

- [Table of Contents](#)  
**Defend I.T.: Security by Example**  
By Ajay Gupta, Scott Laliberte

Publisher: Addison Wesley  
Pub Date: May 19, 2004  
ISBN: 0-321-19767-4  
Pages: 384

[Copyright](#)

[Preface](#)

[How the Book Is Structured](#)

[Format of the Case Studies](#)

[Audience](#)

[Acknowledgments](#)

[About the Authors](#)

[Primary Authors](#)

[Contributing Authors](#)

[Introduction](#)

[Disclaimers](#)

[Part I: Basic Hacking](#)

[Chapter 1. Getting to Know the Enemy: Nmap the Target Network](#)

[Section 1.1. Network Architecture](#)

[Section 1.2. Port Scans](#)

[Section 1.3. OS Identification](#)

[Section 1.4. Partial Picture](#)

[Section 1.5. Hiding](#)

[Section 1.6. Lessons Learned](#)

[Chapter 2. Home Architecture](#)

[Section 2.1. Introduction](#)

[Section 2.2. Background](#)

[Section 2.3. The Incident](#)

[Section 2.4. Incident Reconstruction](#)

[Section 2.5. Repercussions](#)

[Section 2.6. Aspen's Response](#)

[Section 2.7. Lessons Learned](#)

[Chapter 3. No Service for You!](#)

[Section 3.1. The Discovery](#)

[Section 3.2. The Response](#)

[Section 3.3. The Process](#)

[Section 3.4. Lessons Learned](#)

[Section 3.5. References](#)

[Part II: Current Methods](#)

[Chapter 4. Look, Ma, No Wires!](#)

[Section 4.1. Introduction](#)

[Section 4.2. Background](#)

[Section 4.3. The Project](#)

[Section 4.4. Existing Security](#)

[Section 4.5. Recommendations](#)

[Section 4.6. The End State](#)

[Chapter 5. Virus Outbreak I](#)

[Section 5.1. Introduction](#)

[Section 5.2. How Did You Get In?](#)

[Section 5.3. How Much Have We Lost?](#)

[Section 5.4. Lessons Learned](#)

[Chapter 6. Virus Outbreak II: The Worm](#)

[Section 6.1. Introduction](#)

[Section 6.2. Background](#)

[Section 6.3. The Worm Infection](#)

[Section 6.4. Lessons Learned](#)

[Chapter 7. Changing Face](#)

[Section 7.1. Introduction](#)

[Section 7.2. The Assessment](#)

[Section 7.3. Lessons Learned](#)

[Part III: Additional Items on the Plate](#)

[Chapter 8. Protecting Borders: Perimeter Defense with an IDS](#)

[Section 8.1. Background](#)

[Section 8.2. The Company](#)

[Section 8.3. Developing Requirements](#)

[Section 8.4. Market Research](#)

[Section 8.5. Pilot Testing](#)

[Section 8.6. Implementation on Production](#)

[Section 8.7. Implementation Follow-up](#)

[Section 8.8. Lessons Learned](#)

[Chapter 9. Disaster All Around](#)

[Section 9.1. Introduction](#)

[Section 9.2. Disaster Strikes](#)

[Section 9.3. Analyzing the Incident](#)

[Section 9.4. The Solution](#)

[Section 9.5. Lessons Learned](#)

[Chapter 10. Security Is the Best Policy](#)

[Section 10.1. Introduction](#)

[Section 10.2. The Company](#)

[Section 10.3. The Call](#)  
[Section 10.4. You Have a Policy . . . Now What?](#)

[Chapter 11. HIPAA: Security by Regulation](#)

[Section 11.1. Introduction](#)  
[Section 11.2. The Assessment](#)  
[Section 11.3. Analysis](#)  
[Section 11.4. Consequences](#)  
[Section 11.5. The Solution](#)  
[Section 11.6. Conclusion](#)

[Part IV: Old School](#)

[Chapter 12. A War-Dialing Attack](#)

[Section 12.1. War Dialing](#)  
[Section 12.2. The Attack](#)  
[Section 12.3. Lessons Learned](#)

[Chapter 13. A Low-Tech Path into the High-Tech World](#)

[Section 13.1. Introduction](#)  
[Section 13.2. Doing Your Homework](#)  
[Section 13.3. The Hack](#)  
[Section 13.4. The Fallout](#)  
[Section 13.5. Lessons Learned](#)

[Part V: Computer Forensics](#)

[Chapter 14. Industrial Espionage](#)

[Section 14.1. Spies All around Us](#)  
[Section 14.2. The Investigation](#)  
[Section 14.3. Lessons Learned](#)  
[Section 14.4. Intellectual Asset Protection](#)  
[Section 14.5. Chain of Custody](#)  
[Section 14.6. Federal Guidelines of Computer Evidence Admissibility](#)

[Chapter 15. Executive Fraud](#)

[Section 15.1. Introduction: The Whistle-Blower](#)  
[Section 15.2. Preparation](#)  
[Section 15.3. Evidence Collection and Chain of Custody](#)  
[Section 15.4. Drive Imaging](#)  
[Section 15.5. Review of the Logical File Structure](#)  
[Section 15.6. Review of Unallocated Space and File Slack](#)  
[Section 15.7. Smoking Gun](#)  
[Section 15.8. Reporting](#)  
[Section 15.9. Lessons Learned](#)

[Chapter 16. Cyber Extortion](#)

[Section 16.1. Introduction](#)  
[Section 16.2. To Press or Not to Press Charges](#)  
[Section 16.3. The Investigation](#)  
[Section 16.4. Lessons Learned](#)  
[Section 16.5. What Would Be Done Differently Today?](#)

[Conclusion](#)

[Further Investigations](#)  
[Public Key Infrastructure](#)

[Identity Management](#)  
[Single Sign-On](#)  
[Biometrics](#)  
[Secure Architecture](#)  
[Firewalls and VPNs](#)  
[The Home User](#)  
[Identity Theft](#)  
[Keeping Up with the Latest Trends](#)  
[Recommended Reading](#)  
[General Topics](#)  
[Nmap](#)  
[Secure Architecture](#)  
[Denial of Service](#)  
[Wireless](#)  
[Viruses](#)  
[Web Security](#)  
[Intrusion Detection Systems](#)  
[Disaster Recovery](#)  
[Security Policy](#)  
[HIPAA](#)  
[War Dialing](#)  
[Social Engineering](#)  
[Computer Forensics](#)  
[Public Key Infrastructure](#)  
[Identity Management](#)  
[Biometrics](#)  
[Firewalls and VPNs](#)  
[Home Security](#)  
[Identify Theft](#)

What are some examples of security goals that you may have for an organization? Check all that apply. to prevent unauthorized access to customer credentials to protect customer data from unauthorized access; These are super important goals. It detects vulnerabilities on your network and systems; A vulnerability scanner will scan and evaluate hosts on your network. It does this by looking for misconfigurations or vulnerabilities, then compiling a report with what it found. What are some restrictions that should apply to sensitive and confidential data? Check all that apply. What's the goal of mandatory IT security training for an organization? Check all that apply. IT security maintains the integrity and confidentiality of sensitive information while blocking access to hackers. IT security is a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers. Watch overview (2:17). Small Business Cyber Security. How IT Security Works. Types of IT Security. Related Topics. Contact Cisco. Defend I.T.: Security by Example draws on detailed war stories to identify what was done right and what was done wrong in actual computer-security attacks, giving you the opportunity to benefit from real experiences. Approaches to securing systems and networks vary widely from industry to industry and organization to organization. By examining a variety of real-life incidents companies are too embarrassed to publicly share, the authors explain what could have been done differently to avoid the losses incurred--whether creating a different process for incident response or having better security countermeasures in place to begin with.