Cybersecurity Disclosure Timing and Market Reactions: An Empirical Analysis of Information Asymmetry in Communications Companies

1. Scientific Method Framework

Research Question

How does cybersecurity disclosure timing affect market reactions in communications companies, and does firm governance quality moderate this relationship?

This research question is:

- **Specific**: Focuses on cybersecurity disclosure timing in communications sector
- **Measurable**: Uses quantifiable market reaction metrics (cumulative abnormal returns)
- **Relevant**: Addresses critical policy questions about mandatory vs. voluntary disclosure
- **Time-bound**: Achievable within course timeline using existing datasets

Hypothesis

H1: Immediate cybersecurity disclosure results in more negative short-term market reactions compared to delayed disclosure due to signaling effects, but this penalty is moderated by firm governance quality.

Testable Predictions:

- $\beta_1 < 0$: Immediate disclosure associated with more negative market reactions
- $\beta_2 > 0$: Higher governance quality associated with better market reactions
- $\beta_3 > 0$: Governance quality moderates the disclosure timing penalty

Falsifiable Conditions: The hypothesis would be rejected if immediate disclosure shows positive market reactions or if governance quality does not moderate the relationship.

2. Problem Definition and Business Relevance

Problem Statement

Current regulatory frameworks require varying disclosure timelines for cybersecurity incidents, but lack empirical foundation for optimal timing. The SEC's recent cybersecurity disclosure rules highlight the need for evidence-based policy recommendations.

Theoretical Foundation

This research extends the Myers-Majluf (1984) information asymmetry framework to cybersecurity contexts. While original work focused on capital structure decisions, we adapt it to disclosure timing in multi-stakeholder environments.

Key Innovation: Incorporating governance quality as a moderator of information asymmetry effects in cybersecurity disclosure decisions.

Business Impact

- **Regulatory Policy**: Inform SEC disclosure timing requirements
- **Corporate Strategy**: Guide firms' disclosure optimization strategies
- **Investor Relations**: Improve market efficiency in cybersecurity risk pricing

3. Data Sources and Accessibility Assessment

Primary Data Sources

WRDS (Wharton Research Data Services)

- **Content**: Stock price data, trading volumes, firm financials
- **Coverage**: 1990-present for publicly traded companies
- **Quality**: High-quality, professionally maintained
- **Accessibility**: Available through university subscription

SEC EDGAR Database

- **Content**: 8-K filings, 10-K reports, governance data
- **Coverage**: All public company filings since 1996
- **Quality**: Official regulatory filings
- **Accessibility**: Free public access via SEC API

Privacy Rights Clearinghouse Breach Database

- **Content**: Cybersecurity incident details, timing, severity
- **Coverage**: 2005-present, 500+ record minimum
- **Quality**: Independently verified incidents
- **Accessibility**: Public database with structured format

Governance Data (ISS/MSCI)

- **Content**: Board composition, SOX compliance, restatement history
- **Coverage**: S&P 1500 companies
- **Quality**: Professional governance ratings
- **Accessibility**: Available through WRDS institutional access

Sample Construction

- **Target Sample**: 59 communications companies with cybersecurity incidents (2010-2023)
- **Industry Focus**: SIC codes 4810-4899 (Communications)
- **Incident Criteria**: Publicly disclosed breaches affecting 10,000+ records

- **Data Availability**: Complete WRDS and governance data required

Data Quality Assessment

- **Completeness**: 95%+ data availability expected based on preliminary analysis
- **Accuracy**: Cross-validation between multiple disclosure sources
- **Timeliness**: Real-time market data with precise event timing

4. Analytical Methods and Technical Implementation

Empirical Strategy

Event Study Methodology:

$$CAR\_it = \alpha + \beta_1(Immediate\_Disclosure\_it) + \beta_2(SOX\_Weakness\_it) + \beta_3(Restatement\_History\_it) + \beta_4(Firm\_Controls\_it) + \beta_5(Market\_Conditions\_t) + \varepsilon\_it$$

Key Variables:

- **Dependent**: Cumulative Abnormal Returns (CAR) [-1,+1] around disclosure
- **Independent**: Disclosure timing (immediate vs. delayed)
- **Moderator**: Governance quality (SOX weaknesses, restatement history)
- **Controls**: Firm size, leverage, industry conditions, market volatility

Python Implementation Plan

Phase 1: Data Collection and Preprocessing

- SEC API integration for filing retrieval
- WRDS data extraction via Python interface
- Breach database web scraping and parsing
- Data cleaning and standardization

Phase 2: Event Study Analysis

- Abnormal return calculation using market model
- Statistical significance testing
- Robustness checks with alternative event windows

Phase 3: Regression Analysis

- OLS estimation with robust standard errors
- Interaction term analysis for governance moderation
- Diagnostic tests for model assumptions

Phase 4: Visualization and Dashboard

- Interactive event study plots
- Governance quality heat maps
- Timeline analysis of disclosure patterns

Validation Approach

- **Statistical**: Multiple event windows, alternative market models
- **Economic**: Magnitude interpretation and practical significance
- **Robustness**: Industry controls, time fixed effects, alternative governance measures

5. Value Proposition and Success Metrics

Research Contribution

- **Theoretical**: First application of Myers-Majluf framework to cybersecurity disclosure
- **Empirical**: Novel evidence on governance moderation effects
- **Policy**: Data-driven recommendations for disclosure timing regulations

Success Criteria

Academic Impact:

- Statistical significance of key coefficients ($p < 0.05$)
- Economically meaningful effect sizes (>2% abnormal returns)
- Robustness across alternative specifications

Business Impact:

- Actionable insights for corporate disclosure strategies
- Policy recommendations for regulatory agencies
- Risk management framework for communications companies

Expected Outcomes

- **Primary**: Evidence that governance quality moderates disclosure timing penalties
- **Secondary**: Identification of optimal disclosure timing strategies by firm type
- **Policy**: Framework for evaluating mandatory disclosure requirements

Course Requirement Alignment

This project directly fulfills all final portfolio components:

- **Database**: SEC EDGAR API integration and structured data storage
- **Analysis**: Event study methodology and statistical modeling

- **Dashboard**: Interactive Streamlit application for stakeholder use
- **Deployment**: Cloud-hosted dashboard for regulatory and corporate access

6. Technical Implementation Timeline

Phase 1: Data Infrastructure (Weeks 1-3)

- SEC EDGAR API integration and Python automation
- Financial statement parsing and data extraction
- Market data API connections (yfinance/Alpha Vantage)
- Cybersecurity incident identification in 8-K filings
- Governance metrics extraction from proxy statements
- Initial data quality assessment and validation

Phase 2: Core Analysis (Weeks 4-6)

- Event study implementation
- Abnormal return calculations
- Statistical testing framework
- Preliminary results generation

Phase 3: Advanced Analysis (Weeks 7-9)

- Governance moderation analysis
- Robustness testing
- Alternative model specifications
- Sensitivity analysis

Phase 4: Visualization and Documentation (Weeks 10-12)

- Dashboard development using Streamlit/Dash
- Interactive visualizations
- Final documentation and presentation
- Repository organization and deployment

7. Repository Structure and Version Control

```
TSpivey-Assignment-3/
├── src/
│   ├── data_collection/     # SEC API integration
│   ├── analysis/            # Event study and regression modules
│   ├── visualization/       # Dashboard and plotting functions
│   └── utils/               # Helper functions and utilities
├── data/
│   ├── raw/                 # Original data files
│   ├── processed/           # Cleaned datasets
```

```
│   └── external/          # Reference datasets
├── notebooks/
│   ├── exploratory/       # Initial data exploration
│   ├── analysis/          # Main analytical notebooks
│   └── validation/        # Robustness checks
├── tests/
│   └── unit_tests/        # Testing framework
├── docs/
│   ├── methodology/       # Technical documentation
│   └── results/           # Analysis output
└── dashboard/             # Streamlit application
```

8. Risk Assessment and Limitations

Potential Challenges

- **Data Access**: WRDS institutional access requirements
- **Sample Size**: Limited number of communications company breaches
- **Endogeneity**: Disclosure timing may be endogenous to breach severity

Mitigation Strategies

- **Alternative Data**: Use Compustat if WRDS unavailable
- **Sample Expansion**: Include related telecommunications/media companies
- **Instrumental Variables**: Use regulatory changes as instruments for timing

Scope Limitations

- **Industry Focus**: Communications sector only (generalizability questions)
- **Time Period**: Post-2010 data availability constraints
- **Causality**: Correlation vs. causation interpretation challenges

9. Conclusion

This project provides a rigorous empirical test of information asymmetry theory in cybersecurity contexts, with clear policy and business implications. The focus on communications companies leverages domain expertise while maintaining analytical rigor. The technical implementation aligns with course requirements for database integration, statistical analysis, and dashboard development.

The research addresses a critical gap in understanding how governance quality affects market reactions to cybersecurity disclosures, providing actionable insights for both corporate managers and regulatory policymakers.

Contact: Timothy Spivey - ts2427@jagmail.southalabama.edu
Repository: https://github.com/ts2427/cybersecurity-disclosure-analysis
Project Timeline: September 2024 - December 2024