ISSN: 2473-4901
v11 n6374

# CyberPASS – A Cyber Security Personality Assessment for Organizations

Bryan Reinicke
breinicke@saunders.rit.edu

Richard P. Mislan
rmislan@saunders.rit.edu

Gustav Blom
gkb4521@rit.edu

MIS, Marketing and Analytics
Saunders College of Business
Rochester Institute of Technology
Rochester, NY 14623, USA

## Abstract

One of the challenges in cyber security is making it accessible to the businesses that need it. The technical guidelines that are published by various agencies require expertise to understand – expertise that smaller companies tend to lack. The purpose is to provide businesses with more approachable guidance on what they should be doing to maximize their cyber security measures with a minimum of technical jargon. Small businesses face unique challenges in managing cybersecurity due to limited resources, lack of technical expertise, and evolving threats. To address these challenges, this paper introduces cyberPASS (Personality Assessment for Security Solutions), a theoretical tool designed to simplify cybersecurity planning for small businesses by aligning security strategies with business personalities. Drawing from established cybersecurity frameworks like NIST, cyberPASS tailors its recommendations based on an organization's personality traits, providing a more intuitive and accessible approach to security planning. This paper outlines the theoretical foundation behind cyberPASS, its potential impact, and how it could transform cybersecurity efforts by making them more relevant, actionable, and manageable for non-technical business owners. By providing small businesses with customized, practical cybersecurity strategies, cyberPASS holds the potential to significantly improve their resilience to cyber threats.

**Keywords:** Cyber Security, Personality Assessment

©2025 ISCAP (Information Systems and Computing Academic Professionals)

ISSN: 2473-4901
v11 n6374

# CyberPASS – A Cyber Security Personality Assessment for Organizations

*Bryan Reinicke, Richard P. Mislan, and Gustav Blom*

## 1. INTRODUCTION

As the cost of Cyber Crime has risen to roughly $8.4 Trillion globally (Intellegence Unit, 2024; Ponemon Institute, 2015), Cyber security has become a critical area in research (Acquisti et al., 2019) and for every type of business (Chen et al., 2012). However, most of the guidelines for cyber security are very technical in nature and are not designed for those who are not cyber security experts (Kleinberg et al., 2015). This is a problem for small businesses that cannot afford a dedicated expert on staff.

Small businesses face unique challenges in managing cybersecurity due to limited resources, lack of technical expertise, and constantly changing threats. To address these challenges, this paper introduces CyberPASS (Personality Assessment for Security Solutions), a theoretical tool designed to simplify cybersecurity planning for small businesses by aligning security strategies with business personalities.

Small businesses play a vital role in the global economy, yet they remain disproportionately vulnerable to cyber threats. Unlike large corporations, small businesses often lack dedicated resources, technical expertise, and formalized processes for addressing cybersecurity risks (National Institute of Standards and Technology, 2024). This vulnerability is further compounded by the complexity of existing frameworks, which, while comprehensive, are not always accessible to smaller organizations. Consequently, small businesses face a daunting challenge: how to implement effective cybersecurity strategies that are both scalable and practical for their unique needs.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is widely regarded as a gold standard for managing cybersecurity risks (National Institute of Standards and Technology, 2024). However, its generalization and breadth can pose challenges for small businesses with limited technical expertise or constrained budgets. These businesses often struggle to interpret and adapt the framework's high-level recommendations into actionable steps that align with their specific operations. As a result, they may adopt fragmented or reactive approaches to security, leaving critical vulnerabilities unaddressed.

To address this gap, CyberPASS introduces a novel approach to cybersecurity planning designed specifically for small businesses (see Appendix A). Grounded in the theoretical foundation of personality-based assessments, CyberPASS tailors cybersecurity strategies by identifying a business's unique personalities and operational styles. By integrating insights from personality assessments and subject matter experts while aligning with the NIST Cybersecurity Framework, CyberPASS offers a structured yet flexible solution. Its ultimate goal is to empower small businesses to create security plans that are practical, personalized, and effective, making cybersecurity both accessible and impactful for this vital sector.

While the CyberPASS framework emphasizes cybersecurity personality traits as the primary lens for tailoring recommendations, it also recognizes the critical role of other organizational dimensions in shaping cybersecurity strategies. Factors such as industry, organizational size, and maturity level are integral to the practical application of the framework. These dimensions help refine the recommendations to ensure they are both actionable and relevant to the specific challenges and opportunities faced by different organizations.

For example, a "Customer-Centric Business" in the retail industry may prioritize secure payment systems and point-of-sale encryption, while a similar personality in healthcare may focus on patient data protection and compliance with HIPAA regulations. Likewise, the cybersecurity needs of a small startup will differ from those of a large multinational enterprise, even if they share a similar personality profile. Smaller organizations might lean towards cost-effective, easily deployable solutions, whereas larger enterprises may implement complex, integrated systems with robust incident response capabilities.

By integrating these organizational dimensions, CyberPASS ensures that its recommendations are

©2025 ISCAP (Information Systems and Computing Academic Professionals)

not only behaviorally aligned but also contextually appropriate, making it a versatile and practical tool for businesses of all types and sizes. This dual approach strengthens the framework's ability to meet the nuanced and diverse cybersecurity needs of small and medium-sized enterprises.

## 2. THE CyberPASS MODEL

The NIST Cybersecurity Framework (NIST CSF) has become a cornerstone for organizations seeking to strengthen their cybersecurity posture (National Institute of Standards and Technology, 2024). Originally designed to help critical infrastructure sectors manage and mitigate cyber risks, the framework provides a flexible, risk-based approach that is widely applicable across industries. It is organized around five core functions—Identify, Protect, Detect, Respond, and Recover—that outline a comprehensive lifecycle for managing cybersecurity threats. These functions are further supported by categories and subcategories, offering detailed guidance to organizations on implementing robust security practices.

For small businesses, the NIST CSF offers a clear roadmap to addressing cybersecurity risks, but its scope and complexity can pose challenges. Many small businesses lack the resources to translate the framework's high-level guidance into actionable plans tailored to their specific operations (Heidt et al., 2019a). As a result, there is a pressing need for tools that can bridge this gap, helping small businesses align their security practices with the framework without requiring extensive technical expertise.

### Personality-Based Approaches in Business and Cybersecurity

Personality-based approaches, long used in business management and marketing (Aluja et al., n.d.; Gander et al., 2012), offer an innovative perspective on tailoring strategies to align with individual or organizational traits. In these contexts, understanding a personality profile helps decision-makers predict behavior, preferences, and challenges, leading to more effective and customized solutions. This approach has proven especially effective in areas like employee management, customer engagement, and leadership development.

In cybersecurity planning, the application of personality-based methods remains relatively unexplored. Yet, businesses exhibit unique operational styles, risk tolerances, and cultural attitudes that influence their approach to cybersecurity (Chatterjee et al., 2015; Chen et al., 2012; Lili Sun et al., 2006). A personality-based assessment allows for identifying these traits and adapting strategies to better fit the organization's natural tendencies and capabilities. This shift from a one-size-fits-all approach to a tailored strategy ensures that recommendations are not only relevant but also actionable, making cybersecurity adoption more feasible and effective.

### The Role of Personality Traits in Cybersecurity Strategies

Every business has distinctive characteristics that shape its approach to risk management (Dhillon & Backhouse, 2000; Lili Sun et al., 2006). For instance, a tech-savvy startup may be more inclined to adopt cutting-edge cybersecurity tools, while a legacy business might prioritize stability and compliance over innovation. By recognizing these personality traits, cybersecurity strategies can be crafted to complement a business's strengths and address its vulnerabilities.

Personality traits also influence how businesses perceive and respond to cybersecurity risks. A data-driven organization, for example, may prioritize protecting sensitive information, while a customer-centric business might focus on safeguarding customer trust and relationships. Understanding these priorities helps ensure that cybersecurity solutions are not only effective but also aligned with the organization's goals and values.

This alignment enhances engagement, as businesses are more likely to adopt strategies that feel intuitive and manageable within their existing frameworks. Ultimately, integrating personality-based assessments into cybersecurity planning creates a more user-centric and adaptable approach, making it easier for small businesses to build and sustain resilient security practices.

### Conceptual Framework of CyberPASS

The foundation of CyberPASS lies at the intersection of personality-based assessments and established cybersecurity frameworks. Drawing on theories from organizational psychology, behavioral economics, and cybersecurity planning, CyberPASS leverages the idea that businesses, like individuals, have unique personalities and traits. These traits shape their approach to risk, resource allocation, and decision-making—critical factors in crafting effective cybersecurity strategies. By identifying these personalities, CyberPASS delivers tailored

recommendations that align with a business's operational style, making solutions both practical and impactful. The initial development of these traits was done by a panel of experts in cyber security who have worked extensively with a variety of businesses.

CyberPASS is built around four Major Personalities:

1. **The Security-Conscious Business** – Focused on minimizing risks and maintaining compliance.
2. **The Customer-Centric Business** – Driven by a commitment to protecting customer trust.
3. **The Innovative Business** – Adaptable and focused on adopting advanced solutions.
4. **The Data-Driven Business** – Centers on securing critical data assets and analytics.

Each Major Personality branches into two Minor Personalities, which are further refined into two Focused Personalities each, resulting in 16 distinct profiles. For example, under the Security-Conscious Business:

- The Compliance-Focused Business includes:
- Highly Regulated Business
- Privacy-Centric Business
- The Legacy Business includes:
- Sustainable Operator
- Crisis-Ready Business

Other Major Personalities similarly branch into their own Minor and Focused Personalities, creating a comprehensive framework for addressing the diverse cybersecurity needs of small businesses (see Appendix A). These personalities were developed through preliminary research, expert consultations, and an analysis of diverse small business case studies. Each personality represents a distinct operational style, helping businesses identify their alignment and areas for improvement in cybersecurity strategies.

To capture a comprehensive view of an organization's cybersecurity needs, CyberPASS encourages a collaborative approach. While the cybersecurity officer might initiate the assessment, representatives from other departments and organizational levels should also participate. This multi-perspective approach reveals variations in how employees perceive cybersecurity risks and priorities, uncovering potential gaps or misalignments in strategy.

CyberPASS integrates seamlessly with the NIST Cybersecurity Framework, aligning each personality with the framework's core functions: Identify, Protect, Detect, Respond, and Recover. By mapping these functions to the specific traits and priorities of each personality, the tool generates actionable, relevant recommendations. For instance, a Security-Conscious Business may focus on compliance and risk management, while an Innovative Business emphasizes advanced threat detection technologies. Further refinement might guide a Privacy-Centric Business toward adopting advanced data encryption, whereas a Crisis-Ready Business would prioritize disaster recovery protocols.

**Contextual Factors in Cybersecurity Needs**

While personality traits are central to the CyberPASS framework, cybersecurity priorities and implementations are also shaped by contextual factors such as industry (De Kinderen et al., 2024), size (Heidt et al., 2019b), and organizational maturity. These dimensions define the specific risks an organization faces and the resources it can allocate to address them effectively.

**Industry**:
Industry dictates regulatory compliance requirements and common threats. For example, a financial institution may prioritize safeguarding customer transactions and adhering to PCI DSS, while a manufacturer focuses on protecting proprietary designs and operational technology from intellectual property theft or ransomware attacks.

**Size**:
Organizational size significantly impacts cybersecurity strategies. Small businesses with limited budgets and IT resources may favor lightweight, cloud-based security tools or managed security services. Conversely, larger enterprises with more extensive assets and risk profiles often implement multi-layered security infrastructures, including advanced threat detection and dedicated incident response teams.

**Maturity**:
An organization's cybersecurity maturity influences its priorities. Startups with nascent security programs might focus on foundational practices, such as endpoint protection and basic password policies. Mature organizations, however, may prioritize advanced measures, including predictive analytics and proactive threat hunting.

By incorporating these contextual factors alongside personality traits, CyberPASS ensures that recommendations are nuanced and actionable. This holistic approach aligns cybersecurity strategies not only with operational

style but also with the organization's unique circumstances and capacities.

**The Role of Additional Dimensions in Enhancing Accuracy**
Although personality serves as the primary lens of the CyberPASS framework, its effectiveness is significantly enhanced by incorporating additional organizational dimensions such as industry-specific regulations, organizational size, and other contextual factors. These dimensions bridge the gap between theoretical insights and practical application.

**Industry-Specific Regulations:**
Regulations shape baseline cybersecurity requirements. For instance, healthcare organizations must comply with HIPAA's stringent data privacy standards, while retail businesses handling payment card transactions must adhere to PCI DSS. Aligning with these frameworks ensures both compliance and security.

**Organizational Size:**
The scale of cybersecurity needs varies by organization size. Small businesses often prioritize cost-effective solutions addressing immediate vulnerabilities, while larger organizations require layered systems protecting expansive networks and diverse operations.
By integrating these practical dimensions into the CyberPASS framework, recommendations are fine-tuned to meet the challenges of real-world scenarios. This approach enhances the framework's accuracy and relevance, fostering tailored cybersecurity strategies that are both effective and sustainable. The inclusion of these dimensions ensures CyberPASS remains adaptive and valuable, capable of meeting the unique needs of diverse organizations.

**Development Process**
The development of CyberPASS was a collaborative and iterative process, shaped by input from subject matter experts, preliminary research, and an understanding of the unique needs of small businesses. The goal was to create a tool that could bridge the gap between general cybersecurity frameworks, like the NIST Cybersecurity Framework, and the specific operational styles of small businesses, making cybersecurity both accessible and effective. To achieve this, the CyberPASS team engaged experts across a variety of domains, including cybersecurity practitioners, organizational psychologists, and business owners, to ensure the tool was grounded in practical and theoretical knowledge.

**Subject Matter Experts**
Subject matter experts (SMEs) played a pivotal role in shaping the design of CyberPASS. These professionals contributed valuable insights into the challenges small businesses face when implementing cybersecurity solutions, particularly in how generalized frameworks such as NIST often fail to consider the distinct personalities and operational styles of smaller organizations. Experts provided guidance on how these traits might influence cybersecurity priorities, resource allocation, and risk management. Their expertise was essential in helping to refine the structure of the tool, ensuring that the personalities identified within CyberPASS were not only representative of different business models but also aligned with cybersecurity best practices.

**Preliminary Research**
Preliminary research formed the foundation for identifying the four major personalities: Security-Conscious, Customer-Centric, Innovative, and Data-Driven. Through an initial review of small business case studies, industry reports, and consultations with SMEs, we identified common patterns of behavior and operational priorities that influenced how these businesses approached security. This research also helped to ensure that the framework would address the diverse needs of small businesses without overwhelming them with technical jargon or complex requirements.

**Methodology**
The methodology used to map personality traits to cybersecurity strategies was designed to be both systematic and flexible. It began with an exploration of established personality models from organizational psychology, particularly those that consider how individuals' traits impact decision-making and risk-taking. These models were then adapted to fit the context of small businesses, recognizing that businesses, like individuals, have different approaches to problem-solving, prioritization, and resilience. Each of the four major personalities was mapped to key cybersecurity functions from the NIST Cybersecurity Framework—Govern, Identify, Protect, Detect, Respond, and Recover—and aligned with specific strategies and actions that would resonate with each personality's operational style.

**The Iterative Development Process**
The iterative nature of the framework's design allowed for ongoing refinement based on feedback from both subject matter experts and potential users. After the initial personality profiles were developed, the team conducted pilot

assessments with a select group of small businesses, collecting valuable feedback on how well the tool addressed their specific cybersecurity concerns. This feedback was used to refine the personas and enhance the recommendations provided by CyberPASS, ensuring that the tool remained adaptable to the diverse challenges faced by small businesses.

The iterative process also involved incorporating lessons learned from other business tools and cybersecurity frameworks, adjusting for ease of use and practical applicability. As new research and insights emerged, the framework was continuously adjusted to stay relevant to the evolving landscape of cybersecurity threats. This ongoing process of evaluation and refinement ensures that CyberPASS remains a dynamic tool that can evolve alongside the needs of small businesses and the constantly shifting cybersecurity environment.

In summary, the development of CyberPASS was informed by a combination of expert guidance, research, and feedback from real-world use cases. By integrating theory and practice, and continuously refining the tool, CyberPASS aims to provide a robust yet adaptable framework for small businesses looking to implement personalized cybersecurity strategies.

**Simplifying Cybersecurity Planning for Non-Technical Users**

One of the most significant barriers to cybersecurity adoption for small businesses is the complexity of planning and executing security measures. Traditional cybersecurity frameworks, such as those outlined by NIST, often assume a level of technical knowledge that small business owners or managers simply do not have. This creates a gap, where the security needs of the business are identified but the steps to address those needs remain unclear or overly complicated. CyberPASS simplifies this process by providing an intuitive, user-friendly interface that transforms complex cybersecurity tasks into actionable steps.

The platform's use of personality-based assessments is particularly powerful in this context. Rather than simply offering a set of generic recommendations, CyberPASS customizes the advice and action items based on a business's unique characteristics, ensuring that each recommendation is both relevant and understandable. For instance, a small business owner might not know how to implement advanced encryption protocols, but CyberPASS can provide clear, step-by-step guidance on how to secure their customer data, tailored to the business's size, industry, and specific security needs. By using language and instructions that resonate with non-technical users, the tool minimizes the intimidation factor that often accompanies cybersecurity planning. This approach not only enables business owners to understand their security risks but also empowers them to take practical, informed actions to protect their assets, their customers, and their reputation. In essence, CyberPASS serves as a bridge between complex cybersecurity principles and the non-expert business owner, making cybersecurity more approachable and manageable.

## 3. LIMITATIONS AND NEXT STEPS

While CyberPASS presents a promising tool for small businesses to improve their cybersecurity posture, it is important to acknowledge that the tool has not yet been tested or implemented in real-world scenarios. As of now, the framework remains theoretical and is based on preliminary research, expert insights, and the assumption that personality-based cybersecurity strategies can effectively address the unique needs of small businesses. However, the lack of real-world application means that there are still unknowns regarding the tool's effectiveness, usability, and applicability across a wide range of small business environments. In its current form, CyberPASS offers a conceptual framework but requires further validation to assess its true impact and potential.

**Pilot Studies and User Feedback**

To bridge the gap between theory and practice, pilot studies and direct user feedback are essential next steps in the development of CyberPASS. By conducting pilot studies with a select group of small businesses, researchers can gather critical data on how the tool performs in real-world scenarios. These studies would involve using CyberPASS within businesses of varying sizes and industries to identify potential challenges, usability issues, and areas for improvement. User feedback is particularly valuable, as it will provide insights into how small business owners, who may have limited technical expertise, interact with the tool and its recommendations. This feedback can inform adjustments to the user interface, clarify the language used in the tool, and help refine the recommendations to better align with the diverse cybersecurity needs of small businesses.

Additionally, pilot studies will allow for the testing of key features, such as the personality-based

security assessments and the tailored cybersecurity plans, in a dynamic business environment. The results of these studies will offer insights into whether the tool can indeed simplify cybersecurity planning and make it more accessible for non-technical users. Moreover, pilot studies can identify any gaps in the framework, such as the need for additional security measures or more industry-specific customization, ensuring that CyberPASS evolves into a truly comprehensive and effective solution for small businesses.

**Plans for Future Research**

Future research will focus on expanding the scope of CyberPASS by integrating real-world data and further refining the tool based on findings from pilot studies. Testing with a broader range of small businesses is crucial to understanding how the tool can address the specific needs of different industries and sizes. This validation process is essential to ensure the framework's versatility and its ability to provide meaningful guidance across diverse contexts. Furthermore, this research will evaluate whether the personality-based approach can truly improve cybersecurity outcomes, considering both practical implementation and measurable impact.

Longitudinal studies will play a key role in this evaluation, tracking the effectiveness of CyberPASS over time. These studies will measure key indicators such as the reduction in security breaches, the level of user engagement, and improvements in cybersecurity knowledge among business owners and employees. By focusing on diverse organizational dimensions, including industry-specific challenges and variations in business size, the research will provide a more nuanced understanding of how these factors influence the framework's performance.

Additionally, integrating real-world data into the framework will enhance its predictive capabilities and make its recommendations more robust. Incorporating data from actual cyberattacks, security incidents, and compliance breaches will allow CyberPASS to evolve as a living, adaptive tool. This ensures that the framework remains responsive to the constantly changing cybersecurity landscape, offering small businesses up-to-date and effective guidance that reflects emerging threats and best practices.

Another key area of future research will explore the scalability of CyberPASS. As small businesses grow and their cybersecurity needs become more complex, understanding how the framework can be adapted to larger organizations or businesses with advanced technical requirements is essential. Future iterations of CyberPASS will account for these shifts, ensuring that the tool evolves to accommodate changing needs while maintaining its accessibility and usability.

By emphasizing the importance of validating CyberPASS across diverse industries and sizes, as well as refining the framework to better address contextual factors, future research will solidify its role as a comprehensive tool. This adaptive approach ensures that CyberPASS remains effective and relevant, empowering small businesses to confidently navigate the complexities of cybersecurity.

## 4. CONCLUSIONS

In conclusion, CyberPASS represents a highly innovative approach to cybersecurity planning for small businesses. By combining personality-driven insights with tailored security recommendations, it offers a unique framework that simplifies the complex landscape of cybersecurity. This approach not only acknowledges the diverse needs of small businesses but also addresses the challenge of delivering security solutions in a way that is accessible to non-technical users. The tool has the potential to transform how small businesses approach cybersecurity, making it easier for them to implement essential security measures and reduce their vulnerability to cyber threats.

The theoretical value of CyberPASS lies in its ability to bridge the gap between the often overwhelming and generic cybersecurity frameworks and the specific needs of small businesses. While traditional frameworks like NIST provide valuable guidance, they may not always be suitable for smaller organizations that lack the technical expertise or resources to apply them effectively. By using personality assessments to tailor the recommendations, CyberPASS offers a more intuitive and customized path for businesses to follow. This theoretical framework not only simplifies the process but also empowers small business owners to take ownership of their cybersecurity efforts, fostering a culture of proactive risk management.

However, the tool's full potential can only be realized through real-world testing and iterative refinement. This paper emphasizes the importance of collaboration and further research in validating CyberPASS and enhancing its capabilities. Pilot studies, user feedback, and real-world data will be critical to understanding how the tool performs in different business

environments and industries. Engaging with small business owners, cybersecurity experts, and other stakeholders in this process will ensure that CyberPASS is not only effective but also scalable and adaptable to the evolving cybersecurity landscape.

Ultimately, the development of CyberPASS underscores the need for continued innovation and research in the cybersecurity space, particularly when it comes to small businesses. As these businesses increasingly face sophisticated cyber threats, solutions like CyberPASS can provide them with the tools they need to build resilience and protect their digital assets. The success of CyberPASS could pave the way for similar frameworks in other areas of business management, making complex topics more accessible and actionable. By collaborating with researchers, practitioners, and businesses alike, CyberPASS has the potential to become a cornerstone of cybersecurity efforts for small businesses, helping them navigate the complexities of the digital world with greater confidence and security.

## 5. REFERENCES

Acquisti, A., Dinev, T., & Keil, M. (2019). Editorial: Special issue on cyber security, privacy and ethics of information systems. *Information Systems Frontiers*, *21*(6), 1203–1205. https://doi.org/10.1007/s10796-019-09971-5

Aluja, A., Balada, F., Atitsogbe, K., Rossier, J., & Garcia, L. (n.d.). Convergence of the dimensional assessment of personality pathology (DAPP-BQ) and the five-factor personality inventory for the international classification of diseases 11th edition (FFiCD) in the context of the five-factor model and personality disorders. *BMC Psychiatry*, *24*(386), 1–14.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. *Journal of Management Information Systems*, *31*(4), 49–87. https://doi.org/10.1080/07421222.2014.1001257

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, *29*(3), 157–188.

De Kinderen, S., Kaczmarek-Heß, M., & Hacks, S. (2024). A Multi-level Reference Model and a Dedicated Method for Cyber-Security by Design: On the Example of the Electricity Sector. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-024-00899-y

Dhillon, G., & Backhouse, J. (2000). Technical Opinion: Information System Security Management in the New Millennium. *Commun. ACM*, *43*(7), 125–128. https://doi.org/10.1145/341852.341877

Gander, F., Proyer, R. T., Ruch, W., & Wyss, T. (2012). The good character at work: An initial study on the contribution of character strengths in identifying healthy and unhealthy work-related behavior and experience patterns. *Int Arch Occup Environmental Health*, *85*(895–904), 895–904.

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019a). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, *21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019b). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, *21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Intellegence Unit, T. E. (2024, May 17). Unexpectedly, the cost of big cyber-attacks is falling. *The Economist (Online)*. https://www.proquest.com/abicomplete/docview/3055936123/abstract/421919F9F56D48FAPQ/1

Kleinberg, H., Reinicke, B., & Cummings, J. (2015). Cyber Security Best Practices: What to do? *Journal of Information Systems Applied Research*, *8*(2), 52–59.

ISSN: 2473-4901
v11 n6374

Lili Sun, Srivastava, R. P., & Mock, T. J. (2006). An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems*, *22*(4), 109–142.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (No. NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Ponemon Institute. (2015). *2015 Cost of Cyber Crime Study: Global* (p. 30). Ponemon Institue.

ISSN: 2473-4901
v11 n6374

## Appendix A: Personality Framework