Lavontay Johnson

Prof. Cartledge

CS 465

14 April 2025

Final Project

Executive Summary

In March 2025, QIR experienced a significant cybersecurity breach that compromised critical internal systems and exposed serious weaknesses in the organization's information assurance practices. As the newly appointed Chief Information Assurance Officer (CIAO), I believe it is crucial to assess the incident thoroughly, understand the vulnerabilities that were exploited, and propose a plan to strengthen our defenses. The breach impacted not just the integrity of our systems but also our reputation, client trust, and overall operational stability. This report presents a complete analysis of the breach, including a detailed vulnerability assessment, threat matrix risk evaluation, communication strategies, and a full set of recommendations to rebuild and protect QIR's infrastructure. I feel that moving forward, cybersecurity must become a fundamental part of our business identity and not just a background IT function.

The breach highlights the need for a shift in how cybersecurity is approached at QIR. Information assurance must be prioritized at every level of the organization. Also, I believe we must build an environment where security is ingrained in our processes, from employee onboarding to client data handling and vendor management. By investing in a culture of security, we can rebuild client trust, strengthen operational resilience, and ensure regulatory compliance. The recommendations laid out in this report provide both immediate actions and long term strategies to transform QIR’s security posture and restore our position as a trusted leader in the financial services industry.

Organizational Background

QIR is a mid-sized organization that provides financial technology services, including transaction processing, data analytics, and payment gateway solutions to a wide client base. Our business revolves around handling large volumes of sensitive data every day. I would say that I think it’s fair to say that safeguarding client information and our proprietary technologies like our encryption algorithms and predictive modeling tools, is not just important, it’s essential to our survival and competitive edge.

Before the breach, QIR maintained basic security measures like firewalls, antivirus protections, and role based access controls. However, I feel that these defenses were no longer sufficient against the evolving cybersecurity landscape we face today. There was an organizational mindset that cybersecurity was mainly the IT department’s problem rather than an enterprise wide priority. Also, our growing reliance on third party vendors while expanding our capabilities, increased our exposure to external risks that were not being monitored or managed suitably. From my perspective, I think it’s clear now that our previous approach to cybersecurity was reactive and fragmented, which left us vulnerable when the attack occurred.

Also, one area I believe deserves more attention is our vendor management strategy. QIR relies heavily on third party vendors to deliver essential parts of our services, such as cloud hosting, payment gateways, and security tools. Each vendor relationship introduces new cybersecurity risks because their security practices directly affect our own. I think it’s critical that we treat vendors as extensions of our own infrastructure. Without strong oversight, third party vulnerabilities can easily become internal vulnerabilities. Going forward, I feel we must implement a standardized vendor risk assessment process, including regular security audits, contract clauses mandating breach notification, and clear requirements for cybersecurity standards compliance like SOC 2 or ISO 27001 certification (International Organization for Standardization, 2013).

Incident Description

The breach was first detected on March 17, 2025, when network monitoring tools flagged unusual outbound traffic from one of our core payment processing servers. At first, the anomaly was brushed off as a system glitch, which I think was a costly mistake. Further investigation showed that attackers had infiltrated our systems using stolen employee credentials gathered through a spear phishing attack.

Attackers sent emails crafted to look like urgent internal messages related to tax filing deadlines. These emails tricked employees into entering their login credentials into fake websites. With valid credentials in hand, attackers were able to bypass external defenses, escalate privileges, and move across multiple internal systems. They accessed client databases, payment systems, internal communications, and proprietary R&D files. I believe the attackers used legitimate administrative tools to mask their movements, which allowed them to operate undetected for nearly four days.

Containment efforts began after system errors started affecting customer transactions. We shut down compromised servers, reset credentials, and engaged external forensic experts. However, by that point, I believe significant data exfiltration and manipulation had already occurred.

Looking back, I feel that a stronger monitoring and detection strategy could have allowed us to catch the intrusion much earlier and limit the damage.

Reflecting on the breach, I think it’s important to recognize that several early warning signs were missed. Unusual login times, multiple failed login attempts, and subtle shifts in network traffic patterns were visible in system logs, but no one was actively reviewing them or correlating them with threat intelligence feeds (National Institute of Standards and Technology (NIST), 2012). I truly believe that had we invested in centralized log analysis and anomaly detection earlier, we could have detected the breach within hours instead of days. Also, I think better employee education on how to report suspicious emails and system behavior could have provided an additional early warning layer. Early detection is not just about tools, it’s about culture and vigilance.

Consequences of the Incident

I would say that the consequences of the breach were immediate and severe. Operationally, the disruption of payment processing and client services lasted for more than thirty six hours. This downtime violated several service level agreements (SLA) with key clients, resulting in financial penalties and strained relationships.

Financial impacts went beyond direct costs like forensic investigations, legal fees, and customer notifications, which totaled over $2.5 million. I think the long term financial consequences, including lost contracts, delayed projects, and increased insurance premiums, will ultimately be much larger. In an industry where trust is everything, I feel the reputational damage was even more serious. News outlets reported on our breach extensively, and our brand quickly became associated with cybersecurity failures. Also, strategic partners delayed new initiatives, pending a full review of our security practices.

I believe regulatory risks added another layer of complexity. Under GDPR, QIR was required to notify European clients and regulators within 72 hours of detecting a breach involving personal data (General Data Protection Regulation, 2018). Similar requirements applied under CCPA for U.S. based clients (California Consumer Privacy Act, 2020). Investigations were launched, and we had to demonstrate that we had taken reasonable steps to protect personal data. I believe that failure to do so could still expose us to heavy fines and even class action lawsuits.

Internally, spirits suffered, especially among IT and cybersecurity teams. Burnout, frustration, and a sense of betrayal set in as employees realized that leadership had not prioritized security. Several talented team members left in the following months, creating additional gaps in our defense capabilities just when we needed strength the most. I also believe that the psychological impact of a breach on internal culture is often underestimated. Employees feel vulnerable, exposed, and anxious about job security, and rebuilding internal trust can take months if not years. Also, we must recognize that the breach has complicated future client acquisition efforts. In competitive industries like ours, reputation lingers long after the technical issues are solved. Even if we patch every system and meet every compliance checkbox, clients will remember that we failed once, and regaining their full trust will require a sustained and very visible commitment to excellence in our cybersecurity practices. I feel that we cannot simply focus on technical recovery, we must address reputational recovery with the same seriousness.

Vulnerability Assessment

After the breach, I led a comprehensive vulnerability assessment to understand where we went wrong. Technically, I would say we had serious gaps. Our servers were running outdated operating systems with known vulnerabilities. Some critical patches had been delayed for months due to lack of oversight. Encryption was inconsistently applied to data at rest and in transit. Also, multi-factor authentication (MFA) was only partially rolled out, which left critical systems exposed to credential theft.

Human vulnerabilities played a major role as well. Cybersecurity training was treated as a formality, and employees completed online modules once a year without much engagement or follow up. There were no phishing simulations or practical exercises to reinforce secure behaviors. I believe that if employees had been better trained to spot suspicious emails, the phishing attack might have been stopped early.

Beyond the technical vulnerabilities, I think human factors were a major underlying cause of the breach. Weak password practices, such as password reuse across systems and the absence of strong complexity requirements, created easy entry points for attackers once credentials were stolen. Password policies existed on paper but were not consistently enforced or audited. Also, there was no system for monitoring unusual credential behavior, such as simultaneous logins from different geographic locations, which could have detected stolen credentials early. I believe that stronger identity management practices, including enforced password rotations, mandatory complexity standards, and behavioral login analytics, would have significantly reduced our exposure. I feel that we must recognize that human behavior is both our greatest vulnerability and potentially our strongest line of defense if trained and supported correctly.

Procedurally, incident response plans existed but were poorly understood across departments. When the breach happened, confusion over roles and responsibilities delayed containment efforts. Vulnerability scanning and penetration testing were inconsistently performed, and our vendor risk management processes were weak, leaving third party integrations unchecked.

All four pillars of information assurance (confidentiality, integrity, availability, and non repudiation) were compromised. Client data was stolen, billing records were altered, systems went offline, and transaction logs were tampered with, making it hard to verify legitimate operations. I think this breach exposed not just technical failings, but a broader failure of governance and culture around cybersecurity.

Threat Matrix Risk Assessment

After evaluating the breach and studying our vulnerabilities, I built a small threat matrix to prioritize where QIR faces the greatest risks. I believe this is an important step because it helps us focus resources where they are needed most.

First, phishing attacks were identified as the highest risk threat. The success of the phishing campaign that started this breach proves that social engineering is our biggest weakness. Employees were caught off guard by authentic looking emails and fell for it pretty quickly. I think we underestimated how sophisticated phishing tactics have become and how urgently we need to counter them with training and better technical controls like email filtering and authentication.

Second, unpatched system vulnerabilities represent another high risk category. It’s clear that missing critical patches gave attackers a backdoor to escalate privileges once they were inside. I feel that patch management must become a non negotiable, prioritized operational routine, not something left to chance (Center for Internet Security, 2021).

Third, insider threats (both intentional and negligent) were identified as a serious medium level risk. Although no evidence of malicious insiders was found in this breach, poor security behaviors like weak password practices and unauthorized device use were contributing factors. I believe that a proactive insider threat program, combining technical monitoring and employee education, would greatly strengthen our defenses.

I believe the insider threat risk deserves even more emphasis. Even top employees often bypass security controls for convenience, such as emailing sensitive files to personal devices, using unauthorized cloud storage services, or sharing passwords internally. These seemingly minor behaviors create opportunities for attackers to exploit or amplify breaches.

Also, while ransomware was not deployed in the March breach, I think it would be a serious mistake to assume it won't be attempted in the future. Financial services organizations are increasingly targeted by ransomware gangs seeking large payouts. A ransomware attack that encrypts critical payment systems could devastate operations and create regulatory violations if recovery timelines exceed allowable thresholds. Without strong, regularly tested offline backups and fast restoration procedures, our risk profile remains dangerously high.

Supply chain vulnerabilities emerged as a real concern too. I think it's easy to forget that a breach at one of our vendors could be just as damaging as a breach within our own walls. Without strict vendor assessments and clear contractual security obligations, we are exposed to unnecessary risk.

Finally, the absence of real time monitoring and sufficient incident detection made every other threat worse. Attackers were able to move around undetected for days. I feel that investing in advanced detection capabilities must become a core strategic priority. When looking at all the threats we face at QIR, I felt it made the most sense to organize them visually using a basic threat matrix. I believe that breaking them down by likelihood and impact really helped highlight which risks needed urgent attention and which ones could be monitored without immediate action. High likelihood, high impact threats like phishing attacks and ransomware clearly stood out as our top priorities, and I think focusing on them first gives us the best chance at strengthening our defenses quickly. Lower risk issues, like minor policy violations were still important but didn't need the same level of immediate response. I feel that this way of organizing threats made it a lot easier to prioritize our next steps. Also, I kind of based this approach this on best practices from NIST (2012) and the Center for Internet Security (2021), and I believe it gave us a much clearer path when building out the recommendations for how to move forward. The threat matrix below shows how these risks were categorized based on this evaluation.

QIR Threat Matrix

	Low Impact	High Impact
Low Likelihood	Minor policy violations	Supply chain vulnerabilities
High Likelihood	Insider negligence	Phishing attacks and ransomware

Organizational Communication Plan

I think that one of the biggest lessons from the breach was how vital effective communication is during and after an incident. Without a clear communication plan, confusion and mistrust can spiral out of control internally and externally I feel like.

Internally, we must create a formal Cyber incident response team (CIRT) with clearly defined roles and escalation procedures. Every employee must know exactly who to contact if they suspect something is wrong. I feel that the CIRT must be empowered to make fast decisions and provide daily situation reports during active incidents to keep leadership informed. I also feel that this alone would have cut hours off our response time during the March breach.

Externally, we must restrict public communication to a single point of contact, particularly the Chief communications officer (CCO) working closely with legal and executive leadership. Public statements should be carefully worded, fact checked, and focused on transparency without disclosing sensitive details that could aid further attacks. Also, clients, partners, and regulators must be notified in accordance with law but also in a way that maintains as much trust as possible.

I believe post incident communications are just as important. I think it's critical to update stakeholders on our remediation efforts and demonstrate the changes we're making. Silence after a breach damages trust more than admitting that improvements are underway. Offering services like free credit monitoring to affected clients is a small investment that can pay off in long term loyalty.

Recommendations

I believe QIR must undertake a serious, phased approach to improving information assurance. A reactive patch won't be enough, and we need a cultural shift. I think the best way forward is to structure our corrective actions into short term, medium term, and long term initiatives.

In the short term, over the next six months, we need to take immediate steps to close the biggest gaps. I believe the first priority must be to implement full multi-factor authentication (MFA) across all systems, users, and vendors without exception. We also need to roll out company wide phishing training and run simulated phishing attacks on a quarterly basis to build employee awareness. I feel that establishing a strict 30 day patch cycle for all critical vulnerabilities is another non negotiable action. Patch compliance should be actively tracked and reported to leadership. At the same time, we need to deploy a modern endpoint detection and response (EDR) solution across all devices to enhance threat detection capabilities. Also, a full cybersecurity audit of our current vendors should be conducted to identify supply chain vulnerabilities and ensure that third parties meet our new security standards.

In the medium term, looking at the next six to eighteen months, I think QIR should start redesigning its internal network using Zero Trust principles. Instead of assuming trust based on network location or role, we should verify every access attempt every time. Micro segmentation of networks and strict least privilege access policies are key elements of this redesign (International Organization for Standardization, 2013). Also, I believe we need to develop and launch a formal insider threat program, which combines behavioral analytics, education, and confidential reporting mechanisms to detect risks early. Regular penetration testing and internal red team exercises should become a standard operating practice at least twice a year to validate our defenses. I feel that disaster recovery procedures must also include cybersecurity specific scenarios such as ransomware recovery not just traditional server restoration.

In the long term, over the next eighteen months and beyond, cybersecurity must become part of QIR’s leadership culture. I believe forming a cybersecurity focused committee at the board level would institutionalize this commitment and ensure cybersecurity risk is monitored alongside financial and operational risk. We should also work toward achieving external certifications such as ISO 27001 and SOC 2 not just for compliance, but to prove to our clients and partners that security is part of our DNA. In addition, developing an in house threat intelligence capability would allow us to proactively monitor emerging threats and adjust our defenses accordingly. Finally, and maybe most importantly, I feel we must adopt a cybersecurity first culture across the company. Executive leadership must model secure behaviors, and cybersecurity must be seen as a shared responsibility. Recognition programs and positive incentives can help reinforce this mindset over time. Slowly but surely we will get there.

Conclusion

The March 2025 breach was a wake up call for QIR. It showed that no matter how strong our business model is, without strong information assurance, everything can be put at risk. I believe that cybersecurity must be treated as a strategic priority, not just an operational concern. It must become embedded in our processes, our decision making, and our culture.

I believe this report has laid out the incident, the vulnerabilities that were exploited, the threats we face, and a set of clear recommendations for recovery and transformation. Also, I believe that if we approach this crisis not with fear but with commitment, we can emerge stronger, smarter, and better equipped for the future.

I feel like the path forward requires real investment and time, not just in technology, but in people, processes, and governance. I feel that cybersecurity should not be viewed as an obstacle to business operations, but as a spark for client trust, regulatory compliance, innovation, and sustainable growth. Organizations that invest properly in cybersecurity are the ones that earn client loyalty and industry respect over the long term. I think it's important for QIR to realize that a strong cybersecurity culture is also a competitive advantage in today's digital economy. We can position ourselves not as victims of a breach, but as leaders who faced a crisis head on and used it as a catalyst to build something better, smarter, and stronger for the future. That transformation starts now.

References

California Consumer Privacy Act. (2020). California Civil Code Sections 1798.100–1798.199. Retrieved from https://oag.ca.gov/privacy/ccpa

Center for Internet Security. (2021). CIS Controls v8: Critical Security Controls for Effective Cyber Defense. Retrieved from https://www.cisecurity.org/controls/v8

General Data Protection Regulation. (2018). Regulation (EU) 2016/679 of the European Parliament and of the Council. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

International Organization for Standardization. (2013). ISO/IEC 27001: Information Technology — Security Techniques — Information Security Management Systems — Requirements.

National Institute of Standards and Technology. (2012). Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf