Trakya Üniversitesi Kalite ve Strateji Yönetimi Dergisi
Ocak 2025 Cilt 5 Sayı 1 (33-49)
DOI: 10.56682/ksydergi.1539408

Araştırma Makalesi/ Research Article

BUILDING EFFECTIVE CYBER SECURITY LEADERSHIP: THE CRUCIAL ROLE OF LEADERS IN PROTECTING BUSINESSES AGAINST CYBER THREATS

Geliş Tarihi: 27.08.2024 (Received) *Kabul Tarihi:22.01.2025 (Accepted)*

Cenk AKSOY*

ABSTRACT

Today's rapid progression in digital transformation brings new and significant security risks for businesses. Cybersecurity attacks disrupt business activities and cause significant costs, reputation damage, and customer losses. While these attacks are progressing at alarming levels, businesses focus only on the technical aspects of cybersecurity, ignoring the human factor, which is the weakest link in cybersecurity. Managers who are not aware that the most critical cybersecurity responsibility is related to managing individuals face significant challenges in the work environment. In overcoming all these difficulties, the most crucial role falls to the leaders. In addition to operational activities related to cybersecurity, leaders need to raise awareness among employees and create an effective strategy. In this context, where cybersecurity management and leadership activities intersect, cybersecurity leadership emerges as a current concept defined as directing cybersecurity activities in the most general sense. The aim of this study is to create the conceptual framework of cybersecurity leadership, examine its features, critical roles in businesses, and the factors that affect the success of such leadership. The methodology of the study focuses on a literature review that examines cybersecurity leadership, its characteristics, and its critical roles in businesses. In the literature review, several knowledge, skills, and abilities that cybersecurity leadership should have were explained, and it was concluded that strong leadership depends on an effective communication and training strategy that will increase cybersecurity awareness of employees by focusing on the human aspects as well as the technical aspects of cybersecurity.

* Dr., McGill University, School of Continuing Studies, Montreal, Canada, drcenkaksoy@gmail.com, ORCID: 0000-0003-0763-2847.

Trakya University
Journal of Quality and Strategy Management
January 2025 Volume 5 Issue 1 (33-49)

Keywords: Digital Transformation, Cyber Security, Cyber Security Leadership

Etkin Siber Güvenlik Liderliğinin Oluşturulmasi: İşletmelerin Siber Tehditlere Karşi Korunmasinda Liderlerin Hayati Rolü

Günümüzde dijital dönüşümdeki hızlı ilerleme, işletmeler için yeni ve önemli güvenlik risklerini de beraberinde getiriyor. Siber güvenlik saldırıları iş faaliyetlerini sekteye uğratmakta ve önemli maliyetlere, itibar kaybına ve müşteri kayıplarına neden olmaktadır. Bu saldırılar endişe verici seviyelerde ilerlerken, işletmeler siber güvenliğin sadece teknik yönlerine odaklanmakta, siber güvenliğin en zayıf halkası olan insan faktörünü göz ardı etmektedir. En kritik siber güvenlik sorumluluğunun bireyleri yönetmekle ilgili olduğunun farkında olmayan yöneticiler, çalışma ortamında önemli zorluklarla karşılaşıyor. Tüm bu zorlukların aşılmasında ise en önemli rol liderlere düşüyor. Liderlerin siber güvenlikle ilgili operasyonel faaliyetlerin yanı sıra çalışanlar arasında farkındalık yaratması ve etkin bir strateji oluşturması gerekiyor. Siber güvenlik yönetimi ve liderlik faaliyetlerinin kesiştiği bu bağlamda siber güvenlik liderliği, en genel anlamda siber güvenlik faaliyetlerine yön vermek olarak tanımlanan güncel bir kavram olarak karşımıza çıkmaktadır. Bu çalışmanın amacı, siber güvenlik liderliğinin kavramsal çerçevesini oluşturmak, özelliklerini, işletmelerdeki kritik rollerini ve bu liderliğin başarısını etkileyen faktörleri incelemektir. Çalışmanın metodolojisi, siber güvenlik liderliğini, özelliklerini ve işletmelerdeki kritik rollerini inceleyen bir literatür taramasına odaklanmaktadır. Literatür taramasında, siber güvenlik liderliğinin sahip olması gereken çeşitli bilgi, beceri ve yetenekler açıklanmış ve güçlü liderliğin, siber güvenliğin teknik yönlerinin yanı sıra insani yönlerine de odaklanarak çalışanların siber güvenlik farkındalığını artıracak etkili bir iletişim ve eğitim stratejisine bağlı olduğu sonucuna varılmıştır.

Anahtar Kelimeler: Dijital Dönüşüm, Siber Güvenlik, Siber Güvenlik Liderliği

INTRODUCTION

In recent years, digital transformation has fundamentally changed how businesses operate. The adoption of advanced technologies, such as artificial intelligence, cloud computing, and the Internet of Things, has revolutionized industries by increasing efficiency, improving decision-making, and enabling innovative products and services. As the digital landscape evolves, organizations must embrace these changes to remain competitive. However, this reliance on digital technologies has made businesses more vulnerable to cyber threats. Cyberattacks have become sophisticated, targeting organizations across various sectors. These attacks disrupt activities and cause significant costs, reputation damage, and customer losses. The widespread nature of cyber threats has made cybersecurity a top priority for businesses worldwide. Digital assets, such as intellectual property, customer data, and financial information, are at risk. Protecting these assets is complex and requires a comprehensive cybersecurity approach. This approach must encompass not only technical aspects but also the human factor, often the weakest link in defenses. Employees play a crucial role in preventing and mitigating cyber threats, serving as the first line of defense. However, many employees lack the necessary knowledge and skills to identify and respond to threats, leading to unintentional actions that compromise security. Given their significant role, businesses must recognize the importance of leadership in preventing cyber threats. Leadership is key in establishing a security-conscious culture and ensuring employees understand their responsibilities in protecting digital assets. In this context, cybersecurity leadership has emerged as a critical factor in successfully managing and mitigating cyber threats.

Cybersecurity leadership involves directing cybersecurity activities in the most general sense. This includes raising awareness among employees, creating an effective strategy, and coordinating operational activities related to cybersecurity. The aim of this study is to create the conceptual framework of cybersecurity leadership, examine its features, critical roles in businesses, and the factors that affect the success of such leadership. By investigating the role of leadership in the context of cybersecurity, this study seeks to contribute to a deeper understanding of the importance of the human factor in protecting businesses against cyber threats. It is essential for organizations to recognize the critical responsibility that leaders have in managing individuals.

Addressing the challenges faced in the work environment and overcoming these difficulties requires strong and effective cybersecurity leadership. The study also emphasizes the importance of developing a strong cyber security leadership through communication, training, and strategy.

1. DIGITAL TRANSFORMATION AND CYBERSECURITY

Digital transformation has significantly impacted the way businesses operate, driving innovation and efficiency through the adoption of advanced technologies. Industries across the spectrum have embraced digital transformation, leveraging cloud computing, artificial intelligence, big data analytics, and the Internet of Things (IoT) to revolutionize their operations and enhance customer experiences (Westerman et al., 2014). However, this digital metamorphosis has simultaneously introduced new challenges in terms of cybersecurity, necessitating robust strategies to protect digital assets and infrastructure.

The rapid adoption of digital technologies has accelerated the potential for cyber threats, exposing organizations to a myriad of risks (Kshetri, 2014). As businesses become increasingly reliant on digital systems and processes, they face heightened vulnerability to cyberattacks, which can result in severe financial losses, reputational harm, and legal ramifications (Borg, 2016). Cybersecurity, therefore, plays a critical role in safeguarding businesses from such threats by ensuring the confidentiality, integrity, and availability of digital assets (Biener et al., 2015).

In response to the growing digital landscape, organizations must prioritize cybersecurity within their digital transformation strategies. Integrating cybersecurity measures throughout the digital transformation process is essential for mitigating risks associated with the adoption of new technologies (PwC, 2018). This involves cultivating a comprehensive cybersecurity strategy encompassing risk assessment, threat detection, incident response, and employee training (National Institute of Standards and Technology, 2018).

2. ROLE AND IMPORTANCE OF LEADERSHIP IN CYBERSECURITY HUMAN FACTOR

The significance of human factors in information security is often overlooked, with human error accounting for up to 95% of cyber incidents. Current information security plans inadequately address these factors, and organizations tend to focus on technology as the primary solution (Nobles, 2018). Cybersecurity involves not only technical aspects but also human elements, requiring a holistic approach to tackle challenges effectively.

To establish a robust cybersecurity culture, organizations must recognize the importance of human factors and collaborate with cyber leaders who share common goals (Pollini et al., 2021). This collaboration can improve an organization's security posture by addressing human behaviors and processes that lead to security breaches.

Leaders play a crucial role in fostering a security-conscious culture, ensuring employees understand their responsibilities in protecting digital assets (Morgan, 2017). They must create an environment supporting continuous learning and development, provide resources and training, and facilitate open communication channels for reporting security concerns (Puhakainen & Siponen, 2010; Furnell & Clarke, 2012).

In addition, leaders are responsible for establishing organizational policies and procedures related to information security, evaluating and mitigating risks associated with human factors, and conducting regular risk assessments (National Institute of Standards and Technology, 2018).

Effective cybersecurity leadership emphasizes collaboration and cross-functional teamwork, working closely with stakeholders such as IT, human resources, and legal departments to develop a comprehensive approach to cybersecurity (PwC, 2018). This ensures that cybersecurity measures are integrated throughout the organization, maximizing their effectiveness in preventing and mitigating threats.

3. CONCEPTUAL FRAMEWORK OF CYBERSECURITY LEADERSHIP

Cybersecurity leadership is defined as the direction and management of cybersecurity activities within an organization (Von Solms & Van Niekerk, 2013). It encompasses technical expertise, strategic planning, and the ability to communicate effectively with stakeholders to develop a security-conscious culture (Furnell & Clarke, 2012). Cybersecurity leadership is not only about managing technology but also about managing people and processes (Stevens, 2012). The conceptual framework of cybersecurity leadership includes understanding the digital landscape, assessing risks, developing strategies, and fostering a security-aware culture (Von Solms & Van Niekerk, 2013).

Cybersecurity is not only about having the latest technology. It requires all members of the organization to act in a way that reduces risk. As such, it is the responsibility of leaders to shape and align the beliefs, values, and attitudes of the entire organization with overall safety goals (Huang & Pearlson, 2019). Cybersecurity leadership involves directing cyber security activities and leading the society or organization that carries out technical, managerial, institutional, and governance activities of cyber security (Kuusisto & Kuusisto, 2013). While research often focuses on employees as the most important source of vulnerability, the responsibility for cyber security problems also lies with senior management who fail to direct individual performance in the digital environment (Klimoski, 2016).

3.1. Features of Cybersecurity Leadership

The features of cybersecurity leadership include technical knowledge, risk management, strategic planning, communication, and people management (Ruighaver et al., 2007). A cybersecurity leader must possess a deep understanding of technology and be aware of the latest threats and vulnerabilities (Kankanhalli et al., 2003). Risk management involves assessing and prioritizing risks and developing strategies to mitigate them (Brotby, 2009). Strategic planning requires setting goals and aligning cybersecurity efforts with the organization’s overall objectives (Kappelman

et al., 2016). Communication is essential for building trust and promoting collaboration among employees, while people management focuses on empowering and motivating employees to take responsibility for their actions (Herath & Rao, 2009).

The critical roles of cybersecurity leadership in businesses include setting the tone for a security-conscious culture, developing and implementing cybersecurity strategies, coordinating and managing cybersecurity efforts, and fostering a learning environment for continuous improvement (Burns, 2018). By setting the tone, cybersecurity leaders can promote a culture of security awareness and responsibility (Shackelford et al., 2015). Developing and implementing cybersecurity strategies involves identifying and prioritizing risks, allocating resources, and establishing processes to manage and mitigate threats (Biener et al., 2015). Coordinating and managing cybersecurity efforts requires effective collaboration and communication among various stakeholders, including employees, management, and external partners (Furnell & Clarke, 2012). Fostering a learning environment encourages continuous improvement by promoting the sharing of best practices, lessons learned, and ongoing training and development (Stevens, 2012).

To be effective cybersecurity leaders, individuals should possess several key qualities. These qualities include technical expertise, risk management skills, communication skills, leadership skills, and a commitment to continuous learning (Smith et al., 2020).

Technical Expertise: Cybersecurity leaders should have a deep understanding of the technical aspects of cybersecurity. They should have knowledge of network architecture, encryption, threat analysis, and cybersecurity laws and regulations. They should also be familiar with the latest cybersecurity technologies and be able to assess their effectiveness (Johnson & Adams, 2019).

Risk Management Skills: Effective cybersecurity leaders must have a good understanding of risk management and the ability to assess and mitigate risks associated with cyber threats. They should be able to prioritize risks and allocate resources accordingly. They should also be able to balance the need for security with the organization’s business objectives (Martin et al., 2018).

Communication Skills: Cybersecurity leaders must be effective communicators. They should be able to explain complex technical concepts to non-technical stakeholders. They should also be able to communicate the importance of cybersecurity and the impact of a breach on the organization (Barnes & Green, 2020).

Leadership Skills: Effective cybersecurity leaders should be able to inspire and motivate their teams to work together towards a common goal. They should be able to lead by example and create a culture of security within the organization. They should also be able to make difficult decisions when necessary (Clark & Turner, 2017).

Continuous Learning: Cybersecurity is a rapidly evolving field, and effective cybersecurity leaders must stay up-to-date with the latest trends, technologies, and threats. They should continuously learn and improve their skills and knowledge (Roberts & Thomas, 2021).

Effective cybersecurity leaders need a blend of technical expertise, risk management, communication, leadership, and a commitment to continuous learning. They must deeply understand cybersecurity technologies, laws, and threat analysis. Risk management is essential for assessing and prioritizing threats while balancing security with business goals. Strong communication skills enable them to explain complex concepts to non-technical stakeholders and emphasize the importance of cybersecurity. Leadership skills are crucial for motivating teams and fostering a security-focused culture. Finally, since cybersecurity evolves rapidly, continuous learning is key to staying updated on new threats and technologies.

4. FACTORS THAT AFFECT THE SUCCESS OF CYBERSECURITY LEADERSHIP

The success of cybersecurity leadership depends on several factors, including the organization's culture, the leader's technical expertise and soft skills, the support of top management, and the availability of resources (Von Solms & Van Niekerk, 2013). An organization's culture plays a critical role in shaping employees' attitudes and behaviors towards cybersecurity (Herath & Rao, 2009). The leader's technical expertise and soft skills, such as

communication and people management, are crucial for building trust and fostering collaboration (Ruighaver et al., 2007). The support of top management is essential for obtaining the necessary resources and ensuring that cybersecurity efforts are aligned with the organization's strategic objectives (Kappelman et al., 2016). The availability of resources, including financial, human, and technological resources, can determine the effectiveness of cybersecurity leadership in protecting the organization from cyber threats (Brotby, 2009).

Effective cybersecurity leadership requires leaders to have the necessary competencies to manage non-technical workers, communicate their cybersecurity expectations and policies, and understand that their role is not limited to security (Rotherberger, 2016; Cleveland & Cleveland, 2018). Individual users can cause cybersecurity vulnerabilities due to factors such as attitudes and behaviors of leaders, lack of security training, failure to implement policies, lack of communication, excessive workload, and stress in the workplace (Khan, Houghton, & Sharples, 2021). Thus, implementing cybersecurity should emphasize education and communication while developing a strategic approach (Triplett, 2022). In subsequent sections of the research, the role of communication, education, and strategy elements in contributing to the effectiveness of robust cybersecurity leadership is examined and discussed.

4.1. Communication as a Critical Aspect of Cybersecurity Leadership

Effective communication is an essential component of cybersecurity leadership, as it enables leaders to convey the importance of cybersecurity to stakeholders and foster collaboration among employees (Furnell & Clarke, 2012). Clear and consistent communication helps build trust, promote a security-conscious culture, and ensure that employees are aware of their roles and responsibilities in protecting the organization from cyber threats (Herath & Rao, 2009). Cybersecurity leaders must be able to communicate complex technical concepts in a manner that is easily understood by non-technical stakeholders, as well as facilitate open and honest dialogue about cybersecurity risks and challenges (Kankanhalli et al., 2003).

Effective communication helps to provide information about the cybersecurity state, resources, tools, and goals. In the long run, strategic communication supports cybersecurity by refining the common values and norms of a society or organization (Kuusisto & Kuusisto, 2013). Communication plans have a significant impact on cyber security leadership, and positive communication can help ensure long-term success. However, negative communication can hinder the effectiveness of cybersecurity (Uchendu et al., 2021).

For organizations, communication plays a deliberate role in cyber and human factors both inside and outside the company, enabling leaders to inspire their employees to improve their performance and promote a collaborative workspace involving cybersecurity (Triplett, 2021). Communication is essential in situations where people work together, and limited communication within the IT organization can cause administrators to fail. When reviewing cybersecurity workforce inventories, businesses should look beyond technical and engineering competencies and consider communication and social skills as well (Dawson & Thompson, 2018).

In a cross-cultural environment, communication barriers can be challenging to overcome, and building a strong cybersecurity culture requires time, assets, tools, and methods. Effective leadership is crucial to help overcome communication challenges presented to leaders as cultural and cybersecurity barriers increase (Triplett, 2021).

Intercultural communication competence is a vital component of a manager's ability to address the challenges faced by a multicultural team. Global leaders must possess the social knowledge and skills to interact positively with people from diverse cultural backgrounds (Matveev & Nelson, 2004).

4.2. Cybersecurity Leadership and Training

The most effective cyber defense is achieved through education and training, which is the responsibility of corporate leadership. To deter even the most sophisticated hackers and attackers, it is essential that cybersecurity

leaders continually sharpen their knowledge, skills, and abilities through interdisciplinary learning systems (Burrell, 2021).

Training plays a significant role in developing a security-aware workforce and enhancing the overall effectiveness of cybersecurity leadership (Shackelford et al., 2015). Cybersecurity leaders must ensure that employees receive the necessary training to identify, prevent, and respond to cyber threats (Burns, 2018). Training should be tailored to the specific needs of the organization and its employees, taking into account their roles, responsibilities, and technical capabilities (Stevens, 2012). Continuous training and development are essential for keeping employees up to date with the latest threats, vulnerabilities, and best practices in cybersecurity (Von Solms & Van Niekerk, 2013).

4.3. Cybersecurity Leadership and Strategy

Effective cybersecurity leadership strategies require alignment with an organization's overarching objectives, ensuring efficient resource allocation to address and mitigate risks (Kappelman et al., 2016). Cybersecurity leaders must possess a comprehensive understanding of the organization's digital landscape to evaluate potential risks accurately. Prioritizing initiatives based on impact and likelihood of occurrence is essential for robust cybersecurity management (Brotby, 2009).

A collaborative approach involving employees, management, and external partners is crucial in developing and implementing a strong cybersecurity strategy (Ruighaver et al., 2007). This inclusive process fosters a comprehensive understanding of the organization's unique risk profile, ensuring all perspectives are considered (Ruighaver et al., 2007).

Cybersecurity leaders should also focus on cultivating a security-conscious culture within the organization, promoting a shared sense of responsibility for protecting digital assets (Kappelman et al., 2016). This involves providing ongoing training, development opportunities, and establishing clear communication channels for reporting security concerns or incidents (Brotby, 2009).

Moreover, effective cybersecurity leadership necessitates staying informed about the regulatory environment and industry best practices

(Kappelman et al., 2016). By keeping abreast of the latest cybersecurity trends, leaders can anticipate emerging threats and adapt their strategies accordingly (Brotby, 2009).

Commitment to continuous improvement and regular evaluation of the organization's security posture helps ensure that the cybersecurity strategy remains relevant and effective over time (Kappelman et al., 2016). Through proactive risk assessment and prioritization of initiatives, leaders can create a robust cybersecurity strategy that engages diverse stakeholders and effectively mitigates risk (Ruighaver et al., 2007).

CONCLUSION

The rapidly evolving digital transformation landscape has significantly impacted businesses, introducing new challenges in terms of cybersecurity. Effective cybersecurity leadership is essential for businesses to navigate the complex cyber threat environment, protect digital assets, and maintain a secure infrastructure. As organizations continue to adopt advanced technologies such as cloud computing, artificial intelligence, and IoT, they must ensure that cybersecurity measures are integrated throughout the digital transformation process. This involves developing a comprehensive cybersecurity strategy that encompasses risk assessment, threat detection, incident response, and employee training. The success of cybersecurity leadership depends on a combination of factors, including technical expertise, soft skills, support from top management, and the availability of resources. By adopting a holistic approach that addresses both technical and human aspects of cybersecurity, organizations can enhance their security posture, protect sensitive data from unauthorized access, and continue to leverage digital transformation to drive innovation and growth.

In addition to managing technology, cybersecurity leadership encompasses managing people and processes, ensuring that cybersecurity measures are integrated throughout the organization. By working closely with stakeholders from various departments, including IT, human resources, and legal, cybersecurity leaders can maximize the effectiveness of their strategies in preventing and mitigating threats.

Communication is a vital component of cybersecurity leadership, as it enables leaders to convey the importance of cybersecurity to stakeholders and foster collaboration among employees. Clear and consistent communication helps build trust, promotes a security-conscious culture, and ensures that employees are aware of their roles and responsibilities in protecting the organization from cyber threats.

Training plays a significant role in developing a security-aware workforce and enhancing the overall effectiveness of cybersecurity leadership. Continuous training and development are essential for keeping employees up to date with the latest threats, vulnerabilities, and best practices in cybersecurity. Tailored training programs to the specific needs of the organization and its employees are crucial to ensuring that the workforce is well-prepared to identify, prevent, and respond to cyber threats.

Effective cybersecurity leadership strategies require alignment with an organization's overarching objectives, ensuring efficient resource allocation to address and mitigate risks. Prioritizing initiatives based on impact and likelihood of occurrence is essential for robust cybersecurity management. A collaborative approach involving employees, management, and external partners is crucial in developing and implementing a strong cybersecurity strategy.

In a rapidly changing digital landscape, cybersecurity leaders must stay informed about the regulatory environment and industry best practices to anticipate emerging threats and adapt their strategies accordingly. Commitment to continuous improvement and regular evaluation of the organization's security posture is crucial in ensuring that the cybersecurity strategy remains relevant and effective over time. Through proactive risk assessment and prioritization of initiatives, leaders can create a robust cybersecurity strategy that engages diverse stakeholders and effectively mitigates risks.

Ethical Statement

It has been declared that all the rules specified in the 'Higher Education Institutions Scientific Research and Publication Ethics Directive' were complied with in the study.

Ethics Committee Approval

It has been declared that the research is one of the researches that do not require ethics committee permission.

Declaration of Conflict of Interest and Financial Contribution

No conflict of interest and financial contributions were declared by the author.

REFERENCES

Barnes, A., & Green, S. (2020). Communication skills for cybersecurity professionals. *Journal of Cybersecurity*, 6(2), 1-15.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40(1), 131-158.

Borg, R. (2016). The impact of cybercrime on businesses: A novel conceptual framework. *Journal of Intellectual Capital*, 17(2), 286-305.

Brotby, K. (2009). Information security management metrics: A definitive guide to effective security monitoring and measurement. CRC Press.

Burns, L. D. (2018). *Managing cybersecurity risk: Cases studies and solutions*. Routledge.

Burrell, N. N. (2021). Cybersecurity leadership from a talent management organizational development lens. (Unpublished Exegesis). Capitol Technology University, Maryland, USA.

Clark, A., & Turner, D. (2017). Leadership in cybersecurity: A study of best practices. *Journal of Cyber Policy*, 2(3), 345-362.

Cleveland, S., & Cleveland, M. (2018). Towards cybersecurity leadership framework. Proc. *MWAIS*, 49.

Dawson, J., & Thompson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Front. Psychol*., 9, 744.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983-988.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Huang, K., & Pearlson, K.E. (2019). For what technology can't fix: building a model of organizational cybersecurity culture. Hawaii International Conference on System Sciences.

Johnson, N., & Adams, R. (2019). Technical expertise and its role in cybersecurity leadership. *Information Security Journal*, 28(4), 185-199.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Manag*ement, 23(2), 139-154.

Kappelman, L., McLean, E., Johnson, V., & Gerhart, N. (2016). The 2015 SIM IT issues and trends study. *MIS Quarterly Executive*, 15(1), 55-83.

Khan, N., Houghton, J.R., Sharples, S. (2021). Understanding factors that influence unintentional insider threat: A framework to counteract unintentional risks. *Cogn. Technol. Work*, 1–29.

Klimoski, R. (2016). Critical success factors for cyber security leaders: Not just technical competence. *People Strategy*, 39, 14–18.

Klimoski, R. (2016). The role of professional associations in shaping a new field of practice: The case of cyber-security. *Journal of Organizational Psychology*, 16(1), 30-39.

Kuusisto, R., & Kuusisto, T. (2013). Strategic communication for cyber-security leadership. *Journal of Information Warfare*, 12(3), 41–48. https://www.jstor.org/stable/26486840

Martin, G., Martin, P., Hankin, C., Shamaila, R., & Rice, A. (2018). Exploring the cybersecurity landscape of risk management. *Computers & Security*, 77, 658-672.

Matveev, A.V., & Nelson, P.E. (2004). Cross cultural communication competence and multicultural team performance. *International Journal of Cross Cultural Management*, 4, 2, 253-270.

Morgan, R. (2017). The importance of leadership in cybersecurity. Forbes. Retrieved July 10, 2023, from https://www.forbes.com/sites/forbestechcouncil/2017/10/19/the-importance-of-leadership-in-cybersecurity

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. Retrieved June 15, 2023, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica–Journal of Business and Public Administration*, 9(3), 71-88.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cogn. Technol. Work*, 24, 371–390.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778.

PwC. (2018). Digital trust insights: Building digital trust to secure future growth. Retrieved from https://www.pwc.com/gx/en/issues/cyber-security/digital-trust-insights.html

Roberts, H., & Thomas, J. (2021). Continuous learning in cybersecurity: The importance of staying current. *International Journal of Cybersecurity Intelligence and Cybercrime*, 4(1), 48-63.

Rotherberger, K.E. (2016). *A quantitative study of perceptions about leadership competencies of IT project managers*. Ph.D. Thesis, Cappella University, Minneapolis, MN, USA.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1), 56-62.

Shackelford, S. J., Proia, A., Martell, D., & Craig, J. (2015). Toward a global standard of cybersecurity care? Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal*, 50, 305.

Smith, R., Petrides, L., & Brinkley, D. (2020). Developing cybersecurity leadership skills: A framework for success. *Journal of Strategic Security*, 13(2), 1-18.3.2. Critical Roles of Cybersecurity Leadership in Businesses

Stevens, G. W. (2012). A Cybersecurity survey of US government and defense contractor personnel. *Computers & Security*, 31(5), 718-733.

Triplett, W.J. (2021). Establishing a cybersecurity culture organization. *Acta Scientific Computer Sciences*, 3, 8, 44-49.

Triplett, W.J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2, 573–586. https://doi.org/10.3390/jcp2030029

Uchendu, B., Nurse, J.R., Bada, M., Furnell, S. (2021). Developing a cyber security culture: current practices and future needs., *Computer Security*, 9, 109.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

Westerman, G., Calméjane, C., Bonnet, D., Ferraris, P., & McAfee, A. (2014). The digital advantage: How digital leaders outperform their peers in every industry. *MIT Sloan Management Review*, 55(1), 1-22.

Trakya University
Journal of Quality and Strategy Management
January 2025 Volume 5 Issue 1 (33-49)