ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Vol 10, Issue 10, October 2023

Deciphering Generative AI Risk Trends to Integrate Compliance as an Industry Practice

[1] Dr. Rachel John Robinson

[1] Cybersecurity, Department of IT, IU University of Applied Sciences, Berlin, Germany
https://orcid.org/0000-0002-1079-1358
Corresponding Author Email: [1] info@rachel-johnrobinson.de

Abstract*— The top challenges IT compliance professionals face with the advent of new technologies like Artificial Intelligence (AI) and what they could be focused on to elevate challenges are the objective of the paper. A prime coverage of 1,000 survey respondents who are industry cyber practitioners talk about their pain points, IT risk particularly in terms of AI and compliance budgets, staffing, risk management best practices, and much more to provide an in-depth view of the current state and what to prepare for future as focus points. In 2022, 1 in 2 companies with 1,000-5,000 employees suffered a security breach, indicating that threat actors are as motivated as ever to gain access to lucrative and corporate data. 57% of surveyed organizations expect to spend more time on risk compliance management in 2023, as opposed to last year's 35%. Additionally, 63% of survey respondents expect to spend more money on IT compliance and risk management, an increase from 45% in 2022. With security breaches on the rise is there attention from the C-Suite and board on how to prevent them? Known is that companies are poised and ready to level up their risk and compliance management processes in the coming years, but where, when majority of survey respondents report handling risk and compliance are still in silos. More of this will be investigated through this paper with level up options.

Keywords*— Artificial Intelligence (AI), IT risk, IT compliance, risk compliance.

I. 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.

One of the latest popular technologies is generative AI. McKinsey describes generative AI as "algorithms (such as ChatGPT) that can be used to create new content such as audio, code, images, text, simulations, and videos." [15] Recent advances in this area have the potential to change the way we approach content. The global generative AI sensation could be thanks to ChatGPT, which launched to the general public in November 2022. Two months after launch, it has 100 million monthly active users. ChatGPT set a record for the fastest growing platform with its launch. With such rapid adoption, companies will have to assume that their employees will use ChatGPT or other generative AI services in some way. With such rapid adoption, companies will have to assume that their employees will use ChatGPT or other generative AI services in some way. New technology offers unique benefits to users. For example, generative AI services can improve user productivity by generating content based on prompts without the need for human expertise or expertise. Users can use different generative AI services for different purposes. For example, creating works of art, writing computer code, explaining complex topics, understanding new areas, and so on.

But hype aside, using new technology is not without risks. Management should be aware of the potential negative impacts and risks to the organization. In the case of OpenAI's ChatGPT, the service was taken down for 10 hours after a data breach occurred and users realized they could see the titles of other users' chat histories [4]. In addition, personal information of its 1.2 million of ChatGPT Plus subscribers may have been exposed as well.

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:

ISSN (Online) 2456 -1304
International Journal of Science, Engineering and Management (IJSEM)
Vol 10, Issue 10, October 2023

- Understanding the increase in budget prioritization and allocation with C-suite involvement
- Power 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.

II. LITERATURE ON CURRENT 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[4].

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 [15]. 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 [8]. 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[8].

III. LITERATURE-IMPORTANCE OF 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[9].

One of the benefits of taking risks is that when considering investing in a new project, management considers different risk scenarios for the project and decides, "If the project fails, the organization could lose its entire investment." is likely to attempt to provide an answer to the question This margin is determined by the organization's risk appetite. The biggest challenge for companies today is defining their risk appetite. A study by the National Association of Corporate Directors found that only 26% of organizations have a defined risk appetite statement, and about 70% do not have a clear risk appetite statement. An organization's risk appetite statement is an important part of the organization. An enterprise risk Enterprise Risk Management (ERM) framework must align with business strategy. Risk appetite should be expressed in quantitative terms[9].

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

Defining risk appetite is the responsibility of the board of directors and, while defining risk appetite, the following aspects should be considered by the board [5]:

- Board and management judgment about risk materializing
- Total earnings of the organization and the equity capital that will decide the upper limit
- Compliance requirements, particularly legal and regulatory
- Level of achievement of business objectives and the impact of risk on them
- Stakeholder expectations from the organization.
- Historical data and experience on risk materialization
- Risk scenario analysis

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 [5].

- Increase risk awareness and build the desired risk culture
- Align business strategy with risk management and enable mapping between financial and risk response action plans
- Ensure residual risk is acceptable
- Key risk development indicators (KRIs), key performance indicators (KPIs) and monitoring processes

ISSN (Online) 2456 -1304
International Journal of Science, Engineering and Management (IJSEM)
Vol 10, Issue 10, October 2023

- Value creation, risk optimization, security and economic sustainability Understanding stakeholder expectations related to possibilities.

IV. LITERATURE STUDY ON RECENT 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[6].

1. Advancing technical capabilities carries inherent risks. While many GPT risk areas have been documented, there are undoubtedly many more, given the current nature of GPT-4. Misuse of technology, whether intentional or unintentional, is inevitable. Prevention planning, governance, risk management and ongoing research are essential.
2. Language models can reinforce prejudices and perpetuate stereotypes. It continues to focus on computational factors (such as presented data and fairness) but ignores human and organizational biases and social factors. In many cases, the input is already biased, as the information users provide to generative AI tools is used to shape future results.
3. For a long time the law has not kept up with technological progress. The explosion of generative AI has raised various intellectual property issues and highlighted the need for effective privacy laws (especially in the US) and oversight.
4. Automated systems pose risks not only during processing, but also when poorly designed, implemented, operated, or lacking proper oversight. Providing users with clear, concise notifications that provide accessible, understandable documentation of the functionality and role of automation across systems is just as important as human alternatives. Additionally, companies have a responsibility to provide clear guidelines for using technology in the workplace.
5. The mismatch between supply and demand for technical talent has historically spawned a variety of vendor solutions that claim to solve every business problem. Currently, his GPT-4 usefulness in cybersecurity is limited. GPT-4 is expected to make phishing emails more credible, making social engineering more difficult to contain and necessitating 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[11].

In IT-related fields, the explosion of technologies like GPT-4 is more likely to lead to job restructuring and redeployment of specific business functions than worker displacement.

Generative AI and Digital Trust - This is the foundation of the aforementioned AI insights, Digital Trust. Recent advances in AI make digital trust even more difficult to achieve. Digital trust is the evolution of digital transformation and a modern imperative. And AI technology is not immune to errors and violations. Digital trust must be earned and maintained. It is neither voluntary nor voluntarily given. Lack of visibility into how technology is developed, operated and secured can cause serious problems, ranging from operational problems to irreparable brand damage. Today, consumers are largely forced to sacrifice privacy in exchange for access to all-or-nothing services. Unfortunately, we rely heavily on the law to curb business practices that take advantage of careless or ignorant people [6].

V. INFOSEC PROFESSIONALS ARE PREPARING FOR REGULATORY CHANGES (LITERATURE 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 [16].

A. 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 [7].

B. Privacy regulation sin China

China’s Personal Information Protection Law (PIPL), which took effect in November 2021, has had a ripple effect across global industries. It somewhat aligns with European

ISSN (Online) 2456 -1304
International Journal of Science, Engineering and Management (IJSEM)
Vol 10, Issue 10, October 2023

Union GDPR and other global privacy regulations, including that the data subject has the right to access, right to withdrawal, and the right to deletion. However, it vastly differs in key areas: the state-based agency, The Cyberspace Administration of China (CAC), will oversee PIPL compliance, departing from the global norm of independently operated agencies who oversee compliance. It's not clear what the precise terms of applicability are yet, but it's reasonable to assume many mid to-large-sized entities will need to comply with PIPL. Additionally, as other neighboring countries draft their own privacy laws, there's a chance PIPL may carry significant influence over the future of regulation in parts of Asia.

C. 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 cyberdefense 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.

D. 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.

VI. RESEARCH PROCESS

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.

A. Methodlogy and Method

The Qualitative research is non-numeric data and the Quantitative research is numeric data and these both can be collected in a variety of ways including field notes, surveys and interviews offering deeper insights into topics or experiences [3]. Although less accepted than quantitative research in certain fields such as psychology, the qualitative approach has matured despite "paradigm wars" within this field [14]. Considering this, for the work undertaken the qualitative iterative to form retrospective casual comparisons is undertaken.

For an effective statistical analysis of the received data through these mediums, assessment needs to be undertaken through experimentation of the design for impact assessment through intervention [10]. Qualitative method undertaken, and experimentation of that method requires an iterative approach. An example is shown in Figure 1.

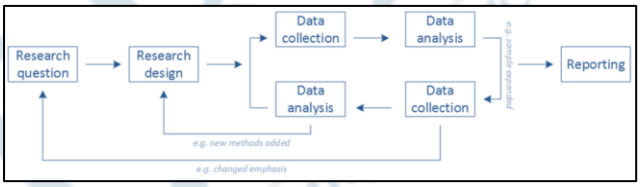

Figure 1: Qualitative Iterative Research Approach [1]

Approach taken in this research is a Qualitative retrospective casual comparative positivism approach using primary data. This fits the scheme due to primarily utilizing risk issues and its performance data [10].

The importance of research planning cannot be understated as it seeks to align goals and objectives, resource requirements, expected results delivering focus within the research process[12]. Considering this, the Qualitative retrospective casual comparative is mapped to the research objectives to frame conclusions.

B. Data source

The graph Figure 2 below shows the categories or the number of companies who were involved in the research to source the prime data [2]. The IT Compliance and Risk Survey gathered 1010 responses during December 2022 and January 2023. All organizations come from the following industries.

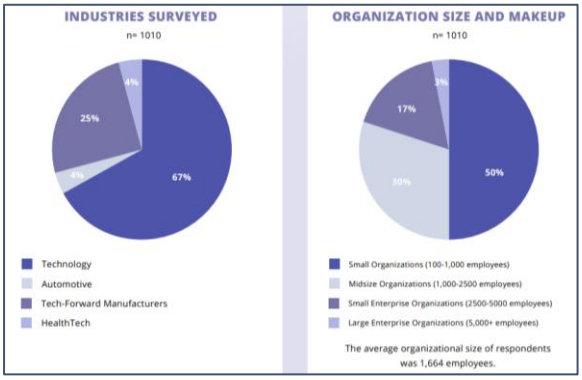

Figure 2: Profile of the Organisations in research

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Vol 10, Issue 10, October 2023

In addition the profile of the participants in terms of the job function as in Figure 3 was also gathered. 83% of all respondents said they are directly involved in decisions regarding cybersecurity and data privacy risks for their organizations. 16% percent said they're knowledgeable enough to understand the requirements and needs regarding cybersecurity and data privacy for their organization. 1% said they do not make decisions but are involved in maintaining IT security and data privacy for their company. 81% of respondents said they are the sole decisionmaker in decisions regarding data security and data privacy compliance for their organization. 16% said they are one of the decision-makers within their organization; 2% said they are part of a team or committee, and 1% said they gather information and provide research regarding data security and data privacy compliance.

Figure 3: Job profile of participants

C. Research Limitation:

As it is for every study, this research had the following limitation:

- Qualitative research adopted is not allowing the exact measurement of the examined problems.
- In some cases, participants refused to answer with the required exact data requirements for the research.

VII. 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.

A. Understanding the increase in budget prioritization and allocation with C-suite involvement

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.

As in Figure 4 in 2022 and 2023, $1M-$5M was the most frequently reported amount of money lost via a data breach. Diving deeper, we can see trends in cost of data breaches by company size. Companies with greater than 2,500 employees were more likely to incur $5M-$20M in money lost via data breaches, whereas smaller companies with less than 2,500 employees were more likely to incur $100k-$1M.

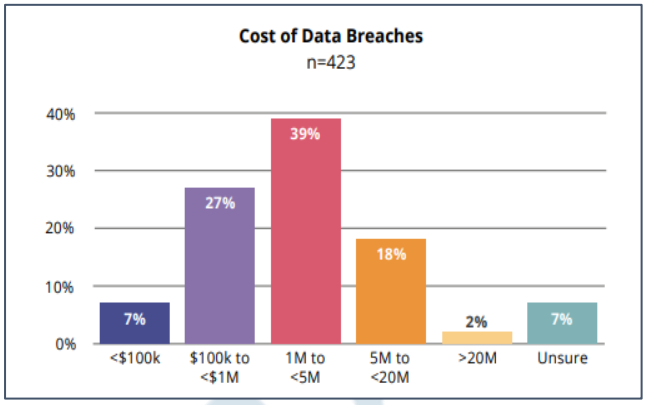

Figure 4: Cost of breaches

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.

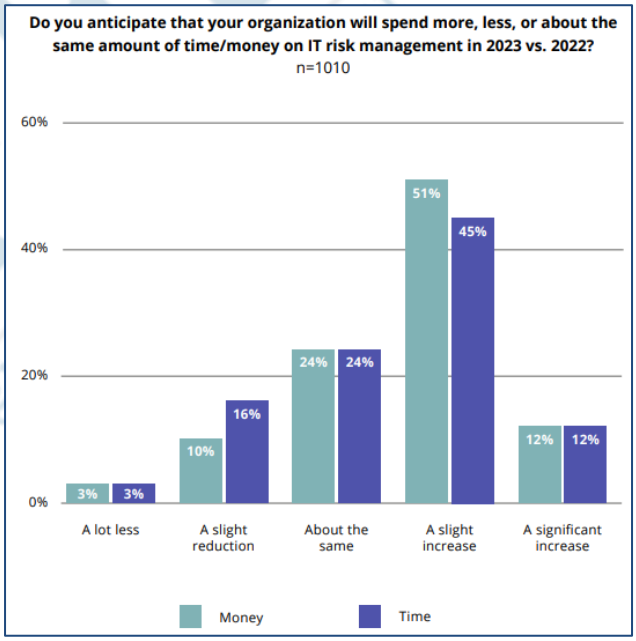

Figure 5: Spending on IT Risk Management

Further 63% of companies are planning to spend more money on compliance and risk in 2023 (vs. 45% in 2022), with an average estimated percent increase in GRC budget in the next 12 to 24 months of 25%. Of the respondents increasing their budgets, 76% expect to increase spend by at least 10%. Only 13% said they will reduce spending, and 3% said they will spend "a lot less money" on IT risk management and compliance operations in 2023. Further, 57% of respondents said they would spend more time on IT risk management and compliance in 2023, whereas in the prior year only 35% expected to spend more time on IT risk management which entails heightened level of involvement from the C-Suite level.

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Vol 10, Issue 10, October 2023

B. Power 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.

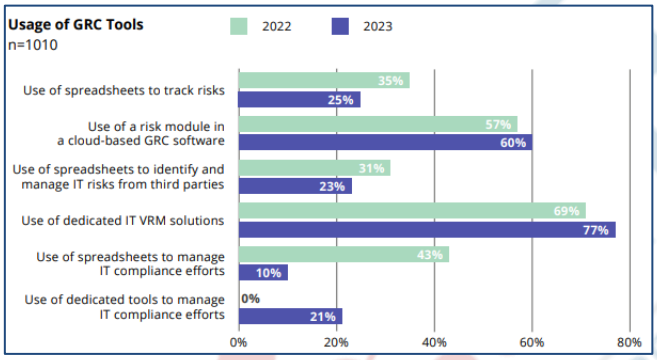

Figure 6: Experience of security breaches

Compliance tools usage has grown in the last year, with 65% in 2023 using integrated risk management solutions compared to 57% in 2022. The usage of tools is no longer a nice-to-have but a need-to-have as the landscape has changed drastically with the advent of newer, more powerful technology tools — both for companies and threat actors alike.

In 2023, 25% of all respondents use spreadsheets to track risks versus 35% in 2022. Use of the risk module in a cloud based GRC software has slightly increased from 57% last year to 60% this year. In 2023, 23% of all respondents use spreadsheets to identify and manage IT risks from third parties versus 31% in 2022. Use of dedicated IT solutions increased from 69% last year to 77% this year. Only 10% of respondents use spreadsheets to manage their IT compliance efforts in 2023, versus 43% in 2022 as referred in Figure 7.

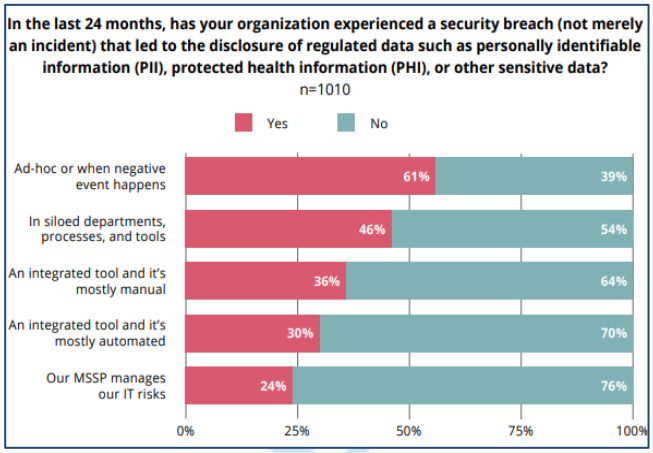

Figure 7: Experience of security breaches

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.

VIII. CONCLUSIONS AND RESULTS

As anxiety around cybersecurity increased, along with the amount of legislation in response, security breaches became hot topics in the news. Regulatory bodies increased their emphasis on individual accountability, especially for senior corporate officers and other prominent organizational figureheads. This change in posture, combined with the results of the survey conducted, indicate a larger shift towards enforcement, particularly for organizations that don't have adequate controls around the protection and disposition of consumer data [17].

An integrated approach to risk and compliance operations allows organizations to focus on individual risks while avoiding duplication of risk and compliance management processes. Organizations adopting this approach typically begin their risk management process by conducting a risk assessment. From there, create a security policy and implement internal controls aligned with the results of your risk assessment. This improves coordination across the organization by getting input from all stakeholders, not just a select few [13]. It also helps create a compliance program that is embedded in risk operations. The study found that companies that take an integrated approach to GRC achieve significantly better security and business performance results than those that still view compliance as a separate oversight function. This paper wanted to check if there was strong evidence that organizations that take an integrated approach have better security postures than others that view compliance solely as a function of enforcing rules and regulations and conclude as:

On average, organizations that take an integrated approach are less likely to score low on risk management. They are more likely not to commit security breaches than those who see compliance functions as rule enforcers.

Overall, organizations that take an integrated approach spend less time on repetitive administrative tasks than organizations that believe that the purpose of the compliance function is to enforce rules.

REFERENCES

[1] Busetto, L, et al. 2020. How to use and assess qualitative research methods [online]. USA. biomedcentral.com. Available From: https://neurolrespract.biomedcentral.com/articles/10.1186/s42466-020-00059-z#citeas

[2] Duenas, A.G and Robinson, R. J. (2023). Data modelling and analytical techniques employed for forecasting. The Research Monograph Series in Computing, Electrical & Communication Networks. https://www.bohrpub.com/data_modeling_analytic_technique

[3] Economy Identity through Information Technology and its Safety by Rachel John Robinson - Books on Google Play. (o. D.). https://play.google.com/store/books/details/Rachel_John_Robinson_Economy_Identity_through_Info?id=haykEAAAQBAJ&pli=1

[4] Engadget is part of the Yahoo family of brands. (o. D.). https://consent.yahoo.com/v2/collectConsent?sessionId=3_cc-session_a90ec541-5553-4236-80d8-5d60a0188dc9

[5] Engadget is part of the Yahoo family of brands. (o. D.-b). https://consent.yahoo.com/v2/collectConsent?sessionId=3_cc-session_088c68cf-b779-418f-a54d-26204cc8859c

[6] Generative AI is here: How tools like ChatGPT could change your business. (2022, 20. Dezember). McKinsey & Company. https://www.mckinsey.com/capabilities/quantumblack/our-insights/generative-ai-is-here-how-tools-like-chatgpt-could-change-your-business

[7] Heikkilä, M. (2022, 13. April). 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/

[8] Hu, K. (2023, 2. Februar). 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/

[9] ISACA Risk Appetite (2021). ISACA USA, https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2021/volume-6/helpsource-joa-eng-1221.pdf

[10] Jackson, R. et al, 2007. What Is Qualitative Research? [online]. Researchgate.net. Available from https://www.researchgate.net/publication/233325570_What_Is_Qualitative_Research

[11] National Association of Corporate Directors (NACD), (2013-2014) Public Company Governance Survey, USA, https://www.nacdonline.org/analytics/ survey.cfm?ItemNumber=66753

[12] Pickton, M. 2013. Writing your research plan. [online]. In: Grant, M. J., Sen, B. and Spring, H. (eds.) Research, Evaluation and Audit: Key Steps in Demonstrating Your Value. London: Facet Publishing. Available From: http://nectar.northampton.ac.uk/5703/1/Pickton20135703.pdf

[13] Robinson, R. J. (2020). Structuring IS framework for controlled corporate through statistical survey analytics. Journal of Data, Information and Management, 2(3), 167-184.

[14] Spencer, R. et l. 2014. Philosophical Approaches to Qualitative Research [online]. Chicago, USA. Ecommons.luc.edu. Available From: https://ecommons.luc.edu/cgi/viewcontent.cgi?article=1109&context=socialwork_facpubs

[15] Vincent, J. (2023, 6. Februar). 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

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

[17] Will Divergent Copyright Laws Between the US and UK Influence Where You Do Business as an Artificial Intelligence Company? (2022, 8. September). JD Supra. https://www.jdsupra.com/legalnews/will-divergent-copyright-laws-between-4352051/