European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2023.11.65

ICTHM 2023
International Conference in Technology, Humanities and Management

DIGITAL DISRUPTION AND CYBERSECURITY THREATS: REDEFINING THE ROLE OF INTERNAL AUDITING

Zulaikha Amirah Johari (a), Aziatul Waznah Ghazali (b)*, Yusarina Mat Isa (c), Nur Aima Shafie (d), Soliha Sanusi (e)
*Corresponding author

(a) Faculty of Economics and Management, Universiti Kebangsaan Malaysia, Bangi, Malaysia, zulaikhamirah@gmail.com
(b) Faculty of Economics and Management, Universiti Kebangsaan Malaysia, Bangi, Malaysia, aziatul.ghazali@ukm.edu.my
(c) Faculty of Accountancy, Kampus Puncak Alam, Selangor, Malaysia, yusarina@uitm.edu.my
(d) Accounting Research Institute, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia, aimashafie@uitm.edu.my
(e) Faculty of Economics and Management, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia, solihasanusi@ukm.edu.my

Abstract

The global digital disruption sweeping across industries has ushered in a new era of challenges and opportunities, profoundly altering the landscape of business environments. As organizations increasingly rely on advanced information technology (IT) systems and confront growing cybersecurity risks, the role of the internal audit function has evolved to meet these changing demands. The present study aims to provide a comprehensive understanding of how the role of the internal audit function evolves in the current waves of digital disruption and cybersecurity threats. To achieve this objective, interviews were conducted with qualified internal auditors. The analysis reveals that a digitalized business environment impacts the internal audit function in three key ways. First, it affects the capacity and capabilities of internal auditors, requiring them to be proactive and agile in acquiring the necessary digital knowledge and analytical skills, particularly with regard to potential cybersecurity threats. Second, there is a growing demand for consulting activities carried out by internal auditors, and thirdly, the implementation of new audit technologies is becoming more prominent. Therefore, information technology skills among internal auditors are considered a critical asset. The internal audit function needs to be competent with innovative technology, integrate IT and data analytics skills. In addition, the internal audit function should develop consulting activities to help organisation deal with the digitalisation of the business environment. It is imperative that internal audit functions continue to adapt, ensuring they are not only competent with cutting-edge technology but also poised to contribute meaningfully to organizational resilience and success in the digital era.

Keywords: Cyber Security, Digital Disruption, Internal Auditing

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The global digital disruption, rapid globalisation, industry convergence and automation are transforming the business environment and its related parameters (Kronblad & Envall Pregmark, 2021). These developments have revolutionized traditional practices, accelerated processes, and enhanced efficiency, productivity, and competitiveness (Priambada et al., 2020; Stonehouse & Konina, 2020). The proliferation and rapid adoption of vanguard technology such as artificial intelligence, machine learning, and data analytics have changed the way businesses operate. These technologies offer significant advantages, including increased efficiency, better decision-making, and improved customer experiences. However, digital disruption also brings in new IT and cybersecurity risks that need to be managed.

As businesses become more reliant on these new IT capabilities, they become more vulnerable to cyber-attacks, data breaches, and other IT-related risks (Kuziemski & Misuraca, 2020). For instance, AI and machine learning algorithms rely on large amounts of data, and if this data is compromised or inaccurate, it can affect the accuracy and effectiveness of the algorithm. Additionally, data analytics tools can be vulnerable to hacking, and the insights gained from data analysis can be used to target cyber-attacks more effectively (Islam et al., 2022). To mitigate these risks, businesses must prioritize IT and cybersecurity as part of their overall strategy. This includes investing in cybersecurity technologies and solutions, such as firewalls, intrusion detection and prevention systems, and antivirus software (Ben Daoud & Mahfoudhi, 2022; Skoff, 2017). It also involves training employees on cybersecurity best practices and implementing strict access controls to limit the risk of insider threats (Ben Daoud & Mahfoudhi, 2022; Islam et al., 2022; Skoff, 2017). Consequently, organisations must prioritize IT and cybersecurity within their overall strategies to mitigate these risks effectively.

Another crucial aspect of managing IT and cybersecurity risks is to stay up-to-date with the latest technologies and security threats. This requires ongoing monitoring, risk assessment (Blanke & McGrady, 2016; Dias et al., 2021) and regular updates to IT and cybersecurity policies and procedures. Associated risks with digital disruption and cybersecurity should be manage proactively, so that businesses can leverage these technologies to gain a competitive advantage while protecting their assets and reputation (Blanke & McGrady, 2016; Dias et al., 2021; McCarthy & Harnett, 2014). As cybersecurity risks advances, internal audit serves as the critical barrier and the overall line of defence for an organisation. In a survey of 579 Chief Audit Executives (CAE) carried out by the European Confederation of Institute of Internal Auditors (ECIIA), cybersecurity (CS) has been recognized as one of the top five business risks (European Confederation of Institutes of Internal Auditors, 2020). In this digital age, the role of internal auditor has progressively evolve from simply checking compliance to evaluating effectiveness and act as an adversary.

As cybersecurity threats and violations becomes more frequent and complex with significant losses (Falowo et al., 2022). It is vital for organisations to respond to this issue. It is crucial to effectively exploit and manipulate diverse cross-functional innovation strategies for planning and implementation of operations. In this vein, internal audit, whose role has expanded due to modern changes, must actively contribute to safeguarding security of online services and processes (Abu-Musa, 2008; Sarens & De Beelde, 2006). The role of internal audit has expanded to serves as a critical barrier and line of defence for organisations, responsible for identifying and mitigating IT and cybersecurity risks. Moving forward,

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

internal audit function is taking a reactive assurance stance and take on a more proactive, business-enabling role, positioning itself as a trusted advisor on technology issues and driving return on today's unprecedented levels of disruptive technologies and cybersecurity threats.

While digitalization has gained significant prominence within the IAF in recent years as noted by the European Confederation of Institutes of Internal Auditing (2019) and the Institute of Internal Auditors (2019), it is evident that the IAF does not consistently align its activities and role with the ongoing digital transformation of the business landscape. The demand for digital expertise among internal auditors has surged, yet many departments lack these crucial competencies, as highlighted in reports by the Institute of Internal Auditors (2018, 2019). Consequently, organizations continue to seek external service providers to bridge the gap in digital skills within their internal audit units. Given the prevailing digitalized context, it is imperative for the IAF to refocus its activities to revolve around IT and digital challenges. Moreover, digitalization also opens up opportunities for the IAF to undergo transformation and growth. Within the Internal Audit Function (IAF), digital tools present a myriad of opportunities to enhance their operational methodologies. One such example of these digital tools is data analytics. Recent reports reveal that top-performing internal audit departments are leveraging these technologies. Nonetheless, these reports also highlight that internal audit units do not sufficiently embrace new technologies, despite their integration into other organizational departments, as reported by Deloitte (2018) and PwC (2018, 2019).

Previous research has predominantly focused on the digitalization of organizations external to the realm of internal audit, as evident in the works of Beasley et al. (2018), Kane et al. (2016), and Verhoef et al. (2021). While Betti and Sarens (2021) recently conducted a qualitative study exploring the evolution of the Internal Audit Function (IAF) in a digitalized context, including changes in its scope of work, role, and internal auditors' working practices, there remains a scarcity of empirical research specifically addressing the transformation of IAF's activities and methodologies (Betti & Sarens, 2021; Roussy & Perron, 2018). Hence, the present study aims to investigate the impact of digital disruption and cybersecurity threats on the role of internal audit, encompassing changes in its capacity and capabilities, consulting activities, and how digitalization alters the day-to-day tasks of internal auditors.

2. Literature Review

Digital disruption refers to the swift and substantial transformations occurring within industries and markets due to the introduction and widespread adoption of innovative digital technologies (Skog et al., 2018). Multiple factors, such as technological advancements, shifts in consumer behavior, and the emergence of novel business models, can instigate digital disruption (Legner et al., 2017). A pivotal driver of digital disruption lies in the capacity of digital technologies to facilitate fresh business models that overhaul conventional practices (Bharadwaj et al., 2013). These technologies have empowered businesses to address and fulfill needs and demands in ways that were previously unattainable. Nevertheless, organizations that lag in adapting to the changes brought about by these new digital technologies and neglect to adjust run the risk of being surpassed by competitors, losing their market foothold, and ultimately becoming obsolete.

While undeniably a potent catalyst reshaping industries and global markets, the swift upheaval brought about by digital technologies comes with its drawbacks. Within a mere span of a few years, the

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

realm of cybersecurity has evolved into one of the paramount issues in the realm of risk management, encompassing virtually every category of organization. The intricacy, sophistication, and magnitude of cybersecurity threats are on the rise, constituting a substantial peril to businesses on a global scale (Wallace et al., 2020). As highlighted in a report, there has been a remarkable surge in the frequency of cyber-attacks on businesses, particularly following the onset of the COVID-19 pandemic (Pranggono & Arabo, 2021). According to the 2022 Cost of a Data Breach Report by IBM, the average financial toll of a cyber breach in 2022 stood at $4.35 million. Projections suggest that cybercrime inflicted an estimated $7 trillion worth of damage on the global economy in 2022, with expectations that this figure will climb to $10.5 trillion by 2025.

Cyber threats such as data breaches, ransomware attacks, phishing attacks, malware attacks, Denial of Service (DoS) attacks and insider threats could pose a detrimental business disruption and loss of revenue (Bhagwani & Balasinorwala, 2023). Furthermore, it has the potential to inflict harm upon critical IT assets and infrastructure, and the recovery may prove insurmountable in the absence of the necessary financial resources or support. In addition to direct financial losses, these cybersecurity threats can also cause significant reputational damage, leading to loss of customers and reduced trust in the organization. Cybersecurity threats also have regulatory implications, with various laws and regulations requiring businesses to protect sensitive data and report breaches. Failure to comply with these regulations can result in substantial fines and penalties.

The role of cybersecurity is becoming substantial for business organisations globally, it is a risk that are not to be taken lightly (Haapamäki & Sihvonen, 2019). In parallel with the advancement of digital technology, cyber attackers are also getting more extensive and sophisticated (Radanliev et al., 2018). Moreover, despite having an adequate security precaution, cyber-attacks are on the rise (Škrjanc et al., 2018). As the world's business are being transform by disruptive data science, tight and technological interconnections within the business sector can facilitate the quick spread of attacks through the entire system, potentially causing widespread disruption and loss of confidence. In other words, cybersecurity is all about securing the business data (Perwej, 2017). Therefore, intelligent cyber security systems and services is vital for the current time and the future. Hence, businesses globally have elevated cybersecurity to be a top priority (KPMG, 2019).

Among the initiatives to enhance cybersecurity measures that can help thwart the costly cyber-attacks is by having an independent review of security measures and performance which is being placed on the shoulders of internal auditors (Deloitte, 2018). Furthermore, Steinbart et al. (2018) emphasize the need for internal auditors to possess a strong understanding of information technology, cybersecurity threats, and risk management practices. Their unique role in providing both assurance and advisory services makes them invaluable in the effort to enhance cybersecurity within organizations (Steinbart et al., 2018). Recently, PwC (2022) in its research report recommends that internal audit functions need to be 'disruption-ready', capable of responding to the rapid pace of change brought about by digital technologies. They propose that this readiness requires a shift in mindset, processes, and tools, with a greater emphasis on data analytics, continuous auditing, and predictive risk assessment (PwC, 2022).

In embracing these expectations, the role of internal auditors would somehow be interrupted 360 degrees. It is imperative that internal auditors to be equipped with a deep understanding of cybersecurity

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

risks and be able to help organizations develop and implement effective controls. Neglecting this aspect raises the stakes concerning intrusions, and the aftermath of data breaches can yield substantial economic and business-related repercussions that significantly affect stakeholders. These repercussions can significantly impact stakeholders, making it crucial for internal auditors to play a proactive role in safeguarding the integrity and security of sensitive information and systems. By embracing this shift and embracing their role as cybersecurity allies, internal auditors can effectively enhance the overall risk management framework, fortify the organization's defenses, and protect the interests of stakeholders.

The inherent technical complexity and the requisite level of vigilance associated with cybersecurity threats necessitate the indispensable involvement of internal auditors within the organisation. The involvement of internal auditors has gained prominence as a crucial element in safeguarding an organization's assets and reputation, emphasizing their proactive role in enhancing organizational resilience. Their unique position allows them to gain insights into different departments and processes, enabling them to assess the effectiveness of cybersecurity controls across the entire organization. By collaborating with IT teams and management, internal auditors can foster a comprehensive approach to risk management. The new role and extensive involvement of internal auditors in the context of cybersecurity risks enhances an organization's resilience and ability to bounce back from cyberattacks.

Within the contemporary digital business landscape, internal auditors are experiencing a notable shift from their traditional designations as "bean counters" and "number crunchers" to more expansive roles that entail active involvement in virtually all facets of an organization's operations, thus bringing the internal audit function into prominence. To effectively embrace this evolving role, it is incumbent upon internal auditors to reassess their audit skill sets, with certain skills becoming imperative or gaining increased significance in today's digital technological milieu. Furthermore, there is an expectation for internal auditors to acquire new proficiencies pertinent to emerging technologies. As business entities adopt tools like bots, artificial intelligence, and robotic process automation, internal auditors contribute value by scrutinizing the utilization and management of these technologies.

3. Research Methodology

This research adhered to the interpretivist research philosophy, which is founded on the characteristics of the data and employs an inductive approach. A qualitative methodology was chosen to delve deeper into the transformation of the internal audit function's role in response to contemporary challenges posed by digital disruption and cybersecurity threats. Kumar (2014) contends that the qualitative research approach is distinguished by its adaptable and unstructured essence, aiming to delve into the depth and variety of the acquired data, rather than quantifying it. The use of semi-structured interviews permits respondents to provide detailed and unrestricted responses to open-ended questions (Flick, 2011). This evaluation style is distinguished by the lack of predetermined response options and the avoidance of dichotomous categorization of responses. According to Kumar (2014), a key advantage of this method is its inherent adaptability, which enables the interviewer to capture the necessary data in a manner that is most pertinent to the research being conducted.

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Figure 1 below describes the procedure used to acquire qualitative data. After completing each of the interview session, the data were analysed. Nonetheless, each interview could be analysed independently without completing the subsequent interviews with other participants. The conclusion of this iterative procedure depended solely on the outcome of the most recent interview. Thematic analysis was selected as the data analysis method for this study. The researchers interpreted the results indirectly, affected by their subjective reflections. This study examines the text in depth and critically, going beyond a simple organisation of its surface meanings. Prior research has demonstrated that the incorporation of literary works in academic research validates personal reflections (Castleberry & Nolen, 2018; Lambert & Loiselle, 2008).

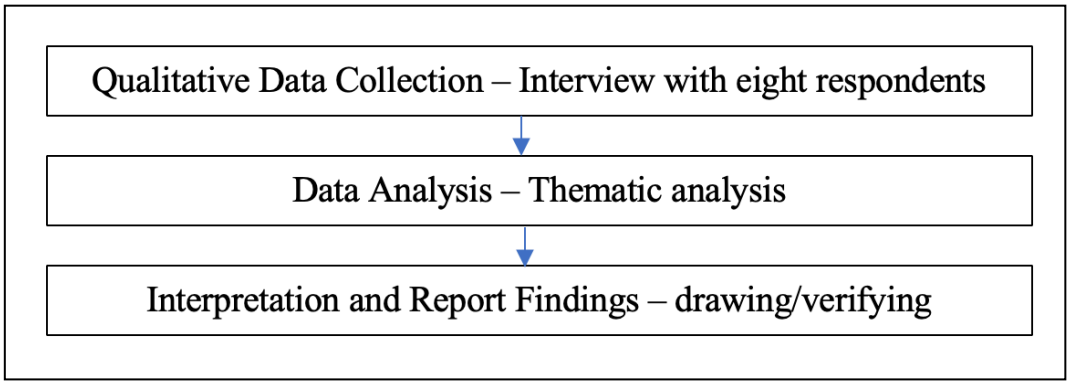

Figure 1. Qualitative Approach Process

3.1. Sample Selection

To understand how the digital disruption and digital technologies have change the role of internal audit, this study realised on the necessity to conduct interview with the internal auditors who specialises in IT audit. This is because they are the responsible party to conduct assessment on the organisation cyber risk. A random sampling of respondents was identified from social media, LinkedIn as it provide a professional profile of potential respondents. From 15 invitation sent through their personal message, only five (5) of them agree to joint for the interview session. Besides their job position, another criterion to be selected as respondent is their working experience. The interview invitation was sent to internal auditor who have at least eight (8) to 10 years of IT audit. After they reply to be respondent of this study, a formal invitation letter was sent through their email. Together with the letter, interview protocol and interview questions were given out as well.

Before conducting the interviews, an interview protocol guide was developed for the participants. These protocols were created in advance to encompass the subjects of interest and guarantee comprehensive coverage of all relevant topics. They served as a framework for the interviewers during the interview sessions, facilitating the systematic acquisition of dependable information from the interviewees. The design of the interview protocols was informed by previous literature and contextual analysis. The interview protocols primarily consisted of open-ended questions, with subsequent extended follow-up inquiries, as needed, to elicit supplementary information.

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

3.2. Data Collection

Due to the exceptional challenges posed by the COVID-19 pandemic, in-person interviews became impractical, and instead, virtual interviews were conducted with the participants. Virtual interviews offered a platform where both the researcher and interviewees could interact more freely and provide additional insights, as the researcher had the ability to discern facial expressions and evaluate body language during the interview sessions. Each interview session spanned approximately 45 to 120 minutes. These interviews were recorded, and field notes were taken when deemed necessary during the interview process. Subsequently, the recorded interviews were transcribed, and an internal cross-check procedure was carried out in comparison to responses from other interviewees. Furthermore, the responses were aligned with existing literature. The processes were done to overcome any potential bias answer and to obtain greater internal validity and reliability (Sekaran & Bougie, 2013).

Semi-structured interview was preferred as it promotes standardization of the questions asked and answer provided. Although it has a sequence of themes to be covered as well as suggested questions, semi-structured interview allows openness to any changes of sequence and forms of questions in order to follow up the specific answer by the interviewees (Kvale, 2008). It allows interviewees to share their experience and provide opportunities to the interviewer to post questions to have an in-depth understanding on the subject matter. The interview questions were adapted from study Jung (2018) on cybersecurity management – an examination of risk and cybercrime involving industrial security.

4. Findings and Discussions

Five (5) respondents have agreed to do the interview session. They were selected from LinkedIn platform based on their experience as internal auditor who did the IT audit, or they also known as IT Auditor. As for the introduction, the respondents were asked on their background including job position and years of experience as an internal auditor. From the interview, all of the five (5) respondents mentioned that they have more than 10 years working in internal audit who assessing the IT risk. In terms of education background, two (2) of the respondents are from Bachelor of Accounting, two (2) are from Bachelor of Computer Science and one (1) from business management. Each of the respondent represent their organisation business sector. Each of them is from education sector, regulators sector, banking institution, non-banking financial institution and telco.

4.1. Experiences on Cybersecurity Threats

After the background session, the interview proceeds with the questions on experience in cyber threat or cyber-attack such as ransomeware or malware. Four (4) of the respondents replied that they had faced an attempt in data leaking but their IT department able to bypass the attempt of attack. This is because they received an alert on intruder. It is supported by the following excerpt:

"……..it has happened that someone wants to hack our clients data. However, our IT department managed to stop the attempt. Because there is an alert in our IT system…" (Respondent 5)

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

"….we had experienced with a cyber-attack.. they managed to grab hold of a little bit of data.. we also waited if someone wanted to ask for money.. but the attacker was silent.... and nothing else happened after that incidents.."(Respondent 3)

However, only one respondent replied that they have not encounter any attack or any issues on cybersecurity. In regards of the question on the relationship between cybersecurity and internal audit, five (5) of the respondents replied that their job as internal audit is to check on the compliance of cybersecurity risk assessment. It is supported by the following excerpt:

"…….if in terms of our position, our job is to check the risks related to cybersecurity. So, we will check based on the manual and also the report from the IT department because they are dealing with this security issue." (Respondent 5)

Meanwhile, two of the respondents further explained that besides checking compliance on cybersecurity, they also provide training and consultation with IT department regarding the cybersecurity. They also are responsible on spreading awareness on cybersecurity issues among employees in the organisation. It is supported by the following excerpt:

"….we will make sure every employee before logging in to the computer will receive an alert notification about phishing and password protection"

(Respondent 3)

During the interview also, question on the reason why they faced cyber attempt is due to lack of awareness among employees and also their client data is valuable to the hacker. This is because the data contains personal information including the financial information of the client.

4.2. Capacity dan capabilities

From the interview, this study found that the significant theme concluded for professional qualification and experience is competency. Two (2) of the respondents replied that having education on accounting and IT as well as experience in IT is important. Besides that, having professional qualification in IT audit is also a bonus so that it could help the internal auditor more objective in deliver their judgment on risk. It is supported by the following excerpt:

"..In my opinion, accounting and IT background is important to become an internal auditor because it will help them in understanding the risk process. In addition... experience in IT related audits is also important because through that experience, internal auditors will better understand their work. Because if the senior wants to help for a long time, it's hard too. They also need to audit other things. If you have a professional qualification such as ISACA, it will be a good addition…"

(Respondent 5)

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Meanwhile, one (1) of the respondents mentioned that education and experience in cybersecurity does not really the key factor to determine the effectiveness of cybersecurity assessment. But, another aspect that is important is having a business acumen where the understanding of business will ensure that the internal auditor assess the risk effectively. This is supported by the following excerpt:

"…I want to say that experience and education are very important to me. My own opinion, I have a business management background, but I can still be an IT audit not only because of my IT skill experience, but my previous experience in a different company helped me to understand that when we understand the business, we understand what risks will be faced by the company. So, in my opinion, understanding the business is more important because the others can be taught. After all, sometimes those who have this experience are too rigid. So, the openness to accept new opinions is a bit less…"

(Respondent 3)

On the other hand, (1) respondent stated that having computer science background solely is not sufficient to conduct internal audit function in organisation. Hence, to cater the insufficiency, he took a professional accounting examination to enhance his competency as internal audit so that he can understand the role internal audit functions as a whole. He also mentioned that by having both skills help him to understand better on how to help organisation combating cyber threats.

"….I am from computer background. But, to do this job, you need to also know accounting. It is hard to ask your colleagues to explain everything to you when you try to understand the situation. So, I decided to take professional accounting exam. ACCA. Once you learn about accounting, your perspective is much wider and you can understand better when you did internal audit…."

(Respondent 1)

This statement is aligned from study by (Ta & Doan, 2022) where there is a limitation on the IT functions where they do not know much on how to structure the risk and relate it to governance. Hence, to have a skill that can understand the management is a bonus to the internal auditor.

5. Consultation

One (1) of the respondents mentioned that sometimes they provide consultation to the IT department in terms of how to manage the cyber threat. This is because the IT department aware on the threat but to identify which is major threat or not, they do not have the knowledge. So, the internal audit provides guidance for that.

"…..Indeed, we also engage in consultations with the Information Technology (IT) department. These individuals possess a high level of expertise in effectively managing and mitigating the risks associated with this particular cyber threat. However, our assistance primarily involves aiding individuals in identifying the magnitude of this particular threat. In the event of a significant threat to the organisation, what is the standard operating procedure (SOP) to be followed?…"

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

(Respondent 3)

Some of the respondent also mentioned that they provide training to employee of the organisation.

"….we do training and also provide awareness to staff such as passwords should not be written down or placed in places that can be easily accessed, how to handle when you find a phishing email or a virus and much more. We also tell you not to visit any websites that may expose you to ransomware attacks…"

(Respondent 2)

5.1. Regulatory Compliance

The researcher also asked about the ISO on cybersecurity. Three (3) of the respondents replied that their manual also was derived from ISO 27001 which is related to information security standard. They also mentioned that having ISO auditor to audit their information security is helpful because they got extra monitoring. Besides that the internal audit are more motivated to meet the requirement of ISO and hence make them do audit thoroughly. This is supported by the following excerpt:

"….because we are an agency under the act, so the ISO requirement is very important to show that we really take care of this cybersecurity issue. After all, if there is an ISO auditor, make our work more focused on assessing the risk. Because there is extra monitoring…"

(Respondent 3)

6. Conclusion

In the face of disruptive technology infrastructure demands, market pressure for constant technology evolution, and persistent cybersecurity threats, businesses need to ensure that they are ever ready to face both expected and unexpected challenges. Due to various uncertainties, challenges and risks exposure, the role of internal audit are shoved to move beyond its traditional. Today, instead of taking reactive assurance stance, the internal auditors are expected to take on a more proactive, business-enabling role, positioning itself as a trusted advisor on technology issues and driving return on today's unprecedented levels of digital disruption and cybersecurity threats. The changes of internal audit's role has to be redefined in making sure that the professional judgment and skepticisms of the profession are intact and secured.

The findings synthesized that all the respondents are in agreement stating the role of internal auditing have progressed immensely in line with the drastic evolution of digital disruption as well as increased cybersecurity threats. Internal auditors are required to possess the knowledge, skills and experience to perform digital audit and managing risks related to digital disruption and cybersecurity threats. Nowadays, information technology skills among internal auditors are considered a critical asset. Having professional qualification in IT audit such as ISACA would significantly enhance the capabilities of internal auditors especially with IT consultancy engagement. Moreover, internal auditors are also expected to provide internal training to other personnel in their organisation to create awareness and

managing the issue of cybersecurity threats. It is also imperative for internal auditors to keep up with the recent regulatory requirement is related to information security standards.

These findings hold significant implications for various stakeholders, including the general public, policymakers, managers, shareholders, and academics. Specifically, the findings suggests that the role of internal auditors has significantly evolved due to advancement of disruptive information technology and cybersecurity threats. The fact that current internal audit tasks require advance IT knowledge and skills, their training should start as early as possible. Therefore, it is worth to have relook at the role and job scope definitions of internal auditing. The result of this study will be of assistance to practitioners, particularly those in the assurance service sector as a groundwork to heighten their quality of assurance in the digital age.

The results of this study have the potential to offer both theoretical and practical contributions, which can advance future research and enhance the existing practices within internal audit assurance. Furthermore, the study's findings may address the existing knowledge gap regarding the transformation of internal auditing when confronted with challenges related to digital disruption and cybersecurity threats. It is worth noting that the present study exclusively solicited responses from internal auditors specialized in IT audit, which implies that certain insights, particularly those related to the broader implications of internal auditing, remain beyond the scope of this research. Hence, it is recommended that future research should aim to collect responses not only from internal auditors across various industries and regulatory bodies but also from the relevant end stakeholders of assurance services. A comparative analysis of responses from diverse sources has the potential to offer valuable insights from different angles, thereby enriching our comprehension of the research context. Beneficiaries, clients, or customers of assurance services can provide a more comprehensive perspective regarding the implications of digital disruption and cybersecurity threats, as well as the pivotal role that internal audit plays in this context.

Acknowledgement

The authors would like to extend their gratitude to the Universiti Teknologi MARA for funding this research under the ‘Geran Penyelidikan Khas’ - Integrated Cyber Security Model for Retail Businesses: Combating Cyber Threats in Building Sustainable Economy 600-RMC/GPK 5/3 (104/2020).

References

Abu-Musa, A. A. (2008). Information technology and its implications for internal auditing: An empirical study of Saudi organizations. *Managerial Auditing Journal, 23*(5), 438-466. https://doi.org/10.1108/02686900810875280

Beasley, M., Branson, B., & Hancock, B. (2018). *The state of risk oversight: an overview of enterprise risk management practices*. NC State. erm.ncsu.edu/library/research-report/2018-the-stateof-risk-oversight-an-overview-of-erm-practices

Ben Daoud, W., & Mahfoudhi, S. (2022). SIMAD: Secure Intelligent Method for IoT-Fog Environments Attacks Detection. *Computers, Materials & Continua, 70*(2), 2727-2742. https://doi.org/10.32604/cmc.2022.020141

Betti, N., & Sarens, G. (2021). Understanding the internal audit function in a digitalised business environment. *Journal of Accounting & Organizational Change, 17*(2), 197-216. https://doi.org/10.1108/jaoc-11-2019-0114

Bhagwani, V., & Balasinorwala, S. (2023). Cyber Security. *Interantional Journal Of Scientific Research In Engineering And Management*.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly, 37*(2), 471-482. https://doi.org/10.25300/misq/2013/37:2.3

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management, 36*(1), 14-24. https://doi.org/10.1002/jhrm.21230

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning, 10*(6), 807-815. https://doi.org/10.1016/j.cptl.2018.03.019

Deloitte. (2018). The innovation imperative: forging internal audit's path to greater impact and influence. *Deloitte's 2018 Global Chief Audit Executive Research Survey*. https://www2.deloitte.com/us/en/pages/audit/articles/global-chief-auditexecutive-survey.html

Dias, F. M., Martens, M. L., Monken, S. F. d. P., Silva, L. F. da, & Santibanez-Gonzalez, E. D. R. (2021). Risk management focusing on the best practices of data security systems for healthcare. *International Journal of Innovation, 9*(1), 45-78. https://doi.org/10.5585/iji.v9i1.18246

European Confederation of Institutes of Internal Auditing. (2019). *Risk in focus 2019: hot topics for internal auditors.* www.eciia.eu/wp-content/uploads/2019/02/Risk-in-Focus_2019.pdf

European Confederation of Institutes of Internal Auditors. (2020). *Risk in focus 2021*. Hot topics for internal auditors. https://www.eciia.eu/wpcontent/uploads/2020/09/100242-RISK-IN-FOCUS-2021-52PP-ECIIA-Online-V2.pdf

Falowo, O. I., Popoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. *IEEE Access, 10*, 134038-134051. https://doi.org/10.1109/access.2022.3231847

Flick, U. (2011). *Introducing Research Methodology. Beginner's Guide to Doing a Research Project* (1st ed.). SAGE Publications Ltd.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808-834. https://doi.org/10.1108/maj-09-2018-2004

Institute of Internal Auditors. (2018). *North American pulse of internal audit: the internal audit transformation imperative*. www.theiia.org/centers/aec/Pages/2018-Pulse-ofInternal-Audit.aspx

Institute of Internal Auditors. (2019). *North American pulse of internal audit: defining alignment in a dynamic risk landscape*. www.theiia.org/centers/aec/Pages/2019-Pulse-ofInternal-Audit

Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., Khan, J. A., Rehman, A. U., & Shafiq, M. (2022). Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models. *Sustainability, 14*(14), 8374. https://doi.org/10.3390/su14148374

Jung, J. (2018). A Study of Cyber Security Management within South Korean Businesses – An examination of risk and cybercrime involving industrial security. *Student thesis: Doctoral Thesis.*

Kane, G. C., Palmer, D., Nguyen Phillips, A., Kiron, D., & Buckley, N. (2016). Aligning the organization for its digital future. *MIT Sloan Management Review, 58*(1), 1-27.

KPMG. (2019). *Transparency Report Committed to driving audit quality*. Retrieved on 23 October, 2023 from https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/12/2019-transparency-report.pdf

Kronblad, C., & Envall Pregmark, J. (2021). Responding to the COVID-19 crisis: the rapid turn toward digital business models. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/jstpm-10-2020-0155

Kumar, R. (2014). *Research Methodology, A step by Step Guide for Beginners* (Forth Edit.). SAGE Publication Ltd.

Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy, 44*(6), 101976. https://doi.org/10.1016/j.telpol.2020.101976

Kvale, S. (2008). *Doing Interviews*. SAGE Publications Ltd., Thousand Oaks.

Lambert, S. D., & Loiselle, C. G. (2008). Combining individual interviews and focus groups to enhance data richness. *Journal of Advanced Nursing, 62*(2), 228-237. https://doi.org/10.1111/j.1365-2648.2007.04559.x

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., & Ahlemann, F. (2017). Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. *Business & Information Systems Engineering, 59*(4), 301-308. https://doi.org/10.1007/s12599-017-0484-2

McCarthy, C., & Harnett, K. (2014). *National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles*.

Perwej, Y. (2017). An experiential study of the big data. *for published in the International Transaction of Electrical and Computer Engineers System (ITECES), USA*, *4*(1), 14-25.

Pranggono, B., & Arabo, A. (2021). COVID -19 pandemic cybersecurity issues. *Internet Technology Letters, 4*(2). https://doi.org/10.1002/itl2.247

Priambada, S., Korthaus, A., Bennett, R. M., & Scifleet, P. (2020). *Exploring Dynamic Capabilities, Digital Business Transformation and Indonesia's Creative Industry Sector*. ACIS.

PwC. (2018). State of the internal audit profession study. *Moving at the speed of innovation: the foundational tools and talents of technology-enabled internal audit*. www.pwc.com/sg/en/publications/assets/state-of-the-internal-audit-2018.pdf

PwC. (2019). Annual global CEO survey: *CEOs' curbed confidence spells caution*. www.pwc.com/mu/pwc-22nd-annual-global-ceo-survey-mu

PwC. (2022). *PwC Global Risk Survey: Internal Audit's Response to the new risk multiverse*. https://www.pwc.com/gx/en/services/audit-assurance/assets/pwc-global-risk-survey-internal-audits-response-to-new-risk-multiverse.pdf

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry, 102*, 14-22. https://doi.org/10.1016/j.compind.2018.08.002

Roussy, M., & Perron, A. (2018). New Perspectives in Internal Audit Research: A Structured Literature Review. *Accounting Perspectives, 17*(3), 345-385. https://doi.org/10.1111/1911-3838.12180

Sarens, G., & De Beelde, I. (2006). The Relationship between Internal Audit and Senior Management: A Qualitative Analysis of Expectations and Perceptions. *International Journal of Auditing, 10*(3), 219-241. https://doi.org/10.1111/j.1099-1123.2006.00351.x

Sekaran, U., & Bougie, R. (2013). *Research Methods for Business: A Skill-Building Approach* (6th Edition). Wiley, New York.

Skoff, D. N. (2017). Exploring potential flaws and dangers involving machine learning technology. *Missouri S&T's Peer to Peer*, *1*(2), 4. https://scholarsmine.mst.edu/peer2peer/vol1/iss2/4

Skog, D. A., Wimelius, H., & Sandberg, J. (2018). Digital Disruption. *Business & Information Systems Engineering, 60*(5), 431-437. https://doi.org/10.1007/s12599-018-0550-4

Škrjanc, I., Ozawa, S., Ban, T., & Dovžan, D. (2018). Large-scale cyber-attacks monitoring using Evolving Cauchy Possibilistic Clustering. *Applied Soft Computing, 62*, 592-601. https://doi.org/10.1016/j.asoc.2017.11.008

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society, 71*, 15-29. https://doi.org/10.1016/j.aos.2018.04.005

Stonehouse, G. H., & Konina, N. Y. (2020). Management Challenges in the Age of Digital Disruption. *Proceedings of the 1st International Conference on Emerging Trends and Challenges in the Management Theory and Practice* (ETCMTP 2019). https://doi.org/10.2991/aebmr.k.200201.001

Ta, T. T., & Doan, T. N. (2022). Factors Affecting Internal Audit Effectiveness: Empirical Evidence from Vietnam. *International Journal of Financial Studies, 10*(2), 37. https://doi.org/10.3390/ijfs10020037

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research, 122*, 889-901. https://doi.org/10.1016/j.jbusres.2019.09.022

https://doi.org/10.15405/epsbs.2023.11.65
Corresponding Author: Aziatul Waznah Ghazali
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Wallace, S., Green, K., Johnson, C., Cooper, J., & Gilstrap, C. (2020). An Extended TOE Framework for Cybersecurity Adoption Decisions. *Communications of the Association for Information Systems, 47*, 338-363. https://doi.org/10.17705/1cais.04716