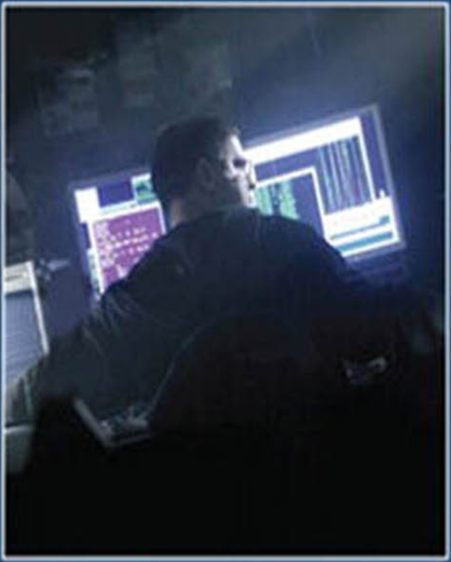
SEI SERIES • A CERT® BOOK

The CERT® Guide to Insider Threats



How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)

Dawn Cappelli

Andrew Moore

Randall Trzeciak

The CERT® Guide to Insider Threats

The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)

Table of Contents

Contents

Preface

Acknowledgments

Chapter 1. Overview

- True Stories of Insider Attacks
  - Insider IT Sabotage
  - Insider Fraud
  - Insider Theft of Intellectual Property
- The Expanding Complexity of Insider Threats
- Breakdown of Cases in the Insider Threat Database
- CERTs MERIT Models of Insider Threats
  - Why Our Profiles Are Useful
  - Why Not Just One Profile?
  - Why Didnt We Create a Single Insider Theft Model?
- Overview of the CERT Insider Threat Center
- Timeline of the CERT Programs Insider Threat Work
  - 2000 Initial Research
  - 2001 Insider Threat Study
  - 2001 Insider Threat Database
  - 2005 Best Practices
  - 2005 System Dynamics Models

Pearson

Table of Contents

2006 Workshops

2006 Interactive Virtual Simulation Tool

2007 Insider Threat Assessment

2009 Insider Threat Lab

2010 Insider Threat Exercises

2010 Insider Threat StudyBanking and Finance Sector

Caveats about Our Work

Summary

Chapter 2. Insider IT Sabotage

General Patterns in Insider IT Sabotage Crimes

Personal Predispositions

Disgruntlement and Unmet Expectations

Behavioral Precursors

Stressful Events

Technical Precursors and Access Paths

The Trust Trap

Mitigation Strategies

Early Mitigation through Setting of Expectations

Handling Disgruntlement through Positive Intervention

Eliminating Unknown Access Paths

More Complex Monitoring Strategies

A Risk-Based Approach to Prioritizing Alerts

Targeted Monitoring

Measures upon Demotion or Termination

Secure the Logs

Test Backup and Recovery Process

One Final Note of Caution

Summary

Chapter 3. Insider Theft of Intellectual Property

Pearson

Table of Contents

Impacts

General Patterns in Insider Theft of Intellectual Property Crimes

The Entitled Independent

Insider Contribution and Entitlement

Insider Dissatisfaction

Insider Theft and Deception

The Ambitious Leader

Insider Planning of Theft

Increasing Access

Organizations Discovery of Theft

Theft of IP inside the United States Involving Foreign Governments or Organizations

Who They Are

What They Stole

Why They Stole

Mitigation Strategies for All Theft of Intellectual Property Cases

Exfiltration Methods

Network Data Exfiltration

Host Data Exfiltration

Physical Exfiltration

Exfiltration of Specific Types of IP

Concealment

Trusted Business Partners

Mitigation Strategies: Final Thoughts

Summary

Chapter 4. Insider Fraud

General Patterns in Insider Fraud Crimes

Table of Contents

- Origins of Fraud
- Continuing the Fraud
- Outsider Facilitation
- Recruiting Other Insiders into the Scheme
- Insider Stressors

Insider Fraud Involving Organized Crime

- Snapshot of Malicious Insiders Involved with Organized Crime
- Who They Are
- Why They Strike
- What They Strike
- How They Strike

Organizational Issues of Concern and Potential Countermeasures

- Inadequate Auditing of Critical and Irregular Processes
- Employee/Coworker Susceptibility to Recruitment
- Verification of Modification of Critical Data
- Financial Problems
- Excessive Access Privilege
- Other Issues of Concern

Mitigation Strategies: Final Thoughts

Summary

Chapter 5. Insider Threat Issues in the Software Development Life Cycle

Requirements and System Design Oversights

- Authentication and Role-Based Access Control
- Separation of Duties
- Automated Data Integrity Checks
- Exception Handling

System Implementation, Deployment, and Maintenance

Table of Contents

Issues

Code Reviews

Attribution

System Deployment

Backups

Programming Techniques Used As an Insider Attack Tool

Modification of Production Source Code or Scripts

Obtaining Unauthorized Authentication Credentials

Disruption of Service and/or Theft of Information

Mitigation Strategies

Summary

Chapter 6. Best Practices for the Prevention and Detection of Insider Threats

Summary of Practices

Practice 1: Consider Threats from Insiders and Business Partners in Enterprise-Wide Risk Assessments

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 2: Clearly Document and Consistently Enforce Policies and Controls

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 3: Institute Periodic Security Awareness Training for All Employees

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 4: Monitor and Respond to Suspicious or Disruptive Behavior, Beginning with the Hiring Process

What Can You Do?

Table of Contents

Case Studies: What Could Happen if I Dont Do It?

Practice 5: Anticipate and Manage Negative Workplace Issues

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 6: Track and Secure the Physical Environment

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 7: Implement Strict Password- and Account-Management Policies and Practices

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 8: Enforce Separation of Duties and Least Privilege

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 9: Consider Insider Threats in the Software Development Life Cycle

What Can You Do?

Requirements Definition

System Design

Implementation

Installation

System Maintenance

Case Studies: What Could Happen if I Dont Do It?

Practice 10: Use Extra Caution with System Administrators and Technical or Privileged Users

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 11: Implement System Change Controls

Table of Contents

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 12: Log, Monitor, and Audit Employee Online Actions

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 13: Use Layered Defense against Remote Attacks

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 14: Deactivate Computer Access Following Termination

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 15: Implement Secure Backup and Recovery Processes

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Practice 16: Develop an Insider Incident Response Plan

What Can You Do?

Case Studies: What Could Happen if I Dont Do It?

Summary

References/Sources of Best Practices

Chapter 7. Technical Insider Threat Controls

Infrastructure of the Lab

Demonstrational Videos

High-Priority Mitigation Strategies

Control 1: Use of Snort to Detect Exfiltration of Credentials Using IRC

Suggested Solution

Control 2: Use of SiLK to Detect Exfiltration of Data Using VPN

Table of Contents

Suggested Solution

Control 3: Use of a SIEM Signature to Detect Potential Precursors to Insider IT Sabotage

Suggested Solution

Database Analysis

SIEM Signature

Common Event Format

Common Event Expression

Applying the Signature

Conclusion

Control 4: Use of Centralized Logging to Detect Data Exfiltration during an Insiders Last Days of Employment

Suggested Solution

Monitoring Considerations Surrounding Termination

An Example Implementation Using Splunk

Advanced Targeting and Automation

Conclusion

Insider Threat Exercises

Summary

Chapter 8. Case Examples

Sabotage Cases

Sabotage Case 1

Sabotage Case 2

Sabotage Case 3

Sabotage Case 4

Sabotage Case 5

Sabotage Case 6

Sabotage Case 7

Sabotage Case 8

Sabotage Case 9

Table of Contents

Sabotage Case 10

Sabotage Case 11

Sabotage Case 12

Sabotage Case 13

Sabotage Case 14

Sabotage Case 15

Sabotage Case 16

Sabotage Case 17

Sabotage Case 18

Sabotage Case 19

Sabotage Case 20

Sabotage Case 21

Sabotage Case 22

Sabotage Case 23

Sabotage Case 24

Sabotage/Fraud Cases

Sabotage/Fraud Case 1

Sabotage/Fraud Case 2

Sabotage/Fraud Case 3

Theft of IP Cases

Theft of IP Case 1

Theft of IP Case 2

Theft of IP Case 3

Theft of IP Case 4

Theft of IP Case 5

Theft of IP Case 6

Fraud Cases

Fraud Case 1

Fraud Case 2

Fraud Case 3

Table of Contents

Fraud Case 4

Fraud Case 5

Fraud Case 6

Fraud Case 7

Fraud Case 8

Fraud Case 9

Fraud Case 10

Fraud Case 11

Fraud Case 12

Miscellaneous Cases

Miscellaneous Case 1

Miscellaneous Case 2

Miscellaneous Case 3

Miscellaneous Case 4

Miscellaneous Case 5

Miscellaneous Case 6

Summary

Chapter 9. Conclusion and Miscellaneous Issues

Insider Threat from Trusted Business Partners

Overview of Insider Threats from Trusted Business Partners

Fraud Committed by Trusted Business Partners

IT Sabotage Committed by Trusted Business Partners

Theft of Intellectual Property Committed by Trusted Business Partners

Open Your Mind: Who Are Your Trusted Business Partners?

Recommendations for Mitigation and Detection

Malicious Insiders with Ties to the Internet Underground

Snapshot of Malicious Insiders with Ties to the Internet Underground

Range of Involvement of the Internet Underground

The Crimes

Use of Unknown Access Paths Following Termination

Table of Contents

Insufficient Access Controls and Monitoring

Conclusions: Insider Threats Involving the Internet Underground

Final Summary

Lets End on a Positive Note!

Appendix A. Insider Threat Center Products and Services

Appendix B. Deeper Dive into the Data

Appendix C. CyberSecurity Watch Survey

Appendix D. Insider Threat Database Structure

Appendix E. Insider Threat Training Simulation: MERIT InterActive

Appendix F. System Dynamics Background

Glossary of Terms

A

B

C

D

E

F

H

I

K

L

M

N

P

R

S

Table of Contents

- T
- U
- V
- W

References

About the Authors

Index