

Corporate Cybersecurity Compliance and Defense Blueprint

Wealth Horizons Academy | \$1497

PROTECT YOUR ORGANIZATION FROM CYBER THREATS

Cybersecurity is no longer an IT issue — it is a business survival issue. The average cost of a data breach in 2025 was \$4.88 million (IBM Cost of a Data Breach Report). This blueprint gives organizations the framework to build effective cybersecurity defenses.

MODULE 1: THE THREAT LANDSCAPE

Understanding Modern Cyber Threats

Ransomware: Malicious software that encrypts your data and demands payment for the decryption key. - Average ransom payment: \$1.54 million (2024) - Average downtime: 24 days - Healthcare and financial sectors are primary targets

Phishing: Fraudulent communications designed to steal credentials or install malware. - 91% of cyberattacks begin with phishing - Business Email Compromise (BEC) cost organizations \$2.9 billion in 2023

Insider Threats: Threats originating from current or former employees, contractors, or business partners. - 60% of data breaches involve insiders - Malicious insiders and negligent employees are both significant risks

Supply Chain Attacks: Compromising a trusted vendor or software supplier to attack downstream customers. - SolarWinds, MOVEit Transfer, and Kaseya attacks demonstrated scale - Organizations must assess security of all third-party vendors

Zero-Day Vulnerabilities: Previously unknown software flaws exploited before patches are available. - Require rapid response and strong security architecture to mitigate

MODULE 2: COMPLIANCE FRAMEWORKS

NIST Cybersecurity Framework

The NIST CSF provides a risk-based approach to cybersecurity built on 5 functions:

1. **IDENTIFY:** Asset management, risk assessment, governance
2. **PROTECT:** Access control, awareness training, data security, protective technology
3. **DETECT:** Anomalies and events, continuous monitoring, detection processes
4. **RESPOND:** Response planning, communications, analysis, mitigation
5. **RECOVER:** Recovery planning, improvements, communications

Industry-Specific Regulations

HIPAA (Healthcare): Requires administrative, physical, and technical safeguards for PHI

PCI-DSS (Payment Card Industry): Required for any organization processing credit card payments

SOC 2 (Service Organizations): Trust Services Criteria covering security, availability, processing integrity, confidentiality, and privacy

CMMC (Defense Contractors): Cybersecurity Maturity Model Certification required for DoD contracts

MODULE 3: BUILDING YOUR SECURITY PROGRAM

The Security Architecture Fundamentals

Defense in Depth: Multiple layers of security controls - Network security (firewalls, segmentation, VPN) - Endpoint security (antivirus, EDR, patch management) - Identity security (MFA, privileged access management) - Data

security (encryption, DLP, backup) - Application security (secure coding, WAF, SAST/DAST) - Physical security (access control, surveillance)

Access Control and Zero Trust

Zero Trust Principle: "Never trust, always verify" - Assume breach mentality - Verify every user, device, and access request - Apply least privilege access (minimum access necessary) - Log and monitor all access

Multi-Factor Authentication (MFA): MFA reduces account compromise risk by 99%. Implement for: - All email accounts - VPN access - Cloud services - Administrative accounts (all of them) - Customer-facing portals

Patch Management

Unpatched vulnerabilities are the leading cause of successful attacks.

Patch Management Policy: - Critical vulnerabilities: Patch within 24-72 hours - High severity: Patch within 7-14 days - Medium severity: Patch within 30 days - Low severity: Patch within 90 days

Automated patch management tools dramatically reduce this burden.

MODULE 4: INCIDENT RESPONSE

Incident Response Plan (IRP)

Every organization needs a documented IRP covering: 1. **Preparation:** Team, tools, contacts, training 2. **Identification:** How will you know when an incident occurs? 3. **Containment:** Stop the bleeding — isolate affected systems 4. **Eradication:** Remove the threat completely 5. **Recovery:** Restore systems to normal operation 6. **Lessons Learned:** What failed? What do you do differently?

Business Continuity and Disaster Recovery

Recovery Time Objective (RTO): How quickly must systems be restored?

Recovery Point Objective (RPO): How much data loss is acceptable?

The 3-2-1 Backup Rule: - 3 copies of data - 2 different media types - 1 copy offsite (preferably cloud)

Test backups regularly. A backup you have not tested is not a backup.

MODULE 5: SECURITY AWARENESS TRAINING

The human element is involved in 82% of breaches (Verizon DBIR 2023).

Annual Security Training Must Cover: - Phishing identification and reporting - Password hygiene and MFA - Data handling and classification - Social engineering awareness - Incident reporting procedures - Remote work security - Physical security

Educational purposes only. Not professional advice. Results vary.

© 2026 Wealth Horizons Academy | wealthhorizonsacademy.org