<td>SHA 1sum</td>
</tr>
<tr>
<td>IHistoryView</td>
<td>Skipfils Web Scanner</td>
</tr>
<tr>
<td>Iftop</td>
<td>skipfish</td>
</tr>
<tr>
<td>Iperf</td>
<td>Splunk</td>
</tr>
<tr>
<td>izArc</td>
<td>S-Tools</td>
</tr>
<tr>
<td>izArc Archiver</td>
<td>TCPDUMP</td>
</tr>
<tr>
<td>Kleopatra</td>
<td>TCPtrak</td>
</tr>
<tr>
<td>MBSA</td>
<td>Tftpd32</td>
</tr>
<tr>
<td>MD5sum</td>
<td>Tripwire</td>
</tr>
<tr>
<td>Metasploit</td>
<td>UltraVNC Viewer</td>
</tr>
<tr>
<td>Microsoft Assessment and Planning (MAP) Toolkit</td>
<td>Webalizer</td>
</tr>
<tr>
<td>Microsoft Baseline Security Analyzer (MBSA)</td>
<td>WinAudit</td>
</tr>
<tr>
<td>Microsoft BitLocker Drive Encryption</td>
<td>WinHex</td>
</tr>
<tr>
<td>Microsoft Encrypting File System</td>
<td>Wireshark</td>
</tr>
<tr>
<td>Microsoft Group Policy Management Tool</td>
<td>Zenmap GUI</td>
</tr>
</tbody>
</table>

CONTACT US TODAY FOR MORE INFORMATION ABOUT THE INFORMATION SYSTEMS SECURITY & ASSURANCE CURRICULUM
Innovative Labs Provide Realistic, Hands-on Experiential Learning

The Information Systems Security & Assurance Curriculum (ISSA) is available with the Virtual Security Cloud Labs 2.0 environment, delivered in a first-of-its-kind cloud computing environment using cutting-edge technology. These hands-on labs provide a fully immersive mock IT infrastructure enabling students to test their skills with realistic security scenarios, scenarios they will encounter in their future careers.

**The Environment Provides:**
- Embedded Lab Manuals
- The Latest Software
- Challenge Questions
- Enhanced User Experience

---

### Fundamentals of Information System Security
SECOND EDITION — Virtual Security Cloud Labs

1. Performing Reconnaissance and Probing Using Common Tools
2. Performing a Vulnerability Assessment
3. Enabling Windows Active Directory and User Access Controls
4. Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
5. Performing Packet Capture and Traffic Analysis
6. Implementing a Business Continuity Plan
7. Using Encryption to Enhance Confidentiality and Integrity
8. Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities
10. Implementing an Information Systems Security Policy

### Access Control, Authentication, and Public Key Infrastructure
SECOND EDITION — Virtual Security Cloud Labs

1. Configuring and Active Directory Domain Controller
2. Managing Windows Accounts and Organizational Units
3. Configuring Windows File System Permissions
5. Configuring Windows Firewall
6. Managing Linux Accounts
7. Configuring Linux File System Permissions
8. Encrypting and Decrypting Files with PKI
9. Authenticating Security Communications with Digital Signature
10. Encrypting and Decrypting Web Traffic with HTTPS

---

Please note that labs may be updated or changed to keep pace with new data in the field.
## Security Strategies in Windows Platforms and Applications

**SECOND EDITION — Virtual Security Cloud Labs**

1. Implementing Access Control with Windows Activity Directory
2. Using Access Control Lists to Modify File System Permissions on Windows Systems
3. Configuring Bitlocker and Windows Encryption
4. Identifying and Removing Malware from Windows Systems
5. Managing Group Policy Within the Microsoft Windows Environment
6. Creating a Scheduled Backup and Replicating System Folders
7. Securing Servers with the Security Configuration Wizard and the Windows Firewall
8. Securing Internet Client and Server Applications on Windows Systems
9. Protecting Digital Evidence, Documentation, and the Chain of Custody

## Security Strategies in Linux Platforms and Applications

**SECOND EDITION — Virtual Security Cloud Labs**

1. Installing a Core Linux Operating System on a Server
2. Configuring Basic Security Controls on a Centos Linux Server
3. Hardening Security with User Account Management and Security Controls
4. Applying Hardened Linux File System Security Controls
5. Hardening Security for Linux Services and Applications
6. Hardening Security by Controlling Access
7. Hardening Security for the Linux Kernel
10. Defining Linux OS and Application Backup and Recovery Procedures

## Network Security, Firewalls, and VPNs

**SECOND EDITION — Virtual Security Cloud Labs**

1. Analyzing Protocols with Wireshark
2. Using Wireshark and Netwitness Investigator to Analyze Wireless Traffic
3. Configuring a pfSense Firewall on the Client
4. Configuring a pfSense Firewall for the Server
5. Penetration Testing a pfSense Firewall
6. Using Social Engineering Techniques to Plan an Attack
7. Configuring a Virtual Private Network Server
8. Configuring a VPN Client for Secure File Transfers
9. Attacking a Virtual Private Network
10. Investigating and Responding to Security Incidents

## Internet Security: How to Defend Against Attackers on the Web

**Virtual Security Cloud Labs**

1. Evaluating Web Server Vulnerabilities
2. Obtaining Personally Identifiable Information Through Internet Research
3. Performing a Post-Mortem Review of a Data Breach Incident
4. Exploiting Known Web Vulnerabilities on a Live Web Server
5. Applying OWASP to a Web Security Assessment
6. Applying Regulatory Compliance Standards
7. Performing Dynamic and Static Quality Control Testing
8. Performing an IT and Web Application Security Assessment
9. Recognizing Risks and Threats Associated with Emerging Technologies
10. Implementing a Security Development Lifecycle (SDL) Plan

## Hacker Techniques, Tools, and Incident Handling

**SECOND EDITION — Virtual Security Cloud Labs**

1. Assessing and Securing Systems on a Wide Area Network (WAN)
2. Applying Encryption and Hashing Algorithms for Secure Communications
3. Data Gathering and Footprinting on a Targeted Web Site
4. Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation
5. Attacking a Vulnerable Web Application and Database
6. Identifying and Removing Malware on a Windows System
7. Analyzing Network Traffic to Create a Baseline Definition
8. Auditing a Wireless Network and Planning for a Secure WLAN Implementation
9. Investigating and Responding to Security Incidents
10. Securing the Network with an Intrusion Detection System (IDS)

## System Forensics, Investigation, and Response

**SECOND EDITION — Virtual Security Cloud Labs**

1. Applying the Daubert Standard to Forensic Evidence
2. Documenting a Workstation Configuration Using Common Forensic Tools
3. Uncovering New Digital Evidence Using Bootable Forensic Utilities
4. Creating a Forensic System Case File for Analyzing Forensic Evidence
5. Analyzing Images to Identify Suspicous or Modified Files
6. Recognizing the Use of Steganography in Image Files
7. Automating E-mail Evidence Discovery Using P2 Commander
8. Decoding an FTP Protocol Session for Forensic Evidence
9. Identifying and Documenting Evidence from a Forensic Investigation
10. Conducting an Incident Response Investigation for a Suspicious Login
Teaching Information Security Just Got Easier with New ISSA Analytics!

Now Information Security instructors can quickly and easily assess student-progress and address knowledge gaps with the new Analytics Dashboard to accompany the Virtual Security Cloud Labs. The Analytics Dashboard includes a number of informative reports that provide actionable student usage data.

- Identify which students are spending the most, or least, amount of time in the labs
- Determine the duration of time each student is spending on a specific lab exercise
- Determine the average amount of time students are spending in the labs in a given time period.

*Please note: screen shots are in draft form.

Click Here to Learn More
Ensure your students are prepared for their future careers using courseware mapped to leading certification standards, including:

- National Center of Academic Excellence Knowledge Units (KUs)
- National Initiative for Cybersecurity Education (NICE)
- NIST SP 800-16-DoD Cyberspace Workforce Initiatives
- CNSS 4011 & 4013
- CompTIA Security+
- Certified Ethical Hacker (CEH)

The ISSA Series Is a CompTIA Authorized Partner!

The Jones & Bartlett Learning Information Systems Security & Assurance Curriculum is an authorized Security+ CompTIA Content Partner. This prestigious stamp of approval validates that the ISSA Curriculum is in compliance with CompTIA Approved Quality Content, and includes the comprehensive coverage, key learning objectives, and sound instructional design that will prepare students to sit for the Security+ exam.
Award-Winning, Immersive Information Security Training in an Engaging Game-Like Environment

Hands-on Training Simulations Identify Cybersecurity Threats and Vulnerabilities

Integrate Into Your ISSA Courseware!
Discount Pricing Available When Bundled with ISSA Courseware

Jones & Bartlett Learning with MAVI Interactive are working together to raise student awareness on information security best practices. These immersive, realistic and engaging games:

- Emphasize an engaging and fun learning environment
- Use adaptive decision trees & scenarios
- Boast a modular structure for easy customization
- Provide detailed user statistics and reporting
- Require NO special software or hardware

These products are recognized as some of the most notable and cutting edge training products on the market and can be easily integrated into your ISSA Series courseware.

Request a Demo Today To learn more or request a demo, contact your Account Specialist at go.jblearning.com/FindMyRep
Course Options

AGENT SUREFIRE SERIES:
These point-and-click adventure games deliver training in 30-40 minutes, then give the trainee a chance to continue practicing by engaging in the “catch the hacker” scenario. Over 120 discoverable challenges help strengthen real-world skills in detecting and eliminating cybersecurity vulnerabilities.

Agent Surefire: Insider Threat
Set in a simulated office environment, Agent Surefire: Insider Threat provides engaging immersive content delivery that allows learning by trial and error, situational awareness, and immersed decision making, by way of identifying violations in a realistic work environment and real-world threat scenario.

Agent Surefire: InfoSec
Agent Surefire: InfoSec is an immersive Information Security training simulation in a game-like format. It is an off-the-shelf e-learning course designed to raise user awareness on information security best practices. It is designed to effortlessly bridge daily experience with the methods of securing sensitive information. After completing this hands-on course, users will recognize their essential role in safeguarding sensitive information inside an office environment.

SENTINEL SERIES:
These mini-games provide an immersive Information Assurance training simulation designed to create awareness of information security threats and vulnerabilities, and change user behavior concerning cybersecurity best-practices.

Sentinel: Travel Security
ISBN: 978-1-284-10536-0
In Sentinel: Travel Security, students are placed in the role as a security inspector and tasked with tracing the progress of an on-going cyber breach. They must catch the hacker by scrutinizing various environments, identifying cyber threats, security violations and vulnerabilities, as well as handle discovered incidents according to company policy.

Sentinel: Office Security
Sentinel: Office Security is a serious game that places the student in the position of a skilled inspector in a real-world cyber breach scenario happening in near-real-time. In the role of Sentinel, the trainee is sent to investigate a company that has become a victim of a cyber breach. He/she is tasked with scrutinizing the environment, categorizing security threats, making incident handling decisions, discovering how the leak might have happened, and stopping the on-going cyber breach.

Click Here to Learn More
Networks have long been regarded as methods to connect resources. While this is still the case, today’s networks are required to support an increasing array of real-time communication methods. Video chat, real-time messaging, and always-connected resources put demands on networks that were previously unimagined. *Fundamentals of Communications and Networking, Second Edition* helps readers understand today’s networks and the way they support the evolving requirements of different types of organizations. It covers the critical issues of designing a network that will meet an organization’s performance needs and discusses how businesses use networks to solve business problems.

**THE COMPLETE CURRICULUM SOLUTION**

The *Information Systems Security & Assurance Curriculum* (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

**Virtual Security Cloud Labs**

The ISSA series is available with *Virtual Security Cloud Labs*—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

**Applied Labs**

The applied labs allow users to experience hands-on, equipment-based labs that mimic real-world IT security scenarios in a realistic mock environment. The majority of the labs used within *Fundamentals of Communication and Networking* incorporate the Virtual Security Cloud Lab environment. Each lab opens with an Introduction and Learning Objectives and then walks learners through the steps necessary to complete the lab, including helpful notes along the way. Assessment worksheets follow each lab and ask learners to look back and discuss specific points from the lab.

For a complete list of the Virtual Security Cloud Labs, visit [www.issaseries.com](http://www.issaseries.com).

**Digital Solutions**

*Fundamentals of Communications and Networking* provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved retention rates. Available in the moodle platform, or customize to fit your LMS. Contact your Account Specialist for details.
Table of Contents

Part 1: Evolution of Communications
Chapter 1: Today’s Personal and Business Communications Requirement
Chapter 2: Solving Today’s Business Communication Challenges
Chapter 3: Circuit-Switched, Packet-Switched, and IP-Based Communications

Part 2: Fundamentals of Networking
Chapter 4: The Evolution of Ethernet
Chapter 5: TCP/IP and Networking
Chapter 6: Layer 2 Networking
Chapter 7: Layer 2 Networking VLANs
Chapter 8: Layer 3 Networking
Chapter 9: Wireless LAN Standards
Chapter 10: Voice over Internet Protocol (VoIP)
Chapter 11: Unified Communications and Session Initiation Protocol

Chapter 12: Fault Management and Network Operations Center
Chapter 13: Configuration Management and Asset Control
Chapter 14: Performance Management
Chapter 15: Security Management

Key Features
- Introduces network basics by describing how networks work
- Discusses how networks support the increasing demands of advanced communications
- Illustrates how to map the right technology to your organization’s needs and business goals
- Outlines how businesses use networks to solve business problems, both technically and operationally

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

About the Authors
Michael G. Solomon (CISSP, CISM, TICSA) is a full-time speaker, consultant, and trainer, and a former college instructor who specializes in development and assessment security topics. As an IT professional and consultant since 1987, he has worked on projects or trained for over 60 major companies and organizations including EarthLink, Nike Corporation, Lucent Technologies, BellSouth, UPS, the U.S. Coast Guard, and Norrell. From 1998 until 2001, he was an instructor in the Kennesaw State University’s Computer Science and Informations Science (CSIS) department, where he taught courses on software project management, C++ programming, computer organization and architecture, and data communications.

David Kim is president and chief security officer for Security Evolutions, Inc. (SEI). SEI provides IT security training and consulting services for organizations around the world. Mr. Kim’s IT and IT security experience encompasses more than 20 years of technical engineering, technical management, and sales and marketing management. Previously, Mr. Kim was chief operating officer of (ISC)2 Institute where he was responsible for content development, educational products, and educational delivery for (ISC)2 and its IT security professional certifications.

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

Click Here to Learn More
Revised and updated with the latest data in the field, the second edition of *Fundamentals of Information Systems Security* provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. It opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part Two is adapted for the official (ISC)² SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the Systems Security Certified Practitioner certification. The text closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws.

**THE COMPLETE CURRICULUM SOLUTION**

The *Information Systems Security & Assurance Curriculum* (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

**Virtual Security Cloud Labs**

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

**Applied Labs**

Lab #1: Performing Reconnaissance and Probing Using Common Tools
Lab #2: Performing a Vulnerability Assessment
Lab #3: Enabling Windows Active Directory and User Access Controls
Lab #4: Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control
Lab #5: Performing Packet Capture and Traffic Analysis
Lab #6: Implementing a Business Continuity Plan
Lab #7: Using Encryption to Enhance Confidentiality and Integrity
Lab #8: Performing a Website and Database Attack by Exploiting Identified Vulnerabilities
Lab #9: Eliminating Threats with a Layered Security Approach
Lab #10: Implementing an Information Systems Security Policy

**Digital Solutions**

*Fundamentals of Information Systems Security* is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.

**Software used in these labs include:** AVG, Damn Vulnerable Web Application, FileZilla, GPG4Win, IZarc Archiver, Kali, MySQL, PuTTY, Wireshark, Zenmap GUI, and more. Please note that the labs and software may be updated or changed to keep pace with new data in the field.
Table of Contents

Part 1: The Need for Information Security
Chapter 1: Information Systems Security
Chapter 2: Changing How People and Businesses Communicate
Chapter 3: Malicious Attacks, Threats, and Vulnerabilities
Chapter 4: The Drivers of Information Security Business

Part 2: The Systems Security Certified Practitioner (SSCP®) Professional Certification from (ISC)²
Chapter 5: Access Controls
Chapter 6: Security Operations and Administration
Chapter 7: Auditing, Testing, and Monitoring
Chapter 8: Risk, Response, and Recovery
Chapter 9: Cryptography
Chapter 10: Networks and Telecommunications
Chapter 11: Malicious Code and Activity

Chapter 12: Information Security Standards
Chapter 13: Information Security Education and Training
Chapter 14: Information Security Professional Certifications
Chapter 15: US Compliance Laws

About the Authors

David Kim is president and chief security officer for Security Evolutions, Inc. (SEI). SEI provides IT security training and consulting services for organizations around the world. Mr. Kim’s IT and IT security experience encompasses more than 20 years of technical engineering, technical management, and sales and marketing management. This experience includes LAN/WAN, internetworking, enterprise network management, and IT security for voice, video, and data networking infrastructures. Previously, Mr. Kim was chief operating officer of (ISC)² Institute located in Vienna, Virginia, where he was responsible for content development, educational products, and educational delivery for (ISC)² (www.isc2.org) and its IT security professional certifications.

Michael G. Solomon, CISSP, CISM, TICSA, is a full-time security speaker, consultant, and trainer, and a former college instructor who specializes in development and assessment security topics. As an IT professional and consultant since 1987, he has worked on projects or trained for over 60 major companies and organizations including EarthLink, Nike Corporation, Lucent Technologies, BellSouth, UPS, the U.S. Coast Guard, and Norrell.

New & Key Features

- Focuses on new risks, threats, and vulnerabilities associated with the transformation to a digital world
- New sections on cloud computing, risk analysis, IP mobility, OMNIBus, and Agile Software Development
- Includes changes in laws, security certificates, standards, amendments, and the proposed Federal Information Security Amendments Act of 2013 and HITECH Act
- Provides new and updated data, statistics, tables, and cases
- Presents a high-level overview of each of the seven domains within the (ISC)² System Security Certification Practitioner certification

Instructor’s Material

- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

Custom Publishing

Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats

Available as an eTextbook through VitalSource.

Click Here to Learn More
Legal Issues in Information Security
SECOND EDITION

Joanna Lyn Grama

Revised and updated to address the many changes in this evolving field, the second edition of Legal Issues in Information Security addresses the area where law and information security concerns intersect. Information systems security and legal compliance are now required to protect critical governmental and corporate infrastructure, intellectual property created by individuals and organizations alike, and information that individuals believe should be protected from unreasonable intrusion. Written by an industry expert, this text provides a unique, in-depth look at the major federal and state laws that regulate information security and data privacy practice. Using numerous cases and activities, it provides a comprehensive explanation of the most pertinent regulatory laws, discussing key concepts common to information security, data privacy, and the American legal system.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor's or certification level.

Lab Manuals

The Information System Security & Assurance Curriculum offers lab manuals available in print and online, which allow students to put their classroom skills to work on numerous laboratory exercises.

Digital Solutions

Legal Issues in Information Security is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.

Applied Labs

Lab #1: Creating an IT Infrastructure Asset List and Identifying Where Privacy Data Resides
Lab #2: Case Study for Activity on Veteran Affairs and Loss of Privacy Information
Lab #3: Case Study on PCI DSS Non-Compliance: CardSystems Solutions
Lab #4: Analyzing and Comparing of GLBA and HIPAA
Lab #5: Case Study on Issues Related to Sharing Customers’ Confidential Information
Lab #6: Identifying the Scope of Your State’s Data and Security Breach Notification Law
Lab #7: Case Study on Digital Millennium Copyright Act
Lab #8: Cyberstalking or Cyberbullying and Laws to Protect Individuals
Lab #9: Recommending IT Security Policies to Help Mitigate Risk
Lab #10: Case Study in Computer Forensics—Pharmaceutical Company

Please note that labs may be updated or changed to keep pace with new data in the field.
# Table of Contents

**Part 1: Fundamental Concepts**
- Chapter 1: Information Security Overview
- Chapter 2: Privacy Overview
- Chapter 3: The American Legal System

**Part 2: Laws Influencing Information Security**
- Chapter 4: Security and Privacy of Consumer Financial Information
- Chapter 5: Security and Privacy of Information Belonging to Children and Educational Records
- Chapter 6: Security and Privacy of Health Information
- Chapter 7: Corporate Information Security and Privacy Regulation
- Chapter 8: Federal Government Information Security and Privacy Regulation
- Chapter 9: State Laws Protecting Citizen Information and Breach Notification Laws
- Chapter 10: Intellectual Property Law
- Chapter 11: The Role of Contracts
- Chapter 12: Criminal Law and Tort Law issues in Cyberspace

**Part 3: Security and Privacy in Organizations**
- Chapter 13: Information Security Governance
- Chapter 14: Risk Analysis, Incident Response, and Contingency Planning
- Chapter 15: Computer Forensics and Investigations

---

**About the Author**

Joanna Lyn Grama, (JD, CISSP, CIPP/IT) serves as the information security policy and compliance director for Purdue University, where she creates the university’s IT security policy and is responsible for compliance governance and activities. She is a member of the Information Systems Audit and Control Association, the organization for IT governance professionals; the American Bar Association, Section of Science and Technology Law, Information Security Committee; EDUCAUSE; and the Indiana State Bar Association. Joanna graduated from the University of Illinois College of Law with honors, and was the editor-in-chief of The Elder Law Journal. She is a frequent speaker on a variety of IT security topics, including identity theft, personal information security, and university compliance issues.

---

**Key Features**

- Includes discussions of amendments in several relevant federal and state laws and regulations since 2011
- Reviews relevant court decisions that have come to light since the publication of the First Edition
- Includes numerous information security data breaches highlighting new vulnerabilities
- Identifies legal issues surrounding the collection, handling, and use of digital evidence
- Illustrates how to create an organizational information security program that addresses compliance requirements

**Instructor’s Material**

- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

**Custom Publishing**

Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

**Alternate Formats**

Available as an eTextbook through VitalSource.
Managing Risk in Information Systems
SECOND EDITION

Darril Gibson

Revised and updated with the latest data in the field, the second edition of Managing Risk in Information Systems provides a unique in-depth look at how to manage and reduce IT-associated risks. It includes a comprehensive overview of the SSCP® Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructures and compliance. Written by industry experts, and using a wealth of examples and exercises, this book incorporates hands-on activities to walk the reader through the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

Lab Manuals

The Information System Security & Assurance Curriculum offers lab manuals available in print and online, which allow students to put their classroom skills to work on numerous laboratory exercises.

Digital Solutions

Managing Risk in Information Systems is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.

Applied Labs

Lab #1: Identifying Threats and Vulnerabilities in an IT Infrastructure
Lab #2: Aligning Risks, Threats, and Vulnerabilities to the COBIT p09 Risk Management Controls
Lab #3: Defining the Scope and Structure of an IT Risk Management Plan
Lab #4: Performing a Qualitative Risk Assessment for an IT Infrastructure
Lab #5: Identifying Risks, Threats, and Vulnerabilities in an IT Infrastructure Using Zenmap GUI (Nmap) and Nessus Reports
Lab #6: Developing a Risk Mitigation Plan Outline for an IT Infrastructure
Lab #7: Performing a Business Impact Analysis for a Mock IT Infrastructure
Lab #8: Developing an Outline for a Business Continuity Plan for an IT Infrastructure
Lab #9: Developing Disaster Recover Back-Up Procedures and Recovery Instructions
Lab #10: Creating a CIRT Response Plan for a Typical IT Infrastructure

Please note that labs many be updated or changed to keep pace with new data in the field.
Table of Contents

Part 1: Risk Management Business Challenges
Chapter 1: Risk Management Fundamentals
Chapter 2: Managing Risk: Threats, Vulnerabilities, and Exploits
Chapter 3: Maintaining Compliance
Chapter 4: Developing a Risk Management Plan

Part 2: Mitigating Risk
Chapter 5: Defining Risk Assessment Approaches
Chapter 6: Performing a Risk Assessment
Chapter 7: Identifying Assets and Activities to be Protected
Chapter 8: Identifying and Analyzing Threats, Vulnerabilities, and Exploits
Chapter 9: Identifying and Analyzing Risk Mitigation Security Controls
Chapter 10: Planning Risk Mitigation Throughout the Organization
Chapter 11: Turning Your Risk Assessment into a Risk Mitigation Plan

Part 3: Risk Mitigation Plans
Chapter 12: Mitigating Risk with a Business Impact Analysis
Chapter 13: Mitigating Risk with a Business Continuity Plan
Chapter 14: Mitigating Risk with a Disaster Recovery Plan
Chapter 15: Mitigating Risk with a Computer Incident Response Team Plan

About the Author
Darril Gibson is an IT trainer who regularly teaches security topics to Air Force personnel. An adjunct professor, he’s written or co-authored several IT books, including CompTIA Security+: Get Certified Get Ahead, and Mastering Windows Server 2008 R2. In addition, he’s also created training videos on multiple topics for Keystone Learning. Mr. Gibson holds numerous certifications, including (ISC)2 CISSP and CompTIA Security+. He’s also been a Microsoft Certified Trainer since 1999.

Key Features
- Illustrates how to identify and analyze threats and vulnerabilities as well as evaluate security controls to mitigate risk
- Includes the discussion of amendments in several relevant federal and state laws and regulations since 2011
- Discusses how to translate a risk assessment into a risk management plan
- Identifies how to perform a business impact analysis and the difference between business continuity plans and disaster recovery plans

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

CONTACT US TODAY FOR MORE INFORMATION ABOUT THE INFORMATION SYSTEMS SECURITY & ASSURANCE CURRICULUM
Security Policies and Implementation Issues
SECOND EDITION

Rob Johnson

Security Policies and Implementation Issues, Second Edition offers a comprehensive, end-to-end view of information security policies and frameworks from the raw organizational mechanics of building to the psychology of implementation. Written by an industry expert, it presents an effective balance between technical knowledge and soft skills, and introduces many different concepts of information security in clear simple terms such as governance, regulator mandates, business drivers, legal considerations, and much more. With step-by-step examples and real-world exercises, this book is a must-have resource for students, security officers, auditors, and risk leaders looking to fully understand the process of implementing successful sets of security policies and frameworks.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

Lab Manuals

The Information System Security & Assurance Curriculum offers lab manuals available in print and online, which allow students to put their classroom skills to work on numerous laboratory exercises.

Digital Solutions

Security Policies and Implementation Issues is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.

Applied Labs

Lab #1: Crafting an Organization-Wide Security Management Policy for Acceptable Use
Lab #2: Developing an Organization-Wide Policy Framework Implementation Plan
Lab #3: Defining an Information Systems Security Policy Framework for an IT Infrastructure
Lab #4: Crafting a Layered Security Management Policy – Separation of Duties
Lab #5: Crafting an Organization-Wide Security Awareness Training Policy
Lab #6: Defining a Remote Access Policy to Support Remote Healthcare Clinics
Lab #7: Identifying Necessary Policies for Business Continuity – BIA and Recovery Time Objectives
Lab #8: Crafting a Security or Computer Incident Response Policy – CIRT Response Team
Lab #9: Assessing and Auditing an Existing IT Security Policy Framework Definition
Lab #10: Aligning an IT Security Policy Framework to the 7 Domains of a Typical IT Infrastructure

Please note that labs many be updated or changed to keep pace with new data in the field.
Table of Contents

Part 1: The Need for IT Security Policy Frameworks
Chapter 1: Governance and Information Security Policy Management
Chapter 2: Business Drivers for Information Security Policies
Chapter 3: U.S. Compliance Laws and Information Security Policy Requirements

Part 2: Types of Policies and Appropriate Frameworks
Chapter 4: Business Challenges Within the Seven Domains of IT Responsibility
Chapter 5: Information Security Policy Implementation Issues
Chapter 6: IT Security Policy Frameworks
Chapter 7: How to Design, Organize, Implement, and Maintain IT Security Policies
Chapter 8: IT Security Policy Framework Approaches
Chapter 9: User Domain Policies
Chapter 10: IT Infrastructure Security Policies
Chapter 11: Data Classification and Handling Policies and Risk Management Policies
Chapter 12: Incident Response Team (IRT) Policies

Part 3: Implementing and Maintaining an IT Security Policy Framework
Chapter 13: IT Security Policy Implementations
Chapter 14: IT Security Policy Enforcement
Chapter 15: IT Policy Compliance Systems and Emerging Technologies

Key Features
- Provides a modern and comprehensive view of information security policies and frameworks
- Examines the technical knowledge and software skills required for policy implementation
- Explores the creation of an effective IT security policy framework
- Discusses the latest governance, regulatory mandates, business drives, legal considerations, and much more.

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

About the Author
Rob Johnson (CISA, CGEIT, CISM, CISSP) has 20 years’ experience dealing with all aspects of information security, IT audit, risk management, and privacy compliance. His diverse background includes hands-on operational experience as well as providing strategic risk assessment and scoring for leadership and board-level audiences. Currently he works in the security risk management division of a large financial services insurance company. Previously he worked as a first vice president and IT audit and security advisory director at Washington Mutual.
Auditing IT Infrastructures for Compliance
SECOND EDITION

Martin Weiss and Michael G. Solomon
ISBN: 978-1-284-09070-3 • Paperback • 400 pages • © 2016

The second edition of *Auditing IT Infrastructures for Compliance* provides a unique, in-depth look at recent U.S.-based Information systems and IT infrastructures compliance laws in both the public and private sector. Written by industry experts, this book provides a comprehensive explanation of how to audit IT infrastructures for compliance based on the most recent laws and the need to protect and secure business and consumer privacy data. Using examples and exercises, this Second Edition incorporates numerous hands-on activities to prepare readers to skillfully complete IT compliance auditing.

THE COMPLETE CURRICULUM SOLUTION

The *Information Systems Security & Assurance Curriculum* (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

**Lab Manuals**

The *Information System Security & Assurance Curriculum* offers lab manuals available in print and online, which allow students to put their classroom skills to work on numerous laboratory exercises.

**Digital Solutions**

*Auditing IT Infrastructures for Compliance* is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.

**Applied Labs**

Lab #1: Assessing the Impact of Sarbanes-Oxley (SOX) Compliance Law on Enron
Lab #2: Aligning Auditing Frameworks for a Business Unit Within the DoD
Lab #3: Defining a Process for Gathering Information Pertaining to a HIPAA Compliance Audit
Lab #4: Aligning an IT Security Assessment—Risk, Threats, and Vulnerability Assessments—to Achieve Compliance
Lab #5: Defining a Process for Gathering Information Pertaining to a GLBA Compliance Audit
Lab #6: Auditing the Workstation Domain for Compliance
Lab #7: Auditing the LAN-to-WAN Domain for Compliance
Lab #8: Auditing the Remote Access Domain for Compliance
Lab #9: Auditing the Systems/Application Domain for Compliance
Lab #10: Charting Your Career Path—Professional Certification

Please note that labs may be updated or changed to keep pace with new data in the field.
Table of Contents

Part 1: The Need for Compliance
Chapter 1: The Need for Information Systems Security Compliance
Chapter 2: Overview of U.S. Compliancy Laws
Chapter 3: What Is the Scope of an IT Compliance Audit?

Part 2: Auditing for Compliance: Frameworks, Tools, and Techniques
Chapter 4: Auditing Standards and Frameworks
Chapter 5: Planning an IT Infrastructure Audit for Compliance
Chapter 6: Conducting an IT Infrastructure Audit for Compliance
Chapter 7: Writing the IT Infrastructure Audit Report
Chapter 8: Compliance Within the User Domain
Chapter 9: Compliance Within the Workstation Domain
Chapter 10: Compliance Within the LAN Domain
Chapter 11: Compliance Within the LAN-to-WAN Domain
Chapter 12: Compliance Within the WAN Domain
Chapter 13: Compliance Within the Remote Access Domain
Chapter 14: Compliance Within the System/Application Domain

Part 3: Ethics, Education, and Certification for IT Auditors
Chapter 15: Ethics, Education, and Certification for IT Auditors

Key Features
- Includes updates on new pertinent laws and regulations, including FISMA and DoD
- References all new standards such as COBIT, SANS, ISACA, ISO/IEC 27001 and CRMA
- New sections added on the Children’s Online Privacy Protection Act (COPPA), Service Organization Control (SOC) Reports, the NIST Cybersecurity Framework, and Certification in Risk Assessment (CRMA)
- Tips, Notes, FYIs, and Warnings appear throughout the text and provide helpful information related to the subject at hand

About the Authors

Martin Weiss is a manager of information security gurus at RSA, The Security Division of EMC, which helps organizations accelerate their business by solving their most complex and sensitive security challenges. He is also on the board of directors for the Connecticut chapter of ISSA and has written several books. He holds a number of certifications, including Security+, CISSP, MCSE: Security, and RSA CSE. Marty received his MBA from the Isenberg School of Management at the University of Massachusetts and currently lives in New England with his wife and three sons.

Michael G. Solomon, CISSP, CISM, TICSA, is a full-time security speaker, consultant, and trainer, and a former college instructor who specializes in development and assessment security topics. As an IT professional and consultant since 1987, he has worked on projects or trained for over 60 major companies and organizations including EarthLink, Nike Corporation, Lucent Technologies, BellSouth, UPS, the U.S. Coast Guard, and Norrell. From 1998 until 2001, he was an instructor in the Kennesaw State University’s Computer Science and Information Sciences (CSIS) department, where he taught courses on software project management, C++ programming, computer organization and architecture, and data communications.

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

Contact Us Today for More Information About the Information Systems Security & Assurance Curriculum
Access control protects resources against unauthorized viewing, tampering, or destruction. They serve as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized disclosure. Revised and updated with the latest data from this fast-paced field, *Access Control, Authentication, and Public Key Infrastructure, Second Edition* defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs. It looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them. It provides a student and professional resource that details how to put access control systems to work as well as testing and managing them.

**THE COMPLETE CURRICULUM SOLUTION**

The *Information Systems Security & Assurance Curriculum* (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor's or certification level.

*Virtual Security Cloud Labs*

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

*Digital Solutions*

*Access Control, Authentication, and Public Key Infrastructure* is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.

*Applied Labs*

Lab #1: Configuring an Active Directory Domain Controller  
Lab #2: Managing Windows Accounts and Organizational Units  
Lab #3: Configuring Windows File System Permissions  
Lab #4: Managing Group Policy Objects in Active Directory  
Lab #5: Configuring Windows Firewall  
Lab #6: Managing Linux Accounts  
Lab #7: Configuring Linux File System Permissions  
Lab #8: Encrypting and Decrypting Files with PKI  
Lab #9: Authenticating Security Communications with Digital Signatures  
Lab #10: Encrypting and Decrypting Web Traffic with HTTPS

Software used in these labs include: Microsoft Assessment and Planning (MAP) Toolkit, Microsoft users and Computers, Active Directory Users and Computers, Microsoft Group Policy Management Tool, Windows Firewall, and GNU Privacy Guard (GnuPG). Please note that the labs and software may be updated or changed to keep pace with new data in the field.
Table of Contents

Part 1: The Need for Access Control Systems
Chapter 1: Access Control Framework
Chapter 2: Assessing Risk and Its Impact on Access Control
Chapter 3: Business Drivers for Access Controls
Chapter 4: Access Control Policies, Standards, Procedures, and Guidelines
Chapter 5: Security Breaches and the Law

Part 2: Mitigating Risk with Access Control Systems, Authentication, and PKI
Chapter 6: Mapping Business Challenges to Access Control Types
Chapter 7: Human Nature and Organizational Behavior
Chapter 8: Access Control for Information Systems
Chapter 9: Physical Security and Access Control
Chapter 10: Access Control in the Enterprise

Part 3: Implementing, Testing, and Managing Access Control Systems
Chapter 11: Access Control System Implementations
Chapter 12: Access Control Solutions for Remote Workers
Chapter 13: Public Key Infrastructure and Encryption
Chapter 14: Testing Access Control Systems
Chapter 15: Access Control Assurance

New & Key Features

- Updated references to Windows 8 and Outlook 2011.
- A new discussion of recent Chinese hacking incidents.
- Examples depicting the risks associated with a missing unencrypted laptop containing private data.
- New sections on the Communications Assistance for Law Enforcement Act (CALEA) and granting Windows folder permissions are added.
- New information on the Identity Theft Enforcement and Restitution Act and the Digital Millennium Copyright Act (DMCA).

About the Authors

Mike Chapple serves as Chief Information Officer of the Brand Institute, a brand identity consultancy based out of Miami, Florida. He previously served as a computer security researcher with the U.S. National Security Agency, participating in the development of advanced network intrusion detection systems. Mike holds both B.S. and M.S. degrees in Computer Science and is a proud alum of the University of Notre Dame.

Bill Ballad has been active in the IT security community since the mid-1990s. He is the co-author and SME for Securing PHP Web Applications (Addison-Wesley Professional, 2008) and wrote the security chapters for PHP & MySQL Web Development All-in-One Desk Reference for Dummies (For Dummies, 2008). Bill is a senior systems engineer working with mission-critical Windows networks.

Tricia Ballad spent several years as a Web applications developer before becoming a full-time freelance writer and technical editor. She has written online courseware on various consumer electronics and computing subjects and has co-authored PHP & MySQL Web Development All-in-One Desk Reference for Dummies (For Dummies, 2008) and Securing PHP Web Applications for Mere Mortals.

Erin Banks (CISSP) is a technical writer and editor. She has been in the network and security industry for more than 15 years in support, management, and technical sales roles in Fortune 500 and not-for-profit organizations.

Instructor’s Material

- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

Alternate Formats

Available as an eTextbook through VitalSource.

Click Here to Learn More
Security Strategies in Windows Platforms and Applications
SECOND EDITION

Michael G. Solomon

The majority of individuals, students, educators, businesses, organizations, and governments use Microsoft Windows, which has experienced frequent attacks against its well-publicized vulnerabilities. Revised and updated to keep pace with this ever changing field, Security Strategies in Windows Platforms and Applications, Second Edition focuses on new risks, threats, and vulnerabilities associated with the Microsoft Windows operating system. Particular emphasis is placed on Windows XP, Vista, and Windows 7 on the desktop, and Windows Server 2003 and 2008 versions. It highlights how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft Windows operating systems and applications. The book also includes a resource for readers desiring more information on Microsoft Windows OS hardening, application security, and incident management.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor's or certification level.

Virtual Security Cloud Labs

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

Applied Labs

Lab #1: Implementing Access Control with Windows Activity Directory
Lab #2: Using Access Control Lists to Modify File System Permissions on Windows Systems
Lab #3: Configure BitLocker and Windows Encryption
Lab #4: Identifying and Removing Malware From Windows Systems
Lab #5: Managing Group Policy Within the Microsoft Windows Environment
Lab #6: Creating a Scheduled Backup and Replicating System Folders
Lab #7: Securing Servers with the Security Configuration Wizard and the Windows Firewall
Lab #8: Securing Internet Client and Server Applications on Windows Systems
Lab #9: Protecting Digital Evidence, Documentation and the Chain of Custody
Lab #10: Hardening Windows Server Security Using Microsoft Baseline Security Analyzer

Software used in these labs include: Windows Active Directory, Icacls.exe, Microsoft Encrypting File System, Microsoft BitLocker Drive Encryption, AVG, Windows Defender, Microsoft Baseline Security Analyzer (MBSA), Windows Server Backup, Microsoft Windows Firewall, Microsoft Windows Security Configuration Wizard, and Microsoft Internet Information Services (IIS). Please note that the labs and software may be updated or changed to keep pace with new data in the field.

Digital Solutions

Security Strategies in Windows Platforms and Applications is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.
Table of Contents

Part 1: The Microsoft Windows Security Situation
Chapter 1: Microsoft Windows and the Threat Landscape
Chapter 2: Security in the Microsoft Windows OS

Part 2: Managing and Maintaining Microsoft Windows Security
Chapter 3: Access Controls in Microsoft Windows
Chapter 4: Microsoft Windows Encryption Tools and Technologies
Chapter 5: Protecting Microsoft Windows Against Malware
Chapter 6: Group Policy Control in Microsoft Windows
Chapter 7: Microsoft Windows Security Profile and Audit Tools
Chapter 8: Microsoft Windows Backup and Recovery Tools
Chapter 9: Microsoft Windows Network Security
Chapter 10: Microsoft Windows Security Administration

Part 3: Microsoft Windows OS and Application Security Trends and Directions
Chapter 11: Hardening the Microsoft Windows Operating System
Chapter 12: Microsoft Application Security
Chapter 13: Microsoft Windows Incident Handling and Management
Chapter 14: Microsoft Windows and the Security Life Cycle
Chapter 15: Best Practices for Microsoft Windows and Application Security

New & Key Features
- New information on Windows 2012 and its four different editions
- New information on malware, ransomware, and spyware
- The latest on Agile Software Development, including its history, purpose, and definition
- Discussion of hacktivists and examples of some of their recent attacks
- New information on Windows 2012 and DAC, Managed Service Accounts, and Expression-based Security Audit Policy
- Discusses new BitLocker features

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

Click Here to Learn More

About the Author
Michael G. Solomon, CISSP, CISM, TICSA, is a full-time security speaker, consultant, and trainer, and a former college instructor who specializes in development and assessment security topics. As an IT professional and consultant since 1987, he has worked on projects or trained for over 60 major companies and organizations including EarthLink, Nike Corporation, Lucent Technologies, BellSouth, UPS, the U.S. Coast Guard, and Norrell. From 1998 until 2001, he was an instructor in the Kennesaw State University’s Computer Science and Information Sciences (CSIS) department, where he taught courses on software project management, C++ programming, computer organization and architecture, and data communications.
Security Strategies in Linux Platforms and Applications
SECOND EDITION

Michael Jang and Ric Messier
ISBN: 978-1-284-09065-9 • Paperback • 512 pages • © 2017

The second edition of Security Strategies in Linux Platforms and Applications covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion on the risks, threats, and vulnerabilities associated with Linux as an operating system, using examples from Red Hat Enterprise Linux and Ubuntu. Part 2 discusses how to take advantage of the layers of security available to Linux—user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk readers through the fundamentals of security strategies related to the Linux system.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

Virtual Security Cloud Labs

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

Lab #1: Installing a Core Linux Operating System on a Server
Lab #2: Configuring Basic Security Controls on a CentOS Linux Server
Lab #3: Hardening Security with User Account Management and Security Controls
Lab #4: Applying Hardened Linux File System Security Controls
Lab #5: Hardening Security for Linux Services & Applications
Lab #6: Hardening Security for Controlling Access
Lab #7: Hardening Security for the Linux Kernel
Lab #8: Applying Best Practices for Secure Software Management
Lab #10: Defining Linux OS & Application Backup & Recovery Procedures

Software used in these labs include: Linux OS, Python, Tripwire, and Rootkit Hunter. Please note that the labs and software may be updated or changed to keep pace with new data in the field.

Digital Solutions

Security Strategies in Linux Platforms and Applications is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.
Table of Contents

Part 1: Is Linux Really Secure?
Chapter 1: Security Threats to Linux
Chapter 2: Basic Components of Linux Security

Part 2: Layered Security and Linux
Chapter 3: Basic Security: Facilities Through the Boot Process
Chapter 4: User Privileges and Permissions
Chapter 5: Filesystems, Volumes, and Encryption
Chapter 6: Every Service Is a Potential Risk
Chapter 7: Networks, Firewalls, and More
Chapter 8: Networked Filesystems and Remote Access
Chapter 9: Networked Application Security
Chapter 10: Kernel Security Risk Mitigation

Part 3 Building a Layered Linux Security Strategy
Chapter 11: Managing Security Alerts and Updates
Chapter 12: Building and Maintaining a Security Baseline
Chapter 13: Testing and Reporting
Chapter 14: Detecting and Responding to Security Breaches
Chapter 15: Best Practices and Emerging Technologies

Key Features
- Focuses on Linux as a server operating system.
- Covers every major aspect of security on a Linux system.
- Explores open source and proprietary tools when building a layered security strategy for your Linux operating system.
- Offers step-by-step instructions for identifying weaknesses and creating more secure systems.

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

About the Author
Michael Jang (RHCE, LPIC-2, UCP, Linux+, MCP) has been a freelance technical writer since 1998. He had previously worked for more than 10 years as a specialist engineer at Boeing Commercial Airplane Group. Michael has written white papers on new products and processes. He’s also the author of more than two-dozen IT books, including LPIC-1 In Depth (2009) and Ubuntu Server Administration Course (for VTC in 2009). Finally, Michael travels overseas extensively to troubleshoot IT issues and manage projects.

Ris Messier is a security professional who has worked with a number of companies from large Internet service provider down to small software companies. He has run a small networking and security consulting practice for the last several years. Additionally, he has taught courses at both the graduate and undergraduate level.

Click Here to Learn More
Network Security, Firewalls, and VPNs
SECOND EDITION

J. Michael Stewart
ISBN: 978-1-284-03167-6 • Paperback • 490 pages • © 2014

Fully revised and updated with the latest data from the field, Network Security, Firewalls, and VPNs, Second Edition provides a unique, in-depth look at the major business challenges and threats that are introduced when an organization’s network is connected to the public Internet. Written by an industry expert, this book provides a comprehensive explanation of network security basics, including how hackers access online networks and the use of Firewalls and VPNs to provide security countermeasures. Using examples and exercises from the field, this book incorporates hands-on activities to prepare the reader to disarm threats and prepare for emerging technologies and future attacks.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

Virtual Security Cloud Labs

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

Applied Labs

Lab #1: Analyzing Protocols with Wireshark
Lab #2: Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
Lab #3: Configuring a pfSense Firewall on the Client
Lab #4: Configuring a pfSense Firewall on the Server
Lab #5: Penetration Testing a pfSense Firewall
Lab #6: Using Social Engineering Techniques to Plan an Attack
Lab #7: Configuring a Virtual Private Network Server
Lab #8: Configuring a VPN Client for Security File Transfers
Lab #9: Attacking a Virtual Private Network
Lab #10: Investigating and Responding to Security Incidents

Digital Solutions

Network Security, Firewalls, and VPNs is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.

Software used in these labs include: Bmon, DVWA, FileZilla, Gufw, Iftop, Iperf, MBSA, Netwitness Investigator, Splunk, PuTTY, pfSense Firewall, Wireshark, and Zenmap GUI. Please note that the labs and software may be updated or changed to keep pace with new data in the field.
Table of Contents

Part 1: Foundations of Network Security
   Chapter 1: Fundamentals of Network Security
   Chapter 2: Firewall Fundamentals
   Chapter 3: VPN Fundamentals
   Chapter 4: Network Security Threats and Issues

Part 2: Technical Overview of Network Security, Firewalls, and VPNs
   Chapter 5: Network Security Implementation
   Chapter 6: Network Security Management
   Chapter 7: Firewall Basics
   Chapter 8: Firewall Deployment Considerations
   Chapter 9: Firewall Management and Security
   Chapter 10: Using Common Firewalls
   Chapter 11: VPN Management
   Chapter 12: VPN Technologies

Part 3: Implementation, Resources, and the Future
   Chapter 13: Firewall Implementation
   Chapter 14: Real-World VPNs
   Chapter 15: Perspectives, Resources, and the Future

About the Author

J. Michael Stewart has been working with computers and technology for more than 25 years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job-skill and certification courses such as CISSP, CEH, and Security+. He is the primary author of the CISSP Study Guide 4th Edition and the Security+ 2008 Review Guide. In addition, Michael has written numerous books on other security and Microsoft certification and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom. Michael holds the following certifications: CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+Security Windows 2000, MCSA Windows Server 2003, MCDST, MCSE NT & W2K, MCP+, Network+, , iNet+. He graduated in 1992 from the University of Texas at Austin with a bachelor’s degree in Philosophy.

New & Key Features

- New information on Internet Protocol Version 4 (IPv4) with clarification on the difference between IPv6 and IPv4
- Discusses some of the faults of DNS
- New information on “Mobile IP” and “Bring Your Own Device”
- Discusses the use of a sniffer tool or Wireshark
- Uncovers VPN implementation via cloud application
- Updated statistical information and industry data

Instructor’s Material

- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

Custom Publishing

Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats

Available as an eTextbook through VitalSource.

Click Here to Learn More
Hacker Techniques, Tools, and Incident Handling
SECOND EDITION

Sean-Philip Oriyano
ISBN: 978-1-284-03171-3 • Paperback • 500 pages • © 2014

Revised and updated to keep pace with changes in this evolving field, Hacker Techniques, Tools, and Incident Handling, Second Edition begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web. Written by a subject matter expert with numerous real-world examples, the Second Edition provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

The Complete Curriculum Solution

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

Virtual Security Cloud Labs

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

Applied Labs

Lab #1: Assessing and Securing Systems on a Wide Area Network (WAN)
Lab #2: Applying Encryption and Hashing Algorithms for Secure Communications
Lab #3: Data Gathering and Footprinting on a Targeted Web Site
Lab #4: Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation
Lab #5: Attacking a Vulnerable Web Application and Database
Lab #6: Identifying and Removing Malware on a Windows System
Lab #7: Analyzing Network Traffic to Create a Baseline Definition
Lab #8: Auditing a Wireless Network and Planning for a Secure WLAN Implementation
Lab #9: Investigating and Responding to Secure Incidents
Lab #10: Securing the Network with an Intrusion Detection System (IDS)

Software used in these labs include: GNU Privacy Guard (GnuPG), BackTrack, Metasploit, Nessus, Zenmap GUI, Damn Vulnerable Web Application (DVWA), AVG, IZArc Archiver, FileZilla Server and FileZilla, NetWitness Investigator, PuTTY, TFTPdump, Wireshark, Aircrack-ng, MySQL, and Basic Analysis and Security Engine (BASE). Please note that the labs and software may be updated or changed to keep pace with new data in the field.

Digital Solutions

Hacker Techniques, Tools, and Incident Handling is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.
Table of Contents

Part 1: Hacker Techniques and Tools
Chapter 1: Hacking: The Next Generation
Chapter 2: TCP/IP Review
Chapter 3: Cryptographic Concepts
Chapter 4: Physical Security

Part 2: A Technical Overview of Hacking
Chapter 5: Footprinting Tools and Techniques
Chapter 6: Port Scanning
Chapter 7: Enumeration and Computer System Hacking
Chapter 8: Wireless Vulnerabilities
Chapter 9: Web and Database Attacks
Chapter 10: Malware
Chapter 11: Sniffers, Session Hijacking, and Denial of Service Attacks
Chapter 12: Linux and Penetration Testing
Chapter 13: Social Engineering

Part 3: Incident Response and Defensive Technologies
Chapter 14: Incident Response
Chapter 15: Defensive Technologies

New & Key Features
- Includes a completely new Chapter 13 on social engineering and what it means in the context of cybersecurity, including a typical attack, identity theft, and best security practices
- Provides new information on cryptography and encryption in network protocols
- Updated references to Windows 8, Server 2008, Server 2012
- Added information on Active Directory and Symantec Security Suite 10
- Includes new material on using social networks, Wardriving and Warflying, detecting rogue access points and WiFi Pineapple
- New section material on cloud computing and cloud security issues.

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

About the Author
Sean-Philip Oriyano has been actively working in the IT field since 1990. Throughout his career, he has held positions as support specialist to consultants and senior instructor. Currently he is an IT instructor who specializes in infrastructure and security topics for various public and private entities. Sean has instructed for the U.S. Air Force, Navy, and Army at locations in North America and internationally.

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.
Internet Security
How to Defend Against Attackers on the Web
SECOND EDITION

Mike Harwood

Internet Security: How to Defend Against Attackers on the Web, Second Edition provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the internet. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

Virtual Security Cloud Labs

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

Applied Labs

Lab #1: Evaluating Web Server Vulnerabilities
Lab #2: Obtaining Personally Identifiable Information through Internet Research
Lab #3: Perform a Post-Mortem Review of a Data Breach Incident
Lab #4: Exploiting Known Web Vulnerabilities on a Live Web Server
Lab #5: Applying OWASP to a Web Security Assessment
Lab #6: Applying Regulatory Compliance Standards
Lab #7: Performing Dynamic and Static Quality Control Testing
Lab #8: Performing an IT & Web Application Security Assessment
Lab #9: Recognizing Risks and Threats Associated with Emerging Technologies
Lab #10: Implementing a Security Development Lifecycle (SDL) Plan

Software used in these labs include: Damn Vulnerable Web Application (DVWA), PuTTY, skipfish, tcpdump, and RATS. Please note that the labs and software may be updated or changed to keep pace with new data in the field.

Digital Solutions

Internet Security: How to Defend Against Attackers on the Web is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.
Table of Contents

Part 1: Evolution of Computing, Communications, and Social Networking
Chapter 1: From Mainframe to Client/Server to World Wide Web
Chapter 2: Security Considerations for Small Businesses
Chapter 3: Security Considerations for Home and Personal Online Use
Chapter 4: Mitigating Risk When Connecting to the Internet

Part 2: Secure Web-Enabled Application Deployment and Social Networking
Chapter 5: Mitigating Web Site Risks, Threats, and Vulnerabilities
Chapter 6: Introducing the Web Application Security Consortium (WASC)
Chapter 7: Securing Web Applications
Chapter 8: Mitigating Web Application Vulnerabilities
Chapter 9: Maintaining PCI DSS Compliance for E-Commerce Web Sites
Chapter 10: Testing and Quality Assurance for Production Web Sites
Chapter 11: Performing a Web Site Vulnerability and Security Assessment
Chapter 12: Securing Mobile Communications

Part 3: Web Applications and Social Networking Gone Mobile
Chapter 13: Securing Personal and Business Communications
Chapter 14: Security Training, Education, and Certification
Chapter 15: Web Application Security Organizations

Key Features
- Addresses the latest Web security issues and solutions from administrator, developer, and user perspectives
- Examines mobile device and connectivity security
- Tips, Notes, FYIs, and Warnings appear throughout the text and provide helpful information related to the subject at hand
- Chapter Assessments, at the end of each chapter, allow readers to test their understanding of key material from the chapter with solutions provided at the back of the book.

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

About the Author
Mike Harwood (MCT, MCSE, A+, Network+, Server+, Linux+) has more than 15 years experience working in information technology and related fields. In that time, he’s held a number of roles within IT, including network administrator, instructor, technical writer, Web site designer, consultant, and online marketing strategist. He’s been a regular on-air technology contributor for CBC Radio and has written numerous computer books, including the best-selling Network+ Exam Cram for Que Publishing and the A+ Faster Smarter title for Microsoft. Currently Mike is employed as the new editor and writer for the www.yoursecondfifty.com/magazine.

Click Here to Learn More
Computer crimes call for forensics specialists, people who know how to find and follow the evidence. Completely revised and rewritten to keep pace with the changing field of computer forensics, *System Forensics, Investigation, and Response, Second Edition* begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field.

**THE COMPLETE CURRICULUM SOLUTION**

The *Information Systems Security & Assurance Curriculum* (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

---

**Virtual Security Cloud Labs**

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

**Applied Labs**

- Lab #1: Applying the Daubert Standard to Forensic Evidence
- Lab #2: Documenting a Workstation Configuration Using Common Forensic Tools
- Lab #3: Uncovering New Digital Evidence Using Bootable Forensic Utilities
- Lab #4: Creating a Forensics System Case File for Analyzing Forensic Evidence
- Lab #5: Analyzing Images to Identify Suspicious or Modified Files
- Lab #6: Recognizing the Use of Steganography in Image Files
- Lab #7: Automating E-Mail Evidence Discovery Using P2 Commander
- Lab #8: Decoding an FTP Protocol Session for Forensic Evidence
- Lab #9: Identifying and Documenting Evidence From a Forensic Investigation
- Lab #10: Conducting an Incident Response Investigation for Suspicious Login

**Digital Solutions**

*System Forensics, Investigation, and Response* is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.

Software used in these labs include: DevManView, WinAudit, WinHex, P2 Commander, FavoritesView, Helix, IECacheView, IEHistoryView, IECookiesView, MyLastSearch, Process Explorer, S-Tools, NetWitness Investigator, Wireshark, and Splunk. Please note that the labs and software may be updated or changed to keep pace with new data in the field.
Table of Contents

Part 1: The System Forensics Landscape
Chapter 1: Introduction to Forensics
Chapter 2: Overview of Computer Crime
Chapter 3: Forensics Methods and Labs

Part 2: Technical Overview: System Forensics Tools, Techniques, and Methods
Chapter 4: Collecting, Seizing, and Protecting Evidence
Chapter 5: Understanding Information-Hiding Techniques
Chapter 6: Recovering Data
Chapter 7: Email Forensics
Chapter 8: Windows Forensics
Chapter 9: Linux Forensics
Chapter 10: Mac Forensics
Chapter 11: Mobile Forensics
Chapter 12: Performing Network Analysis

Part 3: Incident Response and Resources
Chapter 13: Incident and Intrusion Response
Chapter 14: Trends and Future Directions
Chapter 15: System Forensics Resources

New & Key Features
- The Second Edition includes all new content. A complete re-write of the first edition
- The latest data and statistics on computer forensics
- Chapter restructuring with new chapters on:
  - Email Forensics
  - Windows Forensics
  - Mac Forensics
  - Linux Forensics
  - Mobile Forensics

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

About the Author
Chuck Easttom has spent 14 years in the IT industry as a programmer and IT director. He is currently president and chief software architect of a medical software company in North Texas and is also an adjunct instructor for a community college where he teaches classes to working professionals. Chuck holds many industry certifications and has written 10 computer science books, including two others on JavaScript.

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

Click Here to Learn More
Cyberwarfare
Information Operations in a Connected World

Mike Chapple and David Seidl

Cyberwarfare: Information Operations in a Connected World reviews the role that cyberwarfare plays in modern military operations—operations in which it has become almost impossible to separate cyberwarfare from traditional warfare. Part 1 discusses the history of cyberwarfare and the variety of new concerns its emergence has fostered. Part 2 discusses how offensive cyberwarfare has become an important part of the modern military arsenal. Part 3 explores the future of cyberwarfare; its interaction with military doctrine; and the Pandora’s box opened by recent events, which have set the stage for future cyber attacks.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

Virtual Security Cloud Labs

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

Applied Labs

The applied labs allow users to experience hands-on, equipment-based labs that mimic real-world IT security scenarios in a realistic mock environment. The majority of the labs used within Cyberwarfare incorporate the Virtual Security Cloud Lab environment. Each lab opens with an Introduction and Learning Objectives and then walks learners through the steps necessary to complete the lab, including helpful notes along the way. Assessment worksheets follow each exercise and ask learners to look back and discuss specific points from the lab.

For a complete list of labs that accompany Cyberwarfare, visit www.issaseries.com

Digital Solutions

Cyberwarfare: Information Operations in a Connected World is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved student retention rates.
Part 1: The Cyberwarfare Landscape
Chapter 1: Information as a Military Asset
Chapter 2: Targets and Combatants
Chapter 3: Cyberwarfare, Law and Ethics
Chapter 4: Intelligence Operations in a Connected World

Part 2: Offensive and Defensive Cyberwarfare
Chapter 5: The Evolving Threat: From Script Kiddies to Advanced Attackers
Chapter 6: Social Engineering and Cyberwarfare
Chapter 7: Weaponizing Cyberspace: A History
Chapter 8: Nonstate Actors in Cyberwar
Chapter 9: Defense-in-Depth Strategies
Chapter 10: Cryptography and Cyberwar
Chapter 11: Defending Endpoints
Chapter 12: Defending Networks
Chapter 13: Defending Data

Part 3: The Future of Cyberwarfare
Chapter 14: Cyberwarfare and Military Doctrine
Chapter 15: Pandora’s Box: The Future of Cyberwarfare

Key Features
- Incorporates hands-on activities, relevant examples, and realistic exercises to prepare readers for their future careers.
- Includes detailed case studies drawn from actual cyberwarfare operations and tactics.
- Provides fresh capabilities information drawn from the Snowden NSA leaks.

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts
- Handouts
- Projects
- Study Guide
- Time on Task
- Content Map

About the Authors
Mike Chapple is Senior Director for IT Service Delivery at the University of Notre Dame. In this role, he oversees the information security, data governance, IT architecture, project management, strategic planning and product management functions for the Office of Information Technologies. Mike also serves as a concurrent assistant professor in the University’s Computer Applications and Management Departments where he teaches undergraduate courses on Information Security. Mike earned both his BS and PhD degrees from Notre Dame in computer science & engineering. He also holds a MS in computer science from the University of Idaho and an MBA from Auburn University. Mike is a technical editor for Information Security Magazine and has written several books, including Information Security Illuminated, SQL Server 2008 for Dummies, and the CISSP Prep Guide.

David Seidl is the Senior Director of Campus Technology Services at the University of Notre Dame where he is responsible for database, systems, application, email, and platform administration as well as identity and access management. In addition to his role with Notre Dame’s Office of Information Technologies, David teaches a popular Networking and Security class in Notre Dame’s Mendoza College of Business. He has over 13 years of information security experience and holds a Masters degree in Information Security from Eastern Michigan University in addition to CISSP, GCIH, and GPEN certifications.

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

CONTACT US TODAY FOR MORE INFORMATION ABOUT THE INFORMATION SYSTEMS SECURITY & ASSURANCE CURRICULUM
Wireless and Mobile Device Security

Jim Doherty

The world of wireless and mobile devices is evolving daily, with many individuals relying solely on their wireless devices in the workplace and in the home. The growing use of mobile devices demands that organizations become more diligent in securing this growing technology and determining how to best protect their information assets. Written by an industry expert, Wireless and Mobile Device Security explores the evolution from wired networks to wireless networking, and its impact on the corporate world. Using real-world events, it goes on to discuss risk assessments, threats, and the vulnerabilities of wireless networks, as well as the security measures that should be put in place to mitigate breaches. The text concludes with a look at the three major mobile operating systems, the vulnerabilities of each, security solutions, and the management and control of mobile devices on an enterprise scale.

THE COMPLETE CURRICULUM SOLUTION

The Information Systems Security & Assurance Curriculum (ISSA series) provides a flexible, interactive curriculum solutions with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certification level.

Virtual Security Cloud Labs

The ISSA series is available with Virtual Security Cloud Labs—delivered in a first-of-its-kind cloud computing environment—that provides a fully immersive mock IT infrastructure enabling hands-on experiential learning.

Digital Solutions

Wireless and Mobile Device Security is available with digital courseware and LMS functionality that provides a fully customizable course solution with content built around leading course objectives. Students benefit from full interactive lecture presentations and activities that walk them through key content from the course. Instructors are excited by the grade book functionality, integrated teaching resources, and improved retention rates. Available in the moodle platform, or customize to fit your LMS. Contact your Account Specialist for details.

Applied Labs

The applied labs allow users to experience hands-on, equipment-based labs that mimic real-world IT security scenarios in a realistic mock environment. The majority of the labs used within Wireless and Mobile Device Security incorporate the Virtual Security Cloud Lab environment. Each lab opens with an Introduction and Learning Objectives and then walks learners through the steps necessary to complete the lab, including helpful notes along the way. Assessment worksheets follow each lab and ask learners to look back and discuss specific points from the lab.

For a complete list of the Virtual Security Cloud Labs, visit www.issaseries.com.
Table of Contents

Part 1: Introduction to Wireless and Mobile Networks
Chapter 1: The Evolution of Data Networks
Chapter 2: The Evolution of Wired Networking to Wireless Networking
Chapter 3: The Mobile Revolution
Chapter 4: Security Threats Overview: Wired, Wireless, and Mobile

Part 2: WLAN Security
Chapter 5: How Do WLANs Work?
Chapter 6: WLAN and IP Networking Threat and Vulnerability Analysis
Chapter 7: Basic WLAN Security Measures
Chapter 8: Advanced WLAN Security Measures
Chapter 9: WLAN Auditing Tools
Chapter 10: WLAN and IP Network Risk Assessment

Part 3: Mobile Security
Chapter 11: Mobile Communication Security Challenges
Chapter 12: Mobile Device Security Models
Chapter 13: Mobile Wireless Attacks and Remediation
Chapter 14: Fingerprinting Mobile Devices
Chapter 15: Mobile Malware and Application-Based Threats

Key Features
- Discusses the history and evolution of wireless networks
- Explores the impact of wireless on the corporate world
- Focuses on 802.11 WLAN security in both the small office/home office world and for larger organization
- Gives security solutions to the risks and vulnerabilities of mobile devices

Instructor’s Material
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Custom Publishing
Easily create customized texts to fit your course needs. To learn more contact your Account Specialist.

Alternate Formats
Available as an eTextbook through VitalSource.

Click Here to Learn More

About the Authors

Jim Doherty is the Sr. Vice President and Marketing Officer at Ixia. Jim has lead held marketing, sales and engineering leadership positions at Certes Networks, Motorola, Cisco Systems and Ericsson during a 19-year career in the networking and communications sectors. Jim has made a name for himself in the industry due to his ability to explain networking technologies to non-technical audiences in a way that still satisfies technical professionals. He has extensive speaking and presenting experience and is often sought out to explain networking and communication technologies to non-technical audiences.

Jim is also the creator and co-author of the Networking Simplified series of books, and a comprehensive set of CCNA study notes; published in a number of certification guides.
Student Survey Shows ISSA Cloud Labs Provide an Effective Hands-on Learning Experience

The Information Systems Security & Assurance (ISSA) Virtual Security Cloud Labs (VSCL) are hands-on labs delivered in a cloud computing environment that allow students to test their skills with real-world security tools in a setting that mimics what they will encounter in their future careers.

In April 2014, Jones & Bartlett Learning surveyed nearly 130 student users of the ISSA Series with Virtual Security Cloud Labs (VSCL) and asked about their experience with the product. The purpose of the survey was to learn more about student’s level of satisfaction with the VSCL environment and the educational benefits they provide. The survey conclusively shows that the VSCL provide the hands-on, realistic learning experience that students truly value.

“I would definitely recommend the ISSA Virtual Security Cloud Labs because I was pleased with the product. I learned a lot from participating in the action rather than reading and responding. The lab environment made the knowledge more real and more accessible, which is very important to my learning process.”

ISSA Virtual Security Cloud Labs: Preparing Students with Real-World Experiences

Out of those surveyed the results show that students find the VSCL better prepared them for class and for real-world cybersecurity tasks. Beyond that, they indicated that VSCL saved them time and made lab work more enjoyable.

<table>
<thead>
<tr>
<th>Percentage of Students Agreeing with Each Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Security Cloud Labs allowed me to spend more time on hands-on lab activities.</td>
</tr>
<tr>
<td>76%</td>
</tr>
<tr>
<td>Virtual Security Cloud Labs prepared me well for my lab assignments.</td>
</tr>
<tr>
<td>76%</td>
</tr>
<tr>
<td>Virtual Security Cloud Labs made lab work more enjoyable.</td>
</tr>
<tr>
<td>74%</td>
</tr>
<tr>
<td>Virtual Security Cloud Labs prepared me well for real world tasks.</td>
</tr>
<tr>
<td>72%</td>
</tr>
<tr>
<td>Virtual Security Cloud Labs helped me get through my lab work more quickly.</td>
</tr>
<tr>
<td>72%</td>
</tr>
</tbody>
</table>

ISSA Virtual Security Cloud Labs: A Solution Students Support

Students told Jones & Bartlett Learning that ISSA Virtual Security Cloud Labs are educational, informative and effective...

…and overwhelmingly endorsed ISSA Virtual Security Cloud Labs as a helpful learning tool.
Students Overwhelmingly Agree That VSCL Were a Helpful Learning Tool, Which Allowed Them to Spend More Time on Hands-On Lab Activities

- “[ISSA Labs were the] best part of my education.”
- “I would recommend [ISSA Labs] over the other [Virtual Lab] services I have used.”
- “How can we get all cyber security courses to use ISSA Labs?”
- “[ISSA Labs are] a very powerful tool that is a must in the education environment!”

Logistic Regression Analysis shows that the more time students spend in the labs the more likely they are to rate their experience as highly positive.

Overall, how satisfied are you with ISSA Virtual Security Cloud Labs?

<table>
<thead>
<tr>
<th>Satisfied</th>
<th>Somewhat Satisfied</th>
<th>Dissatisfied</th>
</tr>
</thead>
<tbody>
<tr>
<td>71%</td>
<td>18%</td>
<td>11%</td>
</tr>
</tbody>
</table>

Logistic Regression Analysis of the likelihood of rating ISSA Virtual Cloud Labs “Very Good” as a helpful learning tool.

Predicted probability “very good”

\[
\text{Prob ("Very Good") }= \frac{1}{1 + e^{-(-0.971 + 0.002 \times \text{Minutes})}}
\]

Model is statistically significant at \(p<.05\)

\(n=110\)

ISSA Virtual Security Cloud Labs: A Solution That Helps Students Become Better Cybersecurity Professionals

Students agreed that ISSA Virtual Security Cloud Labs prepared them well, even beyond their course of studies, all the way into their Cybersecurity careers.

- 74% agreed that ISSA Virtual Security Cloud Labs prepared them well for their Cybersecurity career
- 76% agreed that ISSA Virtual Security Cloud Labs prepared them well for real world tasks encountered in Cybersecurity careers
- 81% agreed that ISSA Virtual Security Cloud Labs prepared them well for their Cybersecurity program of studies

**Agree** combines “Agree a lot” and “Agree”; “Disagree” combines “Disagree” and “Disagree a lot”. **Neither Agree Nor Disagree**

Percentage of Students Agreeing with Each Statement

<table>
<thead>
<tr>
<th>ISSA Virtual Cloud Labs prepared me well for my Cybersecurity program of studies.</th>
<th>Agree</th>
<th>Neither Agree Nor Disagree</th>
<th>Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>81%</td>
<td>9%</td>
<td>10%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISSA Virtual Cloud Labs prepared me well for real world tasks encountered in Cybersecurity careers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>76%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISSA Virtual Cloud Labs prepared me well for my Cybersecurity career.</th>
</tr>
</thead>
<tbody>
<tr>
<td>74%</td>
</tr>
</tbody>
</table>

n = 75-92
ISSA Virtual Security Cloud Labs: Prepare Students to Sit for Certification Exams

90% of those students who have sat for the Security+ Certification Exam, passed on their first attempt.

Most importantly, students said that ISSA Virtual Security Cloud Labs provided them with a realistic experience, which prepared them effectively for the tasks encountered as Cybersecurity professionals.

- “[ISSA Labs are] the closest thing to actually being in the field or on an actual job assignment.”
- “[ISSA Labs] will provide for, and allow, hands-on experiences, which will help immensely in real-world situations.”
- “[ISSA Labs] are clear and concise and are successful at creating an environment that makes learning easy.”
- “[ISSA Virtual Cloud Labs] allow you to get ample hands-on experiences in relation to the topics taught in the classroom. They are easy to use, and come with a step-by-step guideline on how to complete the labs. You can access these labs at school and/or at home. All in all ISSA Virtual Cloud Labs can be seen as an excellent tool in and out the classroom!”
- “[ISSA Labs] will provide for, and allow, hands-on experiences, which will help immensely in real-world situations.”

“[I] would recommend using ISSA Virtual Cloud Labs in order to get hands-on opportunity to learn your course objectives in depth. I enjoyed using the labs and am happy that it was provided to me.”

Why did students have such a positive experience with the ISSA Series?

More than 80% of students indicated that the Virtual Security Cloud Labs were helpful in their course.

<table>
<thead>
<tr>
<th></th>
<th>Helpful</th>
<th>Somewhat Helpful</th>
<th>Not Helpful</th>
<th>Not Applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Lab</td>
<td>82%</td>
<td>14%</td>
<td>9%</td>
<td>9%</td>
</tr>
<tr>
<td>Lab Manual</td>
<td>72%</td>
<td>14%</td>
<td>8%</td>
<td>6%</td>
</tr>
<tr>
<td>Lab Video</td>
<td>71%</td>
<td>13%</td>
<td>7%</td>
<td>9%</td>
</tr>
<tr>
<td>Assignments</td>
<td>71%</td>
<td>13%</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>Assessment Worksheet</td>
<td>62%</td>
<td>18%</td>
<td>12%</td>
<td>8%</td>
</tr>
</tbody>
</table>
Also Available in Computer & Cybersecurity

Some of the titles below include Navigate 2 Advantage Access that unlocks a comprehensive and interactive eBook, student practice activities and assessments, a full suite of instructor resources, and learning analytics reporting tools.

Elementary Information Security
SECOND EDITION
Includes Navigate 2 Advantage Access

Richard Smith, PhD

An ideal text for introductory information security courses, the second edition of Elementary Information Security provides a comprehensive yet easy-to-understand introduction to the complex world of cybersecurity and technology. Thoroughly updated with recently reported cybersecurity incidents, this essential text enables students to gain direct experience by analyzing security problems and practicing simulated security activities.

Cyberethics
Morality and Law in Cyberspace
SIXTH EDITION
Includes Navigate 2 Advantage Access

Richard A. Spinello, Boston College
ISBN: 978-1-284-08139-8 • Paperback with Navigate 2 Advantage Access • 260 pages • © 2017

AVAILABLE JANUARY 2016

The sixth edition of Cyberethics: Morality and Law in Cyberspace provides a comprehensive examination of the social costs and moral issues emerging from the ever-expanding use of the internet, social media, and new information technologies. The Sixth Edition includes new and updated case studies on such issues as the “right to be forgotten” and the increase of potential online threats.

Secure Software Design

Theodore Richardson, PhD, South University
Charles N. Thies, Regis University
ISBN: 978-1-4496-2632-7 • Paperback • 412 pages • © 2013

Secure Software Design is written for the student, the developer, and management to bring a new way of thinking to secure software design. The focus of this book is on analyzing risks, understanding likely points of attack, and pre-deciding how your software will deal with the attack that will inevitably arise. By looking at the systemic threats in any deployment environment and studying the vulnerabilities of your application, this book will show you how to construct software that can deal with attacks both known and unknown instead of waiting for catastrophe and the cleanup efforts of tomorrow.