© Labyrinth Learning

Contents

Unit 1: Cybersecurity for Everyone

1 The Digital Landscape

1.1 Why Cybersecurity Matters for All
- The Economics of Your Digital Life (and Your Side Hustle)

1.2 The Threat Landscape Has Evolved
- AI: The Digital Con Artist That Never Sleeps
- Deepfake: Trust Nothing You Hear, See, or Smell
- Supply Chain Attacks: Why Your Accountant's Snafu Is Your Problem
- IoT: The Doorbell That Betrayed You
- The Top Cyber Threats
- What Does All This Mean for You?

1.3 Cybercrime's Impact on Daily Life and Business
- The Democratization of Cybercrime
- You (and Your Business): The Perfect Target
- The Ripple Effect

1.4 Developing a Security Mindset at Home and Work
- The Healthy Skeptic Approach
- Security as a Competitive Advantage
- The Realities of Having a Connected Life

2 Cybersecurity Fundamentals and Terminology

2.1 The CIA Triad: Your Three New BFFs
- Confidentiality: Your Digital Diary
- Integrity: Truth in a Digital World
- Availability: Being There When You Need It
- Why This Matters

2.2 The "Always Verify" Principle and Social Engineering
- Never Trust, Always Verify
- Common Social-Engineering Techniques
- Deepfake Social Engineering: The Game Changer
- The Human Element: Why This Works
- The Bottom Line

2.3 Basic Cloud Security: What Happens to Your Files?
- What Cloud Storage Really Means

2.4 Phishing: AI Makes It Personal
- The Many Faces of Phishing

2.5 Understanding Modern Malware
- The Malware Family Tree
- How Malware Spreads
- The Real Impact on Real People

3 Securing Your Digital World

3.1 Password Security: Digital Keys That Actually Work
- Why "Password123!" Isn't Protecting Anything
- The Length Revolution: Password Length Matters More Than Symbols
- The Passphrase Breakthrough
- Password Managers: Your Digital Memory

3.2 Multi-Factor Authentication (MFA): The $0 Security Upgrade You're Ignoring
- Why MFA Works
- The "I Lost My Phone" Problem

3.3 Safe Browsing: Navigating Without Getting Lost
- The HTTPS Protocol Is Nonnegotiable
- Inspect URLs Before Clicking
- Be Disciplined about Downloads
- Browser Security Basics
- Public Wi-Fi: Free Isn't Always Worth It

3.4 Secure Communications: Private Conversations in a Public World
- Email: The Digital Postcard
- Social Media: Forever Is a Long Time
- Tools and Resources: Encrypted Apps
- The VPN: Your Digital Disguise
- Tools and Resources: VPNs

3.5 Securing Your Digital Arsenal: Devices, Routers, and IoT Chaos
- Your Vulnerabilities
- The Router: Your Network's Front Door
- Smart Cameras, Dumb Defaults
- The IoT Everything Problem

3.6 Recognizing and Responding to Threats
- The Incident Response Food Chain
- Security Through Community
- Tools and Resources: Threat Intelligence Network

Unit 2: Cybersecurity for Small Business Entrepreneurs

4 Building Security Culture, Governance, and Risk

4.1 Why Entrepreneurs Set the Tone: Owner Behavior Drives Staff Habits
- The Leadership Mirror Effect
- Real-World Leadership Failures
- Building Security Culture Through Action
- The Trust Paradox

4.2 Creating Simple Protocols Employees Actually Follow
- Why Complex Policies Fail
- Checklists over Manuals
- Making Protocols Visible and Accessible

4.3 Training and Escalation: How Staff Should Report Suspicious Activity
- Why Employees Stay Silent
- What Deserves a Report
- Training That Doesn't Bore Everyone

4.4 Risk Trade-Offs for Business Owners: Fix, Insure, or Accept
- The Risk Management Trinity
- The Decision Framework
- Practical Risk Examples
- Balancing Security with Limited Budgets
- The Budget Reality

4.5 Privacy and Data Protection as Business Assets
- Why It Matters
- Privacy as a Competitive Edge

4.6 Cyber Insurance as a Practical Tool for Cash-Flow Protection
- What Cyber Insurance Actually Covers
- Insurance as a Transfer of Risk Transfer, Not as Risk Management
- Getting the Right Coverage

5 Everyday Cyber Hygiene for Your Business

5.1 The Great Password Manager Battle (and Why Your Team Will Hate You for Three Weeks)
- The Implementation That Actually Survives Contact with Reality
- The Tool Choice That Matters Less Than Everyone Thinks

5.2 Multi-Factor Authentication: The Thing Everyone Knows They Should Do but Doesn't Until Disaster Strikes
- The Rolling Deployment That Preserves Sanity
- The "I Lost My Phone" Protocol That Prevents Panic

5.3 Backup Systems: The First Target of Ransomware
- The 3-2-1-1-0 Rule
- The Daily Routine That Works
- The Budget-Friendly Backup Stack That Costs Less Than Lunch

5.4 Physical Security: Or How Your Coffee Shop Habit Becomes a Liability
- The Screen Lock Muscle Memory Challenge
- The Public Wi-Fi Truth Nobody Wants to Hear
- The $30 Investment That Prevents Surveillance
- The "I Left My Laptop in the Car" Protocol

5.5 Training That Changes Behavior (Without Boring Everyone to Tears)
- Monthly Microtraining: The Five-Minute Revolution
- Quarterly Phishing Simulations: The Game Your Employees Need but Will Dislike

5.6 Detection Instincts: Catching Compromise Before Catastrophe
- The Two-Minute Morning Bank Check
- The Friday Invoice Ritual
- Stay Aware of Login Anomalies
- Create a "Something Feels Weird" Escalation Culture

5.7 The Five-Metric Security Dashboard: Measure What Matters
- The 5-Metric Dashboard
- What to Do if Your Dashboard Looks Terrible

6 Practical Business Security Controls

6.1 Endpoint Protection: The Last Line of Defense When Everything Else Fails
- What EDR Actually Does (in Plain English)
- The Implementation Nobody Warns You About
- What EDR Cannot Do

6.2 Managed Firewalls: Let Someone Else Deal with Configuration Hell
- The Three Managed Firewall Options
- How to Choose Wisely: The Critical Questions to Ask

6.3 Cloud Security Basics: You're Already Paying for Protection You're Not Using
- Why This Matters
- Microsoft 365 Security Features Sitting Dormant
- Google Workspace Security Features You're Ignoring
- Mobile Device Management
- The 30-Minute Security Audit

6.4 Setting Policies for Mobile Phones and Personal Devices Before Devices Walk Out the Door
- The BYOD Policy That Actually Works
- Mobile Device Management (MDM) for the Paranoid
- The Conversation to Have Before Problems Happen

6.5 Encryption Made Simple: Protecting Critical Data Without Overkill
The Only Encryption Types You Really Need
How to Encrypt Data
Key Moves for Payment and Customer Data
What You Shouldn't Do
6.6 Building Security into Vendor Contracts: Simple Cyber Clauses That Protect You
The Four Essential Security Clauses
Vendor Risk Tiers: Who Gets Which Requirements?
Audit Your Existing Vendors

7 Guarding Your Online Presence and Customer Trust
7.1 How a Single Breach Can Destroy Your Reputation
The Asymmetry That Kills You
What Customers Actually Hear
7.2 Website Protection: SSL, E-Commerce Safeguards, and Platform-Specific Patching
SSL Certificates: The Nonnegotiable Padlock
E-Commerce Security: Don't Touch the Money
Why Platform Updates Cause 90 Percent of WordPress's Breaches
The 15-Minute Monthly Security Ritual
7.3 Social Media Safety: Protecting Your Brand
The Fake Account Playbook
Proactive Brand Protection
Nonnegotiable Account Security
A Simple Social Media Policy for Your Business
Crisis Response Protocols
7.4 Securing Customer Transactions: PCI Basics Without Drowning in Jargon
Industry-Specific Compliance: Why We're Starting with PCI
The Golden Rule: Don't Touch Payment Information
PCI-Compliance Levels for Small Businesses
Physical POS System Security
What You Absolutely Must Do
7.5 Monitoring Your Business Online
Google Alerts: Your Free Early Warning System
Have I Been "Pwned" (Compromised)? How to Detect Credential Breaches
Weekly and Monthly Monitoring Routines
7.6 Security as a Business Advantage
What to Communicate (Without Oversharing)
Competitive Positioning

8 Surviving and Recovering from a Cyber Incident
8.1 The "Business as Usual" Mindset: Planning for Downtime Before It Happens
Questions to Answer Now, Not During a Crisis
The One-Page Incident Response Plan
8.2 Incident Response Basics: What to Do First
The Critical First Hour
What You Absolutely Must NOT Do
Who to Call: The Emergency Contact List
8.3 Crisis Communication with Customers, Staff, and Regulators
Who Gets Told What and When
The Communication Rhythm
8.4 Business Continuity During Crisis
The Brutal Math
Payroll: The Nonnegotiables
Keeping Money Moving
8.5 Cyber Insurance Claims: What You Need to Know
Do Small Businesses Need Cyber Insurance?
Approved Provider Networks
Your Pre-Crisis Cyber-Insurance Checklist
8.6 Simplifying Privacy and PCI Compliance
Privacy Notification Requirements
PCI Breach Reporting: When Credit Cards Are Compromised
The Reality
8.7 Learning from Incidents: Building Back Stronger
Recovery vs. Actually Learning Something
Why Post-Incident Reviews Are Often Skipped
The Improvement Action Plan
Post-Incident Review Template: "Bouncing Back Stronger"
Bouncing Back Stronger
The Fundamental Truth

Unit 3: Certification Preparation and Advanced Concepts

9 Mastering the Certiport IT Specialist Cybersecurity Certification

9.1 The Certification Gap: What Chapters 1 Through 8 Didn't Teach You
- Exam Logisitics: Understanding the Exam Structure
- What You Already Know
- What This Chapter Teaches

9.2 Domain 2: Securing the Network
- Network Protocol Vulnerabilities You Must Know
- Legacy Protocols: The Museum Pieces Still Running Your Infrastructure
- Network Security Technologies: The Infrastructure Layer
- Detection vs. Prevention
- Deception and Enforcement: Honeypots, VPNs, and NAC
- Proxy Servers and Cloud Security
- Cloud Security Infrastructure

9.3 Domain 3: Securing Endpoint Devices
- Network Assessment Tools: Your New Vocabulary
- Packet Capture and Analysis: Seeing the Actual Data
- File and Drive Encryption: You Can't Read What You Can't Decrypt
- CIS Benchmarks: The Security Configuration Playbook
- Permissions and Privilege Management: Don't Give Everyone the Keys
- The Takeaway

9.4 Domain 4: Vulnerability Assessment and Risk Management (The Intelligence Layer)
- Vulnerability Databases and Threat Intelligence
- Risk Assessment and Vulnerability Management
- Penetration Testing and Application Security Testing
- The Takeaway

9.5 Domain 5: Incident Handling: The Frameworks and Forensics You're Missing
- SIEM and SOAR: The SOC Arsenal
- Digital Forensics—CSI: Cyber
- Attack Frameworks: How Professionals Think About Breaches
- The NIST Incident Response Lifecycle: The Official Procedure
- Compliance Frameworks and Incident Notification
- Disaster Recovery and Business Continuity
- The Takeaway

9.6 Advanced Security Principles: Filling the Remaining Gaps
- Encryption
- Zero Trust Security Models
- Security Governance and Compliance
- The Takeaway

9.7 Special Topics for Certification Success
- Social Engineering and Human Factors
- Mobile Device Security
- IoT and Operational Technology Security
- The Takeaway

10 Mastering the TOSA CyberCitizen Certification

10.1 Understanding TOSA CyberCitizen Assessment Structure
- Exam Format and Scoring
- Question Characteristics

10.2 Domain 1: The Cybersecurity World – Threat Recognition and Impact Assessment
- SSL/TLS Certificates and Trust Verification (Level 3)
- Data Breach Assessment (Level 4)

10.3 Domain 2: Applied Professional Protocols for Security in the Workplace
- Handling Unknown External Storage Devices (Level 4)
- Software Source Verification (Level 4)
- Social-Engineering Response (Level 4–5)

10.4 Domain 3: Security on the Move – Mobile and Traveling Device Security
- Smartphone Access Control (Level 3)
- Wireless Network Security Classification (Level 3–4)
- VPN Usage and Limitations (Level 4)
- MDM Software: Usage and Limitations (Levels 4–5)

10.5 Domain 4: Security at Home – Personal Device and Data Security
- File Analysis Using VirusTotal (Level 4)
- Dangerous File Extensions (Level 3)
- File Metadata and Privacy (Level 5)
- Multichannel Phishing Detection (Levels 3–4)

Appendices

A Exam Preparation and Test-Taking Strategies

Your Study Plan: Because You're Not an Imaginary Average Person
Practice Tests: Stop Wasting Them
Memorize Less, Understand More
Adaptive Tests and Time Pressure
Exam Day: The Surprisingly Simple Rules
Postcertification Learning
Ongoing Professional Development
The Takeaway

B Free Tools for Cybersecurity for Everyone

Personal Security Essentials
Business and Website Security
Advanced Scanning and Vulnerability Detection
Quick Start Guide: Pick Your Priority
The Takeaway

Glossary