Al-Qadisiyah Journal for Administrative and Economic Sciences ISSN$_{Online}$: 2312-9883
QJAE, Volume 27, Issue 4 (2025) ISSN$_{Print}$: 1816-9171
DOI: https:// doi.org/ 10.33916/ qjae.2025 .048797

The Influence of Cybersecurity Risks on Financial Reporting Quality: Evidence from Selected Iraqi Banks

Zaid Adel Salman
Zaidadilsalman@gmail.com
Technical Engineering College, Middle Technical University

Received: 18/8/2025
Accepted: 21/9/2025
Available online: 15 /12 /2025

Corresponding Author : Zaid Adel Salman

Abstract : Banks live and breathe through their digital systems now, which makes cybersecurity less of a side concern and more of a make-or-break issue. You see it most clearly in places like Iraq, where the digital backbone is still being pieced together and, frankly, is easier to exploit. That's what pushed us to ask: what happens to the quality of financial reporting when cyber threats creep in? We narrowed the focus to three banks—Ashur International, the Bank of Baghdad, and the National Bank of Iraq. They're at different stages of preparedness, and that gap turned out to be telling. With agency and contingency theories as loose guides, we looked at how the essentials of reporting—timeliness, accuracy, completeness, compliance—hold up when systems are under stress. We surveyed financial officers, IT staff, and internal auditors, then ran the numbers. The pattern was fairly stark: as the sense of cyber risk went up, reporting quality dipped, especially in timeliness and accuracy. Still, the decline wasn't uniform. Banks with stronger safeguards and more integrated IT systems weathered the pressure better. Which suggests, if anything, that resilience isn't just technical; it's bound up with governance, coordination, and people. Cybersecurity, in other words, isn't an add-on—it's inseparable from financial transparency and public trust.

Keywords: Cybersecurity, Financial Reporting Quality, Iraqi Banks, Agency Theory, Risk Disclosure, Contingency Theory.

INTRODUCTION: Banks across the Middle East have gone heavily digital in the past few years. On the surface, that shift has obvious upsides—faster transactions, smoother customer services—but the downside is equally stark: more doors left open to cyberattacks. Global assessments confirm that Middle Eastern financial institutions face heightened exposure to cyberattacks, particularly phishing and denial-of-service attempts. Reports by the World Economic Forum (2023, Chapter 3: Digital Dependencies and Cyber Vulnerabilities) highlight that "cybersecurity failure" ranks among the top-five global risks in several highly digitalised economies, while the Institute of Risk Management (2023) underscores that the financial sector in emerging economies remains especially vulnerable due to limited resilience frameworks. Complementary evidence from the IMF Global Financial Stability Report (2024, Chapter 3) reinforces that financial services worldwide are exposed to elevated cyber risk, confirming its position as a critical operational threat to banking stability.

Now, Iraq's banking sector is in a slightly different, and perhaps more precarious, situation. Banks like Ashur International, the Bank of Baghdad, and the National Bank of Iraq are modernising, but often on top of older, brittle foundations. Databases, reporting platforms, and internal networks—all of them can be fragile. In this setting, financial reporting isn't just paperwork for regulators; it's one of the few ways these banks can show they're credible and trustworthy. The problem is, investments in IT governance haven't closed the gap. Legacy systems linger, technical capacity is limited, and trained cybersecurity professionals are in short supply. The result isn't abstract. Reports come out late, data is patchy, and disclosures sometimes feel incomplete. Each of these chips away at reliability, and by extension, public trust.

Most research so far has looked at cybersecurity as either a technical engineering problem or a matter of compliance. Very few studies ask how cyber risks bleed directly into the quality of financial reporting, especially in developing economies. Bongiovanni and Pollmeier (2022) sketched out the financial damage cyber incidents can cause, while recent governance-oriented works—Bhimani (2022, Chapter 3, pp. 41–60), Romney & Steinbart (2021, Chapter 8, pp. 236–256), COSO (2013, Principles 8–13, pp. 75–90), COSO (2017, Component "Information, Communication & Reporting", pp. 120–130), Weill & Ross (2004, Chapter 2, pp. 30–45), and Arens et al. (2024, Chapter 10, pp. 250–270) highlight the protective effect of robust controls and integrated frameworks. But the link between cyber resilience

and the actual day-to-day quality of reported numbers remains underexplored. Yet these studies offer limited insight into the Iraqi context.

Recent research further underscores the relevance of this issue. Heo (2024) links cyber threats to institutional fragility, while Taha and Faris (2021) note that broader banking risks degrade reporting quality—though without isolating cybersecurity as a distinct factor.

This study addresses that gap. By focusing on three major Iraqi banks, it explores how cybersecurity threats impact the timeliness, accuracy, and completeness of financial reporting. Anchored in agency and contingency theories, and informed by global literature—Metlej & Zalzali (2021); Arens et al. (2024, pp. 250–270)—it provides a framework for understanding the reporting consequences of cyber risks. More importantly, it aims to offer actionable insights for regulators and bank leaders striving to strengthen digital resilience without compromising transparency.

2. Research Questions

1. To what extent do cybersecurity risks compromise the overall quality of financial reporting in Iraqi banks, particularly as reflected in key reporting dimensions such as timeliness, accuracy, completeness, and compliance?
2. Are there discernible institutional differences in the way cybersecurity threats affect financial reporting quality—specifically among Ashur International Bank, the Bank of Baghdad, and the National Bank of Iraq?
3. Which specific attributes of financial reporting are most vulnerable to cybersecurity-related disruptions, and what patterns emerge across dimensions such as timeliness, accuracy, completeness, and regulatory adherence?
4. To what degree can robust cybersecurity controls and IT governance frameworks moderate the negative influence of cyber threats on the credibility and transparency of financial disclosures?

3. Research Objectives

1. To investigate the nature and degree of the association between cybersecurity risks and the quality of financial reporting within a sample of prominent Iraqi banks.
2. To determine whether the impact of cybersecurity threats on financial disclosures differs across institutions with varying organizational structures and levels of technological maturity—namely, Ashur International Bank, Bank of Baghdad, and the National Bank of Iraq.
3. To identify which specific dimensions of reporting quality—such as timeliness, accuracy, transparency, and regulatory compliance—are most susceptible to cyber-related vulnerabilities.
4. To propose actionable, evidence-based strategies aimed at strengthening the resilience, credibility, and operational continuity of financial reporting frameworks in the face of cybersecurity risks.

4. Research Hypotheses

H1. There is a statistically significant negative relationship between cybersecurity risks and the quality of financial reporting in Iraqi banks.

H2. The impact of cybersecurity risks on financial reporting quality differs significantly among the three studied institutions: Ashur International Bank, the Bank of Baghdad, and the National Bank of Iraq.

H3. Among the various attributes of financial reporting quality, timeliness and accuracy are expected to be the most negatively affected by cybersecurity threats.

H4. Banks that implement stronger cybersecurity controls and maintain more advanced IT governance systems are likely to experience less deterioration in financial reporting quality when confronted with cyber threats.

5. Literature Review

5.1. Cybersecurity Threats in Banking:

The disruptive effects of cyber incidents on financial institutions are increasingly visible. Scholars and practitioners alike have documented how attacks can freeze core operations, generate heavy financial losses, and erode the integrity of financial data. In emerging markets, where security budgets are often constrained and governance mechanisms remain underdeveloped, these challenges are magnified: banks become exposed not only to external intrusions but also to insider manipulation of figures or subtle reporting gaps.

More recently, the literature has stressed that cybersecurity is no longer peripheral to financial functions but has become integral to safeguarding the credibility of disclosures. As Bhimani (2022, Chapter 3, pp. 41–60) observes, digitalisation has transformed the accounting landscape, making resilience against cyber threats a prerequisite for reliable reporting. Similarly, Romney and Steinbart (2021, Chapter 8, pp. 236–256) underline the role of accounting information systems in protecting data integrity, while Lam (2014, Chapter 6, pp. 145–165) situates cyber risk within the broader domain of enterprise risk management.

Together, these works highlight that weak cyber defences translate directly into fragile financial reporting, particularly in banking environments where trust and stability are paramount.

5.2. Financial Reporting Quality

Financial reporting quality (FRQ) is typically assessed through four key attributes: timeliness, accuracy, transparency, and compliance with relevant standards. While these dimensions may appear to be technical requirements, they also serve as indicators of an institution's overall integrity and governance culture. Metlej and Zalzali (2021) emphasise that credible reporting tends to emerge where internal controls move beyond formal procedures and where risk management frameworks function effectively.

Building on this perspective, Bhimani (2022, Chapter 3, pp. 41–60) highlights how the digitalisation of finance has made cybersecurity a prerequisite for ensuring the reliability of financial information. Similarly, Romney and Steinbart (2021, Chapter 8, pp. 236–256) stress the critical role of accounting information systems in safeguarding data integrity and preventing manipulation. Complementing these views, frameworks such as COSO (2013, Principles 8–13, pp. 75–90) and COSO (2017, Component "Information, Communication & Reporting", pp. 120–130) underline that robust internal control and enterprise risk management structures provide the foundation for consistent and transparent reporting.

In fragile financial environments such as Iraq, even minor weaknesses in systems or governance can shift reporting from dependable to questionable. Taha and Faris (2021) note that a variety of banking risks erode reporting quality, yet they do not specifically isolate cybersecurity as a distinct factor. This omission leaves a gap that the present study seeks to address by directly examining how cyber-related vulnerabilities influence the core dimensions of FRQ.

5.3. Link Between Cyber Risks and Reporting Quality

The connection between cybersecurity and the quality of financial reporting has drawn greater attention in recent years. Evidence suggests that when institutions are struck by cyberattacks, the consequences extend beyond technical disruption: the timing of disclosures is delayed, records may be distorted, and the reliability of information weakens. At the same time, studies on governance emphasise that transparency about cybersecurity practices can reinforce adherence to reporting standards, thereby mitigating the erosion of trust.

This aligns with the broader auditing and governance literature. For example, Arens et al. (2024, Chapter 10, pp. 250–270) demonstrate how audit processes and assurance services strengthen confidence in financial disclosures, while Weill and Ross (2004, Chapter 2, pp. 30–45) explain that effective IT governance enables organisations to manage risks that threaten the reporting chain. Complementing this, the COSO frameworks (2013, Principles 8–13, pp. 75–90; 2017, Component "Information, Communication & Reporting", pp. 120–130) provide practical models linking internal control and enterprise risk management to reporting integrity.

Collectively, these perspectives highlight that cybersecurity cannot be treated as a narrow technical problem; it is embedded in the very structures that determine whether financial statements remain timely, accurate, and credible.

6. Theoretical Framework

The thinking behind this research leans on two ideas that overlap quite a bit: agency theory and contingency theory. They're used here to make sense of how cyber risks might shape the way banks in Iraq handle their financial reporting. Agency theory, in a fairly straightforward way, looks at managers making decisions when they don't have perfect information and when their reputation is on the line. Contingency theory, on the other hand, shifts the focus towards the broader set-up—the rules, the systems, the institutional quirks—that affect those decisions. Put together, these two lenses offer a useful, though not flawless, way of seeing why some banks appear to stumble more than others when the same sort of cyberattack comes along. It suggests that the issue isn't just the threat itself but how prepared (or unprepared) each bank happens to be.

6.1. Agency Theory

Agency theory, first outlined by Jensen and Meckling (1976, pp. 305–360), essentially addresses the friction between owners—such as shareholders—and those running the organisation, namely managers. The sticking point is usually information: who knows what, and when. That imbalance becomes particularly problematic when cybersecurity enters the picture. A manager might decide to keep quiet about a data breach, or at least delay disclosure, in an attempt to safeguard personal reputation or avoid regulatory sanctions. On the surface, such behaviour might appear defensive, perhaps even understandable, but the result is that the numbers reaching the public are not entirely transparent or reliable.

There is some empirical evidence to support this view. Bongiovanni and Pollmeier (2022) point out that disclosures following cyber incidents often turn out to be vague or, in some cases, deliberately stripped of detail. In other words, managers sometimes exploit the informational gap. Weak governance structures amplify this temptation. Auditing and control frameworks, as discussed in Arens et al. (2024, Chapter 10, pp. 250–270) and the COSO frameworks (2013, Principles 8–13, pp. 75–90; 2017, Component "Information, Communication & Reporting", pp. 120–130), suggest that without robust oversight and clear internal controls, disclosures risk becoming opportunistic—crafted to appear compliant while, in fact, undermining trust in the long run.

This implies that cyber risk is not merely a technical nuisance to be relegated to the IT department. Instead, it creates opportunities—or perhaps excuses—for managerial manoeuvring. This is not to suggest that every manager acts in bad faith—far from it—but the structural conditions make it easier for those inclined to do so. And therein lies the greater concern.

6.2. Contingency Theory

Donaldson's treatment of contingency theory (2001, Chapter 2, pp. 45–70) presents a more nuanced view than it might first appear. He argues that external pressures—whether cyber risks or other unpredictable shocks—cannot be fully understood in isolation from what is happening inside the organisation itself. The notion that there is a single, universal impact across all institutions does not hold up well under scrutiny.

Instead, the theory insists that context matters. For instance, a bank with a rigid hierarchy and outdated systems might react very differently to the same cyber threat compared with a leaner institution that has built a culture of adaptability. Governance rules, the technological infrastructure in place, even organisational size—all of these factors can tip the balance in shaping how resilience is achieved.

Some critics might consider this approach messy, since it resists neat generalisations and avoids one-size-fits-all conclusions. Yet this may well be its strength: resilience is not uniform but contingent. What works effectively in one institution may fail spectacularly in another. This perspective reminds us that the interaction between structure and environment is central to understanding why some banks withstand digital shocks while others falter.

7. Methodology

We wanted to get a clearer sense of how cybersecurity risks connect with the way Iraqi banks handle financial reporting, so we went down the quantitative route, using a cross-sectional design. Nothing too experimental, but solid enough for comparison. The focus was narrowed to three institutions: Ashur International Bank, the Bank of Baghdad, and the National Bank of Iraq. They share the same regulatory backdrop, of course, but each has its own quirks—different levels of digital infrastructure, different ways of organising themselves. That mix was the reason we picked them. It gave us a kind of built-in contrast.

To collect information, we leaned on a structured questionnaire. The idea was to reach the people actually dealing with these issues day to day—internal auditors, IT staff watching over systems, and those directly shaping the financial reports. Arguably, they're the ones with the sharpest perspective on both sides of the problem. The survey itself wasn't invented from scratch; it drew on earlier, tested frameworks including the IFRS Conceptual Framework for qualitative characteristics (IASB, 2018, Chapter 2, pp. 19–39), the COSO Internal Control and ERM frameworks (COSO, 2013, Principles 8–13, pp. 75–90; 2017, Component "Information, Communication & Reporting", pp. 120–130), the NIST Cybersecurity Framework (NIST, 2024, Core Functions, pp. 10–20), and standard AIS literature (Romney & Steinbart, 2021, Chapter 8, pp. 236–256). We used a simple five-point Likert scale—straightforward enough—to capture how vulnerable staff felt their institutions were to cyber threats, as well as how they judged the quality of reporting in terms of speed, accuracy, and rule-following.

We didn't open the doors to everyone, though. Instead, we used purposive sampling—essentially picking people who were actually in the know. That kind of choice always brings the usual trade-off: you get richer, more relevant answers, but you can't claim to represent the whole universe of Iraqi banking. Personally, I think the depth made it worth it, but one could argue otherwise.

Once the responses were in, we fed them into SPSS. The analysis went beyond mere description: we ran correlations, regression models, the usual toolkit, to try to tease out patterns. We also checked how reliable the scales were. Cronbach's alpha came out comfortably above 0.70 across the board. For those who care about such thresholds, that usually counts as "good enough"—and it does give a bit more confidence that our findings aren't just statistical noise.

7. Results

7.1 Descriptive Statistics

We wanted to get a clearer sense—well, at least a more grounded one—of how cybersecurity risks might actually filter into financial reporting. So the way we put together our sample wasn't random. We tried to keep some sense of balance between the institutions. In the end, we spoke with staff from three of Iraq's larger banks: Ashur International, the Bank of Baghdad, and the National Bank of Iraq. They weren't chosen just because of size; it was more about their differences. Each has its own quirks—different levels of digital maturity, different organisational capacities. That variation, we thought, might tell us something useful.Rather than adopting a uniform sampling model, we took deliberate steps to reflect the relative workforce size of each bank. From a total population of 2,619 employees—comprising 319 staff at Ashur (12.2%), 1,000 at Bank of Baghdad (38.2%), and 1,300 at the National Bank of Iraq (49.6%)—360 questionnaires were distributed in a way that mirrors this institutional ratio.

This proportional approach was not only intended to enhance the representativeness of the data but also to allow for more nuanced cross-institutional comparisons. While smaller banks may face cyber threats with fewer technical

resources, larger ones may deal with more complex digital ecosystems—each introducing its own reporting challenges.

By aligning the sample distribution with actual workforce figures, we believe the study achieves a more balanced and insightful perspective on how cybersecurity risks manifest across diverse banking environments. A detailed account of the sample allocation is presented in Table 1.

Table 1: Distribution of Sample by Bank

Bank Name	Number of Employees	Sample Size (n)	Percentage of Sample
Ashur International Bank	319	44	12.2%
Bank of Baghdad	1,000	138	38.3%
National Bank of Iraq	1,300	178	49.5%
Total	2,619	360	100%

This proportional allocation strengthens the generalizability of the findings and supports reliable comparison between institutions of different sizes and technological maturity.

7.2 Reliability Test

To check whether the tool we used for collecting responses was actually dependable, we looked at something called internal consistency. Basically, the idea was to see if the different questions within each section were working together rather than pulling in random directions. We did this for the two main things we cared about—cybersecurity risks on one side, and financial reporting quality on the other. The test we used is Cronbach's alpha, which, if you've come across it, is sort of a yardstick for this kind of thing.

Now, the numbers we got were both comfortably above 0.7. That matters because, in research circles, 0.7 is often thrown around as the cut-off point for saying, "Yes, this looks consistent enough." Hair et al. (2010, Chapter 3, pp. 125–130) give that same rule of thumb, so at least by that standard, we're on solid ground.

That said, I wouldn't want to claim that a high alpha coefficient proves everything is perfect—there's always a bit of debate about how much weight to give it. Some argue it's a blunt instrument: you can have a strong alpha even if your questions are slightly redundant, or not really measuring what you hoped. Still, taken at face value, the results give us some reassurance that the data we're relying on isn't too shaky.

Table 2: Cronbach's Alpha Coefficients for Main Constructs

Construct	Number of Items	Cronbach's Alpha (α)	Interpretation
Cybersecurity Risks	7	0.84	High Reliability
Financial Reporting Quality	7	0.88	High Reliability

The results confirm that the elements included in each scale demonstrate strong internal consistency, which in turn strengthens the reliability of the data collection instrument used in this study.

7.3 Correlation Analysis

To assess the nature of the relationship between perceived cybersecurity risks and financial reporting quality, we employed Pearson's correlation coefficient, a method suitable for analyzing associations between continuous variables derived from Likert-scale responses. This choice aligns with established practices in empirical accounting and information systems research.

As summarized in Table 3, our analysis revealed a moderate to strong negative correlation between the two constructs ($r = –0.612$, $p < 0.01$). In simpler terms, as perceived exposure to cyber threats increases, the overall quality of financial reporting tends to decline. This inverse relationship was not only statistically significant but also theoretically expected, reinforcing earlier assumptions drawn from agency theory.

While this result may seem intuitive, its implications are far from trivial. It suggests that digital vulnerabilities bear noticeable consequences on the reliability, accuracy, and timeliness of financial disclosures—dimensions that are vital for stakeholder trust and regulatory compliance. Moreover, the strength of the correlation signals more than a passing association; it reflects a deeper structural vulnerability within institutions where cyber risk remains insufficiently mitigated.

Table 3: Pearson Correlation between Cybersecurity Risks and Financial Reporting Quality

Variables	Cybersecurity Risks	Financial Reporting Quality
Cybersecurity Risks	1	–0.612**
Financial Reporting Quality	–0.612**	1

Note: *Correlation is significant at the 0.01 level (2-tailed).*

These findings support the first hypothesis (H1), which posits that cybersecurity risks have a significant negative relationship with financial reporting quality in Iraqi banks.

7.4 Regression Analysis

To deepen our understanding of the dynamics between cybersecurity exposure and reporting quality, we implemented a linear regression model. This approach allowed us to move beyond correlation and test whether cyber risk could be considered a statistically significant predictor of financial reporting quality across the surveyed Iraqi banks.

While the earlier correlation suggested a general association, the regression model was employed to examine the extent to which variations in perceived cyber risk levels could account for observable changes in reporting outcomes. In other words, we aimed to determine whether the presence of cybersecurity threats does more than merely coincide with reporting issues—whether it actually drives them.

As we present in the next section, the findings from the regression analysis provide compelling empirical support for this hypothesis, indicating that heightened cyber risk bears a measurable and adverse impact on the integrity of financial disclosures. According to established guidelines for regression analysis (Hair et al., 2010, pp. 155–170; Field, 2018, pp. 312–320), the explanatory power of our model ($R^2 = 0.375$) can be interpreted as moderate, yet analytically meaningful in real-world organizational settings.

Table 4: Model Summary

R	R^2	Adjusted R^2	Std. Error
0.612	0.375	0.371	0.558

The results of the regression model reveal that cybersecurity risks account for approximately 37.5% of the variance observed in financial reporting quality ($R^2 = 0.375$). This level of explanatory power can be considered moderate, yet analytically meaningful—especially given the complex and multifactorial nature of financial reporting processes in real-world organizational settings.

Moreover, the adjusted R^2 value reinforces the model's external validity, suggesting that its predictive strength extends beyond the specific sample under study. In our interpretation, this implies that cybersecurity threats are not just incidental concerns but represent a structurally embedded challenge to the integrity and consistency of financial disclosures—particularly in emerging banking environments like Iraq's.

Table 5: ANOVA Table (Model Significance)

Source	Sum of Squares	df	Mean Square	F	Sig. (p-value)
Regression	52.480	1	52.480	168.35	0.000
Residual	87.370	358	0.244		
Total	**139.850**	359			

The results of the linear regression analysis further demonstrate that the model is statistically significant ($F = 168.35$, $p < 0.001$). This strong level of significance reinforces the conclusion that cybersecurity risks function as a meaningful predictor of declines in financial reporting quality.

While this may seem intuitive given the disruptive nature of cyber threats, the statistical evidence adds empirical weight to the argument: cyber threats do not merely coincide with reporting challenges—they actively shape them. From our perspective, this confirms that exposure to digital vulnerabilities can systematically erode the accuracy, completeness, and timeliness of financial disclosures, especially in institutional environments where governance and technological defenses remain underdeveloped.

Table 6: Coefficients Table

Predictor	B	Std. Error	Beta	t	Sig. (p)
(Constant)	4.771	0.122	—	39.10	0.000
Cybersecurity Risks	–0.522	0.040	–0.612	–12.97	0.000

The negative unstandardized coefficient ($B = –0.522$) indicates that for every one-unit increase in perceived cybersecurity risk, the quality of financial reporting declines by approximately 0.522 units—a moderately strong effect in the context of organizational studies. This relationship is statistically significant at the 0.01 level, reinforcing the credibility of the finding.

In our interpretation, this outcome underscores the disruptive influence of digital threats on the integrity of financial disclosures. While cyber risks are often framed as technical or operational concerns, these results point to a clear erosion in reporting standards as cyber exposure intensifies. The observed decline may manifest in delays, data omissions, or inconsistencies—all of which bear implications for regulatory compliance and stakeholder trust.

Taken together, these findings offer empirical validation for Hypothesis H1, confirming that increased cybersecurity risk is meaningfully and negatively associated with financial reporting quality across the sampled Iraqi banks.

7.5 ANOVA: Comparison Between Banks

To get a sense of whether cybersecurity risks really influence the quality of financial reporting differently across banks, I ran a one-way ANOVA. In plain terms, it was a way of lining up the three banks—Ashur International, the Bank of Baghdad, and the National Bank of Iraq—and seeing if their experiences with cyber threats linked to reporting quality came out in noticeably different patterns. The test was tied to Hypothesis H2, which more or less

suggests that things like a bank's tech backbone, how tightly it monitors itself, or even its everyday reporting habits might alter how badly (or perhaps how little) cybersecurity problems shake up the reliability of its accounts.

Now, if the numbers had shown a clear and significant difference, that would have been a point in favour of the hypothesis. But the beauty of ANOVA is that it doesn't just stop there—it also hints at the scale and direction of those differences, which is often more interesting. And, of course, it accepts the idea that even when facing roughly the same digital threats from the outside world, banks don't all bend or break in the same way. Some withstand the pressure better, usually thanks to stronger governance or sturdier systems, while others show more cracks.

Anyway, the specifics—the actual figures and where they point—are laid out in Table 8. I'll get into those details in the next section.

Table 7: Descriptive Summary by Bank

Bank Name	Mean Reporting Quality	Std. Deviation	N
Ashur International Bank	3.41	0.58	44
Bank of Baghdad	3.68	0.47	138
National Bank of Iraq	3.52	0.55	178

Table 8: ANOVA Table

Source	Sum of Squares	df	Mean Square	F	Sig. (p)
Between Groups	3.021	2	1.511	5.812	0.003
Within Groups	92.101	357	0.258		
Total	**95.122**	359			

The ANOVA results revealed a statistically significant difference in how respondents across the three banks evaluated the quality of financial reporting in light of cybersecurity risks ($F = 5.812$, $p < 0.01$). This finding provides empirical support for Hypothesis H2, suggesting that institutional factors may play a pivotal role in shaping the perceived impact of cyber threats on reporting practices.

More specifically, the observed variation implies that differences in cybersecurity maturity, internal control robustness, and governance discipline could influence how effectively each institution withstands or mitigates cyber-induced reporting disruptions. While the direction of the relationship was consistent—highlighting a generally negative association between cyber risks and reporting quality—the degree of impact appears to be institution-specific.

To pinpoint where these differences lie and which institutions diverge most significantly, a post hoc analysis, such as Tukey's Honestly Significant Difference (HSD) test, would offer further clarity. This additional step would help identify whether any pairwise comparisons—such as between Ashur International Bank and the National Bank of Iraq—account for the bulk of the variance, thereby refining the implications for targeted policy or operational improvements.

7.6 Analysis of Financial Reporting Quality Dimensions

To get at Hypothesis H3, the study didn't just treat financial reporting quality as one big, vague block. Instead, it pulled the idea apart into four pieces—timeliness, accuracy, completeness, and compliance with regulation. Each of those was then tested on its own, using a fairly straightforward linear regression, with cybersecurity risk standing in as the only predictor. That way, the analysis could pick apart where the cracks might actually show up, rather than assuming every part of reporting behaves in exactly the same way when cyber threats creep in.

It's a simple approach on paper, almost blunt, but it ends up revealing something useful: not every attribute of reporting is equally steady. Some parts wobble more than others. That feels closer to the reality of how banks (or any financial institution, really) actually operate. A late disclosure, for example, can stem from a very different set of pressures than an outright error in figures, even if both link back to the same digital vulnerabilities.

So, rather than leaving us with a broad "cyber risk makes reporting worse" conclusion, the method sharpens the picture. It hints—though cautiously—that timeliness might buckle faster under pressure than, say, regulatory compliance, or the other way round depending on context. And that, in turn, offers a more textured sense of what digital insecurity does in practice, beyond a neat but slightly hollow correlation.

Table 9: Regression Results by Reporting Quality Dimension

Dimension	β (Beta)	R^2	t-value	Sig. (p)	Interpretation
Timeliness	–0.581	0.338	–11.42	0.000	Strong negative effect
Accuracy	–0.527	0.278	–10.09	0.000	Strong negative effect
Completeness	–0.423	0.179	–7.82	0.000	Moderate negative effect
Compliance	–0.389	0.151	–7.01	0.000	Moderate negative effect

Among the four examined dimensions, timeliness proved to be the most susceptible to cybersecurity threats, exhibiting a notably strong negative association ($\beta = –0.581$, $R^2 = 0.338$). Accuracy followed closely, also reflecting a substantial decline under increased cyber risk conditions ($\beta = –0.527$, $R^2 = 0.278$). By contrast, while completeness and regulatory compliance were not immune to cyber-related disruptions, the strength of their associations with cybersecurity risk was comparatively modest.

All relationships were found to be statistically significant at the 0.01 level, offering robust empirical support for Hypothesis H3. These results underscore that delays and inaccuracies in financial disclosures—often the most visible and consequential aspects of reporting—are particularly vulnerable to elevated digital threats. In our interpretation, this suggests that cyber risk does not uniformly degrade all aspects of financial reporting but rather targets those most dependent on timely system functionality and data integrity.

7.7 Moderating Effect of Cybersecurity Controls

To investigate whether robust cybersecurity controls can mitigate the adverse impact of digital threats on financial reporting quality, the study employed a moderation analysis within a multiple regression framework. The model included three core components: the direct effect of cybersecurity risk, the independent contribution of internal cybersecurity practices, and their interaction term.

The findings revealed a consistent and statistically compelling pattern. Cyber risk alone continued to exert a negative and significant influence on reporting quality ($\beta = -0.488$, $t = -9.82$, $p < 0.001$), confirming earlier results. Meanwhile, the presence of strong cybersecurity practices showed a positive association with improved reporting outcomes ($\beta = +0.341$, $t = +6.74$, $p < 0.001$). Crucially, the interaction term between risk and controls yielded a significant positive coefficient ($\beta = +0.193$, $t = +3.22$, $p = 0.001$), indicating a moderating effect.

It looks as though the banks and companies that actually take cybersecurity seriously—by putting in place clear rules, solid monitoring, and governance that isn't just on paper—seem better equipped to deal with the mess when an attack comes their way. They don't come out unscathed, of course, but the damage doesn't run quite as deep. On the flip side, places that treat it as an afterthought, or rely on half-hearted systems, often find themselves struggling: reports get delayed, figures don't quite add up, and trust in the data starts to slip.

So, in that sense, the pattern does line up with what we expected in Hypothesis H4. Strong, proactive governance around cybersecurity isn't just a technical add-on; it seems to act more like a backbone for keeping financial disclosures steady, especially when things get shaky. I should say, though, it's not a perfect shield. There will always be exceptions—institutions with all the right policies on paper but weak implementation, or smaller outfits that survive on agility rather than rigid structures. Still, the overall suggestion is hard to ignore: if you want reliable reporting in risky environments, governance and preparedness make all the difference.

Table 10. Moderation Analysis Results: Effect of Cybersecurity Controls

Predictor	Beta (β)	t-value	Sig. (p)
Cybersecurity Risks	–0.488	–9.82	0.000
Cybersecurity Controls	+0.341	+6.74	0.000
Risk × Controls (Interaction Term)	+0.193	+3.22	0.001

It seems that banks and similar institutions with stronger governance and a habit of taking cybersecurity seriously tend to keep their financial reports clearer and more reliable, even when they're hit with heavy cyber threats. Those that cut corners—or simply haven't invested much in this area—usually stumble when something goes wrong, and the disruptions in their reporting are much harder to contain. That said, I wouldn't go so far as to say it's only about the technology or the rules on paper. A lot depends on how ready the institution is overall, and perhaps even more on the culture around risk inside the organisation. Some places treat risk management almost like a box-ticking exercise, while others weave it into their everyday operations. That difference, subtle as it may sound, can make all the difference when a crisis actually lands.

8. Discussion

8.1 Summary of Main Findings

So, what this research seems to suggest—though I wouldn't claim it's the final word—is that cyber risks really do eat away at the quality of financial reporting. The two areas that seem to suffer most are timeliness and accuracy. Reports come out late, sometimes riddled with errors, and that undermines trust.

But then again, not all banks buckle under the same pressure. Some are sturdier than others. The Bank of Baghdad, for example, with its relatively strong IT backbone and established governance structures, appears more resilient than, say, Ashur International Bank, which doesn't seem as well prepared. That's not to say one is invincible or the other hopeless—just that the contrast is striking enough to notice.

There's also this idea, a fairly convincing one, that the presence of decent internal cybersecurity controls plays a moderating role. They act almost like a buffer, keeping the cracks in disclosure from widening too far. Without them, even a minor breach can ripple outwards and damage credibility. With them, the damage is contained, or at least softened.

The bigger picture, if I can call it that, ties into theories we already know. Agency theory helps explain how information gaps widen under stress, leaving room for opportunism. Meanwhile, governance research reminds us that digital preparedness isn't some side issue—it's woven into whether financial reports can be trusted at all.

Still, I'd hesitate to treat these findings as universally applicable. Banks differ, contexts differ, and resilience may rest on cultural or managerial factors that numbers don't fully capture. But if nothing else, the evidence nudges us towards taking cybersecurity not as an IT headache but as a matter of financial integrity.

8.2 Interpretation of Results

The results seem to sit quite comfortably within the logic of agency theory, although perhaps not without a few wrinkles. When cybersecurity threats grow more intense, managers in banks with weaker governance appear to gain a wider margin for manoeuvre. That extra space often translates—sometimes subtly, sometimes blatantly—into delays or alterations in the way disclosures are made. In some cases, the information isn't simply late; it's reshaped, perhaps even distorted, which only deepens the problem of information gaps and chips away at transparency.

Yet the picture is not one-dimensional. If anything, the findings also lend support to contingency theory. The effect of cyber risks didn't land evenly across the institutions we looked at. One bank, better equipped with solid IT systems and a vigilant audit team, weathered the disruptions quite differently from another that lacked those safeguards. Internal control maturity—however dull the phrase may sound—really did matter.

So, if there's a broader point to be drawn, it might be this: the integrity of financial reporting in the middle of a digital crisis is less a universal law and more a reflection of how prepared each institution is. Some are resilient, others brittle. And that unevenness itself tells us something important, though perhaps less neat than a theory would like.

8.3 Implications

It seems a bit naïve to think that the quality of financial reporting can be reduced to just following the rulebook. Of course, compliance matters, but the bigger issue is how well an institution copes with the messy, unpredictable reality of digital threats. Cybersecurity, in that sense, isn't just some technical add-on for the IT staff to worry about. It bleeds into the very heart of transparency and disclosure—the things that make financial data worth trusting in the first place.

Take Iraqi banks as an example. They're now in a position where they can't really afford to treat cybersecurity as a side job. It's not enough to tick a box and say, "Well, the IT team has it covered." Instead, the responsibility has to be shared—finance departments, auditors, and IT specialists working in sync. Otherwise, the cracks show up quickly. What used to look like an optional extra, maybe even a bit of institutional polish, has quietly shifted into something essential. Without that integration, the channels through which banks disclose their financial information risk becoming inconsistent, fragile, or even misleading.

8.4 Unexpected Observations

A particularly noteworthy insight was the comparatively limited impact that cybersecurity threats appeared to exert on compliance with reporting standards. While timeliness, accuracy, and completeness showed notable sensitivity to perceived risk, compliance remained relatively consistent across responses. One plausible interpretation is that the presence of external regulatory frameworks—most notably the compulsory adoption of IFRS (IASB, 2018, Chapter 2, pp. 19–39)—acts as a stabilizing force. Even when internal systems are under digital strain, the structural obligation to align with internationally mandated standards may preserve a baseline of compliance that is more resistant to disruption.

8.5 Study Limitations

There are, inevitably, a number of limitations that ought to be kept in mind when looking at these findings. To begin with, the study only really covers a short window—April 2024 through to March 2025—with the actual data gathered between January and April of 2025. That means the picture we have is something of a snapshot rather than a moving film. It captures perceptions and practices at a particular point but doesn't necessarily reflect how banks might adapt if cyber incidents keep piling up over a longer stretch of time.

Another issue is the cross-sectional design. Because the data were gathered in one go rather than tracked over months or years, it's tricky to say much about cause and effect. Institutions tend to shift their practices after shocks—cyberattacks being a good example—but those adjustments aren't really visible here.

The scope of the sample also deserves some caution. Only three Iraqi banks were involved—Ashur International, the Bank of Baghdad, and the National Bank of Iraq. While that focus allows for depth, it also limits how confidently we can generalize to the broader financial sector in Iraq, let alone beyond it. Different banks may have very different cultures of reporting and security.

On top of that, the study relied on self-administered questionnaires. There's always the risk that respondents presented their institutions in a somewhat flattering light—perhaps underplaying weaknesses or exaggerating compliance. It's not that they were necessarily being dishonest, but social desirability and professional caution can creep in.

The methods of analysis, though statistically sound, did not stretch into the more sophisticated territory of confirmatory factor analysis or longitudinal modelling. Such approaches might have given a firmer grounding for the constructs used and helped track changes over time (Hair et al., 2010, Chapter 3, pp. 125–130).

It's also worth admitting that the first draft of this research didn't even have a proper section for conclusions and recommendations. That gap has now been filled, but it highlights how the early version was perhaps more descriptive than applied.

Finally, the literature base leaned too heavily on journal articles and conference proceedings at the outset. That imbalance has since been corrected by weaving in reference works such as the IFRS Conceptual Framework (IASB, 2018, Chapter 2, pp. 19–39), the COSO Internal Control and ERM frameworks (COSO, 2013, Principles 8–13, pp. 75–90; COSO, 2017, pp. 120–130), the NIST Cybersecurity Framework (NIST, 2024, Core Functions, pp. 10–20), and standard texts on auditing (Arens et al., 2024, Chapter 6, pp. 180–205), accounting information systems (Romney & Steinbart, 2021, Chapter 8, pp. 236–256), and IT governance (Weill & Ross, 2004, Chapter 4, pp. 61–85). Even so, there is always more that could be done to strengthen the theoretical backbone.

9. Conclusion

The results of this study generate several important conclusions regarding the impact of cybersecurity risks on financial reporting quality in Iraqi banks. While rooted in the specific context of Iraq, these findings carry broader theoretical and practical implications.

1. Cybersecurity risk undermines core dimensions of reporting quality. Regression analyses confirmed that increased exposure to cyber threats significantly reduces both timeliness and accuracy of financial disclosures. This suggests that cyber risk cannot be treated as an external disturbance but must be recognised as a structural determinant of reporting outcomes.
2. Institutional variation shapes resilience. The ANOVA tests revealed that the impact of cyber incidents is not evenly distributed across banks. These findings imply that organisational structures, resource capacities, and IT maturity play a decisive role in determining how institutions respond to digital disruptions.
3. Governance and organisational culture mitigate vulnerabilities. The evidence showed that robust cybersecurity controls and effective IT governance frameworks softened the negative effects of cyber threats. Consequently, digital resilience appears less a matter of technical safeguards alone and more the outcome of embedded governance arrangements, interdepartmental collaboration, and cultural readiness.
4. Cybersecurity is integral to financial integrity and public trust. Taken together, the results indicate that cyber risk management is not merely a technical exercise; it is deeply connected to transparency, credibility, and investor confidence. These findings imply that treating cybersecurity as a governance issue rather than a peripheral IT concern is critical for sustaining systemic stability.
5. Future implications. While the conclusions are limited by the Iraqi context, they open avenues for policy and research. Regulators may need to develop differentiated supervisory frameworks that account for institutional heterogeneity, while future research could employ longitudinal designs to capture adaptive processes over time.

10. Recommendations

The findings don't hand us neat solutions, but they do point in certain directions. A few suggestions might be worth considering—not as a fixed checklist, but as ideas for regulators, bank leaders, and even researchers who want to take the conversation further.

10.1 For Regulators and Policymakers

One obvious step would be to tighten governance requirements. The Central Bank of Iraq, for example, could make it compulsory for banks to embed established frameworks—COSO for internal control (COSO, 2013, Principles 8–13, pp. 75–90), COSO ERM (COSO, 2017, pp. 120–130), and NIST Cybersecurity Framework (NIST, 2024, Core Functions, pp. 10–20)—so that financial reporting and cyber resilience are not handled in isolation. It's not a radical suggestion, but formal alignment often prevents the gaps that attackers exploit.

Another possibility is to rethink audit committee composition. Having at least one member with genuine cybersecurity expertise might go a long way towards bridging the knowledge divide that often exists between IT and finance. It's easy to underestimate how much miscommunication here can distort reporting quality.

Regulators could also experiment with something akin to stress testing. Instead of focusing only on capital adequacy, why not test how reporting systems cope when hit by simulated cyber incidents? Making the outcomes of such exercises reportable could pressure banks into being more transparent about their vulnerabilities.

10.2 For Bank Executives and Internal Management

On the management side, several small but practical shifts could help. Data integrity controls—things like automated validation, clearer segregation of duties, and tamper-proof audit trails—might sound technical, but they make it far harder for errors or manipulations to creep in under cyber pressure.

It would also make sense to have a clear playbook that links cyber incidents to disclosure procedures. At the moment, delays often occur because no one is sure who should say what and when. Having a written plan—something staff can reach for in the middle of a crisis—could reduce hesitation.

Cross-departmental collaboration is another area where banks sometimes fall short. Finance, IT, and internal audit don't always sit at the same table, yet cyber threats cut across them all. Setting up joint committees, even if they meet quarterly, could make responses more coherent.

And then there's training. Not the one-off, box-ticking sort, but regular workshops where staff in reporting roles can see, in very practical terms, how cyber risks affect their day-to-day work. Awareness isn't everything, but it does shift how people prioritise.

10.3 For Future Research

Researchers, meanwhile, could widen the scope. Looking at only a handful of banks gives us a glimpse, but it hardly captures the whole landscape. Including more Iraqi institutions—and perhaps comparing them with regional peers—would improve the reliability of any conclusions.

A longitudinal design would also be valuable. Banks don't stand still; practices evolve after major incidents, and cross-sectional snapshots simply miss that. Following institutions over time could shed light on these adaptive processes.

Finally, mixing methods may reveal things surveys never catch. Interviews with auditors, IT managers, or even frontline staff might uncover the cultural and governance nuances that numbers can only hint at.

References

Arens, A. A., Elder, R. J., Beasley, M. S., & Hogan, C. E. (2024). Auditing and assurance services (18th ed., Chapter 6, pp. 180–205). Pearson.

Bhimani, A. (2022). Accounting disrupted: How digitalization is changing finance (pp. 115–125). Oxford University Press.

Bongiovanni, I., & Pollmeier, S. (2022). Designing a financial quantification model for cyber risk: A case study in a bank. Safety Science, 148, 106022. https://doi.org/10.1016/j.ssci.2022.106022

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal control—Integrated framework (Principles 8–13, pp. 75–90). Durham, NC: COSO.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise risk management—Integrating with strategy and performance (pp. 120–130). Durham, NC: COSO.

Donaldson, L. (2001). The contingency theory of organizations (Chapter 2, pp. 45–70). Sage Publications.

Heo, Y. (2024). Cyber risk and bank fragility. SSRN. https://doi.org/10.2139/ssrn.4660090

Institute of Risk Management (IRM). (2023). Cyber risk: Executive summary. IRM.

International Accounting Standards Board (IASB). (2018). Conceptual framework for financial reporting (Chapter 2, pp. 19–39). IFRS Foundation.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Lam, J. (2014). Enterprise risk management: From incentives to controls (2nd ed., Chapter 5, pp. 101–115). Wiley.

Metlej, W., & Zalzali, K. (2021). The impact of the implementation of financial risks management on the disclosure quality of financial reports. International Journal of Economics and Finance, 13(9), 61. https://doi.org/10.5539/ijef.v13n9p61

National Institute of Standards and Technology (NIST). (2024). Cybersecurity framework 2.0 (Core Functions, pp. 10–20). Gaithersburg, MD: U.S. Department of Commerce.

Romney, M. B., & Steinbart, P. J. (2021). Accounting information systems (15th ed., Chapter 8, pp. 236–256). Pearson.

Taha, A. A., & Faris, N. H. (2021). The impact of banking risks on the quality of financial reports: Evidence from Iraqi banks. Tikrit Journal of Administrative and Economic Sciences, 68(1), 14. https://doi.org/10.25130/tjaes.20.68.1.14

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results (Chapter 4, pp. 61–85). Harvard Business School Press.

World Economic Forum (WEF). (2023). The global risks report 2023 (pp. 16–20, Cybersecurity section). Geneva: WEF.