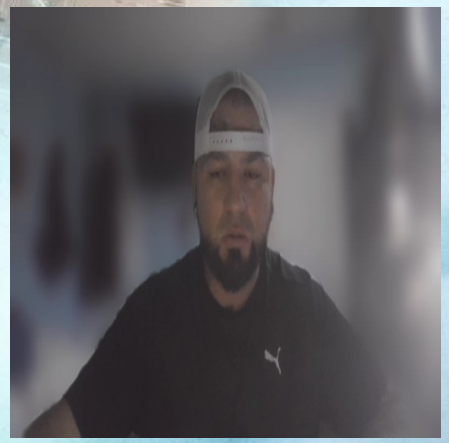
CONTINGENCY PLAN PRESENTATION

- **LOUIE S. VENEGAS**
- **SEC305 COURSE PROJECT, SCENARIO EXERCISE**
- CUSTOMER DATA REPOSITORY
  RANSOMWARE RESPONSE PLAN
- *PROTECTING FINANCIAL DATA & ENSURING BUSINESS CONTINUITY | SCENARIO: A FICTIONAL FINANCIAL INSTITUTION*



PLAN OBJECTIVES

DATA PROTECTION

Safeguard sensitive customer information (NPI) under GLBA requirements during ransomware incidents

RAPID RECOVERY

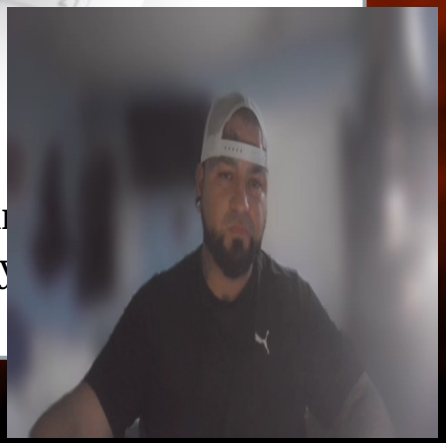
Restore critical systems within defined timeframes to minimize business disruption

COMPLIANCE

Meet regulatory notification requirements and maintain audit trails for examination

BUSINESS CONTINUITY

Ensure essential ba
continue during sy



FOUR-PHASE RESPONSE FRAMEWORK

1

Immedi[illegible]solation

(0-4 hours)

- Disconnect infected systems
- Activate air-gapped backups
- Begin threat containment

2

Assessment & Planning

(4-24 hours)

- Evaluate damage scope
- Develop recovery priorities
- Notify regulators

3

Syste[illegible]ecovery

(1-7 days)

- Restore from clean backups
- Validate data integrity
- Implement security patches

4

Post-Incident Review

(Ongoing)

- Strengthen defenses
- Update procedures
- Document lessons learned

PLAN MAINTENANCE STRATEGY

Regular Testing

Quarterly

Practice response procedures and walk-through scenarios

Backup Validation

Monthly

Verify backup integrity and data accessibility

Full Recovery Test

Annually

Complete restoration from air-gapped backups with audit

Success Criteria:

- Recovery within target timeframes
- Zero data loss or corruption
- Complete containment of threats
- Full regulatory documentation

SUMMARY & BENEFITS

- **GLBA Compliance: Meets all regulatory requirements**
- **Rapid Recovery: 3-2-1 backup strategy ensures quick restoration**
- **Data Protection: Air-gapped systems immune to encryption**
- **Business Continuity: Minimizes operational disruption**

Questions?

Louie S. Venegas

SEC305 Course Project, Scenario Exercise

"Prepared today, protected tomorrow"