# Incident Report and Information Assurance Plan for QIR, LLC

Harold Vernon

Old Dominion University

CS465_26975

Professor Charles Cartledge

April 27, 2025

## Abstract

This report seeks to critically examine the data breach at QIR, LLC by looking at the incident's causes and consequences. After that examination, a vulnerability assessment will be provided and a threat matrix will be crafted and proposed to prioritize risks. In addition to those two measures, a communications plan is to be outlined to manage messaging both internal and external to prepare for the prospect of future breaches. Finally, recommendations to prevent incidents such as this from recurring are to be presented. This report is intended for the senior leadership of QIR, LLC, - especially the Chief Executive Officer – to supplement informed decision making in regards to information assurance policies.

## Table of Contents



## List of Tables

## Summary of What Happened

The incident happened when QIR, LLC experienced a cybersecurity breach that resulted in unauthorized access to internal communications and confidential information. This access was then used to publicly disclose these company secrets, directly harming the company's financial performance. This breach was carried out no doubt by external threat actors who had gained access to restricted systems and then used said access to expose sensitive data and harm QIR, LLC's competitive stance.

The data leaked by the breach directly exposed the Inconsistencies between QIR's public statements and internal communications to be exposed to the public. This created widespread public backlash that has damaged the company's reputation and led to a downturn in company performance. This backlash has been spearheaded by various media outlets which have further damaged QIR, LLC's public standing. Due to both the leaked data itself and the consequences of the leak, stakeholders have begun questioning the credibility and viability of QIR, LLC. This could potentially lead to a sharp downturn in investor confidence and stock prices as they relate to QIR, LLC.

The details of the breach clearly indicate failures in QIR's information assurance policies, system access controls, and incident detection capabilities. This crisis must be handled through a twofold approach: firstly to mend public relations and secondly to strengthen QIR's cybersecurity posture. To mend public relations, there should be some token terminations of the worst offenders found in the leaked communications as well as heavy publicization of QIR's cybersecurity efforts. The cybersecurity efforts themselves should involve a reassessment of vulnerabilities, the implementation of new policies, and a review of preexisting capabilities. Failure to do so could possibly doom the company.

## Background of the Organization

QIR, LLC is a small private company in a highly competitive market where the maintenance of proprietary information is absolutely essential to securing economic advantages. As is the case with many other organizations, QIR's business model relies a great deal on its ability to ensure the confidentiality of internal communications, trade secrets, and strategic plans – as well as secure its intellectual property. The company's ventures in research, development, and client services all involve sensitive data that could erode QIR LLC's market position as the recent incident clearly shows.

QIR LLC is responsible for delivering products and services to a wide range of clients. In doing this, it must ensure the integrity and confidentiality of all communications and transactions. Sensitive client data, proprietary research information, and internal business strategies are all handled by QIR LLC – all of which are valuable assets both to QIR LLC and potentially its competitors. QIR LLC has obligations to the law, the public, and its stakeholders to ensure honesty and accuracy in its public statements so as to not mislead investors or consumers.

The intellectual property held by QIR LLC is extensive. It includes proprietary processes, trade secrets, and even some patented technologies and methods key to the company's competitive advantage. Safeguarding these intellectual assets is not only a matter of legal compliance, but also one of ensuring the company's continual market advantage. Unauthorized access, proliferation, or replication of these information assets by external actors could result in further financial losses and damage to the company's reputation.

In addition to the assets directly held by QIR LLC, the company also has several strategic and organizational alliances that must be considered when constructing a profile. It maintains

partnerships with several suppliers, vendors, research collaborators, and long-running customers. Every organization that engages with QIR LLC trusts that QIR LLC can safeguard sensitive information. A breach of QIR LLC's systems, therefore, not only threatens the company itself but its partners too. This could lead to legal complications in addition to the direct harm to QIR LLC. It is necessary for the company's success that the trust placed in it by these external entities is maintained and – when breached – restored as soon as possible.

QIR LLC does not appear to have an impressive history in terms of cybersecurity practices and doctrines. In the past, it has been known to make misleading public statements in order to hide its internal activities. There are arguments that can be made for the necessity of such moves from a business perspective, but it is an objective fact that these misleading statements could lead to significant hardships when exposed. This is especially true should they be exposed through unauthorized access gained by malicious actors. Exposing these misleading statements can lead to a cascade effect as QIR LLC gains a reputation as a lying company. This reputation makes it significantly less attractive to investors, partners, and customers.

Within its operational structure; QIR LLC's internal communications systems, customer databases, intellectual property repositories, and financial systems should all be considered critical assets. Cybersecurity principles state that the confidentiality, integrity, and availability of these systems is a vital function. The recent breach, however, shows that QIR LLC has not been adhering to these principles. Generally, from what can be deduced from the description of the breach and the related documents provided, QIR LLC's cybersecurity policy failed to meet industry standards. It is a fact that QIR LLC has a history of making statements contradictory to publicly available information. This shows a general disregard for standards and regulations in regards to company conduct.

## Consequences of the Breach

The information breach has had severe and far-reaching consequences for the company, its market performance, and its public reputation. While unauthorized access is a serious situation in and of itself, the disclosure of information indicating inconsistencies between QIR LLC's public messaging and private discussions has led to media scrutiny, public distrust, and stakeholder uncertainty. All of this culminating in a situation directly harmful to the company and its future financial prospects.

It is expected that QIR LLC will experience significant losses as a direct result of this leak of information. Stakeholder unease will lead a significant number to abandon QIR LLC. It is also projected that QIR LLC will lose numerous investors, as they feel that investing in the company is a poor decision due to the increase in media scrutiny. This will lead directly to stock devaluation and capital devaluation which could have harsh consequences for QIR LLC as a publicly traded company.

In addition to the severing of investor confidence, it is also projected that the data breach will have significant operational consequences. Strategic partners, vendors, and clients may feel pressured by the breach and its consequences to terminate their cooperation with QIR LLC due to concerns about the security of their data in QIR LLC's hands. The breach has exposed a multitude of critical weaknesses in QIR LLC's information assurance policies and systems which require immediate attention from cybersecurity teams – attention that will cost money. In addition, the breach may lead to a decline in internal morale as employees questioning the company's leadership and prospects. Lastly, the breach could carry legal consequences with it depending on what data was exposed and how it was being stored.

## Vulnerability Assessment

The data breach at QIR LLC exposed several vulnerabilities across the organization on multiple levels – namely its technical, procedural, and organizational structures. A comprehensive assessment of the company's vulnerabilities reveals several critical weaknesses. It is imperative that these weaknesses be addressed to prevent further incidents and to restore the trust of investors and customers.

Firstly, the internal communications systems used by QIR LLC are themselves a critical vulnerability. These systems handle sensitive operational, strategic, and client-related data which should be treated with caution by organizations entrusted with them. However, QIR LLC failed to implement sufficient encryption, access control, and information monitoring systems to protect these data. Given the sensitivity of the data mentioned, confidentiality and integrity of internal communications can be classified as critical to QIR LLC's operations.

Secondly, QIR LLC did not adequately protect customer databases and repositories of sensitive client information. Due to QIR LLC's lack of authentication protocols and intrusion detection systems, unauthorized and malicious actors were able to gain access to confidential customer data. These assets are a key part of QIR LLC's business model, as is the trust placed in QIR LLC to maintain them securely. Any breach of this trust or of the assets' security is a direct threat to QIR LLC's financial operations. Because of this, customer information systems must be classified as critical assets requiring immediate application of data security protocols.

Thirdly, intellectual property is another area of high vulnerability. QIR LLC's intellectual property – its confidential methods and patents as well as its proprietary research and trade secrets – are critical to its success as a business. In fact, it could be considered to be the

foundation of QIR LLC's competitive advantage. A breach of intellectual property harms QIR LLC's advantage by giving competitors access to its trade secrets or the ability to replicate its innovations. Thus, the company's intellectual property must also be considered a critical asset.

Fourth, QIR LLC's financial management systems also play a vital role in the company's functions. These systems are responsible for processing transactions, receiving payments, and managing operational expenses. A data breach could mean exposing these systems to unauthorized access and tampering. This could allow threat actors to steal money directly from QIR LLC. The confidentiality, integrity, and availability of financial systems are therefore paramount for the organization's operations. These systems must then be classified as critical assets.

In addition to the technical vulnerabilities outlined previously, the breach was also caused by organizational weaknesses within QIR LLC. The company does not appear to have sufficiently trained its employees in cybersecurity best practices. As a result, this leaves it vulnerable to social engineering attacks such as phishing and impersonation of authority figures. This lack of cybersecurity training might also lead to employees selecting weak passwords or downloading suspicious files. While these failures to follow cybersecurity best practices may be considered ancillary vulnerabilities, they do act as risk multipliers and should therefore be addressed by QIR LLC.

The breach demonstrates general failure to adhere to cybersecurity principles. Confidentiality was broken through unauthorized data access, integrity was compromised through the exposure of inconsistent messaging, and availability is endangered by the potential for future disruptions. As demonstrated in this assessment, cybersecurity correction measures are urgently needed for the sake of QIR LLC as an organization.

## Threat Matrix Risk Analysis

Table 1: Information Assurance Threat Matrix

| Threat | Vulnerability Targeted | Likelihood | Impact | Risk Rating | Recommendations |
|---|---|---|---|---|---|
| External Hackers | Internal Communications Systems | 5 | 4 | 20 | Encrypt communications |
| Insider Threat | Intellectual Property Repositories | 3 | 5 | 15 | Implement need-to-know controls |
| Phishing Attack | Employee Credentials | 4 | 3 | 12 | Conduct cybersecurity training |
| Data Leak | Financial Systems | 2 | 5 | 10 | Apply strict auditing controls |

To put the situation described thus far into easier to understand terms, an information assurance threat matrix was constructed based on the vulnerability assessment conducted prior. The threats identified were evaluated according to likelihood of occurrence and potential impact on organizational assets. The risk rating was calculated by multiplying likelihood and impact scores on a scale of one to five, allowing prioritization of risks requiring immediate action.

Shown on the matrix are several significant threats, such as hackers targeting internal communications and insiders compromising intellectual property. Phishing attacks are an example given of ways that employees can be socially engineered by threat actors into handing over their credentials. This is considered a credible risk due to the present lack of cybersecurity training. While financial systems vulnerabilities are less likely, they would have catastrophic consequences if exploited.

As seen in this assessment, QIR LLC's main vulnerabilities lie in its internal systems and its handling of human factors. Mitigation actions must be taken immediately that focus on strengthening technical safeguards, enforcing access controls, and initiating cybersecurity training. Resources should be prioritized for high-risk areas, as those vulnerabilities will have to be handled as soon as possible in order to restore stakeholder confidence and ensure QIR LLC's future success.

## Communications Plan

Effective communication is an essential part of any cybersecurity plan, but this is especially true when responding to a crisis such as the recent data breach experienced by QIR LLC. A well-defined, easy to understand communications plan is vital to ensuring the efficient and accurate flow of relevant information to where it is needed. This is necessary to avoid delays caused both by confusion and by a slow dissemination of information to relevant parties. Outlined below are the key stakeholders involved, the communication channels to be used, and the messaging protocols to be followed – particularly during and after a data breach.

Internally, the first party that is to be notified of a breach is the Incident Response Team. The Incident Response Team (IRT) includes the Chief Information Assurance Officer (CIAO), Information Technology Security (ITS) personnel, Legal Counsel (LC), and members of senior management. The CIAO is to serve as the chief coordinator and spokesperson within QIR LLC. They are to be tasked with processing data gathered by the Information Technology (IT) team and gathering this data in a way that can be communicated to executive leadership. Employees are to be regularly updated with easy-to-understand communications through secure channels such as encrypted email services or a company portal in order to prevent the seeding of misinformation and rumors pertaining to matters of security. This should include information about the nature of the breach, the IRT's projected course of action, and what employees can do to help in both recovery and prevention.

In external communications, it is necessary that QIR LLC remain transparent with key stakeholders. Stakeholders include entities such as customers, partners, investors, regulative authorities, and the media. These communications must be maintained in order to both uphold QIR LLC's reputation and ensure the legality of QIR LLC's operations. External

communications are to be managed by the Chief Communications Officer (CCO) in close collaboration with the CIAO and LC. The breach is to be publicly disclosed in a timely manner and with factual, clear statements meant to dissuade speculation and confirm that QIR LLC is presently undertaking remedial action. Customers and partners alike should be directly notified on the protective measures they can take, such as changing passwords or monitoring their accounts for suspicious activity. To ensure legal compliance, regulatory bodies are to be informed as required by laws pertaining to data breaches.

Communications protocols are to be pre-defined to guarantee rapid escalation of information on the breach. Immediately after detection, the IT security team is to immediately alert the CIAO and IRT. Within no more than 24 hours, there is to be a full briefing to executive leadership so that a decision can be made on when to externally disclose. The first public statements should be issued as soon as practical in order to maintain and rebuild public trust. These should be followed up by communications providing updates on investigation progress, the success of containment, and all impacts on services or data. It is essential to establish feedback loops between internal teams and external parties to address concerns and adjust the response.

It Is through the establishment of a structured communications plan that provides clear definitions of roles, responsibilities, channels, and timing that QIR LLC can reduce confusion, regain stakeholder confidence, and respond effectively to security incidents. The plan outlined above supports both operational response and reputational management – which enables the company to recover quickly and reduce long-term damage. In addition, this communications plan calls for several solutions on how communications can be handled with various entities to ensure efficient response to potential future incidents.

## Prevention Strategies

In addition to responding to the most recent security incident, measures must be taken in order to prevent future breaches by strengthening QIR LLC's overall cybersecurity position. These measures are to be extensive – covering the technical, procedural, and organizational domains of QIR LLC. The first measure to be taken is an enhancement of access controls. Multi-factor authentication and strict user access management protocols are to be implemented across systems that contain sensitive information. In addition, role-based access controls are to be established to ensure that employees only have access to the information they need for their duties.

Secondly, there must be a general improvement of endpoint security. Devices and servers used by QIR LLC should be protected by up-to-date antivirus software, Endpoint Detection and Response tools, and firewalls. A policy of regular patches and updates must be implemented and enforced to nullify known vulnerabilities before threat actors can exploit them. In addition to this, data protection measures should be implemented to prevent communications from being viewed by unwanted actors. This would include measures such as modern encryption being implemented across all company communications networks.

Third, employees should be trained in a wide range of best practices in order to prevent social engineering attacks. This can include training courses on how to tell if one is being subjected to social engineering and simulated phishing, impersonation, and other social engineering attacks to ensure employee readiness in a controlled environment conducted by members of the ITS team. By implementing the above procedures and defense, QIR LLC can significantly reduce the likelihood of future security incidents. This is necessary to not just the safety the company, but also the restoration of its image in the eyes of stakeholders.

## Conclusion

The recent data breach experienced by QIR LLC has exposed several serious vulnerabilities in the company's approach to cybersecurity and information assurance, as well as its organizational practices and culture. As a direct result of the breach, stakeholder trust has been eroded due to both financial damages and a tarnishing of the company's public incident. As demonstrated by this incident, QIR LLC's cybersecurity protocols urgently need to be reformed.

Throughout this report, several key areas of improvement have been identified – namely poor access control, inadequate endpoint protection, a flawed workplace culture, and a lack of employee training. A proactive and structured approach is required to address these issues. This approach can be handled by enforcing authentication protocols, hardening system defenses, updating security systems, and implementing employee training programs.

The communication plan, vulnerability assessment, information assurance matrix, and prevention strategies outlined in this report must all be considered as a new cybersecurity policy is constructed by QIR LLC. The information exposed and ideas expressed in those sections of this report provide a clear outline of how cybersecurity must be handled going forward. By implementing the reforms called for in this report, QIR LLC can restore stakeholder confidence and prevent future security incidents.

In general, QIR LLC's philosophy towards cybersecurity must change. Cybersecurity is not a one-time investment but an ongoing process that requires constant improvement, vigilance, and adaptation. This does not just extend to the technical field but also the culture of the company. By treating cybersecurity as the critical function that it is, QIR LLC can prevent incidents such as this recent data breach from recurring.

**End of Report**