INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

A Hiring Guide for Dual Role of IT and Cybersecurity Officers in Small to Medium Businesses

Institute for Homeland Security

Sam Houston State University

Cihan Varol and Narasimha Shashidhar

A Hiring Guide for Dual Role of IT and Cybersecurity Officers in Small to Medium Businesses

Cihan Varol[1] and Narasimha Shashidhar[2]

[1]https://www.linkedin.com/in/cihan-varol-53105012/

[2]https://www.linkedin.com/in/karpoor/

Table of Contents

1. Introduction and Overview

Small to medium-sized businesses (SMBs) face a growing need to manage their IT systems efficiently while defending against cyber threats. Unlike larger organizations with separate IT and cybersecurity teams, SMBs often need to combine these functions into a single dual role. This guide helps SMBs to hire the right person for this critical position, ensuring business stays secure and technology runs smoothly.

The dual role of IT and cybersecurity officer requires someone who can handle daily IT operations while proactively securing the systems and data. The right hire can streamline operations, reduce risks, and strengthen small to medium size businesses. However, hiring the wrong candidate can lead to inefficiencies, vulnerabilities, and compliance issues. This guide shows how to avoid those pitfalls and recruit the talent business needs.

In this work, we walk through each step of the hiring process—from defining the role and creating a job description to interviewing candidates and onboarding them effectively. We'll reflect how to identify candidates with the right mix of technical skills, cybersecurity expertise, and adaptability to thrive in a fast-paced SMB environment.

By following this guide, SMBs will gain the tools to attract top talent and set them up for success. SMBs will also understand how to balance IT management and cybersecurity within a single role while addressing challenges like workload and prioritization. Whether SMBs are hiring for this position for the first time or refining their approach, this guide gives clear, actionable advice to make the process smoother. Overall, a strong IT and cybersecurity officer helps SMBs stay ahead in today's digital world. With this guide, SMBs can confidently hire someone who will protect the systems, optimize the technology, and support business growth.

A. Gap Assessment and Problem Statement

Small to medium-sized businesses (SMBs) face unique challenges when managing IT and cybersecurity due to limited resources. Combining these critical functions into a single role is cost-effective but introduces significant risks if not handled properly. Key gaps include:

- **Limited Specialized Resources**: SMBs often cannot afford separate IT and cybersecurity teams, leading to skillset mismatches in dual-role hires.
- **Hiring Challenges**: Without a clear framework, businesses may hire candidates who excel in one area but lack expertise in the other, resulting in inefficiencies and vulnerabilities.
- **Evolving Threat Landscape**: Cyberattacks grow more sophisticated daily, requiring professionals who can adapt quickly while managing IT operations effectively.
- **Operational Risks**: Mismanagement of IT systems or weak cybersecurity measures can cause downtime, data breaches, and non-compliance with regulations.

- **Talent Scarcity**: Finding candidates with a balanced mix of technical, cybersecurity, and strategic skills is increasingly difficult, especially within SMB budget constraints.

Our guide provides actionable solutions to these challenges, helping SMBs:

- Define the dual role clearly, balancing IT and cybersecurity needs.
- Attract and evaluate candidates with the right mix of skills and experience.
- Address workload challenges through role prioritization and support systems.
- Build a secure, efficient, and scalable IT environment.

By addressing these gaps, SMBs can hire effectively, protect their operations, and support business growth in an increasingly complex digital world.

2. Related Works

Small businesses encounter unique challenges in recruitment, primarily due to their lower visibility and perceived legitimacy compared to larger organizations. Job seekers often lack familiarity with small firms, which can hinder their willingness to apply. Additionally, institutional pressures may further complicate recruitment efforts, as small businesses may not have the same resources or established practices as their larger counterparts (Williamson et al, 2002). According to Williamson et al., to address these barriers, small businesses can implement strategic marketing techniques to enhance their brand awareness and communicate their value effectively to potential job seekers. By adopting established human resource practices through strategic isomorphism, small firms can improve their legitimacy in the eyes of candidates. Furthermore, forming interorganizational linkages can bolster their reputation and attract talent. A balanced approach that combines distinctiveness with isomorphic strategies may lead to more successful recruitment outcomes for small businesses (Williamson et al, 2002). While small businesses often face general recruitment challenges related to visibility and legitimacy, these obstacles become even more pronounced in specialized roles such as the dual position of IT and cybersecurity officer. For SMBs, the need to attract versatile professionals capable of managing both IT infrastructure and cybersecurity defenses adds another layer of complexity to their hiring efforts.

The dual role of IT and cybersecurity officer has emerged as a practical solution for small and medium-sized businesses (SMBs) operating under tight budget constraints. These organizations face the dual challenge of maintaining robust IT systems to support daily operations while simultaneously protecting their digital assets from an ever-evolving array of cyber threats. As digital technologies become increasingly critical to business operations, SMBs must address the growing complexity of IT management and cybersecurity. This convergence of needs has led to the creation of hybrid roles that combine IT and cybersecurity responsibilities.

Despite its cost-effectiveness, the dual-role approach presents significant challenges. Research by the International Association of Privacy Professionals (IAPP) highlights that SMBs often lack the resources to hire separate professionals for IT and cybersecurity, leading to positions that demand a wide range of skills from a single individual (Smith et al., 2020). While this solution reduces costs, it can strain employees, creating the risk of burnout and gaps in service delivery. Similarly, ISACA's "State of Cybersecurity" report emphasizes the difficulty SMBs face in finding candidates who possess the requisite expertise in both domains (ISACA, 2022).

The overlap between IT and cybersecurity functions has become increasingly pronounced in recent years. A study by the Ponemon Institute (2019) found that 68% of SMBs believe integrating IT and cybersecurity operations improves organizational efficiency. However, the study also highlights potential risks, such as skill gaps and the challenge of balancing operational demands with strategic responsibilities. CompTIA's "Trends in IT and Cybersecurity" (2021) echoes this sentiment, noting that as IT managers increasingly encounter security-related tasks, cross-functional expertise becomes essential for success.

Another significant factor driving the adoption of dual roles is the global shortage of skilled cybersecurity professionals. The (ISC)² Cybersecurity Workforce Study (2022) estimated a shortfall of 3.4 million cybersecurity workers worldwide. This shortage disproportionately affects SMBs, which often struggle to compete with larger organizations for top talent. To address this issue, many SMBs prioritize hiring professionals with certifications like CISSP, Security+, or CISM, which demonstrate competency in both IT and cybersecurity domains (Greene & Patel, 2021).

Case studies have demonstrated the importance of clear role definitions and support structures in the success of dual-role implementations. For example, Kramer et al. (2020) analyzed a manufacturing firm that successfully adopted a dual-role position by clearly delineating responsibilities, leveraging automation tools to reduce workload, and outsourcing specific tasks. Conversely, poorly defined roles often lead to failures, as Garcia et al. (2021) observed in healthcare organizations where unclear expectations contributed to employee burnout and high turnover rates.

When effectively managed, the dual role of IT and cybersecurity officer can provide significant benefits to SMBs. According to NIST's Cybersecurity Framework (2020), integrating IT operations and security strategies under a single role facilitates streamlined communication and faster decision-making during crises. Additionally, organizations with unified IT and cybersecurity functions are better positioned to achieve compliance with regulations such as GDPR, HIPAA, or PCI DSS, which require cohesive efforts across both domains.

The dual-role approach, while challenging, offers SMBs a unique opportunity to enhance both operational efficiency and cybersecurity resilience. By building on insights from industry literature and adopting best practices, SMBs can successfully implement and support these hybrid roles. In this guide we aim to provide actionable steps for hiring, defining, and sustaining professionals in this critical capacity.

3. Proposed Guideline

A high-level architectural diagram for the overall picture of the solution is shown in Figure 1. The subsections contain the details of the proposed guideline.

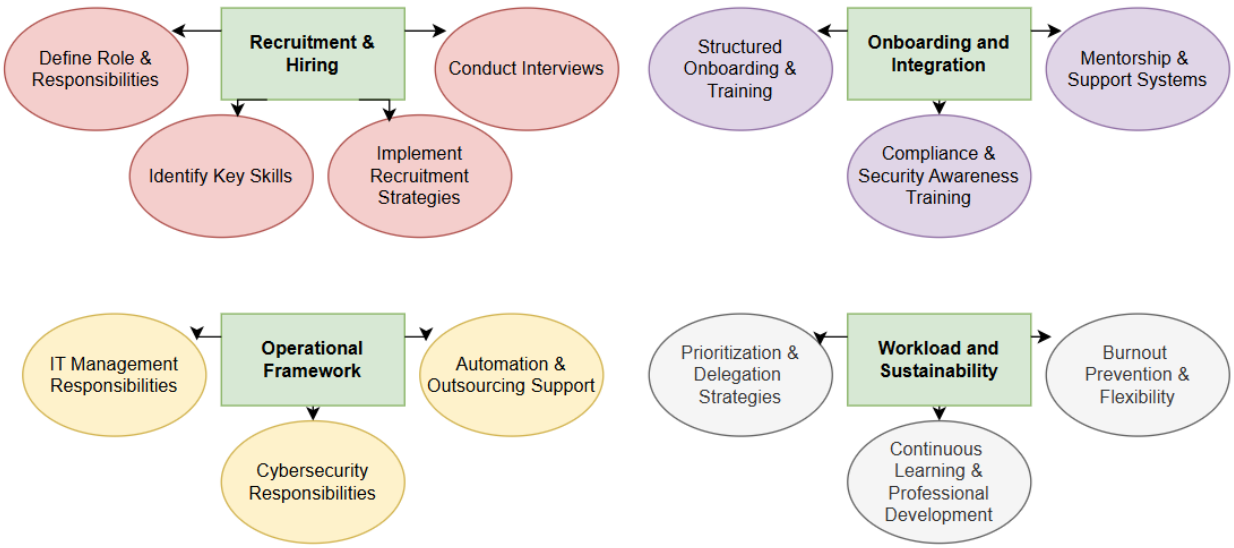

Figure 1: A High-Level Architectural Diagram for Dual – Rol Hiring

A. Understanding of the Dual Role:

The dual role of IT and cybersecurity officer combines the operational oversight of IT systems with the strategic responsibilities of safeguarding an organization against cyber threats. On one side, the individual is responsible for managing and maintaining IT infrastructure, which includes network configurations, hardware and software updates, and user support. This operational aspect ensures that the organization runs smoothly without interruptions caused by technical issues or outdated systems. Simultaneously, the cybersecurity dimension requires a proactive approach to risk management. This includes identifying potential vulnerabilities, implementing robust security measures, and responding swiftly to incidents such as data breaches or ransomware attacks. The professional must also stay ahead of evolving threats by keeping up with the latest trends in cybersecurity, such as zero-trust architectures and advanced threat detection technologies.

Success in this dual role demands a strategic mindset. The professional must align IT and cybersecurity priorities with the organization's broader objectives, ensuring that technological advancements and security enhancements support business growth rather than hinder it. For instance, they may need to balance the rollout of a new productivity tool with the necessity of mitigating associated security risks. This requires exceptional analytical skills and the ability to communicate complex technical concepts to non-technical stakeholders.

Moreover, adaptability is crucial. The dual-role professional often transitions between diverse tasks, such as troubleshooting a network issue in the morning and addressing a potential phishing threat in the afternoon. They must be prepared to shift focus quickly while maintaining accuracy and efficiency. Building strong relationships with other departments is equally important, as creating a culture of security awareness across the organization can significantly reduce risks.

The dual role also involves compliance management. The individual must ensure adherence to industry regulations such as GDPR, HIPAA, or PCI DSS, depending on the organization's domain. This adds an additional layer of responsibility, as failure to comply with these standards can result in severe penalties and reputational damage. By understanding the regulatory landscape and implementing the necessary controls, the professional plays a pivotal role in protecting the organization from legal and financial repercussions.

In summary, the dual role is not merely about technical expertise; it encompasses leadership, strategic thinking, and the ability to juggle competing priorities. A successful candidate will embody these qualities while demonstrating a commitment to continuous learning and professional growth. This section lays the foundation for the subsequent guidelines, which delve into practical steps for identifying, hiring, and supporting such a multifaceted professional.

B. Defining the Job Description

Defining the job description for a dual-role IT and cybersecurity officer is a crucial step in attracting the right talent. The description must strike a balance between clarity and comprehensiveness, providing a precise overview of the role while emphasizing its strategic importance to the organization. Here are the key elements to consider:

Role Overview: Begin the job description with a concise summary of the position. This should highlight its dual nature, emphasizing both IT management and cybersecurity responsibilities. For instance:

"We are seeking a skilled and versatile professional to serve as our IT and Cybersecurity Officer. This critical role involves overseeing our IT infrastructure while implementing and maintaining robust cybersecurity measures to protect our digital assets. The ideal candidate will bring a unique blend of technical expertise and strategic insight, ensuring the seamless operation and security of our systems."

Key Responsibilities: Clearly lay out the core responsibilities of the role, grouped into categories where possible:

<u>IT Management:</u>

- Oversee the maintenance and operation of the organization's IT infrastructure, including servers, networks, and end-user devices.

- Provide technical support and troubleshooting to staff, ensuring minimal disruption to daily operations.
- Plan and execute IT projects, such as system upgrades or new software deployments.
- Manage vendor relationships for IT hardware, software, and services.

Cybersecurity:

- Develop and enforce cybersecurity policies and procedures.
- Monitor for and respond to potential security incidents, such as malware infections or unauthorized access attempts.
- Conduct regular risk assessments and vulnerability scans, implementing appropriate mitigations.
- Ensure compliance with relevant cybersecurity standards and regulations, such as GDPR, HIPAA, or PCI DSS.

Strategic Contributions:

- Align IT and cybersecurity initiatives with the organization's broader business objectives.
- Provide leadership and guidance on emerging technology and security trends, advising management on potential opportunities and threats.
- Create a culture of cybersecurity awareness through training and communication initiatives.

Required Qualifications: Specify the skills, certifications, and experience required for the role. Be realistic and inclusive, recognizing that the perfect candidate may not exist but can grow into the role with the right foundation:

- Proven experience in IT management and/or cybersecurity roles, ideally within an SMB environment.
- Proficiency in managing networks, servers, cloud platforms, and security tools.
- Certifications such as CompTIA Security+, CISSP, CISM, or CCNA (or a willingness to obtain them within a specified timeframe).
- Strong problem-solving skills, with the ability to analyze complex situations and develop effective solutions.
- Excellent communication skills, capable of explaining technical concepts to non-technical audiences.

Preferred Attributes: Include desired but non-essential qualities that would make a candidate stand out:

- Experience with specific technologies used by the organization (e.g., Microsoft Azure, AWS, or specific firewall products).
- Familiarity with regulatory compliance requirements relevant to the industry.
- A track record of implementing successful IT or cybersecurity initiatives.

Performance Metrics: Outline how success in the role will be measured. Examples include:

- Uptime and reliability of IT systems.
- Reduction in cybersecurity incidents or vulnerabilities.
- Achievement of compliance with relevant standards or successful audits.
- Feedback from internal stakeholders on responsiveness and support.

Overall, by drafting a detailed and compelling job description, organizations can effectively communicate their expectations and attract candidates who are well-suited to the dual role. This clarity also sets the stage for the hiring process, ensuring alignment between the organization's needs and the candidate's skills and aspirations.

C. Identifying Key Skills and Qualifications

As we mentioned previously, the dual role of IT and cybersecurity officer requires a diverse and robust skill set that spans technical, strategic, and interpersonal domains. Identifying these skills is vital to ensure that candidates are well-equipped to handle the complexities of managing IT operations while maintaining strong cybersecurity defenses.

From a technical perspective, the candidate should demonstrate expertise in IT infrastructure management, including network configurations, server maintenance, and cloud computing. Familiarity with key cybersecurity practices, such as threat detection, vulnerability assessment, and encryption techniques, is essential. Moreover, they must possess the ability to integrate these technical skills to create a secure yet efficient IT environment.

In addition to technical knowledge, the role demands strong strategic skills. Candidates must be able to align IT and cybersecurity initiatives with the broader business goals of the organization. This involves conducting risk assessments, developing scalable solutions, and advising management on technology trends and security implications. The ability to prioritize and balance these competing objectives is a critical aspect of the role.

Interpersonal skills are equally important for success in this position. Effective communication, both with technical teams and non-technical stakeholders, ensures that IT and cybersecurity

policies are understood and adhered to across the organization. Problem-solving, adaptability, and a proactive mindset further enable the candidate to navigate challenges effectively.

Formal qualifications, such as certifications like CompTIA Security+, CISSP, or CCNA, serve as valuable benchmarks of expertise. While a degree in computer science or a related field can enhance a candidate's profile, practical experience often carries equal weight, particularly in small to medium-sized businesses where hands-on skills are critical.

Ultimately, identifying a candidate with the right mix of technical abilities, strategic insight, and interpersonal acumen lays the foundation for successfully fulfilling the dual-role position. Organizations that prioritize these qualities can ensure that their IT and cybersecurity needs are met effectively, driving both operational efficiency and security resilience.

D. Recruitment Strategies

Recruiting a dual-role IT and cybersecurity officer requires a deliberate and strategic approach to identify candidates with the necessary expertise, adaptability, and cultural fit for small to medium-sized businesses. Given the unique challenges of this role, organizations should adopt multi-faceted strategies that align with their resources and goals.

To this end, the first step in an effective recruitment strategy is leveraging specialized job boards and professional networks. Platforms like LinkedIn, Indeed, and niche sites such as CyberSecJobs or TechCareers are excellent for targeting professionals in IT and cybersecurity. Posting a compelling job description that emphasizes the dual nature of the role and its strategic importance to the organization can attract a broader pool of qualified candidates. Additionally, engaging with professional associations, such as ISACA or CompTIA, allows organizations to tap into a network of certified professionals with relevant expertise.

Internal referrals also play a significant role in identifying strong candidates. Employees who understand the organization's culture and technical requirements can recommend individuals from their professional circles. Offering incentives for successful referrals not only boosts engagement but also expands the candidate pool with trusted and vetted professionals.

Partnering with recruitment agencies that specialize in IT and cybersecurity hiring can be another effective strategy, especially for SMBs with limited in-house HR resources. These agencies possess the expertise to pre-screen candidates based on specific technical and interpersonal requirements, saving time and ensuring quality hires. Moreover, recruitment firms often have access to passive candidates—professionals who are not actively searching for jobs but may be interested in the right opportunity. Moreover, building a talent pipeline is critical for ongoing hiring needs. Organizations can establish relationships with local universities and technical colleges by participating in career fairs, offering internships, or sponsoring hackathons. This approach not only positions the organization as a desirable employer but also provides access to emerging talent that can be nurtured into the dual-role position over time.

Another innovative strategy is utilizing social media and targeted advertising to reach a broader audience. Crafting content that showcases the organization's commitment to innovation and security can resonate with prospective candidates. For example, sharing stories about successful IT or cybersecurity initiatives, or spotlighting employees in similar roles, can build credibility and attract talent.

We need to admit that for small to medium-sized businesses, competitive compensation packages can be a challenge. To address this, organizations should emphasize non-monetary benefits such as flexible work arrangements, opportunities for skill development, and a supportive work environment. Offering a clear career path with opportunities for growth and advanced certifications demonstrates a commitment to the professional development of the hire, making the position more attractive.

Finally, diversity and inclusion can be integral to recruitment strategies. Actively seeking candidates from underrepresented groups can create innovation and also broadens the range of perspectives in problem-solving. Organizations can achieve this by participating in diversity-focused job fairs, partnering with advocacy groups, or ensuring job descriptions use inclusive language.

Overall, by adopting these comprehensive recruitment strategies, SMBs can improve their chances of finding a candidate who not only meets the technical and strategic demands of the dual role but also aligns with the organization’s values and vision.

E. Interviewing for the Dual Role

Interviewing for the dual-role position of IT and cybersecurity officer is a critical step in the hiring process, since it enables organizations to assess a candidate’s technical expertise, strategic thinking, and cultural fit. This process should be structured and comprehensive, utilizing a mix of technical evaluations, behavioral questions, and scenario-based discussions to identify the most qualified individual for the unique demands of the role.

The interview process should begin with a thorough review of the candidate’s background, including their resume, certifications, and previous experiences. This initial review helps identify areas for deeper exploration during the interview. For instance, if a candidate lists experience managing IT projects, interviewers can prepare targeted questions to assess their ability to balance project execution with cybersecurity considerations.

Technical Skills Assessment: A robust technical evaluation is essential for this dual role. Interviewers should assess the candidate’s knowledge of IT infrastructure, such as network configurations, server management, and cloud platforms, alongside cybersecurity principles like threat mitigation, incident response, and compliance frameworks. Practical exercises, such as asking the candidate to troubleshoot a hypothetical network issue or analyze a simulated security incident, can provide insights into their problem-solving abilities and thought processes.

Additionally, the use of technical tests or online platforms that evaluate coding, scripting, or system administration skills can help validate their technical expertise.

Behavioral Questions: Behavioral interview questions are valuable for understanding how the candidate approaches challenges, prioritizes tasks, and collaborates with others. Questions like, "Can you describe a time when you had to manage competing priorities between IT operations and cybersecurity needs?" or "How have you worked with non-technical stakeholders to implement a new security policy?" can help assessing the candidate's adaptability, communication skills, and ability to balance responsibilities effectively.

Scenario-Based Discussions: Scenario-based questions can provide a deeper look into the candidate's strategic thinking and decision-making skills. Presenting hypothetical situations, such as a ransomware attack or a sudden IT system failure, allows the candidate to outline their approach to resolving the issue. Interviewers can evaluate whether their proposed solutions align with the organization's expectations and resources. For example, a candidate's response to securing a remote workforce may reveal their familiarity with modern tools like multi-factor authentication, VPNs, and endpoint protection.

Cultural Fit Assessment: Cultural fit is crucial, especially in small to medium-sized businesses where the dual-role officer often interacts closely with multiple departments. Interviewers should ask questions that gauge the candidate's alignment with the organization's values, such as their approach to teamwork, leadership style, and willingness to mentor others. Questions like, "How do you ensure collaboration across teams while implementing IT or security initiatives?" can provide valuable information on their interpersonal skills and ability to build a culture of security awareness.

Panel Interviews: If possible, conducting panel interviews with representatives from IT, cybersecurity, and executive leadership can provide a holistic assessment of the candidate. Each panelist can focus on a specific aspect of the role, such as technical expertise, strategic alignment, or interpersonal skills, ensuring a well-rounded evaluation. Additionally, this approach allows the candidate to demonstrate their ability to communicate effectively with diverse stakeholders.

Red Flags: Interviewers should also be careful for potential red flags, such as overemphasis on one domain (e.g., cybersecurity) at the expense of the other (IT management), resistance to learning new skills, or an inability to articulate complex concepts in simple terms. A lack of enthusiasm for continuous professional development may also indicate that the candidate is not well-suited for the evolving demands of the dual role.

Conclusion: To conclude the interview process, organizations can request references to verify the candidate's past performance and conduct a follow-up discussion to address any unresolved questions. A structured scoring system can help compare candidates objectively, ensuring that the final decision aligns with the organization's technical and cultural requirements.

F. Mentorship and Integration

The successful onboarding and integration of dual-role IT and cybersecurity officer hinge on robust mentorship and support systems. Given the multifaceted nature of this position, the individual needs to quickly adapt to the organization's technical environment, security protocols, and strategic priorities. Providing structured mentorship and fostering a culture of collaboration are key to ensuring their success.

A well-structured onboarding process sets the stage for smooth integration. This should include an overview of the organization's IT infrastructure, cybersecurity policies, and current projects. Introducing the new hire to key stakeholders, such as department heads and executive leadership, fosters immediate rapport and clarifies cross-departmental expectations. Pairing the new hire with a mentor—preferably someone who has experience in IT or cybersecurity—can provide invaluable guidance as they navigate their new responsibilities. Mentorship programs should begin with setting clear expectations for the role. This involves outlining short-term and long-term goals, such as completing a system audit, implementing new security protocols, or enhancing IT infrastructure efficiency. Regular check-ins with both the mentor and leadership can help track progress, identify challenges, and adjust priorities as needed. Mentorship should include regular feedback sessions that are constructive and supportive. Providing recognition for achievements, such as resolving a critical IT issue or successfully mitigating a security threat, reinforces confidence and motivation. Conversely, identifying areas for improvement should be framed as opportunities for growth, with actionable suggestions to help the individual excel.

We also need to emphasize the importance of continuous learning. Given the rapidly evolving nature of IT and cybersecurity this is essential. Mentors can guide the new hire in identifying relevant training opportunities, such as advanced certifications (e.g., CISSP or CISM) or workshops on emerging technologies like zero-trust architectures. Encouraging participation in industry events, webinars, and local professional networks helps the individual stay updated and build connections within the broader IT and cybersecurity community.

Integration into the organization's culture is as important as technical competence. Encouraging collaboration across teams can ease the new hire's transition while creating a culture of shared responsibility for IT and cybersecurity. For example, joint projects with other departments—such as developing a secure remote work policy—enable the dual-role officer to demonstrate their expertise while building trust and communication channels.

A common challenge for dual-role positions is managing the workload effectively. Mentors and leadership should actively monitor the balance between IT operations and cybersecurity responsibilities to prevent burnout. Delegating tasks when appropriate and providing resources such as automation tools can help the new hire focus on strategic priorities rather than being overwhelmed by routine tasks. Mentorship should not be limited to the initial months of employment. Ongoing support ensures that the dual-role officer remains aligned with the organization's evolving goals. Over time, they may be encouraged to take on leadership roles,

mentor junior staff, or develop a succession plan to ensure continuity in IT and cybersecurity operations.

G. Addressing Workload Challenge

Small and medium-sized businesses (SMBs) will face challenges in ensuring that professionals in this dual role can manage their workload effectively without risking burnout or compromising the quality of their work. Addressing these challenges requires a combination of strategic planning, resource allocation, and support mechanisms.

One of the most effective ways to manage workload is through clear prioritization and task delegation. Dual-role professionals should be equipped with tools and frameworks to identify high-priority issues, such as addressing cybersecurity vulnerability or resolving a critical IT outage, over less urgent tasks like routine system updates. Leveraging automation tools, such as endpoint detection and response (EDR) systems or patch management software, can reduce the manual effort required for repetitive tasks, freeing up time for strategic initiatives. Additionally, delegating non-critical tasks to junior IT staff or external vendors ensures that the dual-role officer can focus on high-impact responsibilities.

Effective time management is key to balancing the dual demands of IT operations and cybersecurity. Organizations can support their dual-role professionals by encouraging the adoption of time management practices, such as blocking out time for deep focus on cybersecurity planning or setting aside specific periods for IT system maintenance. Regularly scheduled meetings with leadership can also help in recalibrating priorities based on the organization's evolving needs. Time-tracking tools can provide insights into workload patterns, enabling the identification of areas for improvement or the need for additional support.

Encouraging collaboration within the organization helps alleviate the burden on dual-role officer. Cross-functional teams can share the responsibility for implementing IT and cybersecurity initiatives, such as rolling out a new software application or conducting company-wide security training. Building a culture where employees across departments understand basic cybersecurity practices reduces the officer's workload in creating and maintaining compliance. Similarly, mentorship relationships with experienced IT or cybersecurity professionals—either within the organization or through external networks—offer valuable guidance and shared problem-solving resources.

Outsourcing specific tasks to managed service providers (MSPs) or cybersecurity firms can significantly ease the workload. Routine IT operations, such as help desk support, and advanced cybersecurity functions, such as threat intelligence monitoring, can be handled by external partners, allowing the dual-role officer to focus on strategic and high-stakes responsibilities. SMBs should assess their budgets and need to determine the most cost-effective areas for outsourcing, ensuring that the outsourced functions complement the officer's expertise.

The ever-evolving nature of IT and cybersecurity means that dual-role professionals must constantly stay updated on new technologies and threats. However, finding time for professional development within an already demanding role can be challenging. Organizations should allocate dedicated time and resources for training, certifications, and participation in industry events. This not only equips the officer with advanced skills but also reduces the risk of inefficiencies caused by outdated knowledge. To this end, the leadership must be also proactive in recognizing signs of overwork and burnout. Regular check-ins to discuss workload concerns, paired with actionable solutions, can create a supportive environment. Providing mental health resources and encouraging the use of vacation time helps ensure that the officer remains engaged and productive. Flexible work arrangements, such as remote work options or adjustable hours, can also contribute to a better work-life balance.

As the organization grows, the dual-role position may become unsustainable due to increasing demands on both IT and cybersecurity fronts. SMBs should periodically evaluate whether the role requires additional personnel, such as a dedicated IT manager or a cybersecurity specialist.

4. Conclusion and Future Work

In this guide we emphasized the significant potential and inherent challenges associated with hiring for the dual role of IT and cybersecurity officers in small and medium-sized businesses (SMBs). By integrating IT management and cybersecurity responsibilities into a single position, SMBs surely can maximize their limited resources while safeguarding their digital assets. However, success in this endeavor hinges on strategic planning, including crafting precise job descriptions, identifying candidates with a blend of technical and interpersonal skills, and ensuring continuous support through mentorship and workload management.

Organizations that is planning to pursue this dual role must recognize the need for clarity in expectations and flexibility in execution. Clearly defining the responsibilities of the role sets the foundation for effective performance, while ongoing professional development helps the hired professional stay updated with rapidly changing technologies and threats. Addressing workload challenges through collaborative strategies, such as leveraging automation tools or outsourcing non-core tasks, can further ensure the sustainability of the dual-role position. A proactive approach that fosters teamwork and communication across departments also enhances the effectiveness of the role by creating a unified focus on organizational goals.

Looking to the future, there are several critical areas for further exploration and practical application. First, there is a pressing need to develop industry-specific guidelines for dual-role professionals. SMBs in sectors such as healthcare, finance, and manufacturing face unique IT and cybersecurity challenges, and specified strategies would enable these businesses to address their specific requirements more effectively. By examining the nuances of each industry, organizations can better align the dual-role position with their operational and regulatory needs.

Another promising area for future work involves automation. Technologies such as artificial intelligence and machine learning can reduce the burden of repetitive tasks, freeing dual-role professionals to focus on higher-level strategic initiatives. Research into how automation can enhance both IT management and cybersecurity functions will provide valuable insights into optimizing the dual role. Similarly, developing training programs that integrate IT and cybersecurity skills into a unified learning framework can equip candidates with the knowledge and confidence needed to succeed in this challenging position.

Additionally, SMBs may benefit from exploring alternative workforce models, such as outsourcing or co-management arrangements. Managed service providers or third-party vendors can take on specific responsibilities, allowing in-house professionals to concentrate on core tasks. Understanding the dynamics of these hybrid approaches will provide SMBs with flexible options to strengthen their IT and cybersecurity capabilities without overburdening their internal staff.

5. References

Garcia, L., Patel, S., & Thomas, R. (2021). Challenges and Failures in Dual-Role Implementation: A Case Study in Healthcare IT. *Journal of Cybersecurity Management, 34*(3), 123-136.

Greene, D., & Patel, N. (2021). Workforce Development in Cybersecurity: Addressing the SMB Skills Gap. *CompTIA Insights*.

ISACA. (2022). State of Cybersecurity 2022: Global Update on Workforce Trends, Threats, and Practices. ISACA.

ISC². (2022). Cybersecurity Workforce Study. (ISC)².

Ponemon Institute. (2019). The Cost of Cybersecurity in SMBs: Trends and Challenges. *Ponemon Research Reports*.

Smith, A., Johnson, R., & Lee, T. (2020). Privacy and Resource Allocation in SMBs: An IAPP Report. *International Association of Privacy Professionals*.

Williamson, I.A., Cable, D.M., & Aldrich, H.E. (2002). Smaller but not Necessarily Weaker: How Small Businesses Overcome Barriers to Recruitment. *Managing People in Entrepreneurial Organizations*, Volume 5, pages 83–106.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water / Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Varol, C., & Shashidhar, N. (2025). A Hiring Guide for Dual Role of IT and Cybersecurity Officers in Small to Medium Businesses (Report No. IHS-2025-1001). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/746FY