

Venture Idea Assessment

William Johnson

Old Dominion University

CYSE 494: Entrepreneurship in Cybersecurity

Professor ROB BATCHELDER

June 2026

Venture Idea 1

1. Overview and Need

Business Idea

CyberShield Insight is an AI-powered cybersecurity platform that creates digital twins of employee security behavior. The platform analyzes employee interactions with phishing emails, security training, and system usage patterns to identify individuals who may be vulnerable to cyberattacks. It then provides personalized cybersecurity coaching and recommendations to reduce organizational risk.

Problem or Need

Human error remains one of the leading causes of cybersecurity breaches. Many organizations invest heavily in security technologies but lack visibility into which employees pose the greatest security risks. Current cybersecurity awareness programs often provide the same training to all employees regardless of their individual risk levels. CyberShield Insight fills this gap by using artificial intelligence to predict security vulnerabilities and provide customized training based on each employee's behavior.

2. Evaluation of Potential

Market Demand

The demand for cybersecurity solutions continues to grow as organizations face increasing cyber threats. According to Verizon's 2024 Data Breach Investigations Report, 68% of breaches

involved a non-malicious human element, such as employee error or social engineering attacks. This highlights the need for solutions that can identify and reduce human-related cybersecurity risks. Businesses are increasingly seeking more effective ways to reduce these incidents, making predictive security awareness platforms an attractive solution.

Scalability

The platform can be delivered as a cloud-based Software-as-a-Service (SaaS) solution, allowing it to scale across organizations of varying sizes. Once developed, additional customers can be added with relatively low operating costs. The growing adoption of AI-driven cybersecurity technologies also supports scalability, as the global AI cybersecurity market is projected to grow from approximately \$31.5 billion in 2025 to \$93.8 billion by 2030.

Profitability

Revenue could be generated through subscription-based pricing based on the number of employees being monitored. Additional revenue opportunities include consulting services, customized training modules, and security assessments.

Challenges and Risks

Potential challenges include privacy concerns related to monitoring employee behavior, regulatory compliance requirements, and competition from established cybersecurity awareness training providers. Organizations may also be hesitant to adopt AI-driven employee risk scoring systems.

3. Discovery Process

This opportunity was discovered through coursework in cybersecurity and observations of how human error frequently contributes to successful cyberattacks. Research into phishing attacks, insider threats, and security awareness training revealed a need for more personalized and proactive approaches to managing cybersecurity risks. The growing use of artificial intelligence in cybersecurity further inspired the concept.

Venture Idea 2

1. Overview and Need

Business Idea

The Predictive Breach Weather Service is an AI-driven cybersecurity platform that forecasts the likelihood of cyberattacks against organizations in specific industries, regions, or business sectors. Similar to how weather services predict storms, the platform analyzes threat intelligence, dark web activity, vulnerability disclosures, attack trends, and geopolitical events to generate cyber risk forecasts.

Problem or Need

Organizations often react to cyberattacks after they occur rather than preparing for them in advance. Security teams receive large amounts of threat data but struggle to determine which threats are most relevant to their organization. The Predictive Breach Weather Service fills this gap by transforming complex cybersecurity data into easy-to-understand risk forecasts that help organizations proactively strengthen their defenses before an attack occurs.

2. Evaluation of Potential

Market Demand

Cybercrime continues to increase globally, costing organizations billions of dollars each year. Cybersecurity Ventures project that global cybercrime damage will reach approximately \$10.5 trillion annually, demonstrating the growing economic impact of cyber threats. Businesses, healthcare providers, government agencies, and financial institutions all need better ways to anticipate cyber threats. A service that provides predictive cyber risk forecasting could help organizations allocate security resources more effectively and reduce the likelihood of successful attacks.

Scalability

The platform can be developed as a cloud-based Software-as-a-Service (SaaS) solution. Once the forecasting algorithms and threat intelligence infrastructure are established, the service can scale to support thousands of customers across multiple industries and geographic regions. Market forecasts indicate that the global cybersecurity market is expected to grow from approximately \$227.6 billion in 2025 to nearly \$352 billion by 2030, demonstrating significant long-term growth opportunities for innovative cybersecurity ventures.

Profitability

Revenue could be generated through subscription plans based on organization size and forecast detail. Premium services could include customized threat reports, real-time alerts, industry-specific forecasts, and cybersecurity consulting services. Additional revenue opportunities may come from partnerships with cyber insurance providers and managed security service providers.

Challenges and Risks

One challenge is ensuring forecast accuracy, as cybersecurity threats can change rapidly. Building trust with customers may require significant testing and validation of prediction models. The company would also need continuous access to high-quality threat intelligence data, which can be expensive to obtain and maintain.

3. Discovery Process

This opportunity was identified through cybersecurity coursework, industry research, and observations of how organizations struggle to prioritize threats. While weather forecasting helps people prepare for natural disasters, there is no widely adopted equivalent for predicting cyberattacks. The increasing availability of threat intelligence, artificial intelligence, and big data analytics inspired the idea of creating a cybersecurity forecasting service that helps organizations prepare for potential attacks before they occur.

Comparative Analysis

Analysis

Both CyberShield Insight and the Predictive Breach Weather Service address major cybersecurity challenges but focus on different aspects of risk management. CyberShield Insight focuses on reducing internal human-related vulnerabilities through AI-driven risk assessments and personalized training. The Predictive Breach Weather Service focuses on external threats by forecasting attack trends and helping organizations proactively prepare for cyber risks.

CyberShield Insight operates in a competitive market that includes cybersecurity awareness training providers. However, its use of AI-powered digital twins creates differentiation. The

Predictive Breach Weather Service faces less direct competition because few organizations currently provide cyber risk forecasting in a simple, weather-style format.

Both ideas align with my cybersecurity education and have strong scalability potential through cloud-based subscription models. However, the Predictive Breach Weather Service offers a more unique value proposition and may create a new market category within cybersecurity. It also aligns closely with my personal interests in threat intelligence, data-driven security analysis, and proactive risk prevention, which are areas I am most motivated to pursue further in my academic and professional development.

Idea with the Most Potential

I believe the Predictive Breach Weather Service has the most potential. The concept is highly innovative, easy for customers to understand, and addresses a growing need for proactive cybersecurity planning. As cyber threats become more sophisticated, organizations need better ways to anticipate attacks rather than simply responding to them. By combining artificial intelligence, threat intelligence, and predictive analytics, the service could help organizations improve security readiness and reduce the impact of cyber incidents. Its unique approach and relatively limited competition make it a promising entrepreneurial opportunity. The rapid growth of the cybersecurity market and the increasing financial impact of cybercrime further support the viability of this venture.

References

- Cybersecurity Ventures. (2025). *Cybercrime damages projected to reach \$10.5 trillion annually*. Cybercrime Magazine. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- Grand View Research. (2025). *AI in cybersecurity market size, share & trends analysis report, 2025–2030*. <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-cybersecurity-market-report>
- MarketsandMarkets. (2026). *Cybersecurity market forecast to 2030*. MarketsandMarkets Research Pvt. Ltd. <https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html>
- Verizon. (2024). *2024 data breach investigations report (DBIR)*. Verizon Business. <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf>