CyberPerimeter Solutions

Business Plan

Prepared 04/19/2025

Contact Information

Bradley Hamilton

bhami014@odu.edu

222-222-2222

CyberPerimeterSolutions.com

4444 Olive Rd

Austin, TX, 78610

Location:
Austin, Texas

Mission Statement:
To provide small and medium-sized businesses with the knowledge and tools to defend against evolving cyber threats through accessible, practical, and expert-led cybersecurity training.

Vision Statement:
To become the leading cybersecurity education partner for businesses worldwide, making digital safety simple, scalable, and sustainable for every organization.

Overview:
CyberPerimeter Solutions is a cybersecurity training company designed to meet the unique security needs of small to medium-sized businesses (SMBs). While corporate-level businesses often have dedicated security teams, SMBs lack the resources or knowledge to effectively protect their digital assets. CyberPerimeter Solutions fills this gap by offering tailored, hands-on training programs that address real-world threats, compliance requirements, and best practices in cybersecurity.

As digital risks increase and strict regulations grow, CyberPerimeter Solutions positions itself as a trusted partner by helping clients build a strong human firewall, reduce vulnerabilities, and stay compliant with industry standards.

Products & Services:

-Cybersecurity Awareness Training: Interactive e-learning modules for employees

-Phishing Simulation & Reporting Tools: Test and improve staff readiness

-Custom Training Programs: Built for client-specific operations or compliance needs

-Virtual CISO Services: Consulting for businesses without internal security leadership

-Policy & Procedure Development: Assist in creating incident response plans, acceptable use policies, etc.

-Certifications & Continuing Education: Partnered or accredited courses for individuals seeking credentials

Company Description

Business Overview:
CyberPerimeter Solutions is a cybersecurity education and consulting firm dedicated to providing tailored security training and strategic guidance to small and medium-sized businesses. In a rapidly evolving, digital world where cyberattacks are increasingly sophisticated, SMBs remain one of the most vulnerable segments due to limited in-house resources and technical experts. CyberPerimeter Solutions is here to change that.

Nature of the Business:
We operate where cybersecurity and education meet, offering engaging, hands-on training programs designed to make cybersecurity accessible, practical, and effective for non-technical teams. Unlike generic online courses or enterprise-focused vendors, we prioritize the unique challenges and budget constraints of SMBs, providing flexible, customizable, and results-driven solutions.

Target Market:

> **Primary:** Small to medium-sized businesses that possess low employee counts, approximately 10–500 employees, particularly in industries like healthcare, finance, law, retail, and logistics.
>
> **Secondary:** Mid-sized organizations looking to remediate or grow teams and prepare for audit., and
>
> **Tertiary:** Larger enterprises seeking specialized training programs or CISO-as-a-service offerings.

The Problem We Solve:
Many SMBs do not typically have the internal expertise to properly train staff on cybersecurity risks, leaving them exposed to threats such as phishing, ransomware, and data breaches. One time buy solutions don't address real-world threats these organizations face. We can solve this by offering:

1. Practical, scenario-based training
2. Custom modules for different industries
3. Ongoing support and education

Unique Strengths & Competitive Advantages:

- We offer industry-specific training rather than a generalized model.
- Our courses focus on real-life scenarios and behavioral change, making technical topics easy to understand and apply.
- Phishing tests, red team drills, and incident response exercises make training more immersive.
- Online, in-person, or hybrid delivery formats to match client needs.
- A scalable option for SMBs to receive executive-level security guidance without hiring full-time employees.
- Designed to be cost-effective without compromising quality, ideal for businesses with limited security budgets.

Value Proposition:
CyberPerimeter Solutions empowers small and medium-sized businesses to confidently navigate today's cybersecurity landscape by delivering customized, accessible, and engaging training that transforms employees into the first line of defense against digital threats.

Organization & Management

Business Structure:
CyberPerimeter Solutions will be structured as a Limited Liability Company (LLC). This structure offers the flexibility of a sole proprietorship or partnership, with the added legal protections of a corporation. It provides personal liability protection for the founder(s), meaning personal assets are shielded from business debts and lawsuits. An LLC also allows for simplified taxation and less administrative complexity, which is ideal in the early stages of growth.

This structure supports the ability of CyberPerimeter Solutions to scale operations while retaining flexibility. As the business expands, additional partners or investors can be brought in without making significant changes to the business framework.

Leadership Team:

- **Founder & CEO – Bradley Hamilton:**
  Brings a strong background in cybersecurity, consulting, and training. Responsible for overall business strategy, service development, partnerships, and acquiring clients. The CEO will also lead client consultations and manage key business relationships.

- **Director of Training & Curriculum Development:**
  Oversees all content creation, including cybersecurity training modules, simulations, and certification prep. Ensures that all learning materials stay up-to-date with evolving threats and compliance standards. Also responsible for tailoring content to different industries.

- **Chief Technology Officer (CTO):**
  Responsible for managing the technical infrastructure, including online training platforms, phishing simulation tools, and internal security systems. Will also guide future product development and tech integrations.

- **Head of Sales & Client Success:**
  Leads the sales team and manages ongoing relationships with clients. Develops scalable onboarding and client success programs to maintain high retention and satisfaction rates.

- **Financial Advisor/CFO:**
  An outsourced financial expert will help manage budgeting, forecasting, and funding strategy in the early phases. As the business grows, this role may transition into a full-time CFO position.

Business Goals

What We Hope to Accomplish:
CyberPerimeter Solutions aims to become the go-to cybersecurity training partner for small to medium-sized businesses by delivering impactful, affordable, and accessible education that transforms how organizations defend against cyber threats. The goal is to heighten cybersecurity knowledge in smaller companies and empower teams to become active participants in their organization's security.

Short-Term Goals (< 12 months):

1. **Launch and Establish Brand Presence:**
    a. Provide service offerings and pricing structure
    b. Build a website with e-commerce or scheduling capability
    c. Develop a full introductory training curriculum
    d. Create content marketing materials, such as social media
2. **Acquire Initial Clients:**
    a. Secure 5–10 clients within the first 6 months
    b. Run free or discounted pilot programs to build rapport and collect performance data
    c. Begin targeted outreach to industries with high compliance demands
3. **Operational Setup:**
    a. Implement a secure LMS (Learning Management System) for online delivery
    b. Set up customer relations and basic sales processes
    c. Formalize the LLC, business bank accounts, and insurance coverage

Long-Term Goals (>12 months):

1. **Grow Nationally:**
    a. Expand client base across multiple industries and U.S. regions
    b. Build a team of part-time or contract cybersecurity instructors and consultants
    c. Develop specialized training modules for compliance
2. **Introduce Software-Based Tools:**
    a. Launch proprietary phishing simulation software or microlearning platform
    b. Offer self-paced certification programs for IT staff and managers

3. **Establish Partnerships:**
    a. Partner with MSPs (Managed Service Providers), insurance companies, and industry associations to reach more clients
    b. Collaborate with government or nonprofit programs aimed at SMB cybersecurity readiness
4. **Position for Certification and Accreditation:**
    a. Align training with industry certifications (e.g., CompTIA, ISC, NIST frameworks)
    b. Seek partnerships with certifying bodies or create courses eligible for CEUs (Continuing Education Units)
5. **Achieve $1M+ Annual Revenue by Year 5:**
   Through a combination of training programs, advisory services, and platform subscriptions

Products & Services

1. Cybersecurity Awareness Training

What it is:

A foundational training program for employees of all levels, designed to increase awareness of everyday cyber threats such as phishing, malware, ransomware, social engineering, password misuse, and remote work vulnerabilities.

- Delivered through an online Learning Management System (LMS) or live virtual/in-person sessions
- Includes interactive lessons, quizzes, real-world case studies, and certificates of completion
- Industry-specific modules (e.g., HIPAA for healthcare, PCI for retail)

Unique Features & Benefits:

- Custom branding and policy integration
- Real-world scenarios tailored to client environments
- Designed to meet compliance needs
- Includes optional knowledge checks and final assessments

Pricing:

- $25–$40 per user (based on volume) for self-paced e-learning
- $500–$2,000 for instructor-led workshops, depending on group size and format

2. Phishing Simulation & Reporting Tools

What it is:
Simulated phishing attempts that test employee readiness in real-time and identify who needs additional training.

How it works:

- Admin panel allows client managers to launch simulated phishing emails
- Reports track who clicked, reported, or ignored emails
- Automatic follow-up training for users who fall for simulated attacks

Unique Features & Benefits:

- Fully customizable campaigns
- Includes “report phishing” button integration
- Helps build a culture of security awareness
- Supports compliance reporting

Pricing:

- $200/month for companies up to 50 users
- Custom enterprise pricing for larger organizations

3. Virtual CISO (vCISO) Services

What it is:
Higher echelon of cybersecurity guidance without the cost of hiring a full-time Chief Information Security Officer.

How it works:

- Monthly or quarterly consulting packages
- Includes risk assessments, policy creation, compliance strategy, vendor security reviews, and incident response planning
- Includes 1-on-1 meetings with executives and IT teams

Unique Features & Benefits:

- Strategic insight from seasoned cybersecurity professionals
- Customizable based on organization size and needs
- Ideal for companies preparing for audits, funding, or certifications

Pricing:

- Starting at $1,500/month
- Premium plans up to $5,000/month depending on scope and complexity

4. Policy & Procedure Development

What it is:
Creation or review of critical cybersecurity policies, customized for the client’s environment and regulatory requirements.

Includes:

- Acceptable Use Policy
- Data Handling Policy
- Incident Response Plan
- Password Policy
- Business Continuity Plan

Pricing:

- $250–$500 per policy
- Full packages (5–7 policies): $1,500–$2,000

5. Certification & Continuing Education Programs

What it is:
Specialized training paths for IT personnel or individuals pursuing certifications (e.g., CompTIA Security+, CISSP, CISA).

How it works:

- Delivered via online platform with optional live tutoring
- Includes practice exams and scenario-based labs

Unique Features & Benefits:

- Affordable and flexible
- Taught by certified cybersecurity professionals
- Includes mentorship options

Pricing:

- Courses: $300–$800 depending on length and certification level
- Tutoring add-on: $50/hour

Intellectual Property Considerations:

- **Trademarks:** We plan to trademark our company name, logo, and potentially the names of any proprietary programs or tools we develop.

- **Patents:** No current need for patents unless we develop proprietary simulation technology or software features in the future.

- **Copyright:** All training materials, written content, videos, and custom modules will be protected under copyright law.

Production Costs vs. Sale Price:

Awareness training: Development costs (content, LMS setup) range from $5,000–$10,000 upfront. Once created, delivery is highly scalable with low marginal cost per user.

Phishing simulations: If using a white-labeled tool, monthly license fees may range from $300–$500/month. Developing in-house could cost $15,000–$25,000+ initially.

Live training & vCISO: Mostly service-based, so costs are mainly time and labor. Profit margins are high but depend on time availability.

Market & Industry Analysis

Industry Overview:

While corporate-level organizations have the resources to invest in internal security teams, small and medium-sized businesses remain underserved. According to the U.S. Small Business Administration, over 43% of cyberattacks target small businesses, yet only 14% are prepared to handle them.

This creates a major opportunity for affordable, accessible, and high-impact cybersecurity training tailored specifically to SMBs.

Target Market Demographics:

Primary Market:

- Small to medium-sized businesses (10–500 employees)
- Located primarily in the U.S. (initially), with future plans for global reach
- Revenue range: $500,000 – $20 million
- Tech usage: Low to moderate cybersecurity readiness
- High degree of regulations

Top industries we'll serve:

- Healthcare (HIPAA compliance, high-value PII)
- Legal firms (confidential client data, case security)
- Retail & eCommerce (payment processing, customer data)
- Professional services (consultants, accountants, insurance)

Competitive Analysis:

Competitor	Strengths	Weaknesses
KnowBe4	Industry leader, massive content library, strong simulation tools	Expensive for SMBs, not highly customizable
Infosec IQ	Comprehensive training catalog, includes certification prep	Less engaging interface, limited small business focus
Curricula	Story-based training, focuses on behavioral change	Higher cost, limited vCISO or consulting options
Local IT consultants	Personalized support, often bundled with IT services	Limited cybersecurity specialization, lack of scalable training models

CyberPerimeter Solutions's Competitive Edge:

- Tailored specifically for SMBs (pricing, content, delivery)
- Personalized, human-centered training
- Offers both training and advisory at an affordable price
- Easy-to-understand delivery for non-tech-savvy staff
- Ability to simulate real attacks and measure behavioral impact
- Strategic roadmap to scale training and software solutions

Growth Strategy:

- Initial client base through outbound sales, webinars, and partnerships with local business associations
- Build long-term recurring revenue through subscriptions (phishing + LMS access)
- Expand into corporate and international markets by Year 4–5
- Long-term vision includes proprietary software development

Marketing & Sales Strategy

Marketing Strategy:

1. Content Marketing & Education

We'll position CyberPerimeter Solutions as a trusted expert in cybersecurity for SMBs through high-value, educational content:

- **Blog Posts & Articles:** Target keywords around cybersecurity tips, compliance, small business breaches
- **Email Newsletters:** Monthly security tips, regulation updates, and new courses
- **Webinars & Live Demos:** Teach and pitch ideas

2. Social Media

- **LinkedIn:** Our main networking channel using targeted content, case studies, and company updates
- **YouTube:** Short demo and teaching videos, course previews, and cybersecurity awareness tips
- **Facebook & Instagram:** Community engagement, especially for small business owners and consultants

3. Paid Advertising

- **Google Ads:** Capture high-intent buyers searching for terms like "cybersecurity training for small business" or "HIPAA employee security course"
- **LinkedIn Sponsored Posts:** Target by industry, company size, job title
- **Retargeting Ads:** For visitors who checked out the site but didn't convert

4. Partnerships & Referrals

- **Cyber Insurance Providers:** Partner on compliance checklists and value-added training
- **Business Associations:** Discounts or workshops for members
- **Referral Program:** Incentives for existing clients to refer new businesses

Sales Strategy:

1. Outbound Sales & Business Outreach

- Identify high-potential leads (via LinkedIn or business directories)
- Reach out with a tailored message and a short free training/demo offer
- Follow-up with proposals and conversion tracking

2. Free Assessments & Entry Offers

- Offer free “Cyber Readiness Assessment” or a one-time phishing simulation
- Use results to pitch full training or advisory services

3. Sales Follow-up & CRM

- Use a customer relations manager to track leads, calls, and deal progress
- Conduct follow-ups to leads who aren’t ready to buy yet

Distribution Plan:

- **Company Website (Primary):**
    - Purchase e-learning access directly
    - Book live workshops or advisory consultations
    - Schedule demos and get quotes
- **Sales Team / Direct Contact:**
    - Custom pricing and packages for larger businesses or vCISO services
    - Proposals sent via email with signable agreements
- **Affiliate/Partner Channels:**
    - Partners can offer services through their existing client base
    - Custom dashboards or partner portals available in the future

Delivery of products:

- **Online Learning Platform (LMS):** Secure, cloud-based portal for training access
- **Live Virtual Sessions:** Via Zoom, Microsoft Teams, or CyberPerimeter Solutions-hosted video platforms
- **On-Site Training (Optional):** Available locally or regionally for larger clients
- **Email & Client Portal:** For sending phishing simulations, reports, policies, and other deliverables

Financial Projections

1. Assumptions

These are some assumptions we're using to forecast financial performance:

- Average price per user for training: **$30** (e-learning)
- Average price per workshop (live): **$1,500** (for 20–30 employees)
- Average monthly cost for phishing simulations: **$300** per client
- Average monthly revenue per Virtual CISO client: **$2,500**
- Growth in clients: Initial acquisition of 20 clients in Year 1, scaling to 200 by the end of Year 3
- Customer retention rate: **80%**
- Marketing & sales expenses increase as business grows
- Labor and overhead costs (trainers, software licenses, etc.)

2. Projected Revenue (3-Year Forecast)

Year	Training Revenue	Phishing Simulations	vCISO Revenue	Total Revenue
Year 1	$75,000 (2,500 users)	$36,000 (12 clients)	$60,000 (20 clients)	**$171,000**
Year 2	$180,000 (6,000 users)	$108,000 (36 clients)	$120,000 (40 clients)	**$408,000**
Year 3	$450,000 (15,000 users)	$300,000 (100 clients)	$300,000 (120 clients)	**$1,050,000**

3. Projected Expenses (3-Year Forecast)

Year	Salaries & Labor Costs	Marketing & Sales	Software & Tools	General Overhead	Total Expenses
Year 1	$100,000 (1-2 employees + contractors)	$50,000 (online ads, content, sales tools)	$10,000 (LMS, simulation tools)	$20,000	**$180,000**
Year 2	$200,000 (hire full-time trainers + salespeople)	$100,000 (growth-focused ads, conferences)	$20,000 (scaling tools, LMS upgrades)	$40,000	**$360,000**

Year 3	$350,000 (expand team, 2–3 full-time employees)	$200,000 (national ad campaigns, partners)	$40,000 (platform integrations, new tools)	$60,000	**$650,000**

4. Net Profit (3-Year Forecast)

Year	Revenue	Expenses	Net Profit
Year 1	$171,000	$180,000	**(-$9,000)**
Year 2	$408,000	$360,000	**$48,000**
Year 3	$1,050,000	$650,000	**$400,000**

5. Break-Even Point:

- Year 2 is when the business hits a break-even point and starts turning a profit. We can anticipate steady growth in Year 1, where initial marketing costs will outweigh revenue as we build brand awareness and customer acquisition strategies.
- From Year 2 onward, the business will experience scaling in revenue due to client retention, upsells (like additional workshops and simulations), and increased customer acquisition.
- By Year 3, the business reaches profitability with a solid net profit margin of approximately 38%.

6. Funding & Investment:

If seeking investment or loans, CyberPerimeter Solutions will need to raise around $100,000–$200,000 to cover initial operating costs, product development, and marketing expenses to drive growth in the first year.

7. Future Financial Growth:

By Year 4, we anticipate that CyberPerimeter Solutions will be in a strong financial position, expanding its offerings and possibly moving into corporate-level contracts, which could drive additional revenue growth. Long-term projections could estimate potential revenue of $5–$10 million by Year 5 with further geographic and product expansion.

Funding Request

Amount Needed: $205,000

CyberPerimeter Solutions is seeking $205,000 in funding to support the initial development and launch of our cybersecurity training platform and increase market penetration in the first year. This capital will be allocated to the primary areas of product development, marketing, staffing, and operational infrastructure, allowing us to meet our revenue goals and position the company for long-term growth.

Use of Funds:

1. **Product Development: $80,000**
   The core of our business is our training platform and simulation tools. These funds will be used to:

   - Create a secure, easy-to-use online portal to deliver cybersecurity courses, track user progress, and issue certificates. Estimated cost: $25,000
   - Develop high-quality training materials, including videos, quizzes, and downloadable resources. Estimated cost: $30,000
   - Build or license tools for phishing simulations, security awareness tests, and custom client reports. Estimated cost: $20,000
   - LMS software, video hosting, collaboration tools. Estimated cost: $5,000

2. **Marketing & Customer Acquisition: $50,000**
   To quickly gain traction in the competitive cybersecurity space, we'll focus on building brand awareness, creating lead-generation content, and running targeted ads:

   - Promote the brand and drive traffic to the website with a focus on cybersecurity awareness and training services. Estimated cost: $20,000
   - Develop engaging content to build thought leadership and provide value to prospective customers. Estimated cost: $10,000
   - Implement CRM software for lead tracking, sales funnels, and customer relationship management. Estimated cost: $5,000
   - Develop partnerships with managed service providers (MSPs), insurance companies, and local business associations to increase market penetration. Estimated cost: $10,000
   - Build a high-conversion website that serves as the main hub for product/service purchases and client interaction. Estimated cost: $5,000

3. **Staffing and Operations: $40,000**
   To successfully launch and operate CyberPerimeter Solutions, we will need to hire a small, capable team, including sales, customer support, and operations:

   - Salaries for Key Hires:
     - To manage outreach, partnerships, and lead generation. Estimated salary: $35,000
     - To handle day-to-day operations, customer queries, and training facilitation. Estimated salary: $5,000

4. **Legal, Administrative & Compliance: $10,000**
   These funds will cover the legal and administrative setup of the business, as well as ongoing compliance costs:

   - Set up LLC, trademark the company name/logo, and any necessary intellectual property filings. Estimated cost: $5,000
   - Cybersecurity liability insurance and business insurance. Estimated cost: $5,000

5. **Working Capital: $25,000**
   This amount will provide the liquidity necessary to cover day-to-day operational costs during the early stages of business, including office supplies, utilities, and other overheads, and to ensure we can scale without cash flow disruptions.

Funding Breakdown Summary:

Use of Funds	Amount
Product Development	$80,000
Marketing & Customer Acquisition	$50,000
Staffing and Operations	$40,000
Legal, Administrative & Compliance	$10,000
Working Capital	$25,000
Total Funding Required	**$205,000**

Expected Outcomes from Funding:

- **Year 1:** Launch of the platform, securing at least 20 clients, with an expected revenue of $171,000. Funds will enable us to cover all operational costs, acquire initial clients, and solidify our position in the SMB cybersecurity market.
- **Year 2:** Expansion to 100 clients, with a projected revenue of $408,000. Continued investment in marketing and customer acquisition, as well as scaling the product offerings to serve a larger market.
- **Year 3:** Expansion to 200 clients and $1M+ in revenue. Reinforced platform capabilities and new product launches, including a potential Software-as-a-Service based tool.

Appendix

1. Resume of Key Team Members:

Bradley Hamilton, CEO & Founder

- **Education:** B.S. in Cybersecurity, Old Dominion University
- **Experience:** 5+ years in cybersecurity, working with SMBs to implement security solutions.
- **Skills:** Cybersecurity risk assessment, security awareness training, compliance, and incident response management.
- **Contact:** bhami014@odu.edu

2. Marketing Slogans & Taglines:

- "Empowering Small Business Security—One Click at a Time"
- "Cybersecurity Training Made Simple for Small Businesses"
- "Protect Your Business. Train Your Team."
- "Your First Line of Defense Starts Here."
- "Secure Your Business, Safeguard Your Future."

3. Logo Ideas:

1. **Logo 1: Shield Icon + Digital Elements**
    - A minimalist shield icon, symbolizing protection and security.
    - Incorporate digital or circuit elements within the shield to represent cybersecurity and technology.
2. **Logo 2: Abstract Security Symbol**
    - A clean, abstract design using overlapping shapes or lines that resemble a secure lock or digital network.