Enhancing Cloud Data Security & Compliance

As the GRC lead for my organization, I was responsible for overseeing data protection and regulatory compliance. I received alerts about unauthorized access attempts to our cloud-based customer database, which contains personal and financial data.

1. What I Identified /The Key Risks

Based on the incident and my review, here are the risks I flagged:

- **Data Breach**: Confidential customer information could be accessed or stolen.
- **Regulatory Exposure**: You may face fines (e.g., under GDPR, CCPA) if there's a breach.
- **Reputation Damage**: Customers will lose trust if data is leaked.
- **Legal Liability**: You could be looking at lawsuits or claims.
- **Operational Disruption**: Investigation, response, and recovery would strain resources.

I've classified this event as a high priority security threat due to its potential impact.

2. Risk Assessment

I assessed the likelihood and impact of a breach like this, based on current alerts and the value of the data:

- **Likelihood**: Medium to High – these access attempts are persistent.
- **Impact**: High to Critical – a data leak would be a major incident.

My risk rating: HIGH
Immediate mitigation steps required.

3. Current Controls Review

I did a quick audit of current safeguards. Here's what I found that is already in place:

- **Access Control**: Role based access; password policy enforced.
- **Encryption**: Data encrypted at rest and in transit.
- **Monitoring**: Alerts are active (you caught this incident).
- **Patch Management**: Cloud environment is regularly updated.
- **Firewall/Segmentation**: Some network level isolation exists.

4. Proposed Next Steps /Stronger Controls

To strengthen our defense, I recommended the following control upgrades:

Multi-Factor Authentication (MFA)

Adds a second layer of security. Even if credentials are stolen, access is blocked.

Cloud Security Posture Management (CSPM)

Tools like Wiz, Prisma Cloud, or AWS Config can help you find misconfigured cloud services fast.

Privileged Access Management (PAM)

Ensures that admin level access is tightly controlled and temporary.

Behavior Based Monitoring (UEBA)

We'll be able to detect unusual access patterns , before damage is done.

Cloud Security Audit (Pen Test)

We want a third party to simulate attacks and show where we're blind.

Security Awareness Refresh

I rolled out a short training session, 80% of breaches start with human error.

5. Cost & Feasibility Review (Leadership-Ready)

Control	Cost to Org	Feasibility	My take
MFA	Low	Easy	Should be activated

			immediately
CSPM tool	Medium-high	Moderate	Worth it, we need visibility into cloud risks
PAM	Medium	Moderate	Protects high risk access, critical long term
UEBA	Medium-high	Moderate	May require integration with existing SIEM
Pen Test	Medium	High	Valuable insights fast, essential post incident
Training	Low	Easy	Quick win with strong impact

Final Risk Plan Summary

> "We've identified a real threat targeting our cloud environment. The risk of a breach is high, given current access attempts. While we have some protections in place, attackers are evolving. I recommend a set of layered security upgrades : MFA, behavior monitoring, cloud security hardening to reduce our exposure. These steps are feasible, cost-aligned, and essential to meet both regulatory expectations and customer trust."