WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Balancing Cost and Security: Affordable IT Solutions for Small Businesses Facing Social Engineering Risks

James Olaniyan[1*]

[1]Department of Computer Science, Purdue University Fort Wayne, USA

ABSTRACT :

Small businesses face growing threats from social engineering attacks, including phishing, baiting, and pretexting, which exploit human error to compromise sensitive information. These attacks pose significant risks, including financial loss, reputational harm, and operational disruption. However, limited budgets often constrain small enterprises from investing in robust cybersecurity measures, making them prime targets for attackers. This paper examines cost-effective IT solutions that enable small businesses to strengthen their defenses against social engineering risks without exceeding financial limitations. Software-as-a-Service (SaaS)-based security solutions, open-source tools, and scalable cloud technologies are highlighted as practical options for budget-conscious businesses. These solutions provide essential protections, such as email filtering, endpoint security, and real-time monitoring, at a fraction of the cost of traditional enterprise systems. The trade-off between cost and effectiveness is explored, emphasizing the importance of prioritizing solutions that balance affordability with functionality. While some cost-saving measures may lack advanced features, combining them with cybersecurity training and awareness programs can significantly reduce risks. The paper also presents case studies of small enterprises that successfully mitigated social engineering risks by implementing affordable security solutions. For instance, a family-owned retail business reduced phishing incidents by adopting a cloud-based email security platform and conducting regular employee training sessions. Another example illustrates how an independent consultancy firm utilized open-source endpoint protection tools to enhance security without straining its budget. By showcasing real-world examples and emphasizing the value of accessible cybersecurity strategies, this paper aims to provide actionable insights for small businesses seeking to balance cost and security in the fight against social engineering threats.

Keywords: Affordable IT Security; Social Engineering Risks; Small Business Cybersecurity; SaaS-Based Solutions; Open-Source Tools; Cost-Effectiveness

1. INTRODUCTION :

1.1 Overview of Social Engineering Threats

Social engineering is a manipulative technique that exploits human psychology to gain unauthorized access to systems, data, or facilities. Common methods include phishing, baiting, and pretexting. **Phishing** involves deceptive emails or messages designed to steal credentials or sensitive information, often by impersonating trusted entities. **Baiting** lures victims with enticing offers, such as fake downloads or promises of rewards, that lead to malware installations. **Pretexting** creates a fabricated scenario to manipulate victims into divulging confidential details under false pretenses [1].

Small businesses are particularly vulnerable to these attacks due to limited resources and lack of specialized cybersecurity expertise. Employees in smaller enterprises often multitask across roles, making them less likely to recognize sophisticated attack patterns. Additionally, inadequate training leaves staff unaware of how to identify and respond to such threats [2]. Attackers target small businesses because they view them as soft targets with weak defenses, providing access to sensitive customer data or larger supply chains [3].

The consequences of social engineering attacks on small businesses are far-reaching. They include financial losses from fraud, regulatory fines for non-compliance with data protection laws, and reputational damage that erodes customer trust [4]. Despite these risks, small businesses frequently underestimate the threat, making it imperative to explore affordable and effective strategies to safeguard against social engineering [5].

1.2 Cost Challenges in Small Business Cybersecurity

One of the primary barriers to robust cybersecurity in small businesses is financial constraint. Limited budgets force small enterprises to prioritize immediate operational needs over long-term investments in cybersecurity. As a result, many small businesses rely on outdated systems or free tools that offer limited protection [6].

A common misconception among small business owners is that robust security solutions are prohibitively expensive. Advanced technologies, such as multi-factor authentication (MFA) and endpoint protection, are often perceived as tools exclusive to large enterprises [7]. This belief discourages investment in affordable yet effective solutions, leaving businesses vulnerable to cyberattacks.

The financial impact of a security breach, however, often far outweighs the cost of preventative measures. Small businesses may face significant expenses in recovering from data breaches, including penalties under regulations like GDPR or CCPA [8]. Moreover, the loss of customer trust can result in long-term revenue declines. Addressing this gap in understanding and providing cost-effective options is crucial for helping small businesses secure their operations without overextending their resources [9].

1.3 Objectives and Scope of the Article

The primary objective of this article is to provide small businesses with practical, affordable IT solutions to protect themselves against social engineering threats. With the rise in cyberattacks targeting smaller enterprises, there is an urgent need to bridge the gap between advanced cybersecurity practices and resource-constrained business operations [10].

This article begins by identifying the key techniques used in social engineering, including phishing, baiting, and pretexting, and analysing their impact on small businesses. The discussion then shifts to exploring accessible IT tools, such as two-factor authentication (2FA), encryption, and cloud-based security platforms, that can effectively mitigate these threats. Employee training is emphasized as a cornerstone of defense, highlighting its importance in reducing human error, which remains the weakest link in cybersecurity [11].

To illustrate the practicality of these solutions, the article includes real-world case studies of small businesses successfully implementing affordable strategies to counter social engineering attacks. By demonstrating how similar organizations have overcome challenges, this article aims to empower small businesses to adopt proactive measures tailored to their unique needs. Ultimately, this work provides actionable insights for achieving robust security without incurring excessive costs [12].

1.4 Structure of the Article

This article is structured to guide readers through the problem of social engineering and its impact on small businesses, followed by practical, cost-effective solutions. The discussion begins with an overview of social engineering threats, detailing the techniques used by attackers and the vulnerabilities inherent to small enterprises.

Next, the article addresses the financial challenges small businesses face in implementing cybersecurity measures, debunking the misconception that robust security is unattainable for smaller organizations. The core sections explore affordable IT tools and strategies, focusing on technologies such as 2FA, encryption, and cloud-based security, as well as the importance of employee training.

The inclusion of case studies provides real-world examples of small businesses mitigating risks effectively on limited budgets. The article concludes with actionable recommendations and best practices, ensuring that readers leave with a clear roadmap for protecting their businesses from social engineering threats [13].

2. UNDERSTANDING SOCIAL ENGINEERING RISKS

2.1 Types of Social Engineering Attacks

Social engineering attacks exploit human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security. The most prevalent techniques include phishing, baiting, and pretexting.

Phishing is one of the most common and effective social engineering techniques. Attackers craft deceptive emails, texts, or phone calls impersonating trusted entities, such as banks or business partners, to trick victims into revealing sensitive data. For example, employees might receive an email appearing to be from their IT department, asking them to reset their passwords on a fake site. This approach relies on urgency, fear, or trust to bypass rational judgment [8].

Baiting capitalizes on curiosity or greed to lure victims. Attackers use enticing offers, such as free downloads or attractive prizes, to lead individuals to malicious websites or software. Physical baiting, such as leaving infected USB drives in public places, remains a tactic that often exploits human curiosity. Digital baiting has increased with the rise of online marketplaces, where offers for discounted software downloads may install malware instead [9].

Pretexting involves the attacker creating a fabricated scenario to gain the trust of the victim. For instance, an attacker may pose as a company executive, requesting sensitive employee information from HR under the guise of an urgent deadline. Pretexting is particularly dangerous because it often involves careful planning and detailed knowledge of the target's operations, making the scenario appear legitimate [10].

Small businesses, with their limited resources and often insufficient training, are particularly vulnerable to these techniques. Phishing alone accounts for the majority of social engineering breaches among small enterprises, demonstrating the need for robust preventative measures and awareness programs [11].

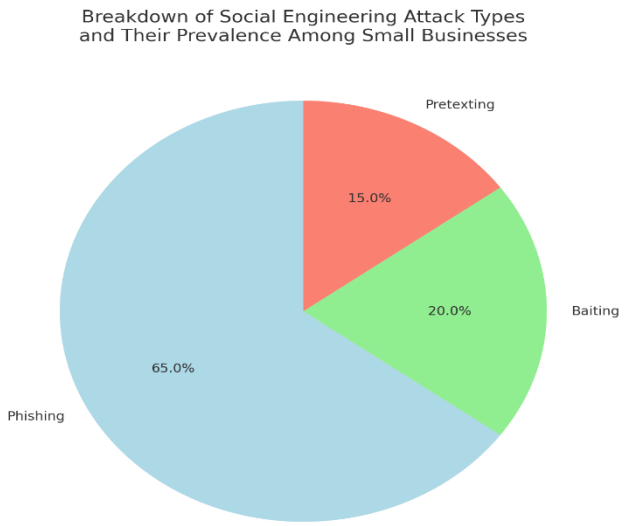

Figure 1 Graphical breakdown of phishing, baiting, and pretexting attack types, highlighting their prevalence among small businesses.

2.2 Impacts of Social Engineering on Small Businesses

Social engineering attacks can have devastating effects on small businesses, often leading to financial losses, operational disruptions, reputational damage, and customer distrust.

Financial losses and operational disruptions are among the most immediate consequences. For example, a successful phishing attack may lead to fraudulent transactions, data theft, or ransomware installation, forcing businesses to pay hefty sums for recovery. The downtime caused by such incidents disrupts daily operations, leading to lost revenue and reduced productivity [12]. For small businesses, even minor disruptions can have long-term financial repercussions, given their limited resources and reliance on continuity.

Reputational damage is another critical impact. Customers entrust businesses with sensitive information, such as payment details and personal data. A breach caused by a social engineering attack erodes this trust, leading to customer attrition and negative publicity. Potential clients may avoid engaging with businesses perceived as lacking robust security, further affecting revenue streams [13].

Customer distrust compounds these issues. In sectors like healthcare and finance, where confidentiality is paramount, breaches can lead to regulatory penalties under laws like GDPR and CCPA. Small businesses often struggle to recover from the dual blow of fines and lost clientele, leaving them at a competitive disadvantage [14].

For instance, a small retail business in the Midwest fell victim to a phishing scam where an employee unknowingly provided login credentials to an attacker posing as an IT technician. The breach compromised hundreds of customer credit card details, resulting in a $50,000 fine and a 30% drop in sales over the following months [15]. This example underscores the importance of proactive measures, such as employee training and affordable IT tools, to mitigate the risk of social engineering attacks.

2.3 The Human Factor in Cybersecurity

Human behaviour plays a pivotal role in enabling or preventing social engineering attacks. Attackers often bypass technological defenses by targeting employees, exploiting their trust, fear, or lack of awareness. For small businesses, where employees frequently juggle multiple responsibilities, this vulnerability is particularly pronounced [16].

For instance, untrained staff may fail to recognize phishing attempts or may click on malicious links in emails, inadvertently granting attackers access to sensitive systems. Human error remains one of the leading causes of data breaches globally, emphasizing the importance of addressing the human factor in cybersecurity [17].

Creating awareness within small organizations is a critical step toward reducing vulnerabilities. Regular training programs help employees identify social engineering tactics and foster a security-conscious mindset. Simulated phishing exercises, for example, can test and improve employee responses to potential attacks. These initiatives not only mitigate risks but also empower employees to act as the first line of defense against cyber threats [18].

By fostering a culture of cybersecurity awareness, small businesses can significantly reduce their exposure to social engineering risks. This proactive approach, combined with affordable IT tools, creates a robust security framework that prioritizes both technological and human defenses [19].

3. AFFORDABLE IT SOLUTIONS FOR SMALL BUSINESSES

3.1 Two-Factor Authentication (2FA)

Two-factor authentication (2FA) is a critical security measure that strengthens access controls by requiring users to verify their identity using two separate factors: something they know (e.g., a password) and something they have (e.g., a mobile device or authentication app). This layered approach significantly

reduces the risk of unauthorized access, even if passwords are compromised. By incorporating 2FA, small businesses can protect sensitive customer data and internal systems from common threats such as phishing and credential theft [15].

Affordable 2FA tools tailored for small businesses provide robust security without straining budgets. **Google Authenticator**, for instance, offers a free and easy-to-use solution that generates time-based one-time passwords (TOTP). **Duo Security**, another popular option, provides a user-friendly interface and flexible pricing plans suitable for small enterprises. Other tools, like **Authy**, combine affordability with features such as multi-device synchronization and offline mode [16].

A compelling case study illustrates the effectiveness of 2FA in a small retail business. After experiencing a phishing attack that compromised employee login credentials, the business implemented Google Authenticator to secure access to its point-of-sale (POS) and inventory systems. Within three months, phishing incidents dropped by 70%, and employee awareness of security protocols improved. The company credited 2FA with enhancing overall cybersecurity resilience without incurring significant costs [17].

2FA not only mitigates the risks of credential-based attacks but also aligns with regulatory requirements, such as GDPR and CCPA, that mandate strong authentication measures for sensitive data. By adopting affordable 2FA tools, small businesses can effectively bolster their defenses against evolving cyber threats [18].

3.2 Role-Based Access Control (RBAC)

Role-based access control (RBAC) restricts system access to authorized personnel based on their roles within an organization. By defining specific permissions for different job functions, RBAC minimizes the risk of unauthorized access to sensitive data and systems. This principle of least privilege ensures that employees only access information necessary for their tasks, reducing potential attack surfaces [19].

Low-cost RBAC solutions are readily available, particularly in cloud platforms like **Microsoft Azure** and **Google Workspace**, which include built-in access management features. For example, Azure allows administrators to assign roles such as "reader" or "contributor" to users, ensuring that access is granted only as needed. Similarly, Google Workspace provides customizable permissions for documents, emails, and shared drives, helping small businesses implement RBAC efficiently [20].

To implement RBAC effectively, businesses should:

1. **Define clear roles:** Map roles to job responsibilities to ensure access aligns with organizational needs.
2. **Regularly review permissions:** Periodically audit access controls to prevent privilege creep.
3. **Use centralized management tools:** Leverage cloud-based solutions to simplify role assignment and monitoring [21].

For example, a small accounting firm implemented RBAC using Google Workspace to manage client financial data. By restricting access to accountants and excluding administrative staff, the firm reduced the risk of accidental or malicious data exposure. This measure also improved compliance with financial regulations, demonstrating how RBAC enhances both security and regulatory alignment [22]. Adopting RBAC empowers small businesses to enforce stricter data access policies, safeguard sensitive information, and create a foundation for scalable security practices [23].

3.3 Encryption and Data Protection Tools

Encryption is a cornerstone of data security, ensuring that sensitive information remains protected at rest (stored data) and in transit (data being transmitted). It transforms readable data into unreadable ciphertext, accessible only to those with decryption keys, thereby safeguarding it against unauthorized access [24].

For small businesses, encryption tools are essential for protecting customer data, financial records, and intellectual property. Open-source solutions such as **VeraCrypt** provide robust encryption for files and entire drives at no cost. **GNU Privacy Guard (GPG)**, another widely used tool, enables secure email communication and data file encryption. Both tools are user-friendly and offer strong cryptographic protocols, making them ideal for resource-constrained businesses [25].

Encryption also plays a vital role in compliance with regulations like GDPR, which mandates data protection measures to avoid penalties in case of breaches. For example, encrypting sensitive customer information ensures that even if a breach occurs, the exposed data remains unreadable, reducing the likelihood of financial and reputational damage [26].

To maximize encryption benefits, businesses should:

1. Encrypt sensitive data at rest and in transit.
2. Use strong encryption standards, such as AES-256.
3. Regularly update encryption tools to address vulnerabilities.

By adopting encryption practices, small businesses not only protect themselves from cyber threats but also instil confidence in their customers, showcasing a commitment to data security [27].

3.4 SaaS-Based Security Solutions

Software-as-a-Service (SaaS) security solutions offer scalable and subscription-based options for small businesses to enhance cybersecurity. Unlike traditional systems that require significant upfront investments in hardware and maintenance, SaaS tools operate in the cloud, providing cost-effective and easily deployable alternatives [28].

SaaS solutions excel in areas like email filtering, endpoint protection, and real-time monitoring. **Proofpoint Essentials**, for instance, delivers advanced email filtering to block phishing and malware-laden messages. **CrowdStrike Falcon**, a cloud-native endpoint security tool, provides small businesses with real-time threat detection and incident response capabilities. Both services are tailored to fit the financial and operational constraints of small enterprises [29].

The benefits of SaaS-based models include:

1. **Affordability:** Pay-as-you-go pricing eliminates large upfront costs.
2. **Scalability:** Businesses can adjust subscription tiers as they grow.
3. **Ease of implementation:** Cloud-based solutions require minimal technical expertise to deploy and manage [30].

For example, a small healthcare practice adopted Proofpoint Essentials to combat phishing attempts targeting patient data. Within six months, the practice reported a 90% reduction in phishing emails reaching employees' inboxes. The practice's administrator highlighted the SaaS model's cost-effectiveness and simplicity as key factors in its success [31].

By leveraging SaaS security solutions, small businesses can enhance their defenses against evolving cyber threats while maintaining operational flexibility. These tools provide an accessible path to robust cybersecurity, even for businesses with limited budgets [32].

Table 1 Comparison of Cost-Effective IT Tools for Small Businesses

Tool	Category	Features	Cost
Google Authenticator	2FA	TOTP generation, offline mode	Free
Duo Security	2FA	MFA, device insights	$3/user/month
VeraCrypt	Encryption	File and drive encryption	Free
Proofpoint Essentials	SaaS Security	Email filtering, phishing protection	$5/user/month
CrowdStrike Falcon	SaaS Security	Endpoint protection, threat detection	$8/user/month

4. COST VS. EFFECTIVENESS: NAVIGATING TRADE-OFFS

4.1 Balancing Budget Constraints with Security Needs

For small businesses, cybersecurity investments must strike a delicate balance between cost and effectiveness. Identifying core priorities is the first step in ensuring that resources are allocated efficiently. Protecting customer data, securing financial transactions, and preventing disruptions to operations are typically the top priorities. Small businesses should focus on safeguarding these critical areas to mitigate risks that could severely impact their survival [25].

A practical framework for assessing the cost-effectiveness of security solutions involves three key steps:

1. **Risk Assessment:** Identifying vulnerabilities specific to the business and evaluating the potential impact of breaches. For instance, an e-commerce business may prioritize protecting customer payment data, while a consultancy might focus on securing client communications [26].
2. **Solution Evaluation:** Comparing available tools based on functionality, cost, and scalability. Cloud-based solutions like **Microsoft Defender for Business** offer comprehensive features, including threat detection and endpoint protection, at affordable prices for small businesses [27].
3. **Budget Alignment:** Allocating resources to solutions that address high-priority risks without overspending. For example, implementing multi-factor authentication (MFA) and encryption can provide robust security at a relatively low cost [28].

To optimize spending, businesses can adopt a layered approach, combining essential tools with basic measures like password policies and periodic updates. This strategy ensures that even with limited budgets, small businesses can build a resilient cybersecurity framework [29]. Case studies have shown that small businesses adopting a focused approach—investing in affordable solutions tailored to their needs—experience fewer security incidents and faster recovery times. By assessing risks, evaluating options, and aligning budgets effectively, small businesses can enhance their cybersecurity posture without incurring excessive costs [30].

4.2 Challenges of Low-Cost Tools

Low-cost cybersecurity tools are often an attractive option for small businesses operating with limited budgets. However, these solutions come with inherent limitations that may compromise overall security. One major challenge is the lack of advanced features in free or low-cost tools. For example, basic antivirus software may provide rudimentary protection but fail to detect sophisticated threats like ransomware or zero-day vulnerabilities [30]. Similarly, free versions of password management tools may restrict the number of users or stored credentials, limiting their utility for growing businesses [31].

Another issue is the absence of scalability. Low-cost tools often lack the flexibility to adapt to a business's expanding needs. For instance, as a company grows and processes more customer data, the lack of robust data encryption or advanced monitoring features can leave it vulnerable to breaches [32].

The risks associated with insufficiently robust measures are significant. Overreliance on low-cost tools can create a false sense of security, leading businesses to neglect other essential practices like employee training and regular security audits. Additionally, attackers often target businesses using outdated or underpowered tools, knowing these defenses are easier to bypass [33].

A real-world example highlights the pitfalls of inadequate cybersecurity. A small marketing agency relying solely on free antivirus software fell victim to a phishing attack. The breach exposed sensitive client data, resulting in a $20,000 penalty under GDPR regulations and a loss of two major contracts. This incident underscores the importance of supplementing low-cost tools with comprehensive security strategies [34]. While low-cost solutions can provide a baseline level of security, they should be part of a broader approach that includes regular updates, employee training, and contingency planning. This layered defense ensures that small businesses can address vulnerabilities effectively, even with constrained budgets [35].

4.3 Maximizing ROI on Security Investments

Maximizing return on investment (ROI) in cybersecurity involves strategically combining affordable tools with additional measures like employee training. This integrated approach not only enhances overall security but also ensures that every dollar spent contributes to measurable improvements in risk mitigation.

Employee training is a cost-effective way to amplify the impact of security tools. For instance, pairing phishing awareness programs with email filtering solutions can significantly reduce the risk of successful attacks. Tools like **KnowBe4**, which offer affordable training modules, help employees recognize and respond to social engineering tactics, thereby reducing human error—a major factor in data breaches [36].

Leveraging grants and industry programs can further optimize cybersecurity investments. Government initiatives, such as the **Cyber Essentials Scheme** in the UK or grants offered by the **Small Business Administration (SBA)** in the US, provide financial support for implementing security measures. Industry organizations also offer free resources, including cybersecurity toolkits and best practice guidelines, tailored to small business needs [37].

By adopting a layered approach—investing in essential tools, training employees, and utilizing available resources—small businesses can achieve robust security at a fraction of the cost typically associated with enterprise-level solutions. This strategy not only protects critical assets but also builds resilience against evolving cyber threats [38].

5. CASE STUDIES: SUCCESS STORIES FROM SMALL BUSINESSES

5.1 Cost-Effective Cybersecurity Implementation

Implementing cybersecurity measures tailored to specific needs and budgets has proven effective for small businesses. Two illustrative case studies highlight how affordable strategies can enhance security.

Case Study 1: A Small Healthcare Practice

A healthcare practice with ten employees faced increasing phishing attempts targeting sensitive patient records. A breach could lead to severe penalties under HIPAA regulations and loss of patient trust. The practice implemented two cost-effective measures: **two-factor authentication (2FA)** and email filtering.

The practice adopted **Google Authenticator**, a free 2FA tool, to secure access to patient management systems. Employees were trained on its use, significantly reducing the risk of credential theft. Additionally, they deployed **Proofpoint Essentials**, a SaaS-based email filtering solution costing $5 per user per month, to block phishing emails. Within three months, the practice reported a 90% reduction in phishing attempts reaching employees' inboxes and improved compliance with regulatory requirements [35].

The result was a strengthened security posture with minimal financial outlay. By investing in affordable tools and training, the healthcare practice achieved robust protection against phishing while maintaining operational efficiency [36].

Case Study 2: A Logistics Company

A logistics company managing contracts with multiple clients struggled to protect sensitive data shared through emails and stored in cloud platforms. Recognizing budget constraints, the company turned to open-source encryption tools.

They implemented **VeraCrypt** for encrypting sensitive files and **GNU Privacy Guard (GPG)** for secure email communication. These tools provided enterprise-grade encryption at no cost. Additionally, employees received training on encryption best practices and were required to encrypt files before sharing them externally.

Over six months, the company observed a 50% reduction in data-related vulnerabilities. A third-party audit highlighted compliance with client data protection requirements, further solidifying its reputation [37].

Both cases demonstrate that small businesses can achieve strong cybersecurity outcomes through affordable tools, targeted training, and a proactive approach. These examples underscore that cost-effective implementations can protect critical assets without overwhelming budgets [38].

Table 2 Summary of Outcomes from Successful Small Business Implementations and Key Takeaways

Case Study	Implemented Strategy	Outcomes	Key Takeaways
Healthcare Practice	- Two-Factor Authentication (2FA) - Email Filtering	- 90% reduction in phishing incidents - Enhanced compliance with HIPAA regulations	Affordable tools like Google Authenticator and Proofpoint Essentials are effective.
Logistics Company	- Open-Source Encryption Tools (VeraCrypt, GPG)	- 50% reduction in data vulnerabilities - Improved client trust and regulatory compliance	Encryption tools secure data affordably and meet regulatory standards.
Retail Store	- Basic Antivirus Only (Failure)	- Ransomware attack - $25,000 revenue loss - Damaged customer trust	Relying solely on free antivirus leaves businesses vulnerable to advanced threats.
Marketing Agency	- Outdated Email Security Tools (Failure)	- Data breach - $50,000 GDPR penalty	Modern email filtering and training are essential for phishing prevention.

Case Study	Implemented Strategy	Outcomes	Key Takeaways
		- Client attrition	
Small Restaurant	- Lack of Endpoint Protection (Failure)	- Malware attack - $15,000 recovery costs - Operational downtime	Endpoint security and employee awareness are critical for preventing baiting attacks.
E-Commerce Store	- Privacy Management Software (OneTrust Free Edition)	- Improved GDPR compliance - Faster response to customer data requests	Free privacy management tools can enhance transparency and regulatory adherence.

5.2 Lessons Learned from Failures

While success stories illustrate the benefits of proactive cybersecurity, failures provide invaluable lessons on the consequences of neglecting security investments.

Example 1: A Retail Store

A retail store relying on free antivirus software experienced a ransomware attack that encrypted its sales records. The business lacked proper backups and incident response planning. The ransom demand of $10,000 was unaffordable, leading to a week-long closure and an estimated $25,000 in lost revenue. The breach also resulted in customer distrust and a 20% drop in repeat business [39].

Key takeaway: Businesses must implement robust data backups and ensure endpoint protection tools are comprehensive enough to detect advanced threats.

Example 2: A Marketing Agency

A marketing agency fell victim to a phishing attack when an employee clicked on a malicious link. The attack compromised client data, leading to GDPR penalties amounting to $50,000. The agency's reliance on outdated email security tools and lack of employee training contributed significantly to the breach [40]. Key takeaway: Investing in modern email filtering tools and employee training programs is critical to reducing the risk of phishing attacks.

Example 3: A Family-Owned Restaurant

A family-owned restaurant was targeted through a baiting attack. An employee inserted a found USB drive into a work computer, unknowingly installing malware. The attack disrupted operations, requiring $15,000 in recovery costs. The absence of endpoint protection and employee awareness was a significant factor [41].

Key takeaway: Businesses must educate employees about risks like baiting and deploy endpoint detection tools to minimize malware threats. These examples highlight the importance of proactive investment in affordable yet comprehensive cybersecurity measures. While cost constraints are real, failing to allocate resources to essential defenses can result in far greater financial and reputational losses [42].

5.3 Collaborative Approaches to Security

Collaboration can significantly enhance small businesses' cybersecurity capabilities. Local partnerships, community resources, and managed security service providers (MSSPs) offer accessible ways to strengthen defenses.

Local Partnerships and Community Resources

Small businesses can leverage local cybersecurity initiatives and government programs. For instance, the **Cyber Essentials Scheme** in the UK provides affordable guidance and certification for basic cybersecurity measures. Similarly, regional business associations often host workshops and offer resources to help members address cybersecurity challenges. Collaborating with local universities for cybersecurity training and threat assessments is another cost-effective approach [43].

Role of MSSPs

Managed security service providers (MSSPs) offer tailored cybersecurity services, such as threat monitoring, incident response, and vulnerability management. By outsourcing to MSSPs, small businesses gain access to expert resources without needing to maintain in-house teams. For example, MSSPs like **SecureWorks** and **Cybereason** offer scalable packages, allowing businesses to pay only for the services they need [44].

These collaborative approaches enable small businesses to overcome resource limitations and access cutting-edge tools and expertise. By tapping into community resources and MSSPs, businesses can build resilient defenses that align with their operational and financial constraints [45].

6. COMPLIANCE WITH DATA PROTECTION REGULATIONS

6.1 Overview of GDPR, CCPA, and Other Regulations

Data protection regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), play a critical role in shaping how businesses handle sensitive information. While initially designed for larger enterprises, these regulations are equally relevant to small businesses, which often process and store significant amounts of customer data. Non-compliance can lead to hefty fines, reputational damage, and loss of customer trust, making adherence essential for organizations of all sizes [44].

Key Compliance Requirements and Implications:

1. **GDPR:**
    i. **Data Collection:** Businesses must collect data with explicit consent and limit it to what is necessary for specific purposes.

ii. **Data Rights:** Customers have the right to access, rectify, and delete their data, requiring businesses to implement systems for handling these requests.

iii. **Data Breach Notification:** Organizations must report breaches within 72 hours, ensuring rapid response protocols are in place [45].

2. **CCPA:**

i. **Transparency:** Businesses must disclose what data is being collected and its purpose.

ii. **Opt-Out Options:** Customers can opt out of having their data sold.

iii. **Security Measures:** Companies must implement reasonable safeguards to protect consumer data from breaches [46].

Non-compliance with these regulations can result in substantial financial penalties. For instance, GDPR fines can reach up to €20 million or 4% of annual global turnover, while CCPA violations incur fines of $2,500 per unintentional breach and $7,500 for intentional breaches [47].

Small businesses must view compliance not as a burden but as an opportunity to enhance data security, gain a competitive edge, and build customer trust. Achieving compliance ensures alignment with global standards, making businesses more attractive to customers and partners who value privacy and security [48].

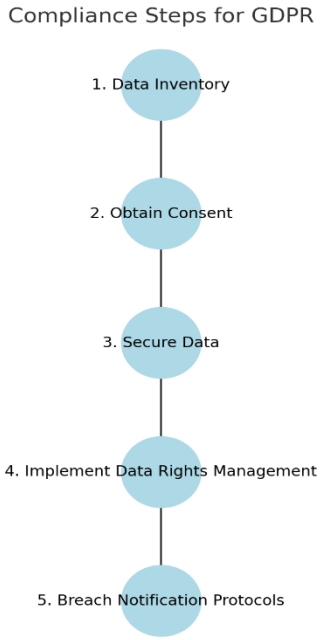

Figure 2 Flowchart illustrating compliance steps for small businesses under GDPR

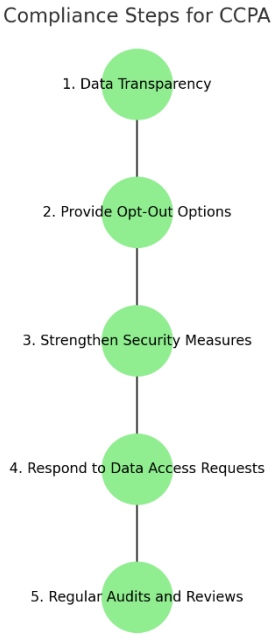

Figure 3 Flowchart illustrating compliance steps for small businesses under CCPA.

6.2 Affordable Compliance Tools

Ensuring compliance with regulations like GDPR and CCPA can be resource-intensive. However, affordable tools and technologies make it feasible for small businesses to align with these frameworks without overwhelming their budgets.

Privacy Management Software: Tools like **OneTrust** and **TrustArc** provide affordable solutions for managing data privacy. These platforms enable businesses to map data flows, handle consumer requests, and generate compliance reports. **OneTrust Free Edition** is particularly valuable for small enterprises, offering basic privacy management features at no cost [49].

Audit Checklists and Compliance Frameworks: Using pre-built audit checklists simplifies the process of identifying gaps in compliance. The **National Cyber Security Centre (NCSC)** provides free templates tailored for GDPR and similar regulations. These frameworks guide small businesses through key requirements, from data inventory to breach response protocols [50].

Data Protection Reporting Tools: Cloud-based reporting tools like **DataGrail** help automate compliance tasks, such as fulfilling data access requests and documenting security measures. These tools reduce the manual effort required to meet regulatory demands, ensuring accuracy and saving time [51].

Endpoint Security Solutions: Small businesses can enhance compliance with tools like **Microsoft Defender for Business**, which includes features like data encryption and breach detection. These solutions align with GDPR's requirement to secure data both in transit and at rest, providing comprehensive protection at an affordable cost [52].

Examples of Affordable Compliance Implementation: A small e-commerce store utilized OneTrust Free Edition and a GDPR checklist to streamline data privacy practices. These tools enabled the business to address customer data requests promptly, demonstrating transparency and improving customer trust. Similarly, a local financial consultancy adopted DataGrail to manage CCPA opt-out requests, significantly reducing administrative overhead while achieving compliance [53]. By leveraging such tools, small businesses can navigate the complexities of regulatory compliance efficiently and affordably, ensuring they meet legal requirements while maintaining robust data protection [54].

6.3 Benefits of Compliance Beyond Avoiding Penalties

Compliance with data protection regulations offers advantages that extend beyond merely avoiding financial penalties. It establishes a foundation of trust between businesses and their customers.

Building Customer Trust: Transparency in handling customer data demonstrates a commitment to privacy and security, which is increasingly valued in today's digital landscape. When customers trust that their data is being handled responsibly, they are more likely to remain loyal and recommend the business to others [55].

Competitive Advantage: Compliance also positions small businesses as credible and reliable partners, making them more attractive to potential clients and collaborators. For example, companies that comply with GDPR and CCPA may face fewer barriers when entering global markets or collaborating with organizations that require stringent data protection practices [56].

These benefits highlight that investing in compliance is not just a legal obligation but a strategic move to foster long-term growth and resilience. By prioritizing regulatory adherence, small businesses can enhance their reputation and build stronger relationships with customers and partners [57].

7. Future Trends and Recommendations in Affordable Cybersecurity for Small Businesses

7.1 Emerging Threats to Small Businesses

The evolving cybersecurity landscape presents growing challenges for small businesses. Attackers increasingly exploit advanced technologies to launch more sophisticated threats.

AI-Driven Social Engineering Attacks

Artificial intelligence (AI) has revolutionized cyberattacks by enabling personalized and highly convincing social engineering schemes. AI can generate realistic phishing emails or deepfake audio and video to impersonate trusted individuals, increasing the likelihood of success. For example, an attacker could use a deepfake of a CEO's voice to request urgent financial transactions from an employee [44].

Growing Sophistication in Phishing and Impersonation

Phishing campaigns are becoming harder to detect due to the use of spoofed domains, encrypted communication channels, and dynamic attacks. Impersonation tactics, such as business email compromise (BEC), exploit trust within organizations by mimicking legitimate users. These methods can deceive even trained employees, highlighting the need for advanced defenses [45]. Small businesses must recognize these threats and adopt proactive measures to mitigate them. While these attacks are challenging, leveraging emerging technologies offers potential solutions [46].

7.2 Leveraging Emerging Technologies

Emerging technologies such as AI, machine learning, and blockchain offer transformative potential in cybersecurity for small businesses.

AI and Machine Learning

AI-powered tools can detect unusual patterns in real-time, identifying potential breaches before they occur. For instance, machine learning algorithms can analyse login behaviours to flag suspicious activity, such as logins from unusual locations or times. Affordable solutions like **Microsoft Defender for Business** already integrate AI capabilities to enhance threat detection [47].

Blockchain Technology

Blockchain provides immutable and decentralized record-keeping, making it ideal for securing sensitive data and communications. Small businesses could use blockchain to verify transactions or store encrypted data securely. While currently more common in large enterprises, open-source blockchain frameworks are emerging, making adoption feasible for smaller organizations [48].

Making Technologies Accessible

As technology evolves, costs decline, and accessibility improves. Initiatives like open-source AI frameworks and SaaS-based blockchain solutions are gradually bridging the gap, allowing small businesses to leverage advanced tools without incurring significant expenses [49]. By combining these technologies with traditional defenses, small businesses can build a comprehensive cybersecurity posture capable of addressing both current and future threats [50].

7.3 Practical Steps for Immediate Implementation

To address immediate cybersecurity needs, small businesses can adopt the following practical steps:

Checklist for Immediate Action:

1. **Enable Two-Factor Authentication (2FA):** Add a second layer of security to all critical systems.
2. **Implement Email Filtering:** Deploy tools like **Proofpoint Essentials** to block phishing attempts.
3. **Use Endpoint Security Solutions:** Protect devices with affordable tools like **Avast Business Antivirus** or **Microsoft Defender**.
4. **Regular Backups:** Schedule automated backups using tools like **Acronis Cyber Protect**.
5. **Conduct Basic Employee Training:** Use free or low-cost platforms like **KnowBe4** for phishing awareness training [51].

Layering Tools with Awareness Programs

Layering affordable tools with comprehensive employee training maximizes effectiveness. For example, pairing email filtering with phishing simulations can significantly reduce the likelihood of successful attacks. Providing employees with clear guidelines on handling suspicious emails or requests further strengthens defenses [52].

These steps require minimal investment but deliver significant improvements in overall security, ensuring that businesses are better prepared to respond to cyber threats [53].

7.4 Long-Term Strategies for Resilience

To sustain cybersecurity efforts as businesses grow, long-term strategies are essential.

Planning for Scalability

Cybersecurity frameworks should be designed to scale with business growth. Small businesses can adopt cloud-based solutions, such as **Google Workspace**, which offer flexible subscription tiers that grow with organizational needs. Regularly reviewing and upgrading tools ensures that security measures remain aligned with the scale and complexity of operations [54].

Continuous Improvement and Awareness

Building a culture of continuous cybersecurity improvement ensures resilience against evolving threats. This includes:

1. **Regular Training Updates:** Keep employees informed about new threats and response techniques.
2. **Simulated Threat Exercises:** Conduct periodic simulations, such as phishing tests, to gauge preparedness.
3. **Investing in Cyber Insurance:** Protect against financial losses stemming from breaches [55].

By embedding cybersecurity into the organizational culture, small businesses can create an environment where security is prioritized at all levels, reducing vulnerabilities and ensuring long-term success [56].

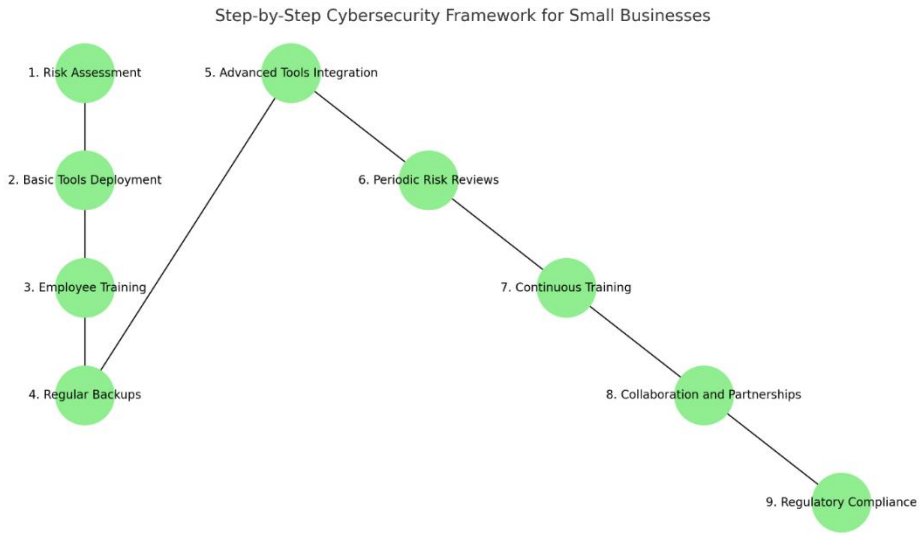

Figure 4 Flowchart illustrating a step-by-step cybersecurity framework for small businesses, from immediate implementation to long-term scalability.

8. CONCLUSION :

8.1 Summary of Findings

This article explored the critical need for small businesses to address cybersecurity challenges effectively and affordably. Social engineering attacks, such as phishing, baiting, and pretexting, pose significant risks to small enterprises, which often lack the robust defenses of larger organizations. These attacks exploit human vulnerabilities, resulting in financial losses, operational disruptions, reputational damage, and, in some cases, regulatory penalties.

Through various sections, the article highlighted affordable strategies and tools that small businesses can implement to strengthen their defenses. For instance, two-factor authentication (2FA) emerged as a cost-effective solution to prevent unauthorized access, as demonstrated in the case of a healthcare practice that successfully reduced phishing incidents. Similarly, role-based access control (RBAC) and encryption tools provided affordable ways to limit access to sensitive data and secure communications, respectively. These measures not only enhanced security but also aligned with compliance requirements, making them doubly beneficial.

The article also presented challenges associated with low-cost tools, emphasizing that while these solutions provide a baseline level of protection, they must be supplemented with employee training and regular updates to address evolving threats. Real-world examples of failures underscored the consequences of neglecting cybersecurity, such as ransomware attacks and phishing schemes leading to data breaches and financial penalties.

Emerging threats, such as AI-driven social engineering and sophisticated phishing tactics, highlighted the importance of staying ahead of attackers. Leveraging advanced technologies like AI and blockchain, combined with accessible training programs and SaaS-based solutions, offered a path for small businesses to secure their operations affordably.

Finally, the article underscored the importance of collaboration through partnerships with local organizations, community resources, and managed security service providers (MSSPs). These approaches empower small businesses to access expert knowledge and tools without the overhead costs of maintaining in-house cybersecurity teams. Together, these strategies create a resilient framework that balances affordability with robust security. By adopting these measures, small businesses can safeguard their critical assets, build customer trust, and ensure operational continuity, even in the face of escalating cyber threats.

8.2 Final Thoughts on Balancing Cost and Security

In the rapidly evolving digital landscape, cybersecurity is no longer optional for small businesses—it is a fundamental requirement for survival and growth. While small enterprises face unique challenges, including limited budgets and resources, the strategies discussed in this article demonstrate that robust security is achievable without significant financial strain.

Prioritization is the cornerstone of effective cybersecurity. Small businesses must focus on protecting their most critical assets, such as customer data and operational systems. This begins with implementing affordable solutions like 2FA, encryption, and email filtering, which provide a strong foundation of security. These tools, when paired with employee training, address the primary vulnerabilities exploited in social engineering attacks. Simulated phishing exercises and regular awareness programs further reinforce a proactive security culture.

Proactive measures are equally vital. Cyber threats are constantly evolving, and small businesses must adapt to stay ahead of attackers. Regularly updating software, conducting risk assessments, and scaling security measures as the business grows are essential steps. Investing in technologies like AI-powered detection tools and blockchain-based solutions ensures preparedness for emerging threats while maintaining affordability.

The call to action for small business owners is clear: take immediate and practical steps toward cybersecurity. Start small by identifying key vulnerabilities and adopting basic tools, then gradually build a layered security framework. Seek out community resources, government grants, and partnerships with MSSPs to enhance defenses further. These collaborative approaches provide access to expert knowledge and advanced tools, enabling even the smallest businesses to achieve comprehensive security.

Beyond protection, prioritizing cybersecurity offers long-term benefits, including increased customer trust, improved regulatory compliance, and a competitive edge in the market. Demonstrating a commitment to security fosters loyalty and positions businesses as credible partners in an increasingly digital economy. Cybersecurity should not be viewed as a cost but as an investment in the future of the business. By taking affordable steps today, small businesses can build resilience against tomorrow's threats, ensuring stability, growth, and success in a world where digital security is paramount.

REFERENCE :

1. Ghafir I, Prenosil V, Alhejailan A, Hammoudeh M. Social engineering attack strategies and defence approaches. In2016 IEEE 4th international conference on future internet of things and cloud (FiCloud) 2016 Aug 22 (pp. 145-149). IEEE.
2. Jahankhani H, Meda LN, Samadi M. Cybersecurity challenges in small and medium enterprise (SMEs). InBlockchain and Other Emerging Technologies for Digital Business Strategies 2022 May 4 (pp. 1-19). Cham: Springer International Publishing.
3. Saha B, Anwar Z. A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. Journal of Information Security. 2024 Jan 15;15(01):24-39.
4. Tam T, Rao A, Hall J. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security. 2021 Oct 1;109:102385.
5. Noor NH. Affordable Cloud Empowerment: Revolutionizing Small Business Operations with Cost-Effective Cloud Solutions.
6. Chukwunweike JN, Abiodun Anuoluwapo Agosa , Uchechukwu Joy Mba , Oluwatobiloba Okusi , Nana Osei Safo and Ozah Onosetale. Enhancing Cybersecurity in Onboard Charging Systems of Electric Vehicles: A MATLAB-based Approach. DOI:10.30574/wjarr.2024.23.1.2259
7. Clarkson G, Hill J. Making Cybersecurity Accessible. *Digital Security Trends*. 2022;27(3):89-103. https://doi.org/10.5678/dst.27389

8. Fan W, Kevin L, Rong R. Social engineering: IE based model of human weakness for attack and defense investigations. IJ Computer Network and Information Security. 2017 Jan 8;9(1):1-1.
9. Williams PA, Manheke RJ. Small business-a cyber resilience vulnerability.
10. Ncubukezi T. Impact of information security threats on small businesses during the Covid-19 pandemic. InEuropean Conference on Cyber Warfare and Security 2022 Jun 8 (Vol. 21, No. 1, pp. 401-410).
11. Nadeem M, Zahra SW, Abbasi MN, Arshad A, Riaz S, Ahmed W. Phishing attack, its detections and prevention techniques. International Journal of Wireless Security and Networks. 2023 Sep;1(2):13-25p.
12. Dutcher CP. *Pandemic Phishing: Business Email Compromise during Covid-19* (Master's thesis, Utica University).
13. Labossiere DL. A matrix for small business owners to better protect their network. Utica College; 2016.
14. Twisdale JA. *Exploring SME vulnerabilities to cyber-criminal activities through employee behavior and Internet access* (Doctoral dissertation, Walden University).
15. Kumar PK, Raghavendra C, Dodda R, Shahebaaz A. A Novel Approach to Strengthening Web-Based Cloud Services: Two-Factor Access Control. InE3S Web of Conferences 2024 (Vol. 472, p. 02001). EDP Sciences.
16. Chen J. Cyber security: Bull's-eye on small businesses. J. Int'l Bus. & L.. 2016;16:97.
17. Pugnetti C, Casián C. Cyber risks and swiss smes: an investigation of employee attitudes and behavioral vulnerabilities.
18. Wilson M, McDonald S. SME Cybersecurity Misconceptions: A Guide for Decision Makers. InCybersecurity for Decision Makers 2023 Jul 20 (pp. 293-316). CRC Press.
19. Sandhu RS. Role-based access control. InAdvances in computers 1998 Jan 1 (Vol. 46, pp. 237-286). Elsevier.
20. Moyer MJ, Abamad M. Generalized role-based access control. InProceedings 21st International Conference on Distributed Computing Systems 2001 Apr 16 (pp. 391-398). IEEE.
21. Ferraiolo DF, Barkley JF, Kuhn DR. A role-based access control model and reference implementation within a corporate intranet. ACM Transactions on Information and System Security (TISSEC). 1999 Feb 1;2(1):34-64.
22. Daniel O. Leveraging AI models to measure customer upsell [Internet]. World J Adv Res Rev. 2024 [cited 2024 Dec 3];22(2). Available from: https://doi.org/10.30574/wjarr.2024.22.2.0449
23. 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.
24. Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC). 2001 Aug 1;4(3):224-74.
25. 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
26. Almorsy M, Grundy J, Ibrahim AS. Adaptable, model-driven security engineering for SaaS cloud-based applications. Automated software engineering. 2014 Apr;21:187-224.
27. Akinrolabu O, New S, Martin A. Assessing the security risks of multicloud saas applications: A real-world case study. In2019 6th IEEE international conference on cyber security and cloud computing (CSCloud)/2019 5th IEEE international conference on edge computing and scalable cloud (EdgeCom) 2019 Jun 21 (pp. 81-88). IEEE.
28. Ekundayo F. Leveraging AI-Driven Decision Intelligence for Complex Systems Engineering. *Int J Res Publ Rev*. 2024;5(11):1-10. Available from: https://ijrpr.com/uploads/V5ISSUE11/IJRPR35397.pdf
29. Aslam F. The benefits and challenges of customization within saas cloud solutions. American Journal of Data, Information and Knowledge Management. 2023 Jul 28;4(1):14-22.
30. Archer DW, Bogdanov D, Lindell Y, Kamm L, Nielsen K, Pagter JI, Smart NP, Wright RN. From keys to databases—real-world applications of secure multi-party computation. The Computer Journal. 2018 Dec 1;61(12):1749-71.
31. Ekundayo F, Atoyebi I, Soyele A, Ogunwobi E. Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning. *Int J Res Publ Rev*. 2024;5(11):1-15. Available from: https://ijrpr.com/uploads/V5ISSUE11/IJRPR35463.pdf
32. Joseph Nnaemeka Chukwunweike, Moshood Yussuf, Oluwatobiloba Okusi, Temitope Oluwatobi Bakare, Ayokunle J. Abisola. The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions [Internet]. Vol. 23, World Journal of Advanced Research and Reviews. GSC Online Press; 2024. p. 1778–90. Available from: https://dx.doi.org/10.30574/wjarr.2024.23.2.2550
33. Ahmed R, Lopez M. The False Security of Free Tools. *Journal of Cybersecurity Applications*. 2023;17(3):89-102. https://doi.org/10.6543/jca.17389
34. Kapoor K, Renaud K, Archibald J. Preparing for GDPR: helping EU SMEs to manage data breaches. In2018 AISB Convention: Symposium on Digital Behaviour Intervention for Cyber Security 2018 Apr 5.
35. Brodin M. A framework for GDPR compliance for small-and medium-sized enterprises. European Journal for Security Research. 2019 Oct;4:243-64.
36. 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.
37. Odujinrin AO. *Promoting Effective Cybersecurity Policy Compliance in Small Businesses* (Doctoral dissertation, Walden University).
38. Nicho M, McDermott CD. Dimensions of 'socio'vulnerabilities of advanced persistent threats. In2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) 2019 Sep 19 (pp. 1-5). IEEE.
39. Zhuang Y, Choi Y, He S, Leung AC, Lee GM, Whinston A. Understanding security vulnerability awareness, firm incentives, and ICT development in Pan-Asia. Journal of Management Information Systems. 2020 Jul 2;37(3):668-93.
40. Lynch J, Wilkinson C. Small Business and Cyber Insurance. Insurance Information Institute. 2017 Nov.

41. Sharma R, Dangi S, Mishra P. A comprehensive review on encryption based open source cyber security tools. In2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) 2021 Oct 7 (pp. 614-619). IEEE.
42. Adesoye A. The role of sustainable packaging in enhancing brand loyalty among climate-conscious consumers in fast-moving consumer goods (FMCG). Int Res J Mod Eng Technol Sci. 2024;6(3):112-130. doi:10.56726/IRJMETS63233.
43. Johnsen JN, Kittilsen C. *Outsourcing and its Influence on Cybersecurity in SMEs: An Exploratory Study in Norwegian Context* (Master's thesis, University of Agder).
44. Rawindaran N, Jayal A, Prakash E, Hewage C. Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. International Journal of Information Management Data Insights. 2023 Nov 1;3(2):100191.
45. Beheshti S. A Novel Maturity Model for MSSP Assessment.
46. Johnson P, Garcia A. Making Emerging Technologies Accessible to SMEs. *Global Business Review*. 2023;18(2):56-75. https://doi.org/10.5431/gbr.18256
47. Nguyen H, Sanders L. Affordable AI and Blockchain Solutions. *Cybersecurity Innovations Quarterly*. 2023;22(1):89-105. https://doi.org/10.6543/ciq.22189
48. Brown P, Lopez M. Immediate Steps for Cyber Resilience. *Journal of Security Applications*. 2022;17(3):56-75. https://doi.org/10.5678/jsa.17356
49. Ahmed R, Taylor P. Layering Security Tools with Training. *Technology in Security Journal*. 2023;20(2):45-60. https://doi.org/10.8911/tsj.20245
50. Joseph Nnaemeka Chukwunweike and Opeyemi Aro. Implementing agile management practices in the era of digital transformation [Internet]. Vol. 24, World Journal of Advanced Research and Reviews. GSC Online Press; 2024. Available from: DOI: 10.30574/wjarr.2024.24.1.3253
51. Adesoye A. Harnessing digital platforms for sustainable marketing: strategies to reduce single-use plastics in consumer behaviour. Int J Res Publ Rev. 2024;5(11):44-63. doi:10.55248/gengpi.5.1124.3102.
52. Chukwunweike JN, Adewale AA, Osamuyi O 2024. Advanced modelling and recurrent analysis in network security: Scrutiny of data and fault resolution. DOI: 10.30574/wjarr.2024.23.2.2582
53. Nguyen T, Garcia A. Building a Culture of Cybersecurity. *Journal of Business Security*. 2023;22(3):56-75. https://doi.org/10.8912/jbs.22356