Horizon J. Hum. & Soc. Sci. Res. 5 (2): 121 – 131 (2023)

Journal of Humanities and Social Sciences Research
www.horizon-JHSSR.com

RESEARCH ARTICLE
Peer-reviewed | Open Access

Inference on Business Best Practices Affinity Despite Conceptual AI Exposure

Rachel John Robinson*

Cybersecurity, Department of IT, IU University of Applied Sciences, Berlin, Germany

ARTICLE INFO

Article history
Received: 28-Sep-23
Revised: 26-Oct-23
Accepted: 06-Nov-23
Published: 01-Dec-23

*Corresponding Author
Rachel John Robinson
E-mail: info@rachel-johnrobinson.de

Citation: Rachel John Robinson (2023). Inference on Business Best Practices Affinity Despite Conceptual AI Exposure. Horizon J. Hum. Soc. Sci. Res. 5 (2), 121–131. https://doi.org/10.37534/bp.jhssr.2023.v5.n2.id1227.p121

ABSTRACT

The background of the study was the experience of the major difficulties that IT compliance professionals face in light of emerging technologies like Artificial Intelligence (AI). For this purpose, an in-depth analysis of the current situation and future focus points are provided by a prime coverage of 1,000 survey respondents who are industry cyber practitioners. One in two businesses with between 1000-5000 workers experienced a security breach in 2022, showing that threat actors are still driven to obtain valuable and sensitive data. In contrast to last year's 35% and 57%. Firms anticipate spending more effort on risk compliance management in 2023. The chosen methodology for analyzing this topic is a qualitative retrospective casual comparative positivism approach. Through this analysis, the paper aims to determine whether the C-Suite and board are actively addressing the escalating incidents of security breaches. It is widely recognized that businesses are prepared to enhance their risk and compliance management practices in the future. The paper intends to provide conclusive insights into the current handling of risk and compliance, with indications that these areas are often managed independently and in isolation. Further details on these findings will be presented in the paper.

Keywords: Artificial Intelligence (AI), IT risk, IT compliance, risk compliance

Introduction

As companies continue to accelerate their digitization efforts, those with an early adopter mindset may be tempted to jump on the next big thing out of curiosity and hype. In recent years, new technologies such as artificial intelligence (AI), cloud services, blockchain, and the Internet of Things (IoT) have proliferated and seen significant adoption. One factor may be the growing number of digital natives among the world's population who are more knowledgeable about digital technologies and the adoption of new technologies. From an organizational perspective, managing the security and risks associated with new technologies can be challenging. Companies may feel pressure to adopt these new technologies without conducting a detailed and balanced risk/benefit assessment to stay ahead. However, the risks associated with using these technologies must be understood and considered so that potential threats do not catch you off guard.

Generative AI, such as ChatGPT, has emerged as a popular technology in recent times. McKinsey defines generative AI as algorithms capable of producing diverse content like audio, code, images, text, simulations, and videos. [Vincent, 2023] The introduction of ChatGPT to the public in November 2022 has sparked a global sensation, attracting a staggering 100 million monthly active users within just two months. This rapid adoption has set a record for the fastest-growing platform. Consequently, companies must anticipate that their employees will engage with ChatGPT or other generative AI services in some capacity.

The utilization of generative AI technology offers users various advantages. For one, it enhances user productivity by generating content based on prompts, eliminating the need for human expertise. Different generative AI services cater to various purposes, such as artistic creation, coding, explanatory tasks, and knowledge acquisition. However, amidst the hype surrounding new technology, it is imperative for management to acknowledge the potential negative impacts and risks that may arise within their organization. OpenAI's ChatGPT, for instance, experienced a 10-hour shutdown following a data breach, which allowed users to view other users' chat history titles [Robinson, 2020]. Furthermore, personal information belonging to approximately 1.2 million subscribers of ChatGPT Plus may be exposed.

As seen above, organizations must be comfortable with both embracing these technologies and managing the uncertainties that come with adopting them to avoid falling into the hype trap. By being motivated by these issues; in this research, we pose the following questions.

- What's your experience with using AI for Risk oriented assessments and business decisions?
- How have you considered the risks arising from this emerging technology?
- Is it a single line item or are there multiple risks identified in your risk register?
- How do the top level executives view such risks?

With these research questions in hand the two main objectives or the aims drawn for the work would be:

1) Exploring the impact of C-suite involvement on budget prioritization and allocation.
2) Examining the effectiveness of unified risk management and compliance operations.

In other words, it is to know if the company is taking a risk-informed approach, where security and risk professionals can navigate the path forward in such a way that balances the potential benefits of emerging technologies with the risk they may pose.

Literature Knowledge on Recent Key Trends

The first section of the literature is solely focused on to see the latest performing trends in the ever-evolving compliance and risk landscape.

85% of company practitioners say their company has a board member with cybersecurity expertise. As the board takes a magnifying glass to cybersecurity, compliance operations, and risk management, security and compliance professionals will need to brace themselves for a barrage of requests for detailed reporting, more internal assessments, and more frequent communication with the board around cybersecurity risk[Robinson, 2020].

A large 51% of practitioners struggle with identifying critical risks to prioritize remediations. Although respondents were highly confident in their abilities to address risk, practitioners also noted that they are still struggling to identify and prioritize risks [Vincent, 2023]. This means that while respondents felt they were doing an adequate job of addressing risk, they still struggle with finding risk related information when they need it and must switch between multiple systems throughout the risk management process. While risk management is improving for many organizations, there are opportunities for further improvement.

In 57% of cyber users anticipate spending more time on IT risk management and compliance in 2023. 32% of respondents said they would postpone adding additional compliance frameworks and/or certifications due to lack of capacity to take on new work and to mitigate stress in the coming months, but this can only happen for so long [Hu, 2023]. With security breaches on the rise and increasing pressure to keep companies safe, compliance managers will need to find ways to reduce their manual administrative tasks to better focus on IT risk management.

70% companies plan to grow their compliance team over the next two years. In a volatile economy, spending on compliance operations and risk management is still expected to increase, as all eyes are on CISOs (Chief Information Security Officer) to prevent data breaches. This willingness to invest in risk management is in sharp contrast to other categories of corporate spending in the current down economy. Yet, this trend to hire more staff is logical, given that 32% of respondents said they had to postpone the pursuit of new compliance frameworks/ certifications due to insufficient resources[Hu, 2023].

Literature Study on Defining Risk Appetite

The goal of risk management is to reduce an organization's risk below an acceptable level. This tolerance level is determined based on the organization's risk appetite and tolerance for certain risks. Risk appetite is how much an organization is willing to lose if the risk materializes or if the project fails to meet its goals. Risk appetite varies from organization to organization based on industry, culture, diversity, size and goals. An organization's risk appetite changes over time[Cao et.al, 2023].

One of the advantages of taking risks is that management considers various potential risks and evaluates the possible loss of investment in the event of project failure. This evaluation helps determine the organization's risk appetite, which is crucial in determining the margin for investing in new projects. However, many companies struggle with defining their risk appetite, with a study revealing that only 26% of organizations have a clear risk appetite statement. It is important for an organization to have a well-defined risk appetite statement as it aligns with the overall business strategy and should be expressed in quantitative terms in order to effectively manage risks. [Cao et.al, 2023].

However, it may also contain qualitative statements. An organization's risk appetite depends on its risk culture.

Characterizing risk hunger is the obligation of the governing body and, while characterizing risk appetite, the accompanying perspectives are to be viewed as by the board [John, 2022]:

- Absolute income of the association and the value capital that will choose as far as possible
- Consistence prerequisites, especially legitimate and administrative
- Level of accomplishment of business targets and the effect of hazard on them
- Partner assumptions from the association.
- Verifiable information and experience on risk appearance
- Risk situation investigation

Additionally, certain aspects need to be part of an ERM framework to ensure the effectiveness of risk appetite and, in turn, the risk management process [John, 2022].

- Increment risk mindfulness and construct the ideal risk culture
- Adjust business procedures with the board and empower planning among monetary and risk reaction activity plans
- Guarantee remaining gamble is fine
- Key risk development indicators (KRIs), key performance indicators (KPIs) and checking processes
- Value creation, risk advancement, security and monetary supportability Understanding partner assumptions connected with potential outcomes

Literature- Related Work on Study of Ai Uncertainities

While privacy and fairness remain central to the AI debate, others are harnessing the power of AI to transform the way nations conduct military operations. It can be used as training input and attract the attention of malicious attackers. When discussing generative AI within the enterprise, keep in mind six messages that can support the discussion of AI opportunities and risks. Increased technological capabilities inherently carry risk. While many GPT risk areas are documented, there will undoubtedly be more given the recency of GPT-4 (latest version). Misuse of technology—intentional or otherwise—is inevitable. Preemptive planning, governance, risk management and continued research are imperative [Chui et.al, 2022].

1. Advancements in technical capabilities come with inherent risks, particularly in the case of GPT-4. While some risk areas in GPT technology have been identified, there are likely numerous others that have not yet been documented. It is inevitable that technology will be misused, whether intentionally or unintentionally. To mitigate these risks, prevention planning, governance, risk management, and ongoing research are crucial.
2. One area of concern is that language models can reinforce biases and stereotypes, perpetuating societal prejudices. Current focus is primarily on computational factors such as data and fairness, while overlooking human and organizational biases and social factors. It is important to recognize that the input provided by users to generative AI tools is often already biased, which influences future results.
3. Furthermore, legal frameworks have lagged behind technological advancements for an extended period. The rapid growth of generative AI has brought to light various intellectual property issues and has underscored the urgent need for effective privacy laws and oversight, particularly in the United States.
4. Automated systems carry risks not only during processing but also when they are poorly designed, implemented, operated, or lacking proper oversight. It is crucial to provide users with clear and concise notifications that offer accessible and understandable documentation of automation's functionality and role across various systems. These notifications should be on par with those provided for human alternatives. Additionally, companies have a responsibility to establish clear guidelines for the use of technology in the workplace.
5. There has been a historical mismatch between the supply and demand for technical talent, leading to the

emergence of vendor solutions claiming to solve all business problems. Currently, the usefulness of GPT-4 in cybersecurity is limited. GPT-4 is anticipated to make phishing emails more convincing, making it harder to contain social engineering attacks and necessitating the need for cybersecurity education and awareness.

6. Fear, uncertainty and doubt (FUD) around AI replacing human jobs is nothing new, but the emphasis seems to be on augmenting human capital now, but that won't always be the case. Importantly, how good an AI is depends on the data you use to train it. Humans therefore still play an important role in situational awareness, creativity and communication. AI may replace some roles, making global and national policy decisions more important. In IT-related areas, the explosion of technologies like GPT-4 is likely to result in job restructuring and redeployment of specific business functions rather than worker mobility[Walters, 2020].

The emergence of technologies like GPT-4 in IT-related fields is more likely to result in job restructuring and the reassignment of specific business functions rather than widespread worker displacement.

Generative AI and Digital trust serves as the foundation for AI insights and plays a critical role in the digital transformation process. However, recent advancements in AI technology have made achieving digital trust more challenging. AI systems are not immune to errors and violations, highlighting the need for organizations to earn and maintain digital trust. Developing, operating, and securing technology without proper visibility can lead to significant issues, ranging from operational challenges to irreversible damage to a brand's reputation. Currently, consumers often have to compromise their privacy in exchange for access to all-or-nothing services. Unfortunately, we heavily rely on legal frameworks to regulate business practices that exploit individuals who may be careless or unaware of the risks involved. [Chui et.al, 2022].

Security Professionals and Regulatory Changes (Relevant Study)

All of the above advances pressure the InfoSec professionals to brace regulatory changes, many of which either went into effect on January 1, 2023 or will go into effect this year. Some of the highest-impact regulatory changes are outlined below [McKinsey, 2023].

- Data Privacy in USA

In 2023, nearly 30 states have some form of privacy protection law in place or in draft for debate and passage. Five states already have comprehensive policies in place: California, Utah, Colorado, Connecticut, and Virginia. California has already implemented GDPR-inspired standards statutes, and Colorado, Connecticut, Utah, and Virginia are following close behind. Additionally, California, Colorado, and Virginia are set to make important updates in 2023 that are shifting the underlying philosophical framework regarding data privacy protection [Heikkilä, 2022].

- Privacy regulations in China

The introduction of China's Personal Information Protection Law (PIPL) in November 2021 has had a widespread impact on global industries. While there are some similarities between PIPL and regulations like the European Union's GDPR regarding data subject rights, such as access, withdrawal, and deletion, there are also significant differences. Unlike other privacy regulations, PIPL is overseen by the state-based agency, The Cyberspace Administration of China (CAC), which deviates from the norm of independently operated agencies for compliance oversight. The specific applicability terms of PIPL are not yet clear, but it is expected that many medium to large-sized entities will be required to comply. Additionally, as neighboring countries work on their own privacy laws, the influence of PIPL on future regulation in parts of Asia could be significant.

- NIST Cybersecurity framework potential updates

In January 2023, the National Institute of Standards and Technology (NIST)announced its intent to make new revisions to its Cybersecurity Framework (CSF) document, with an emphasis on cyber defense inclusivity across all economic sectors. The new CSF could see protocols surrounding increasing international collaboration in cybersecurity efforts while still retaining the level of detail within the existing standards and guidelines to ensure the framework is scalable and useful for as many organizations as possible. Current recommendations for updates include a request for the new CSF to more clearly relate to other NIST frameworks, making improvements to the CSF's website, and expanding coverage and governance outcomes to supply chains.

- New Directives from the EU

The EU Data Governance Act (DGA) will become applicable in late 2023 and will facilitate data access and sharing with the public sector, adding another layer of complexity as organizations try to understand what it takes to facilitate compliant data transfers. The DGA will establish robust procedures to facilitate the reuse of certain protected public sector data and foster data altruism across the EU. It will define a new business model for data intermediation services that would serve as trusted environments for organizations or individuals to share data, support voluntary data sharing between companies, facilitate the fulfillment of data sharing obligation set by law, enable individuals to exercise their rights under GDPR, and enable individuals to gain control over their data and share it with trusted companies.

Research Methodology

It is attempted to outline a type of Qualitative analysis as usage for data collection, data analysis and interpretation of the data of this research. Also, explanation on the data in graphs and diagram to know the details on how risk systems and monitoring around it could be prioritized for implication.

I. Methodology and Method

Qualitative research involves the collection and analysis of non-numeric data, while quantitative research focuses on numeric data. Both approaches utilize methods like field notes, surveys, and interviews to gather information, providing valuable insights into various subjects or experiences [John, 2021]. Although the qualitative approach may be less widely accepted in certain fields, such as psychology, it has grown and developed over time, even amidst debates within the field [Zohny et al., 2023]. In the current study, a qualitative iterative approach is employed to retrospectively examine and compare causal relationships.

For effective statistical analysis of the data collected through these methods, it is important to assess the impact through intervention experimentation [Jackson et al., 2007]. Qualitative methods and the experimentation of those methods require an iterative approach. An example of this approach is illustrated in Figure 1.

The conducted research adopts a qualitative retrospective casual comparative positivism approach and relies on primary data. This approach was selected due to its emphasis on risk issues and performance data [Jackson et al., 2007].

Effective research planning is pivotal in aligning goals, objectives, resource needs, and anticipated outcomes, thereby providing clarity and direction to the research process [Brynjolfsson et al., 2023]. In this regard, the qualitative retrospective casual comparative approach is aligned with the research objectives to ensure appropriate conclusions can be drawn.

II. Data source

Figure 2 displays the categories or the number of companies involved in the research, which served as the primary data source for this study [Robinson, 2023]. The data was gathered through the IT Compliance and Risk Survey, with a total of 1010 responses collected between December 2022 and January 2023. The participating organizations belong to various industries.

Furthermore, the research also collected the profile of the participants in terms of their job functions, as shown in Figure 3. Among all respondents, 83% stated that they are directly involved in making decisions related to cybersecurity and data privacy risks for their organizations. Additionally, 16% reported having sufficient knowledge

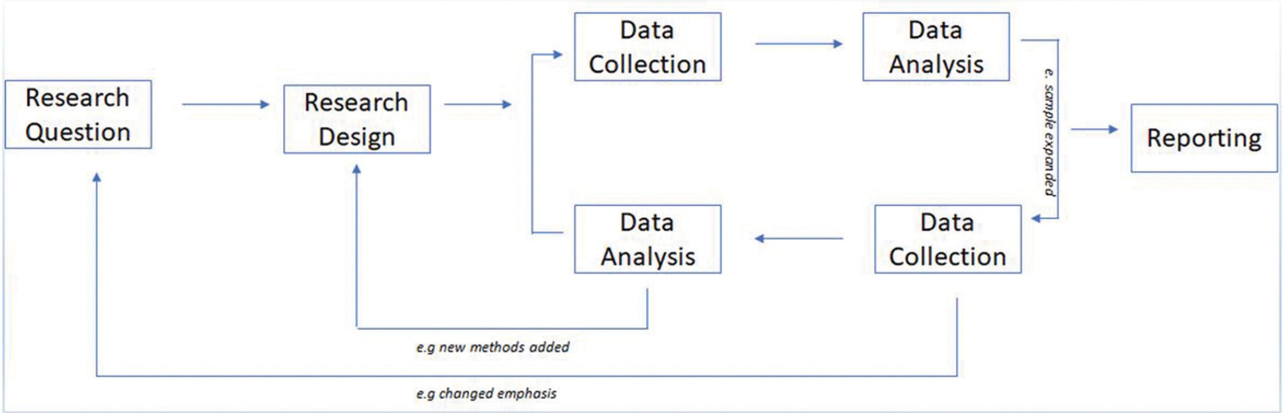

Figure 1. Qualitative Iterative Research Approach [*Busetto et.al, 2020*]

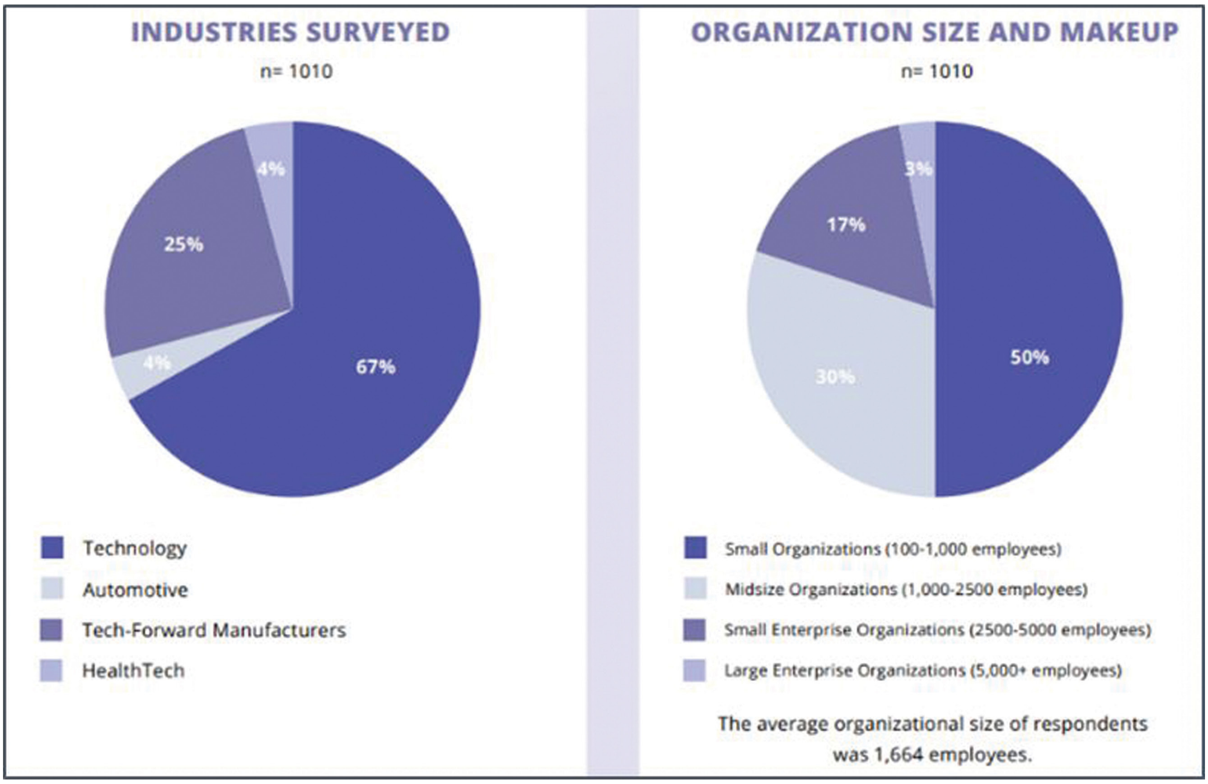

Figure 2. Profile of the Organisations in research

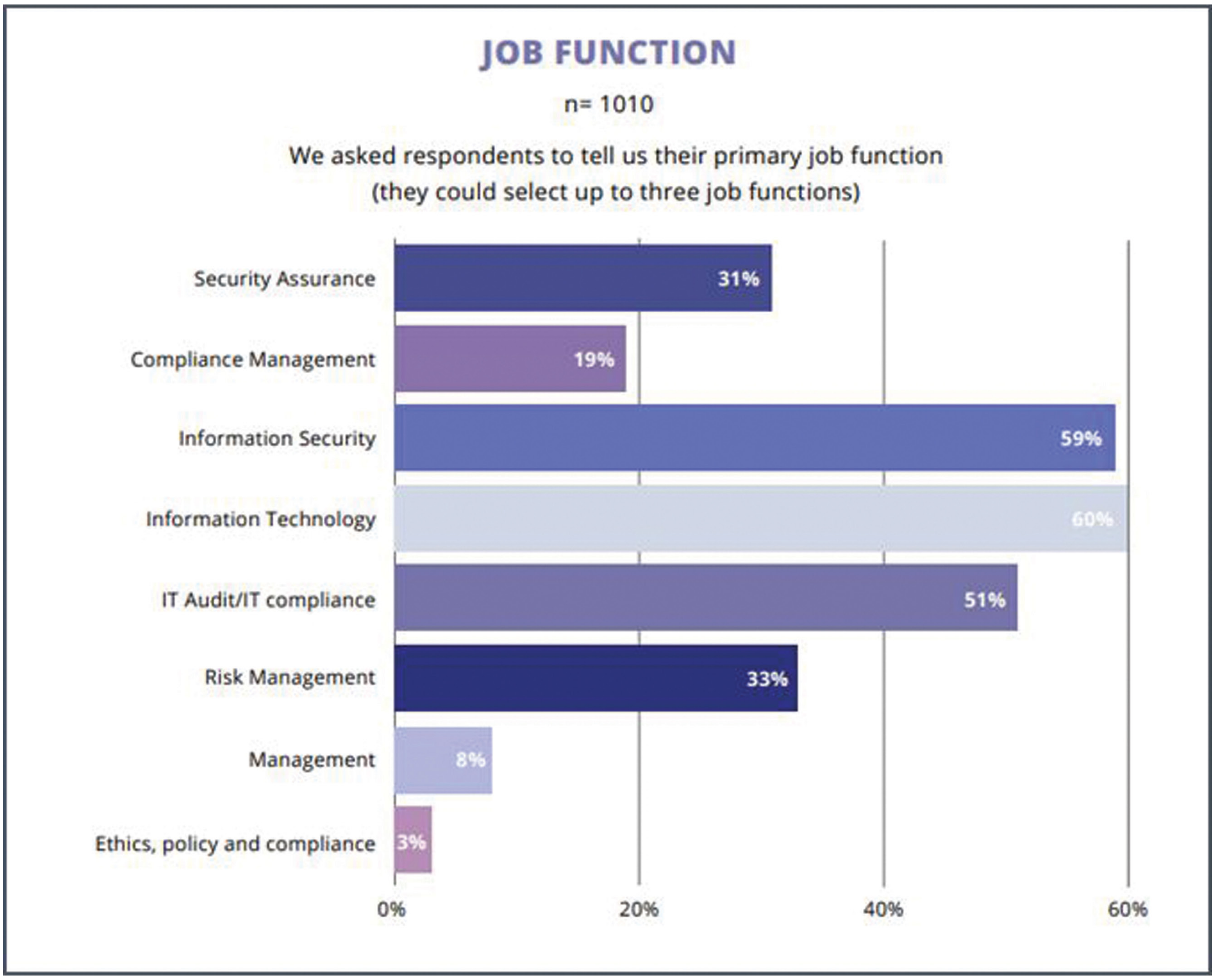

Figure 3. Job profile of participants

to understand the requirements and needs pertaining to cybersecurity and data privacy within their organization. Only 1% mentioned that they do not participate in decision-making but are responsible for maintaining IT security and data privacy. When it comes to decision-making authority for data security and privacy compliance, 81% of respondents claimed to be the sole decision-maker, 16% stated that they are part of a decision-making team within their organization, 2% mentioned being part of a committee, and 1% indicated that their role involves gathering information and conducting research on data security and privacy compliance.

III. Research Limitation:

Like any study, this research had certain limitations that need to be acknowledged.

- Firstly, the qualitative research approach used in this study does not allow for precise measurements of the problems under examination.
- Secondly, some participants were reluctant to provide the exact data requirements needed for the research.

Research Findings

This section is directly going to address the research objective identified in the first hand to find out how the new Generative AI trend have changed the way in which organizations refer the security budget plans and risk management purview, thereby unifying the C-suite level and Board for a collective responsibility. Analysis of the 1010 responses is produced for results as below.

I. Exploring the impact of C-suite involvement on budget prioritization and allocation

When most western companies are preparing for a recession, most security, compliance, and risk management departments are actually planning to level up their efforts and expand their budgets in 2023. This is likely due to mounting stress over cybersecurity risks, which was the largest stressor reported for InfoSec professionals at 36%. Notably, cybersecurity risks were also the highest reported cause of stress in 2022. This requires InfoSec professionals to stay up-to-date on security best practices and adds to the already growing pressure of preventing an attack.

Based on Figure 4, the most commonly reported financial loss resulting from data breaches in both 2022 and 2023 fell within the range of $1M-$5M. However, when examining the data more closely, it becomes evident that there are distinct trends in the cost of data breaches based on the size of the company.

Companies with more than 2,500 employees were found to be more prone to experiencing financial losses ranging from $5M-$20M as a consequence of data breaches. On the other hand, smaller companies with less than 2,500 employees were more likely to incur financial losses within the range of $100k-$1M.

For an average organization from our dataset, spending on technology represents a greater proportion of their organization's GRC (Governance, Risk and Compliance) spend than any other category as in Figure 5. The greater emphasis on technology shows that organizations are attempting to gain efficiencies in managing risks and compliance processes.

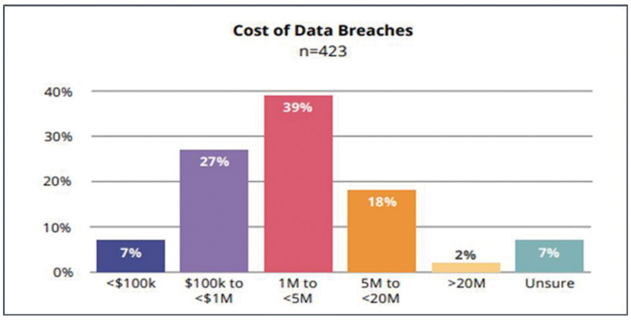

Figure 4. Cost of breaches

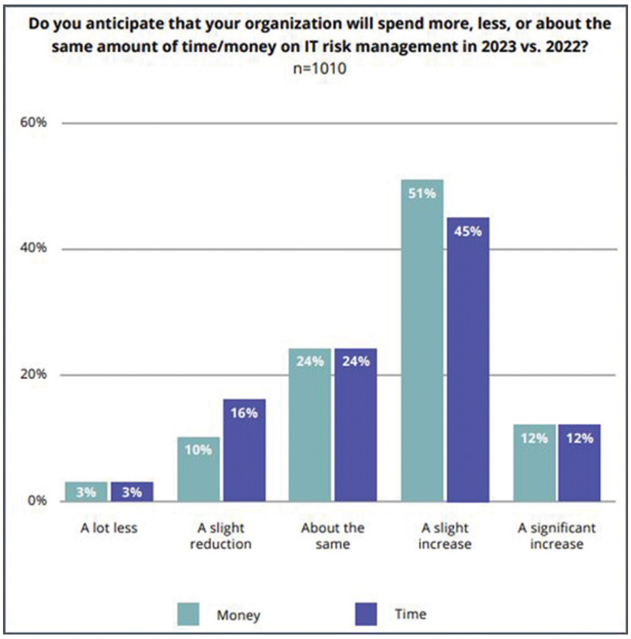

Figure 5. Spending on IT Risk Management

In the upcoming year, 63% of companies plan to allocate more funds towards compliance and risk, a significant increase compared to 45% in the previous year. On average, these companies estimate a 25% increase in their Governance, Risk, and Compliance (GRC) budgets over the next 12 to 24 months. Among those who intend to increase their budgets, 76% expect a minimum 10% increase in spending.

Only 13% of respondents claimed they would reduce their spending, while a mere 3% indicated a substantial decrease in IT risk management and compliance investments for 2023. Additionally, 57% of participants stated their intention to dedicate more time to IT risk management and compliance in the coming year. The heightened level of involvement from the C-Suite is evident, as compared to the previous year where only 35% expected to allocate more time to these areas.

II. Examining the effectiveness of unified risk management and compliance operations

Notably in the survey, 29% of respondents do not have established KRIs (Key risk indicators) linked to their KPIs (Key performance indicators) for any identified high or critical risks, indicating that risk and compliance could still be operating in silos, or respondents haven't figured out how to measure meaningful changes to risk level. Unifying risk and compliance efforts can help solve each of these pervasive challenges. 68% of respondents using integrated tools with both manual and automated processes did not experience a breach in 2022, and 72% of respondents who have tied their risk and compliance activities together did not experience a breach. With 31% of respondents said they manage IT risk in siloed departments, processes, and tools, followed by 24% that manage IT risk in an integrated approach where their processes are mostly automated (Refer Figure 6). These numbers are striking; while respondents clearly see the value in unifying risk management and compliance operations, the overwhelming majority of those surveyed aren't following this best practice. Even the most powerful IT risk management tool can produce inadequate results if critical processes are not in place.

The adoption of compliance tools has witnessed significant growth over the past year, with 65% of respondents in 2023 utilizing integrated risk management solutions, compared to 57% in 2022. The usage of these tools has transitioned from being a mere luxury to a necessity due to the transformative changes in the landscape, driven by the emergence of more advanced and powerful technology tools that are both beneficial to companies and threat actors.

In terms of tracking risks, the usage of spreadsheets has decreased from 35% in 2022 to 25% in 2023. Conversely, the use of the risk module in cloud-based GRC software has seen a slight increase from 57% last year to 60% this year. When it comes to identifying and managing IT risks from third parties, the utilization of spreadsheets has decreased from 31% in 2022 to 23% in 2023. On the other hand, the use of dedicated IT solutions has risen from 69% last year to 77% this year. The reliance on spreadsheets to manage IT compliance efforts has

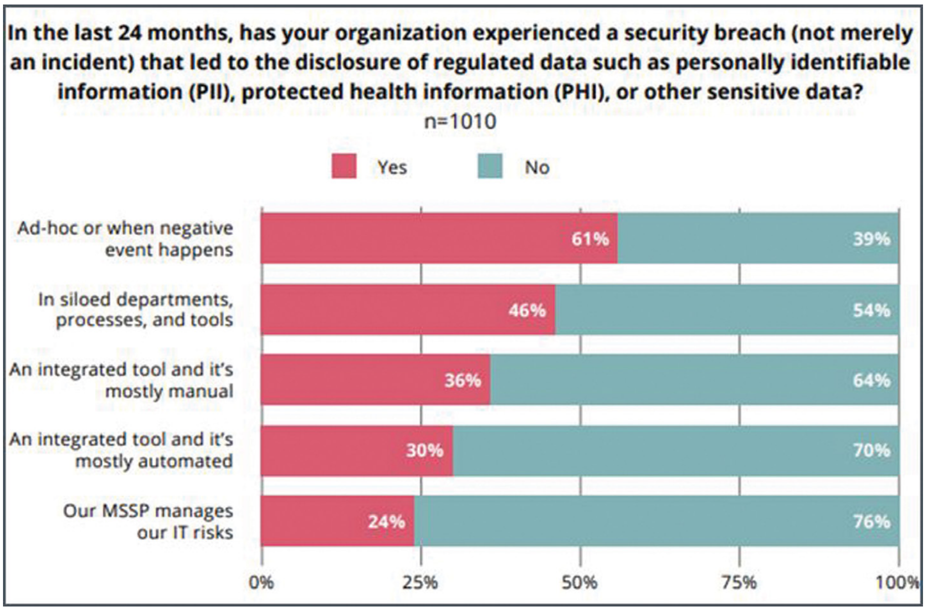

Figure 6. Experience of security breaches

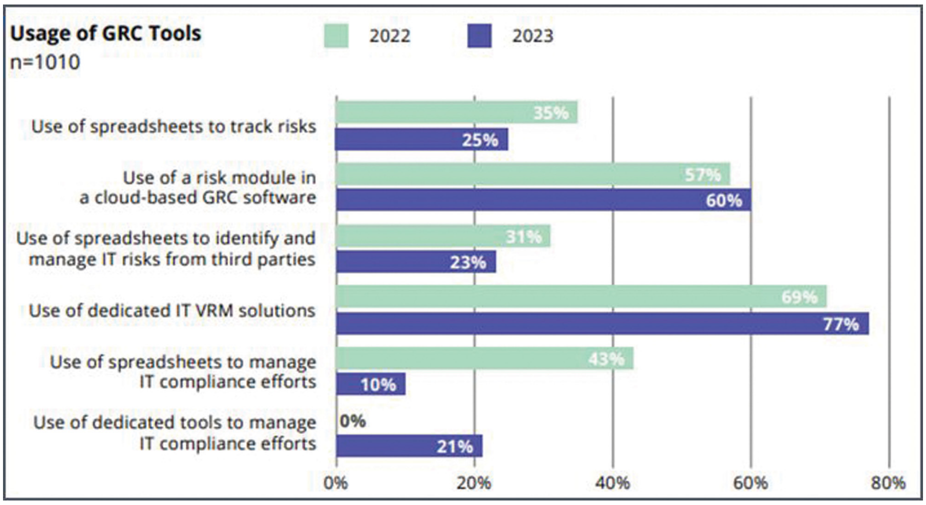

Figure 7. Experience of security breaches

notably reduced from 43% in 2022 to only 10% in 2023, as depicted in Figure 7.

This adoption of new tools aligns with the Technology sector's rapid increase in digital platform usage and Cloud technologies in response to the pandemic, and, as a result, this new mix of GRC tools has helped operationalize compliance efforts and adapt to new compliance requirements. However, the usage of Cloud technology has its downsides: third-party risk vulnerabilities, siloed views of risk and compliance and fractured reporting across multiple solutions.

Conclusions and Results

With the escalating concerns surrounding cybersecurity and the increase in regulatory measures, incidents of security breaches have gained significant attention in the media. Regulatory bodies now place greater emphasis on holding individuals accountable, particularly senior corporate officers and other influential figures within organizations. This shift, coupled with the findings of the survey, indicates a move towards stricter enforcement, particularly for organizations that lack adequate measures to safeguard and dispose of consumer data [Rothwell et al., 2022].

Implementing an integrated approach to risk and compliance operations enables organizations to effectively manage individual risks without duplicating processes. This approach begins by conducting a comprehensive risk assessment and formulating a robust security policy, followed by the implementation of internal controls aligned with the assessment outcomes. Embracing this integrated approach enhances coordination throughout the organization, involving input from all stakeholders and seamlessly integrating compliance into risk operations.

A recent study conducted by Hacker et al. (2023) examined the impact of embracing an integrated approach to Governance, Risk, and Compliance (GRC) on security and business performance outcomes. The research aimed to determine if there was substantial evidence suggesting that organizations adopting this approach achieve better security postures compared to those viewing compliance as a separate oversight function.

The study findings revealed that organizations practicing an integrated approach had a lower likelihood of scoring poorly in risk management and were less susceptible to security breaches compared to those perceiving compliance functions solely as rule enforcers. Moreover, organizations that embraced integration spent less time on repetitive administrative tasks, contrasting with those placing a primary focus on rule enforcement.

Overall, the study supports the proposition that organizations seeking superior security and business performance outcomes should adopt an integrated approach to GRC, recognizing the interconnectedness between governance, risk management, and compliance functions.

Acknowledgements

The authors wish to thank the editors and reviewers of Horizon JHSSR Journal which provided us an opportunity to publish in their scholarly journal.

Funding

The author received no financial support for the research, authorship and/or publication of this article.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article. This article is the sole work of the author and has not been presented or published elsewhere.

References

Brynjolfsson, E., Li, D., & Raymond, L. R. (2023). Generative AI at work (No. w31161). National Bureau of Economic Research. https://www.nber.org/papers/w31161

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. Neurological Research and practice, 2, 1-10. https://link.springer.com/article/10.1186/s42466-020-00059-z

Cao, Y., Li, S., Liu, Y., Yan, Z., Dai, Y., Yu, P. S., & Sun, L. (2023). A comprehensive survey of ai-generated content (aigc): A history of generative ai from gan to chatgpt. arXiv preprint arXiv:2303.04226. https://arxiv.org/pdf/2303.04226.pdf?trk=public_post_comment-text

Chui M, Roberts R, Yee L. Generative AI is here: How tools like ChatGPT could change your business. (2022, December 20). McKinsey & Company. https://www.mckinsey.com/capabilities/quantumblack/our-insights/generative-ai-is-here-how-tools-like-chatgpt-could-change-your-business

Hacker, P., Engel, A., & Mauer, M. (2023, June). Regulating ChatGPT and other large generative AI models. In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (pp. 1112-1123). https://dl.acm.org/doi/pdf/10.1145/3593013.3594067

Heikkilä, M. (2022, April 13). Dutch scandal serves as a warning for Europe over risks of using algorithms. POLITICO. https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/

Hu, K. (2023, February 2). ChatGPT sets record for fastest-growing user base - analyst note. Reuters. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/

Jackson, R. L., Drummond, D. K., & Camara, S. K. (2007). What is qualitative research? Qualitative Research Reports in Communication, 8(1), 21–28. https://doi.org/10.1080/17459430701617879

John, R. (2021). Economy Identity through Information Technology and its Safety by Rachel John Robinson - Books on Google Play. (n.d.). https://play.google.com/store/books/details/Rachel_John_Robinson_Economy_Identity_through_Info?id=haykEAAAQBAJ&pli=1

John, R. (2022). Can project management processes be used to structure active learning tasks? In 100 Ideas for Active Learning. https://doi.org/10.20919/opxr1032/70

McKinsey & Company. What is generative AI? (2023, January 19). McKinsey & Company. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai

Robinson, R. J. (2020). Structuring IS framework for controlled corporate through statistical survey analytics. Journal of Data, Information and Management, 2(3), 167–184. https://doi.org/10.1007/s42488-020-00021-3

Robinson, R. J. (2023). Insights on Cloud Security Management. Cloud Computing and Data Science, 212–222. https://doi.org/10.37256/ccds.4220233292

Rothwell F, Ernst & Manbeck, P.C. Will divergent copyright laws between the US and UK influence where you do business as an artificial intelligence company? (2022, September 8). JD Supra. https://www.jdsupra.com/legalnews/will-divergent-copyright-laws-between-4352051/

Vincent, J. (2023, February 6). Getty Images sues AI art generator Stable Diffusion in the US for copyright infringement. The Verge. https://www.theverge.com/2023/2/6/23587393/ai-art-copyright-lawsuit-getty-images-stable-diffusion

Walters, W. P., & Murcko, M. (2020). Assessing the impact of generative AI on medicinal chemistry. Nature biotechnology, 38(2), 143-145. https://www.nature.com/articles/s41587-020-0418-2

Zohny, H., McMillan, J., & King, M. (2023). Ethics of generative AI. Journal of medical ethics, 49(2), 79-80. https://web.archive.org/web/20230130233417id_/https://jme.bmj.com/content/medethics/49/2/79.full.pdf

Biographical Statement of Author(s)

Rachel John Robinson (F) born in India in 1989, she has a PhD from the University of Madras, India. She is currently practicing Academic in Cybersecurity with IU International University of Applied Sciences, Berlin.

She has a double masters and a Doctorate in Economic IT Security. As an academic, she is Lecturing and guiding students at both bachelors and master's level and supervising their thesis. Alongside that, she is also an active ambassador and advisor for Academic and Workforce Development Advisory Group & SheLeadsTech group at ISACA, USA and an Honorary Global Advisory Council Member in GAFM, International Board of Standards. As part of active research, she holds the Associate Editor position with Horizon Journals (JHSSR).

Her research orientation is mostly in the field of Cybersecurity, IT Security Management and Active Digital Learning. Before being an academician, she served in the industry as being an Auditor, IT Security Specialist in Multinationals and Blue-chip companies.

Dr. Rachel John Robinson
Researcher, Academic, Mentor, Author
Cybersecurity, Department of IT
IU University of Applied Sciences
Berlin, Germany
E-mail: info@rachel-johnrobinson.de
https://orcid.org/0000-0002-1079-1358