Lessons from Recent Qatar Data Breach

Practical Steps for Organisations

Qatar's National Cyber Security Agency (NCSA) announced this month action against a company for a major privacy breach. This enforcement provides a sharp reminder that data privacy and cyber resilience is not merely a compliance control but also a strategic business imperative.

This particular breach exposed personal data and underscored the significant operational and reputational risks that accompany these incidents. Globally, fines against organisations following data breaches have continued to increase in frequency and severity, indicating tightening enforcement. With these actions, the message is clear: organisations that fail to protect customer data risk fines, operational disruption and diminished trust.

Beyond the headlines, what practical steps should organisations take to strengthen their data privacy and cyber resilience?

Understand the data landscape

A prevalent issue among many organisations across industries and geographies is a limited understanding of the data they hold, how it's used and protected, and how it's stored and shared. The risk here is that organisations cannot protect what they're not aware of. To mitigate this risk, it's crucial that organisations perform a rigorous data mapping exercise that will reveal what personal data they hold and verify what technical and organisational measures apply to data processing operations. This is a foundational exercise, and the data map should serve as a single source of truth in the event of a breach or another compliance event.

Implementing comprehensive data classification is also essential, and organisations operating in Qatar have a clear framework to follow. For example, NCSA has established the National Data Classification Policy (current version 3.0), which establishes a unified scheme for government entities and vital sectors and sets requirements for other organizations under NCSA's authority. Government entities must implement a five-tier classification system (C0-C4): Public, Internal, Restricted, Secret and Top Secret, while non-government organisations must use a minimum of four classification levels.

This classification framework is based on risk assessment across confidentiality, integrity and availability, with organisations required to appoint chief data officers and build a data organization programme.

The policy complements and aligns with Qatar's Personal Data Privacy Protection Law (PDPPL), creating a comprehensive approach to data governance that goes beyond simple categorisation to include proper handling protocols and security controls throughout the data lifecycle.

Embed privacy and security by design

Privacy by design is a helpful way to guard against downstream data privacy risks. Put simply, privacy by design means that data privacy requirements should be considered at the design phase and privacy should be built into new products, services and processes, not bolted on afterward. For privacy by design to be truly effective, design and technical teams need to be aware of privacy by design requirements, which should be built into procedural documentation. If embedded correctly, it should identify opportunities to reduce data collection, necessary points to encrypt data both at rest and in transit and implement additional security controls for high-risk processing activities including automated decision-making or cross-border data transfers.

Privacy by design reduces risk and signals to customers and regulators that the organisation takes privacy and security seriously. From a cybersecurity perspective, this approach also strengthens resilience by enforcing secure-by-design principles, minimising the attack surface, and ensuring controls such as access management, logging, monitoring and regular security testing are integrated into the system from the outset. Organisations should establish automated incident response capabilities that can quickly isolate compromised systems and initiate containment protocols when threats are detected.

Train, train and train again

Many data privacy breaches stem from human error rather than sophisticated attacks, despite how it may appear from scanning media headlines. So, how can organisations reduce this risk? As with many areas of compliance, policies, procedures and robust controls can become redundant without targeted and intuitive training methods. Organisations should adopt a multi-layered training approach encompassing the following:

— Regular, role-specific privacy and cybersecurity training

— Breach playbooks and awareness materials

— Simulated phishing and breach response exercises

— When employees know what to look for and how to act, they inherently strengthen an organisation's resilience.

Monitor, detect and respond

The reality is that data breaches are inevitable. What organisations can control is how proactively they monitor and how effectively and quickly they respond. This is often a key point that regulators examine when analysing a data breach and considering regulatory actions.

Key steps to proactively mitigate these risks include:

— Active monitoring for identifying and containing cybersecurity incidents before they escalate. This depends on a combination of robust tooling, skilled people and clearly defined processes. Organisations should deploy integrated monitoring platforms that combine systems for data access logging, data loss prevention tools for real-time data exfiltration detection, and user and entity behaviour analytics to identify suspicious data access patterns and insider threats. These systems should continuously monitor personal data repositories and privacy compliance efforts, track data flows across networks and alert on unauthorised access attempts or privacy policy violations. Such sources should be integrated into existing security tooling and security information and event management (SIEM) systems to ensure correlation can be performed across the estate.

— Implement privacy-focused detection capabilities including automated data classification scanners to identify sensitive personal information, database activity monitoring for unauthorized queries or bulk data extraction and cloud access security brokers to detect suspicious data sharing activities. Detection systems should establish baseline patterns for normal data access and immediately flag anomalous behaviours that could indicate data breaches or privacy violations.

— A tailored and tested incident response plan can significantly impact an organisation's preparedness to handle an incident. Testing the plan through tabletop exercises and technical simulations ensures teams know their roles under pressure and that potential gaps are addressed in advance. Regulators increasingly expect to see documented, regularly rehearsed incident response procedures as evidence of organisational readiness.

— Identify and contract key external partners, such as specialist legal counsel, digital forensics teams and crisis communications experts, in advance of an incident. Pre-arranged agreements ensure that expertise can be deployed rapidly, without delays caused by procurement or legal review during a crisis.

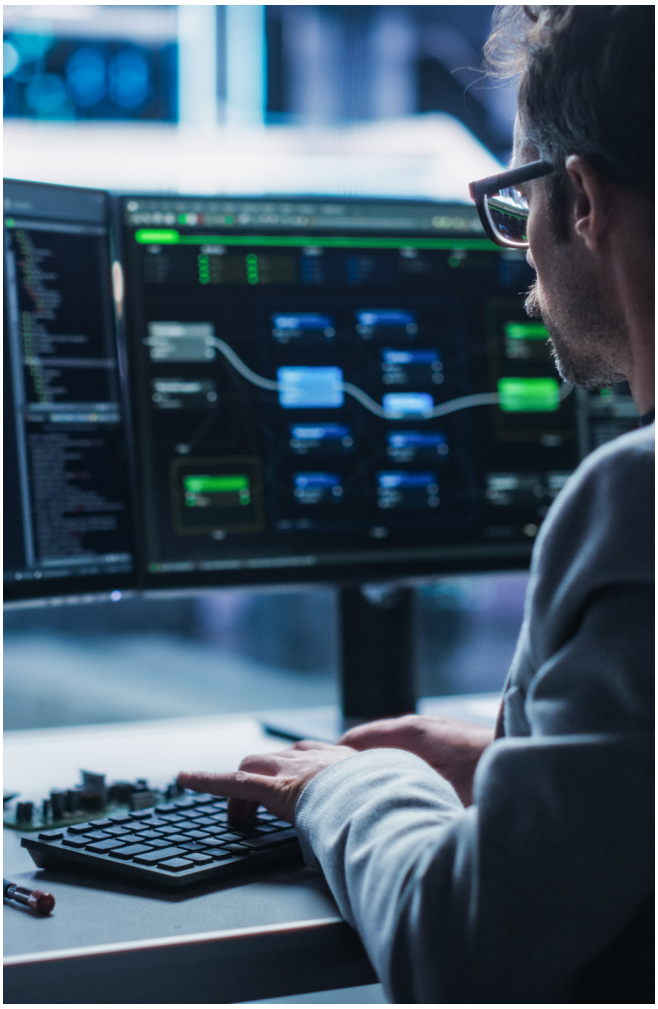
Engage with regulators early

The regulatory environment in Qatar, across the GCC and globally is evolving rapidly. Regulators are more likely to take a cooperative stance where organisations have adopted proactive measures such as those outlined here and where organisations communicate a breach event early. Proactive engagement demonstrates good faith compliance efforts, helps establish cooperative working relationships and shows commitment to continuous improvement in data protection practices. This approach often results in more favourable regulatory treatment, including reduced penalties and enhanced guidance on best practices.

Building resilience

Data privacy and cybersecurity compliance should not be viewed as an exercise to avoid fines. Building organisational resilience and maintaining consumer and third-party trust should be the true driving factors.

FTI Consulting helps organisations across the region map their data, assess risk and embed privacy and cybersecurity controls that are practical, scalable and aligned with local regulations and global best practices. By taking a proactive, structured approach, organisations can turn compliance into a competitive advantage.



GUY NGAMBEKET
Senior Principal,
Strategy & Transformation Public Sector,
Middle East
guy.ngambeket@fticonsulting.com

JACK FLETCHER
Senior Director,
Information Governance and Data Privacy,
Middle East
jack.fletcher@fticonsulting.com

JAD ELIAS
Senior Managing Director,
Strategy & Transformation Public Sector,
Middle East
jad.elias@fticonsulting.com

DAVID DUNN
Senior Managing Director,
Head of Cybersecurity,
EMEA & APAC
david.dunn@fticonsulting.com

NINA BRYANT
Senior Managing Director,
Head of Information Governance, Privacy & Security,
EMEA
nina.bryant@fticonsulting.com