WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Risk Based Security Models for Veteran Owned Small Businesses

Enuma Edmund

Department of Computer Information Systems, Georgia State University, USA

DOI : https://doi.org/10.55248/gengpi.5.1224.250137

ABSTRACT

Veteran-owned small businesses (VOSBs) play a crucial role in the economic landscape, offering unique perspectives and fostering innovation. However, they face distinct security challenges due to limited resources, evolving cyber threats, and vulnerabilities associated with rapidly digitizing business operations. Risk-based security models provide a tailored approach to safeguarding VOSBs by identifying, prioritizing, and mitigating risks based on their potential impact. These models are particularly valuable for VOSBs, as they enable the efficient allocation of scarce resources to address the most critical security threats. This study explores the design and application of risk-based security frameworks for VOSBs, emphasizing the importance of aligning security measures with organizational objectives and compliance requirements. The analysis identifies common vulnerabilities in veteran-owned businesses, including insufficient cybersecurity training, reliance on outdated technologies, and limited access to specialized expertise. Additionally, it highlights best practices such as leveraging scalable security solutions, implementing employee awareness programs, and utilizing government-backed initiatives like the Cybersecurity Maturity Model Certification (CMMC). Policy implications are also discussed, focusing on the need for targeted support programs that address the unique challenges faced by VOSBs, including subsidies for advanced security tools and access to cybersecurity training tailored to small businesses. This research underscores the critical role of proactive risk management in protecting the operational integrity and growth potential of veteran-owned enterprises, ultimately ensuring their resilience in an increasingly complex threat environment.

Keywords: Veteran-owned small businesses, risk-based security models, cybersecurity, small business resilience, threat mitigation, Cybersecurity Maturity Model Certification (CMMC).

1. INTRODUCTION

1.1 Background and Importance of VOSBs

Veteran-owned small businesses (VOSBs) play a vital role in the economic landscape, contributing significantly to job creation and community development. According to recent statistics, over **2.5 million veteran-owned businesses** operate in the United States, accounting for approximately **9% of all businesses nationwide**. Collectively, these enterprises generate over **$1.2 trillion in annual revenues** and employ nearly **6 million individuals**. Their contributions extend beyond financial metrics, as VOSBs often bring values of leadership, discipline, and resilience shaped by military service into the business world [1].

Despite their positive impact, VOSBs face unique challenges in navigating the modern business environment, particularly in managing security risks. Many veteran entrepreneurs run small businesses with limited financial and human resources, making it difficult to implement comprehensive cybersecurity measures. Additionally, VOSBs are frequently targeted by cybercriminals who exploit their lack of robust security infrastructure. For instance, small businesses are increasingly vulnerable to phishing attacks, ransomware incidents, and data breaches, all of which can disrupt operations and erode customer trust [2].

The stakes are even higher for VOSBs involved in government contracting, where compliance with cybersecurity regulations, such as the **Cybersecurity Maturity Model Certification (CMMC)**, is mandatory. These regulations require businesses to safeguard sensitive data, such as Controlled Unclassified Information (CUI), against unauthorized access. Failure to meet these requirements not only jeopardizes contractual relationships but also exposes businesses to potential legal and financial consequences. Addressing these challenges requires targeted solutions that balance the need for effective security measures with the resource constraints that many VOSBs face [3].

1.2 Need for Risk-Based Security Models

The cybersecurity landscape is evolving rapidly, with threats becoming more sophisticated and widespread. Small businesses, including VOSBs, are particularly at risk due to their limited resources and lack of specialized cybersecurity expertise. Cybercriminals often view smaller organizations as "soft targets," exploiting their vulnerabilities to launch attacks such as malware distribution, credential theft, and social engineering schemes. Recent reports indicate that **43% of cyberattacks** target small businesses, with average recovery costs exceeding **$200,000 per incident** [4].

Given these challenges, risk-based security models have emerged as a practical and effective approach for resource-constrained organizations. Unlike traditional "one-size-fits-all" security strategies, risk-based models prioritize threats based on their likelihood and potential impact, allowing businesses to allocate resources more efficiently. For VOSBs, this approach enables the development of tailored security frameworks that address their unique operational needs and vulnerabilities [5].

A key feature of risk-based security models is their reliance on continuous risk assessment. By identifying and evaluating potential threats, businesses can implement proactive measures to mitigate risks before they escalate. For example, a risk-based model might prioritize protecting customer payment data through the implementation of multi-factor authentication and encryption, while assigning lower priority to less critical assets. This approach not only enhances overall security but also ensures that limited resources are deployed strategically [6].

The relevance of risk-based security models is further underscored by the increasing emphasis on regulatory compliance. For instance, the CMMC framework mandates that businesses assess and mitigate cybersecurity risks to achieve certification levels required for government contracts. Risk-based approaches align well with these regulatory requirements, offering a systematic way to identify and address gaps in compliance. By adopting such models, VOSBs can enhance their security posture while maintaining operational efficiency, ensuring both regulatory adherence and business continuity [7].

1.3 Research Objectives and Scope

The primary objective of this article is to explore the applicability and effectiveness of risk-based security models in addressing the cybersecurity challenges faced by veteran-owned small businesses (VOSBs). By examining the intersection of evolving cybersecurity threats, resource constraints, and regulatory requirements, the article seeks to identify actionable insights that can empower VOSBs to enhance their security frameworks.

This study addresses the following research questions:

1. What are the key cybersecurity risks faced by VOSBs, and how do these risks differ from those of other small businesses?
2. How can risk-based security models be tailored to meet the unique needs and constraints of VOSBs?
3. What are the implications of adopting risk-based approaches for regulatory compliance and operational resilience?

The article is structured to provide a comprehensive analysis of the topic. Section 2 reviews the existing literature on cybersecurity challenges and risk-based models for small businesses. Section 3 discusses the methodology used to assess the effectiveness of these models in VOSB contexts. Section 4 presents key findings, including case studies and best practices for implementation. Finally, Section 5 offers recommendations for policymakers, business owners, and cybersecurity professionals on supporting VOSBs in mitigating security risks.

By addressing these questions, the article aims to contribute to the development of practical and scalable solutions that enhance the resilience of VOSBs in the face of evolving cybersecurity threats. The insights provided are intended to inform both strategic decision-making and policy development, ensuring that VOSBs can thrive in an increasingly digital economy [8].

2. SECURITY CHALLENGES IN VETERAN-OWNED SMALL BUSINESSES

2.1 Overview of Common Vulnerabilities

Small businesses, including veteran-owned small businesses (VOSBs), face a unique set of cybersecurity threats. Cybercriminals often target small businesses due to their limited resources and perceived lack of robust security measures. Common threats include **phishing attacks**, which exploit human error to gain unauthorized access to systems; **ransomware**, which locks critical data and demands payment for its release; and **credential theft**, which can lead to account takeovers and data breaches. These attacks disrupt operations, damage reputations, and impose significant recovery costs [9].

VOSBs face additional challenges that compound their vulnerability to cyber threats. Many veteran-owned businesses operate in resource-constrained environments, limiting their ability to invest in advanced cybersecurity technologies or hire specialized personnel. For example, a significant proportion of VOSBs are sole proprietorships or small teams where owners juggle multiple roles, leaving little capacity to prioritize cybersecurity. Furthermore, VOSBs involved in government contracting face heightened risks, as they often handle sensitive data that makes them attractive targets for sophisticated attackers [10].

Another key challenge for VOSBs is the **technical expertise gap**. While veteran entrepreneurs bring valuable leadership and problem-solving skills, they may lack formal training in cybersecurity. This expertise gap can result in overreliance on outdated security measures, such as simple password protections or inadequate firewalls, which are insufficient to counter modern threats. The lack of access to cybersecurity training programs tailored to small businesses further exacerbates this issue [11].

Table 1 Common Vulnerabilities in VOSBs

Vulnerability	**Description**	**Impact**
Phishing Attacks	Deceptive emails or messages tricking users	Unauthorized access, data breaches
Ransomware	Malicious software locking access to data	Operational disruptions, financial losses
Credential Theft	Unauthorized access through stolen login details	Account takeovers, data compromise
Technical Expertise Gap	Lack of cybersecurity knowledge	Overreliance on inadequate or outdated measures
Resource Constraints	Limited budgets for security investments	Insufficient tools and defenses against threats

By addressing these vulnerabilities through tailored solutions, VOSBs can strengthen their cybersecurity posture and mitigate risks effectively [12].

2.2 Financial and Resource Constraints

Limited financial and operational resources represent a significant barrier to robust cybersecurity for VOSBs. With tight budgets, many veteran-owned businesses prioritize immediate operational needs, such as inventory or staffing, over investments in advanced security measures. This underinvestment leaves critical systems exposed to threats, as many VOSBs rely on basic, cost-effective solutions that fail to address evolving risks [13].

For example, businesses using free or outdated antivirus software often lack the capabilities to detect sophisticated malware or phishing attempts. Similarly, the absence of advanced security tools, such as intrusion detection systems or endpoint protection platforms, increases the likelihood of successful attacks. Limited budgets also restrict access to managed security services, which can provide continuous monitoring and rapid response to incidents [14].

The financial strain is further exacerbated by the indirect costs of cybersecurity breaches. Recovery from a ransomware attack, for instance, often involves downtime, legal fees, and reputational damage. A recent report estimated that **60% of small businesses** fail within six months of a major cybersecurity breach, highlighting the severe economic consequences of inadequate security investments [15].

Resource constraints also extend to personnel. Many VOSBs lack dedicated IT staff, forcing business owners to manage cybersecurity alongside their core responsibilities. This multitasking increases the likelihood of oversight and human error, further compounding security risks. Addressing these challenges requires innovative, cost-effective solutions, such as leveraging government grants, public-private partnerships, and scalable security frameworks tailored to small businesses [16].

2.3 Regulatory and Compliance Pressures

In addition to managing cybersecurity risks, VOSBs face significant regulatory and compliance pressures. Government contracting often requires adherence to stringent standards, such as the **Cybersecurity Maturity Model Certification (CMMC)** and the **National Institute of Standards and Technology (NIST)** frameworks. These regulations are designed to protect sensitive data, such as Controlled Unclassified Information (CUI), from unauthorized access and cyber threats. While compliance is essential for maintaining contractual relationships, meeting these requirements poses substantial challenges for resource-constrained VOSBs [17].

The CMMC framework, for example, mandates a tiered approach to cybersecurity, requiring businesses to achieve certification levels ranging from basic to advanced protections. Each level entails specific controls, such as implementing multi-factor authentication, conducting regular vulnerability assessments, and maintaining detailed incident response plans. However, the costs associated with certification, including audits and system upgrades, can be prohibitive for small businesses. A survey revealed that **50% of small businesses** involved in government contracting cited compliance costs as a primary barrier to meeting cybersecurity standards [18].

The NIST standards provide a risk-based approach to managing cybersecurity, emphasizing continuous assessment and mitigation of risks. While these standards are comprehensive, they often require technical expertise and resources that many VOSBs lack. For example, implementing encryption protocols or configuring secure access controls demands specialized knowledge and infrastructure investments that may be beyond the reach of smaller organizations [19].

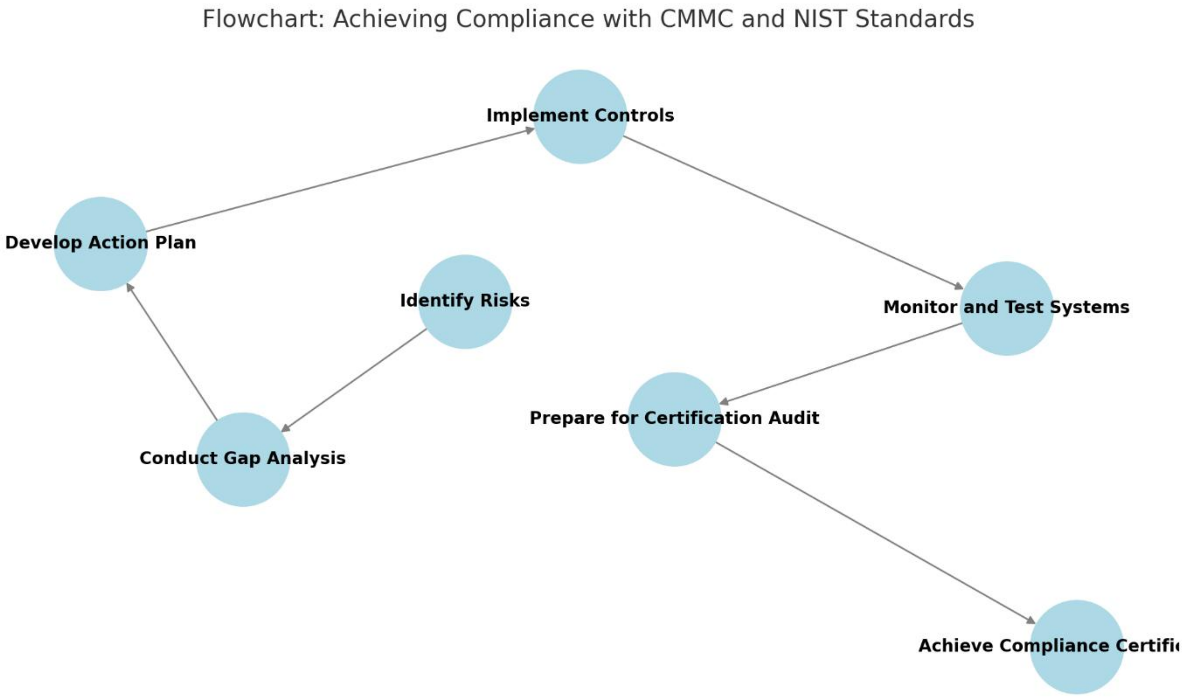
Flowchart: Achieving Compliance with CMMC and NIST Standards
Implement Controls
Develop Action Plan
Identify Risks
Monitor and Test Systems
Prepare for Certification Audit
Conduct Gap Analysis
Achieve Compliance Certifi

Figure 1 Flowchart of Compliance Requirements for VOSBs

Compliance pressures are further complicated by evolving regulations and the dynamic nature of cybersecurity threats. As standards are updated to address emerging risks, VOSBs must continuously adapt their systems and practices to remain compliant. This ongoing effort requires not only financial investments but also time and technical expertise, both of which are often in short supply for small businesses [20].

To navigate these challenges, VOSBs can benefit from targeted support, such as government subsidies for compliance-related expenses, access to training programs, and simplified regulatory frameworks. Collaborative initiatives between public and private sectors can also play a critical role in helping VOSBs achieve compliance while maintaining operational efficiency [21].

3. PRINCIPLES OF RISK-BASED SECURITY MODELS

3.1 Definition and Core Concepts

Risk-based security models are strategic approaches to managing cybersecurity by focusing on identifying, prioritizing, and mitigating risks based on their potential impact and likelihood. Unlike traditional security models that often take a blanket approach, risk-based strategies allocate resources toward addressing the most critical threats, ensuring more efficient use of limited resources. This makes such models particularly valuable for veteran-owned small businesses (VOSBs), which often operate under constrained budgets and personnel limitations [18].

The core components of a risk-based security model include:

1. **Risk Identification**: The process of pinpointing potential threats and vulnerabilities within an organization's systems, such as outdated software, weak passwords, or lack of multi-factor authentication. Threat intelligence tools and vulnerability assessments are commonly used to aid this process.
2. **Risk Prioritization**: Once identified, risks are ranked based on their likelihood of occurrence and the severity of their impact. For example, a phishing attack targeting sensitive customer data would likely be prioritized over low-risk vulnerabilities like outdated software with minimal exposure [19].
3. **Risk Mitigation**: This involves implementing security controls to address identified risks, ranging from technical solutions like firewalls and encryption to administrative measures like employee training and incident response planning. The goal is to reduce the likelihood and impact of threats to acceptable levels [20].

Risk-based models are inherently dynamic, adapting to evolving threats and organizational changes. By aligning security measures with business objectives, these models offer a practical and scalable approach to safeguarding sensitive data and ensuring regulatory compliance, especially for small businesses navigating complex cybersecurity landscapes [21].

3.2 Benefits of Risk-Based Approaches for VOSBs

Risk-based security models offer several advantages for VOSBs, enabling them to optimize their limited resources while effectively managing cybersecurity risks.

Cost-Effective Resource Allocation

One of the primary benefits of risk-based approaches is their ability to prioritize investments in areas with the highest return on security. Instead of spreading resources thinly across all potential threats, VOSBs can focus on critical vulnerabilities that pose the greatest risks. For instance, implementing multi-factor authentication for systems containing customer data can significantly reduce the risk of breaches, even if other lower-priority vulnerabilities remain unaddressed [22].

By concentrating on high-impact areas, VOSBs can achieve a higher level of protection without requiring substantial financial or personnel resources. This cost-effective strategy is particularly valuable for businesses operating on tight budgets, where every dollar spent on security must deliver tangible benefits.

Enhanced Focus on High-Impact Vulnerabilities

Risk-based models enable VOSBs to address the most pressing threats while maintaining flexibility to adapt to new risks. For example, if a ransomware attack targeting small businesses becomes prevalent, a VOSB can allocate resources to strengthen endpoint security and backup protocols. This proactive approach not only mitigates immediate risks but also builds long-term resilience by preparing for emerging threats [23].

Success Stories

Several VOSBs have successfully implemented risk-based security models with measurable outcomes. In one case, a small IT services provider adopted a risk-based approach to secure its infrastructure after experiencing a data breach. By prioritizing the implementation of intrusion detection systems and employee training programs, the company reduced incident response times by **40%** and prevented additional breaches.

Another example involves a logistics firm that identified phishing as a primary risk. Through risk prioritization, the business invested in email filtering tools and simulated phishing campaigns, achieving a **70% reduction in successful phishing attempts** over a six-month period. These success stories illustrate the practical benefits of aligning security investments with organizational needs [24].

3.3 Frameworks and Methodologies

Several established frameworks provide guidance for implementing risk-based security models, each offering unique methodologies for assessing and mitigating cybersecurity risks. For VOSBs, adapting these frameworks to suit their specific needs and constraints is critical for success.

Overview of Key Frameworks

1. **Factor Analysis of Information Risk (FAIR)**: The FAIR framework focuses on quantifying cybersecurity risks in financial terms, enabling businesses to prioritize security measures based on potential economic impact. FAIR's emphasis on cost-benefit analysis makes it particularly useful for small businesses with limited budgets [25].
2. **ISO/IEC 27005**: This international standard provides a structured approach to risk management, emphasizing continuous risk assessment, treatment, and monitoring. ISO 27005 is highly adaptable, allowing VOSBs to scale its application based on their resources and operational complexity [26].
3. **NIST Risk Management Framework (RMF)**: The RMF offers a comprehensive, step-by-step process for identifying, assessing, and mitigating risks. Its integration with other NIST standards, such as the Cybersecurity Framework (CSF), makes it a versatile choice for businesses handling sensitive government or customer data [27].

Adapting Frameworks for Small Businesses

While these frameworks provide robust methodologies, their complexity can be daunting for resource-constrained organizations. To address this, VOSBs can focus on the following adaptations:

1. **Simplified Risk Assessments**: Using streamlined tools, such as checklist-based evaluations, to identify high-priority risks without extensive technical expertise.
2. **Modular Implementation**: Breaking down frameworks into manageable phases, such as starting with basic controls like firewalls and gradually adopting advanced measures.
3. **Collaboration with Experts**: Leveraging external cybersecurity consultants or managed service providers to guide the implementation process.

Table 2 Comparison of Risk-Based Security Frameworks for VOSBs

Framework	Key Features	Adaptability for VOSBs
FAIR	Quantifies risks in financial terms	High (focus on cost-benefit analysis)
ISO/IEC 27005	Emphasizes continuous risk management	Moderate (scalable but requires customization)
NIST RMF	Comprehensive, integrates with NIST standards	High (suitable for government contracts)

By adopting and tailoring these frameworks, VOSBs can implement effective risk-based security models that address their unique challenges while ensuring compliance and resilience [28].

4. IMPLEMENTING RISK-BASED SECURITY IN VOSBS

4.1 Risk Identification

Risk identification is the cornerstone of a robust risk-based security model. This process involves uncovering potential threats to an organization's assets, operations, and data. Techniques such as **risk audits**, **penetration testing**, and **vulnerability scanning** are widely used to identify areas of exposure.

Risk audits systematically review an organization’s processes, identifying weaknesses in physical, technical, and administrative controls. For example, a small business might uncover that its email servers lack encryption or that employees frequently reuse passwords, both of which create opportunities for attackers [28].

Penetration testing, also known as ethical hacking, simulates real-world attacks to identify exploitable vulnerabilities within a system. Penetration tests conducted by certified professionals can reveal gaps in security measures, such as misconfigured firewalls or unpatched software, that would otherwise remain unnoticed. For veteran-owned small businesses (VOSBs), these tests are particularly valuable in assessing whether their defenses can withstand targeted attacks [29].

In addition to audits and testing, **vulnerability scanners** automate the detection of known vulnerabilities within networks and systems. Tools like **Nessus** and **Qualys** provide detailed reports on weaknesses and suggest remediation steps. For VOSBs, these tools are cost-effective resources that enhance their ability to identify risks without extensive technical expertise [30].

Table 3 Recommended Tools and Resources

Tool/Resource	Purpose	Recommended For
Nessus	Vulnerability scanning	Identifying outdated software or weak configurations
Metasploit Framework	Penetration testing	Simulating real-world attacks
OWASP ZAP	Web application security testing	Detecting vulnerabilities in websites
Security Risk Audits	Comprehensive reviews	Assessing overall security posture

Identifying risks early allows VOSBs to prioritize and mitigate vulnerabilities, laying the foundation for a resilient cybersecurity strategy [31].

4.2 Risk Assessment and Prioritization

After identifying potential threats, the next step is evaluating and prioritizing these risks based on their likelihood and potential impact. A structured approach ensures that resources are directed toward addressing the most critical vulnerabilities.

Likelihood vs. Impact Analysis

Risk assessment typically involves analysing the probability of a threat occurring (likelihood) and the potential consequences (impact). For instance, a phishing attack targeting a VOSB might have a **high likelihood** due to the prevalence of such schemes, but its **impact** could vary depending on the sensitivity of the data compromised.

A common tool for visualizing this analysis is a **risk prioritization matrix**, which categorizes risks into four quadrants:

1. **High Likelihood, High Impact**: These risks require immediate action, such as ransomware attacks on sensitive data systems.
2. **High Likelihood, Low Impact**: These risks warrant monitoring and low-cost mitigation measures, like spam filtering for non-critical emails.

3. **Low Likelihood, High Impact**: These risks necessitate contingency planning, such as natural disasters affecting data centers.
4. **Low Likelihood, Low Impact**: These risks are typically deprioritized.

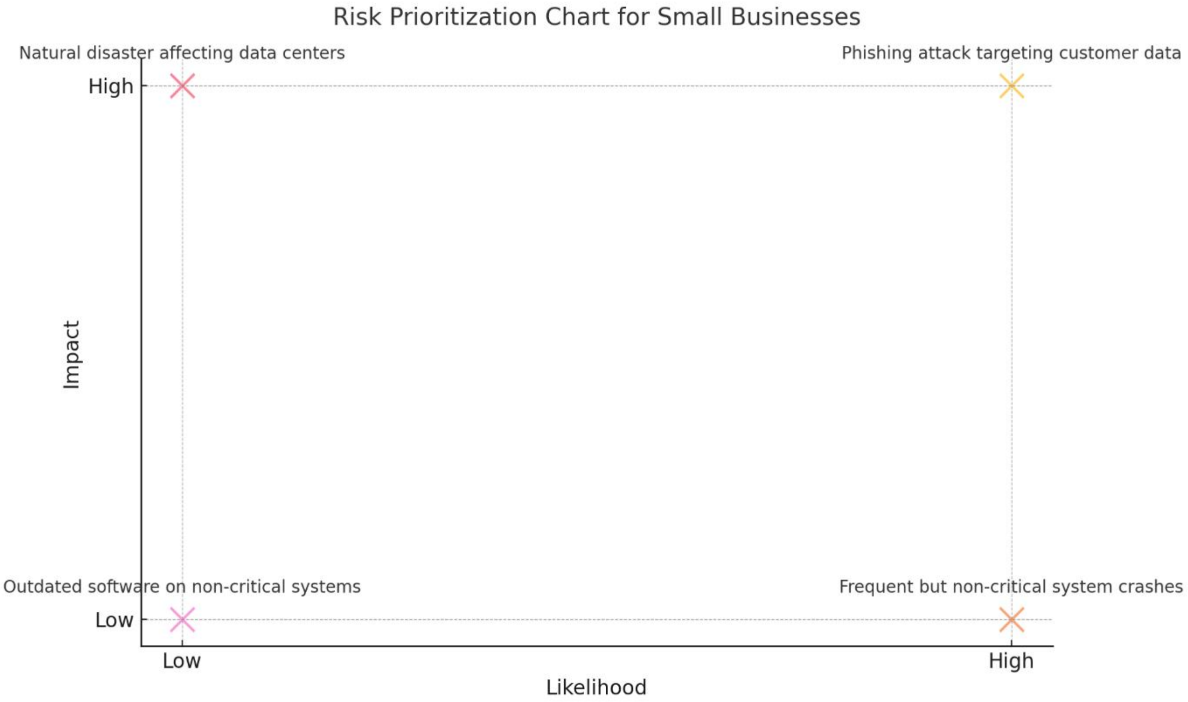

Figure 2

Risk Prioritization Matrix for a Sample VOSB

Prioritization Strategies

Effective prioritization involves both qualitative and quantitative approaches. Qualitative assessments rely on expert judgment and historical data, while quantitative assessments use metrics such as potential financial loss. For example, a VOSB handling sensitive government data might prioritize compliance-related risks due to the legal and financial implications of non-compliance [32].

Additionally, prioritization should align with the organization's strategic goals. For VOSBs aiming to expand their operations, securing customer trust through robust data protection may take precedence over mitigating less visible risks [33].

4.3 Risk Mitigation Strategies

Risk mitigation involves implementing measures to reduce the likelihood and impact of identified threats. These measures can be categorized into **proactive** and **reactive** strategies, both of which are essential for a comprehensive security posture.

Proactive Measures

Proactive measures aim to prevent security incidents before they occur. For VOSBs, investing in foundational security technologies is critical.

1. **Firewalls**: These act as a barrier between internal networks and external threats, blocking unauthorized access. Advanced firewalls with intrusion prevention capabilities can automatically detect and respond to suspicious activities.
2. **Intrusion Detection Systems (IDS)**: IDS tools monitor network traffic for signs of malicious activity. For example, tools like **Snort** and **Suricata** analyse data packets to identify anomalies, providing early warnings of potential breaches [34].
3. **Endpoint Protection**: Securing individual devices, such as laptops and mobile phones, prevents attackers from exploiting vulnerabilities at the user level. Solutions like **CrowdStrike** offer comprehensive endpoint detection and response capabilities.

Reactive Measures

Reactive measures focus on minimizing damage and recovering from incidents. Key components include:

1. **Incident Response Planning**: An incident response plan outlines the steps to be taken in the event of a security breach, including containment, eradication, and recovery. For instance, disconnecting affected systems from the network can prevent further spread of malware.

2. **Data Backup and Recovery**: Regularly backing up critical data ensures that businesses can restore operations quickly after an incident. Cloud-based backup solutions offer scalability and reliability for small businesses [35].
3. **Post-Incident Analysis**: Reviewing incidents helps identify root causes and improve defenses. For example, analysing a phishing breach might reveal gaps in email filtering or employee training.

Importance of Employee Awareness

Human error remains a leading cause of cybersecurity breaches. Training employees to recognize phishing attempts, use strong passwords, and follow best practices significantly reduces vulnerabilities. For VOSBs, cost-effective solutions such as online training modules or simulated phishing campaigns can enhance employee awareness and foster a culture of security [36]. By integrating proactive and reactive measures, VOSBs can build a layered defense that minimizes risk and enhances resilience against cyber threats [37].

4.4 Monitoring and Continuous Improvement

Cybersecurity is an ongoing process that requires regular monitoring and adaptation to evolving threats. Continuous improvement ensures that security measures remain effective and aligned with organizational needs.

Metrics for Assessing Security Effectiveness

Monitoring security effectiveness involves tracking key performance indicators (KPIs) that provide insights into the organization's risk posture. Common metrics include:

i. **Number of Detected Threats**: Indicates the frequency of attempted attacks.

ii. **Mean Time to Detect (MTTD)**: Measures how quickly threats are identified.

iii. **Mean Time to Resolve (MTTR)**: Tracks the time taken to neutralize and recover from incidents.

iv. **Employee Training Completion Rates**: Reflects the organization's commitment to security awareness.

Table 4 Key Metrics for Monitoring Security in VOSBs

Metric	Description	Purpose
Detected Threats	Frequency of blocked or flagged threats	Assessing the efficacy of security systems
MTTD	Average time to detect incidents	Evaluating threat detection capabilities
MTTR	Average time to resolve incidents	Measuring incident response efficiency
Training Completion	Percentage of employees trained	Ensuring organizational security readiness

Role of Audits and Continuous Updates

Regular security audits provide a comprehensive evaluation of the organization's defenses. Audits can identify outdated measures, misconfigurations, or gaps in compliance, allowing VOSBs to address issues proactively. For instance, an audit might reveal that a firewall is not configured to block certain types of traffic, enabling corrective action before an incident occurs [38].

Continuous updates to software, hardware, and policies are also essential to address emerging vulnerabilities. Automated patch management systems can ensure that all devices and applications are up to date, reducing the risk of exploitation. For example, applying timely patches to address known vulnerabilities in widely used software, such as operating systems, prevents attackers from exploiting these weaknesses [39].

By adopting a cycle of monitoring, auditing, and updating, VOSBs can maintain a robust security posture that evolves with the threat landscape. This approach not only mitigates risks but also fosters confidence among stakeholders, including customers, partners, and regulatory bodies [40].

5. CASE STUDIES AND BEST PRACTICES

5.1 Case Study: Effective Implementation in a VOSB

Background

A veteran-owned small business (VOSB) specializing in IT consulting faced increasing cybersecurity challenges as its operations expanded into government contracting. Handling sensitive data, including Controlled Unclassified Information (CUI), necessitated compliance with the **Cybersecurity Maturity Model Certification (CMMC)** and other regulatory frameworks. However, the company's limited budget and lack of in-house cybersecurity expertise posed significant obstacles to implementing robust security measures [35].

Challenges

The primary challenges included:

1. **Resource Constraints**: With a small team and limited financial resources, the VOSB struggled to justify investments in high-end cybersecurity tools and services.
2. **Technical Expertise Gap**: The company lacked trained personnel capable of managing advanced security systems or conducting regular risk assessments.
3. **Regulatory Compliance**: Meeting CMMC requirements was a major hurdle, particularly in areas like multi-factor authentication (MFA) and incident response planning.

Solutions Implemented

To address these challenges, the VOSB adopted a **risk-based security model**, prioritizing threats based on their likelihood and impact. Key steps included:

1. **Risk Identification and Assessment**: The company conducted a risk audit using affordable vulnerability scanning tools like **Nessus**, identifying critical weaknesses, including outdated software and weak password policies.
2. **Prioritization and Mitigation**: High-risk areas, such as endpoint security and access controls, were addressed first. The company implemented MFA for all user accounts and deployed free endpoint protection tools like **Microsoft Defender** to enhance security.
3. **Training and Awareness**: Employees received basic cybersecurity training through free online courses and simulated phishing exercises, significantly reducing susceptibility to social engineering attacks.
4. **Government Resources**: The VOSB leveraged government programs like the **Small Business Cybersecurity Assistance Program**, which provided access to free consulting services and compliance templates [36].

Results

By implementing these measures, the VOSB achieved CMMC Level 2 certification within six months, allowing it to secure additional government contracts. The company also experienced a **60% reduction in detected threats** and improved incident response times by **40%**, demonstrating the effectiveness of a targeted, resource-efficient approach [37].

5.2 Best Practices for Risk-Based Security

Implementing risk-based security models effectively requires practical strategies tailored to the unique challenges of VOSBs.

Practical Recommendations for Resource Optimization

1. **Start with a Risk Assessment**: Conducting a comprehensive risk assessment is crucial for identifying vulnerabilities and prioritizing mitigation efforts. Free tools like **OWASP ZAP** can help small businesses identify web application vulnerabilities, while open-source platforms like **Metasploit** enable cost-effective penetration testing.
2. **Focus on High-Impact Areas**: Limited resources should be directed toward addressing critical risks, such as securing customer data and protecting access credentials. For example, implementing MFA and encrypting sensitive files offer significant protection at relatively low costs.
3. **Leverage Scalable Solutions**: Cloud-based security tools, such as **Google Workspace Security** or **AWS Shield**, provide flexible and affordable options for small businesses to enhance their cybersecurity posture without large upfront investments [38].

Leveraging Free or Affordable Cybersecurity Tools

Many effective cybersecurity tools are available at low or no cost, making them ideal for VOSBs operating on tight budgets. Examples include:

1. **Bitdefender Free Antivirus**: Provides basic endpoint protection against malware and viruses.
2. **Snort**: An open-source intrusion detection system that monitors network traffic for suspicious activity.
3. **Let’s Encrypt**: Offers free SSL/TLS certificates to secure website communications.
4. **Cyber Aware**: A government-funded platform providing free cybersecurity resources and training modules for small businesses.

By integrating these tools, VOSBs can enhance their defenses without incurring significant costs [39].

Role of Government and Private Sector Collaborations

Government and private sector collaborations play a pivotal role in helping VOSBs overcome cybersecurity challenges.

1. **Government Support**: Programs such as the **Small Business Administration's (SBA) Cybersecurity Assistance Program** offer free or subsidized resources, including risk assessment templates and compliance guidance. Additionally, grants and tax incentives for cybersecurity investments provide financial relief to resource-constrained businesses.
2. **Private Sector Partnerships**: Collaborating with managed security service providers (MSSPs) allows VOSBs to access advanced tools and expertise at a fraction of the cost. For instance, MSSPs often offer subscription-based services, enabling small businesses to pay for only what they need.
3. **Information Sharing Initiatives**: Participating in information-sharing programs, such as the **Cybersecurity and Infrastructure Security Agency (CISA) Info Sharing Program**, enables VOSBs to stay updated on emerging threats and mitigation strategies. These initiatives foster a collaborative approach to cybersecurity, enhancing collective resilience [40].

Long-Term Sustainability

To sustain a robust cybersecurity posture, VOSBs should adopt continuous improvement practices, including regular risk reassessments and updates to security protocols. Creating a cybersecurity roadmap that outlines short-term priorities and long-term goals ensures that resources are allocated efficiently over time. Furthermore, fostering a culture of security awareness among employees helps maintain vigilance against evolving threats, reducing the likelihood of breaches [41]. By implementing these best practices, VOSBs can effectively manage cybersecurity risks while optimizing resources, ensuring long-term resilience and success in an increasingly digital business environment.

6. POLICY IMPLICATIONS AND RECOMMENDATIONS

6.1 Importance of Tailored Policies for VOSBs

Veteran-owned small businesses (VOSBs) face distinct challenges that necessitate the development of policies tailored to their specific needs. While existing government programs provide general support for small businesses, many fail to address the unique intersection of cybersecurity risks, limited resources, and compliance requirements encountered by VOSBs.

One critical issue is the lack of targeted cybersecurity funding for VOSBs. Current initiatives, such as the **Small Business Innovation Research (SBIR)** program, often prioritize technological innovation over foundational cybersecurity support. Consequently, many VOSBs lack access to essential tools and training to protect their operations effectively. For instance, a recent survey revealed that **58% of veteran entrepreneurs** reported inadequate financial support for cybersecurity upgrades as a significant barrier to compliance with frameworks like the Cybersecurity Maturity Model Certification (CMMC) [39].

Additionally, VOSBs involved in government contracting face heightened compliance pressures but receive limited guidance on navigating complex regulatory landscapes. Existing resources, such as the CMMC accreditation process, are often geared toward larger organizations with dedicated IT teams, leaving small veteran-owned businesses struggling to interpret and implement requirements. This gap creates vulnerabilities, as non-compliance can lead to penalties or the loss of critical contracts [40].

Further compounding the issue is the lack of accessible cybersecurity training programs tailored to VOSBs. While initiatives like the **Cybersecurity and Infrastructure Security Agency (CISA)** offer free training for small businesses, many veteran entrepreneurs find the content too generic or misaligned with their operational realities. For example, VOSBs operating in highly regulated industries, such as healthcare or defense, require specialized guidance that accounts for both their resource constraints and sector-specific risks [41].

Addressing these gaps through tailored policies would empower VOSBs to strengthen their cybersecurity posture, ensuring both regulatory compliance and business continuity. By acknowledging the unique challenges of VOSBs, policymakers can create targeted interventions that enhance resilience and foster long-term success in a competitive marketplace [42].

6.2 Actionable Recommendations for Policymakers

To address the unique cybersecurity challenges faced by VOSBs, policymakers should consider implementing actionable recommendations designed to provide financial support, foster collaboration, and simplify regulatory compliance.

Subsidies and Grants for Cybersecurity Tools

One of the most impactful measures would be the establishment of targeted subsidies or grants specifically for cybersecurity investments. For instance, a **Veteran Cybersecurity Grant Program** could allocate funding for essential tools such as firewalls, endpoint protection, and intrusion detection systems. By covering a percentage of these costs, such programs would enable VOSBs to prioritize cybersecurity without diverting resources from other operational needs.

Additionally, tax incentives could encourage cybersecurity investments. For example, offering tax deductions for expenses related to compliance with CMMC or implementing advanced security measures would reduce the financial burden on VOSBs while promoting proactive risk management.

Evidence from similar initiatives, such as the **Research and Development Tax Credit**, suggests that financial incentives are effective in driving small business adoption of new technologies [43].

Public-Private Partnerships

Encouraging partnerships between public and private sectors would significantly enhance the cybersecurity capabilities of VOSBs. For example, collaborations with managed security service providers (MSSPs) could provide VOSBs access to advanced tools and expertise at reduced costs. Policymakers could incentivize such partnerships by offering grants or subsidies to MSSPs that provide discounted services to veteran entrepreneurs.

Another promising model is the creation of cybersecurity resource hubs, where VOSBs can access shared infrastructure, such as threat intelligence platforms or compliance software. These hubs, supported by both government and private sector funding, would enable small businesses to leverage collective resources, reducing the cost and complexity of individual investments. Programs like the **National Cybersecurity Center's Cybersecurity Help Desk** demonstrate the potential of such collaborative approaches in supporting small businesses [44].

Simplified Compliance Frameworks

Simplifying compliance requirements is another critical step toward reducing the burden on VOSBs. Policymakers should consider creating tiered compliance frameworks tailored to the size and scope of businesses. For instance, a streamlined version of CMMC could allow VOSBs to achieve baseline compliance without the need for extensive audits or costly system upgrades.

Furthermore, government agencies could provide clearer guidance and hands-on support for navigating compliance processes. This could include offering free webinars, interactive tools, and one-on-one consultations to help VOSBs understand their obligations and implement necessary measures effectively. The inclusion of veteran-specific case studies in training materials would also ensure greater relevance and engagement [45].

Long-Term Collaboration and Awareness

Sustainable solutions require ongoing collaboration between policymakers, industry leaders, and veteran advocacy groups. Regular forums or task forces dedicated to addressing VOSB cybersecurity challenges would ensure that policies remain responsive to evolving threats and business needs. Policymakers should also prioritize raising awareness about available resources through targeted outreach campaigns, ensuring that VOSBs are aware of and can access the support they need.

By implementing these recommendations, policymakers can bridge the gaps in existing support structures, enabling VOSBs to thrive in an increasingly digital and regulated business environment. These interventions would not only enhance cybersecurity resilience but also reinforce the vital contributions of veteran-owned businesses to the economy and national security [46].

7. FUTURE DIRECTIONS AND EMERGING TRENDS

7.1 Emerging Cybersecurity Technologies

Advances in cybersecurity technology offer promising solutions to address the evolving threat landscape, particularly for small businesses such as veteran-owned small businesses (VOSBs). Emerging tools and methodologies powered by **artificial intelligence (AI)**, **machine learning (ML)**, and **blockchain** are transforming the way organizations protect their digital assets and manage risks.

AI and Machine Learning

AI and ML have revolutionized threat detection and response by enabling systems to analyse vast datasets in real-time and identify anomalies indicative of potential cyberattacks. For example, ML models can detect phishing attempts or ransomware activities by analysing behavioural patterns and deviations from established baselines. Tools like **AI-powered intrusion detection systems** can alert VOSBs to emerging threats before significant damage occurs. Furthermore, ML algorithms enhance fraud prevention by predicting vulnerabilities based on historical data, allowing businesses to implement proactive measures [44].

Blockchain Technology

Blockchain technology is gaining traction as a reliable method for securing sensitive data. Its decentralized and immutable ledger system ensures transparency and reduces the risk of tampering or unauthorized access. VOSBs can leverage blockchain for applications such as secure supply chain management, digital identity verification, and contract integrity. For example, blockchain-based identity systems offer robust protection against credential theft by eliminating centralized storage vulnerabilities [45].

Relevance to Small Businesses

For VOSBs, these technologies provide scalable and cost-effective solutions that align with their resource constraints. AI-driven tools, such as automated threat detection systems, reduce reliance on manual monitoring, while blockchain's tamper-proof systems enhance data integrity without requiring extensive IT infrastructure. As these technologies become more accessible, they hold significant potential for transforming how small businesses address cybersecurity challenges [46].

7.2 Opportunities for Further Research and Collaboration

While risk-based security models have demonstrated effectiveness in mitigating cybersecurity threats, there remain significant opportunities for advancing research and fostering collaboration to better support VOSBs.

Research Gaps in Risk-Based Models

One critical area for further research is the development of risk assessment methodologies tailored to the unique operational contexts of VOSBs. Existing frameworks, such as FAIR and NIST RMF, often require extensive customization to address the specific challenges faced by small businesses. For instance, research could focus on designing simplified models that balance affordability and effectiveness while accounting for the resource limitations typical of VOSBs. Additionally, studies examining the long-term impact of risk-based strategies on VOSB resilience and competitiveness would provide valuable insights for policymakers and practitioners [47].

Another area for exploration is the integration of emerging technologies, such as AI and blockchain, into risk-based security models. While these technologies offer significant promise, there is limited empirical evidence on their applicability and scalability for small businesses. Collaborative research efforts could investigate how these tools can be optimized for VOSB environments, ensuring cost-effectiveness and ease of implementation [48].

Academic-Industry Partnerships

Partnerships between academic institutions and industry stakeholders are essential for driving innovation and addressing the cybersecurity challenges faced by VOSBs. Academic researchers can provide theoretical insights and develop prototypes, while industry partners offer practical expertise and resources for scaling solutions. For example, joint initiatives could focus on creating tailored training programs that equip VOSBs with the skills needed to manage advanced cybersecurity tools effectively.

Additionally, academic-industry collaboration can facilitate the development of low-cost cybersecurity solutions specifically designed for small businesses. For instance, partnerships could produce AI-driven threat detection platforms that require minimal technical expertise to operate, enabling VOSBs to strengthen their defenses without hiring dedicated IT staff. Publicly funded research grants, such as those offered by the **National Science Foundation (NSF)**, can further incentivize these partnerships and ensure the equitable distribution of benefits [49].

Fostering Innovation

Innovation in cybersecurity for VOSBs requires a multi-disciplinary approach that integrates technical, operational, and policy perspectives. By fostering collaboration between academia, industry, and government, stakeholders can develop scalable and sustainable solutions that address the evolving needs of VOSBs. These efforts will not only enhance the resilience of veteran-owned businesses but also contribute to broader economic and national security objectives [50].

8. CONCLUSION

8.1 Summary of Key Insights

The discussions in this article have highlighted the critical importance of adopting risk-based security models for veteran-owned small businesses (VOSBs) to effectively manage cybersecurity risks. These models prioritize the allocation of limited resources to address the most pressing threats, ensuring a balance between operational efficiency and robust security. By focusing on risk identification, assessment, and mitigation, VOSBs can build a resilient cybersecurity posture that protects sensitive data, ensures compliance, and enhances overall business continuity. A recurring theme throughout the analysis is the resource constraints faced by VOSBs. Financial limitations, technical expertise gaps, and compliance pressures create unique challenges that necessitate tailored solutions. Emerging technologies such as artificial intelligence, machine learning, and blockchain offer significant promise for addressing these challenges. These tools not only enhance threat detection and response but also provide scalable and cost-effective options for small businesses to safeguard their digital assets.

The case studies presented demonstrate the practical applicability of risk-based models, with successful implementations showcasing reduced security incidents, improved compliance, and operational efficiency. For instance, leveraging tools like intrusion detection systems and multi-factor authentication significantly mitigates common vulnerabilities such as phishing and credential theft. Employee training, as a proactive measure, further complements technical defenses, reducing human error—a leading cause of breaches. Government and private sector collaboration emerged as a pivotal factor in supporting VOSBs. Publicly funded initiatives, tax incentives, and resource hubs provide much-needed assistance in navigating complex regulatory requirements. Meanwhile, private sector partnerships offer access to advanced tools and expertise, enabling small businesses to compete in a rapidly evolving threat landscape. The insights gathered underscore the need for continuous improvement in cybersecurity practices. Regular risk assessments, monitoring, and updating of security protocols are essential for adapting to emerging threats. Policymakers, industry leaders, and veteran advocacy groups must align their efforts to create an ecosystem that fosters resilience and innovation for VOSBs.

8.2 Closing Thoughts and Call to Action

Cybersecurity is no longer a luxury for small businesses—it is a critical necessity. For VOSBs, the stakes are particularly high, as these businesses often operate in sensitive sectors and contribute significantly to the economy and national security. The evolving threat landscape, characterized by sophisticated attacks and increasing regulatory demands, requires proactive risk management strategies that are tailored to the unique challenges of VOSBs. Risk-based security models provide a roadmap for achieving this goal. By focusing on high-impact vulnerabilities, leveraging scalable technologies, and fostering a culture of awareness, VOSBs can enhance their security posture while optimizing resources. These models are not only cost-effective but also adaptable, making them ideal for small businesses that must balance operational priorities with cybersecurity needs. Stakeholders at every level must take action to prioritize security for VOSBs. Policymakers should expand targeted support through grants, subsidies, and simplified compliance frameworks. These measures would alleviate financial and operational burdens, empowering veteran entrepreneurs to invest in robust cybersecurity practices. At the same time, private sector leaders should explore opportunities to collaborate with VOSBs, offering affordable tools and tailored solutions that address their specific risks.

The role of VOSB owners and employees is equally critical. Proactive measures, such as ongoing risk assessments, regular training, and investment in essential cybersecurity tools, are fundamental to maintaining resilience. While external support is valuable, the internal commitment to fostering a culture of security is what ultimately ensures long-term protection against evolving threats. The call to action is clear: protecting VOSBs is a shared responsibility. By working together, stakeholders can create an environment where veteran-owned businesses not only survive but thrive in the face of growing cybersecurity challenges. These businesses have demonstrated resilience and leadership in their contributions to the economy and society; it is imperative to extend the same resilience to their digital operations. The future of cybersecurity for VOSBs lies in innovation, collaboration, and commitment. By addressing the gaps in existing support structures and embracing tailored, risk-based solutions, stakeholders can ensure that VOSBs remain secure, competitive, and equipped to navigate an increasingly complex digital landscape.

REFERENCE

1. Parker HI. Veterans first contracting program preference hierarchy: Effect on veteran-owned small business. Walden University; 2016.
2. Best NA. SAFEGUARDING OPPORTUNITIES FOR AMERICA'S WOUNDED WARRIORS: A PROPOSED SOLUTION TO SUBCONTRACTING ABUSE IN THE SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS PROGRAM AND THE VETERANS FIRST CONTRACTING PROGRAM. Public Contract Law Journal. 2013 Jan 1:347-68.
3. Black DS, Bashur MA, Fuentes AL. What New Veteran-Owned Small Businesses Need to Know about the Rules. Procurement Law.. 2018;54:3.
4. Moye A. Market Orientation in Government Markets and Veteran-Owned Small Businesses. Walden University; 2016.
5. Guillen Jr R, De Miguel TM. Applauding the entrepreneurial spirit: Florida welcomes veteran-owned small businesses. Nova L. Rev.. 2012;37:579.
6. Krusemark TW. *Service-Disabled Veteran-Owned Small Business Perceptions of Subcontracting Training Within the Department of Defense* (Doctoral dissertation, Walden University).
7. Lotspeich-Yadao M, Tolbert C, Carpenter C. Veterans Creating'Good Jobs': The Propensity of Veteran-Owned Small Businesses to Use Service as a Frame of Reference in Providing Non-Monetary Benefits to Their Employees. Available at SSRN 3983674. 2021 Oct 13.
8. David S. What New Veteran-Owned Srnal Businesses Need to Know About the Rules.
9. Anuyah S, Chakraborty S. Can deep learning large language models be used to unravel knowledge graph creation? In: Proceedings of the International Conference on Computing, Machine Learning and Data Science. 2024. p. 1–6.
10. Koshy NR, Dixit A, Jadhav SS, Penmatsa AV, Samanthapudi SV, Kumar MGA, Anuyah SO, Vemula G, Herzog PS, Bolchini D. Data-to-question generation using deep learning. In: 2023 4th International Conference on Big Data Analytics and Practices (IBDAP). IEEE; 2023. p. 1–6.
11. Anuyah S, Bolade V, Agbaakin O. Understanding graph databases: a comprehensive tutorial and survey. *arXiv preprint arXiv:2411.09999*. 2024.
12. Dilger RJ, Lowry S. SBA Veterans Assistance Programs: An Analysis of Contemporary Issues. CRS Report R42695, Version 81. Updated. Congressional Research Service. 2021 Jul 7.
13. West M, Kregel J. Employment Services and Supports Available to Veterans with Disabilities through the US Department of Veterans Affairs and Other Federal Agencies. Mathematica Policy Research; 2014 Mar 30.
14. Anuyah S, Singh MK, Nyavor H. Advancing clinical trial outcomes using deep learning and predictive modelling: bridging precision medicine and patient-centered care. World J Adv Res Rev. 2024;24(3):1-25. https://wjarr.com/sites/default/files/WJARR-2024-3671.pdf
15. Chinedu J. Nzekwe, Seongtae Kim, Sayed A. Mostafa, Interaction Selection and Prediction Performance in High-Dimensional Data: A Comparative Study of Statistical and Tree-Based Methods, J. data sci. 22(2024), no. 2, 259-279, DOI 10.6339/24-JDS1127

16. Chukwunweike JN, Adeniyi SA, Ekwomadu CC, Oshilalu AZ. Enhancing green energy systems with Matlab image processing: automatic tracking of sun position for optimized solar panel efficiency. *International Journal of Computer Applications Technology and Research*. 2024;13(08):62–72. doi:10.7753/IJCATR1308.1007. Available from: https://www.ijcat.com.

17. Muritala Aminu, Sunday Anawansedo, Yusuf Ademola Sodiq, Oladayo Tosin Akinwande. Driving technological innovation for a resilient cybersecurity landscape. *Int J Latest Technol Eng Manag Appl Sci* [Internet]. 2024 Apr;13(4):126. Available from: https://doi.org/10.51583/IJLTEMAS.2024.130414

18. Ameh B. Technology-integrated sustainable supply chains: Balancing domestic policy goals, global stability, and economic growth. *Int J Sci Res Arch.* 2024;13(2):1811–1828. doi:10.30574/ijsra.2024.13.2.2369.

19. Aminu M, Akinsanya A, Dako DA, Oyedokun O. Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*. 2024;13(8):11–27. doi:10.7753/IJCATR1308.1002.

20. Andrew Nii Anang and Chukwunweike JN, Leveraging Topological Data Analysis and AI for Advanced Manufacturing: Integrating Machine Learning and Automation for Predictive Maintenance and Process Optimization https://dx.doi.org/10.7753/IJCATR1309.1003

21. Ameh B. Digital tools and AI: Using technology to monitor carbon emissions and waste at each stage of the supply chain, enabling real-time adjustments for sustainability improvements. Int J Sci Res Arch. 2024;13(1):2741–2754. doi:10.30574/ijsra.2024.13.1.1995.

22. Chukwunweike JN, Stephen Olusegun Odusanya , Martin Ifeanyi Mbamalu and Habeeb Dolapo Salaudeen .Integration of Green Energy Sources Within Distribution Networks: Feasibility, Benefits, And Control Techniques for Microgrid Systems. DOI: 10.7753/IJCATR1308.1005

23. Ikudabo AO, Kumar P**.** AI-driven risk assessment and management in banking: balancing innovation and security. *International Journal of Research Publication and Reviews*. 2024 Oct;5(10):3573–88. Available from: https://doi.org/10.55248/gengpi.5.1024.2926

24. Joseph Chukwunweike, Andrew Nii Anang, Adewale Abayomi Adeniran and Jude Dike. Enhancing manufacturing efficiency and quality through automation and deep learning: addressing redundancy, defects, vibration analysis, and material strength optimization Vol. 23, World Journal of Advanced Research and Reviews. GSC Online Press; 2024. Available from: https://dx.doi.org/10.30574/wjarr.2024.23.3.2800

25. Ndubuisi Sharon Amaka. Intersectionality in education: addressing the unique challenges faced by girls of colour in STEM pathways. *Int Res J Mod Eng Technol Sci*. 2024;6(11):3460. Available from: https://www.doi.org/10.56726/IRJMETS64288.

26. Funari NC. Service-Disabled Veteran-Owned Small Businesses and Government Contracting: Assessing the State of Texas Procurement and Contract Management Guide Using the Federal Acquisition Regulation.

27. Kline BM. Reasonable Interpretation, Unreasonable Results? HowMandated Government Set-Asides for Veteran-OwnedBusinesses Is a Win-Loss Proposition—KingdomwareTechnologies, Inc. v. United States. Mitchell Hamline Law Review. 2017;43(3):6.

28. Gray I, Soss MJ. SBA Certification of VOSBS and SDVOSBS. Contract Management. 2023 Mar 1;63(3).

29. Policie MS. 16 Socio-economic programmes i public procurements. The Applied Law and Economics of Public Procurement. 2013 May 7:246.

30. McGrann K. Benign neglect: Veteran-owned small business in Federal procurement today. Veterans L. Rev.. 2014;6:187.

31. Boldon NY, Maury RV, Armstrong N, Van Slyke R. The state of veteran entrepreneurship research: What we know and next steps.

32. HoAng AC, BAkiEs EL. Assessing the Timeliness Requirements to Protest an Agency's Corrective Action. Procurement Law.. 2018;54:1.

33. Roseboro DD, Rutkovitz JM. *Department of Defense small business (SB) program: a knowledge-level analysis of how customer education relates to meeting SB goals* (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

34. Yesner DL, Ruscus S. Selling Medical Supplies and Services Through the Department of Veterans Affairs Federal Supply Schedule Program. Pub. Cont. LJ. 2007;37:489.

35. GRAY I. VA's" Rule of Two" Decision Passes Muster at GAO. Contract Management. 2024 Jan 1;64(1).

36. Beale HB. Evaluation of the Small Business Procurement Goals Established in Section 15 (g) of the Small Business Act. Microeconomic Applications. 2014. Pp. 54. 2014;103.

37. Abbott TM. CONGRESSIONAL UPDATES. Contract Management. 2011 Mar 1;51(3).

38. Ramish DH. Big Changes in Small Business Regulations: Recent Rule Changes and Their Effect on Contractors. Procurement Law.. 2021;56:3.

39. Harvey R. ‘True\orlh. Contract. 2017 Apr:61.

40. Mushriqui J. MENTOR & PROTÉEÉ: An Overview of the SBA's All Small Mentor protégé Program. Contract Management. 2019 Jun 1;59(6).

41. Engin M, Koc O. Improving the small-business role in Turkish defense acquisitions: recommendations from US best practices. Monterey, California: Naval Postgraduate School; 2010 Jun.

42. Textor MJ. The Procurement System Would Have Broken Einstein's Brain: Government Contracting after Kingdomware. Mil. L. Rev.. 2018;226:197.

43. Maury RV, Tihic M, Pritchard A, McKelvie A, Euto L. 2021 National Survey of Military-Affiliated Entrepreneurs.

44. Schmaltz P. Combat to corporate: A qualitative phenomenological study on injured veterans transitioning to the civilian workforce. University of Phoenix; 2011.

45. Attachment J, Glossary Attachment J, Reserved Attachment J. Section J List of Attachments.

46. Dunn III WH. *Doctrine and elements of a successful coin mentorship protégé program* (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

47. PAGES PO. Amendment of Solicitation/Modification of Contract. Signature. 2009 Sep 29.

48. Callahan R, Archibald SO, Sterner KA, Milward HB. Key Actions That Contribute to Successful Program Implementation.

49. Bakies EL, Cregan N, DalcourtAngle V. The Rise and Fall of Equitable Offset 1 Michael Brustein, Bonnie Graham, Emily Fridman & Megan Trachman Reinforcing the Rule of Two: The Vs Improper Use of Cascading Evaluations 29. PUBLIC CONTRACT LAW JOURNAL. 2019;49(1).

50. David S. What New Veteran-Owned Srnal Businesses Need to Know About the Rules.