

ChatGPT 4 ▾



You

selected\_papers.xlsx  
Spreadsheet

I am sending you an excel file containing the titles and abstracts of 36 academic articles focused on cyber risk. Review the provided articles and categorize them into distinct groups based on their focus. Assign a descriptive name to each group, reflecting the common theme of its articles. List the IDs and titles of the articles in each group. Additionally, explain the rationale behind the groupings, focusing on how the content or perspective on cyber risk unifies the articles within each group. Ensure every article is categorized. Describe the logic or algorithm used for this classification.



ChatGPT

The Excel file contains three columns: "ID," "Title," and "Abstract." There are 36 academic articles focused on cyber risk. To categorize these articles, I will analyze their titles and abstracts to identify common themes or focuses. Here's the process I will use:

1. **Text Analysis:** I will perform a text analysis of the titles and abstracts to identify key themes, technologies, methodologies, or application domains. This includes identifying frequently occurring keywords and concepts.
2. **Clustering:** Based on the identified themes, I will cluster the articles into groups. Each group will represent a specific aspect of cyber risk research, such as technological focus, methodology, application domain, etc.
3. **Naming Groups:** Each group will be given a descriptive name that reflects its common theme.
4. **Rationale Explanation:** I will provide an explanation for each group, focusing on how the articles within the group share a common perspective or subject matter related to cyber risk.

Let's start with the text analysis to identify key themes. [↗]

The articles have been initially clustered into five groups based on the analysis of their titles and abstracts. The distribution of articles across these clusters is as follows:

- Cluster 0: 8 articles
- Cluster 1: 7 articles
- Cluster 2: 13 articles
- Cluster 3: 4 articles
- Cluster 4: 4 articles

Next, I will examine the key terms and themes within each cluster to assign a descriptive name to each group and explain the rationale behind these groupings. This step involves analyzing the most representative terms in each cluster to understand the common theme that unifies the articles within each group. Let's proceed with this analysis. [↗]

Based on the top keywords in each cluster, I have named the groups as follows and provided a rationale for each:

1. **Cluster 0 - "Advanced Detection Technologies in Cybersecurity":**
  - Keywords: Machine, Mobile, Malware, Feature, Network, Intrusion, Cloud, Deep, Detection, Learning
  - Rationale: This cluster focuses on technological advancements in detecting cybersecurity threats, emphasizing machine learning, deep learning, and network intrusion detection.
2. **Cluster 1 - "Cyber Risk Management and Insurance":**
  - Keywords: Audits, Decisions, Incentive, Sharing, Organizations, Cybersecurity, Information, Security, Insurance, Cyber
  - Rationale: Articles in this group discuss cyber risk from a managerial and organizational perspective, including cybersecurity insurance, information sharing, and decision-making processes in organizations.
3. **Cluster 2 - "Cybersecurity in Industry and IoT":**
  - Keywords: Industry, IoT, Infrastructure, Risks, Security, Data, Market, Risk, Insurance, Cyber
  - Rationale: This group addresses cybersecurity challenges specifically in industrial settings and IoT (Internet of Things), focusing on risks, data security, and market-related aspects.
4. **Cluster 3 - "Cybersecurity in Medical Devices and Healthcare":**
  - Keywords: Risks, IMDRF, Telemedicine, Cybersecurity, Safety, Vulnerabilities, Clinical, Devices, Patient, Medical
  - Rationale: Articles in this cluster are centered on cybersecurity in the healthcare sector, particularly regarding medical devices, patient safety, and vulnerabilities in clinical settings.



#### 5. **Cluster 4 - "Information Security in Healthcare and External Threats":**

- Keywords: Threats, External, Health, Care, Phishing, Healthcare, Share, Climate, Information, Security
- Rationale: This group focuses on external cyber threats and information security in the healthcare sector, including aspects like phishing and the sharing of health information.

Now, I will list the IDs and titles of the articles in each group. [6]

The articles have been categorized into five distinct groups based on their focus and common themes related to cyber risk. Here is the breakdown of each group with the IDs and titles of the articles:

#### **Group 1: Advanced Detection Technologies in Cybersecurity**

- **ID 1:** DeepOrigin: End-to-End Deep Learning for Detection of New Malware Families
- **ID 2:** Autoencoder-based feature learning for cyber security applications
- **ID 3:** Cyberattack detection in mobile cloud computing: A deep learning approach
- **ID 4:** Toward an Online Anomaly Intrusion Detection System Based on Deep Learning
- **ID 5:** Network intrusion detection for cyber security using unsupervised deep learning approaches
- **ID 6:** Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic
- **ID 8:** A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks
- **ID 16:** Towards a maturity model for health-care cloud security

#### **Group 2: Cyber Risk Management and Insurance**

- **ID 21:** Incentive Contract for Cybersecurity Information Sharing Considering Monitoring Signals
- **ID 22:** Cyber-Warranties as a Quality Signal for Information Security Products
- **ID 26:** Cyber-Insurance as a Signaling Game: Self-reporting and External Security Audits
- **ID 27:** Post-incident audits on cyber insurance discounts
- **ID 30:** A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation
- **ID 31:** SECONDO: A Platform for Cybersecurity Investments and Cyber Insurance Decisions
- **ID 32:** Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance

#### **Group 3: Cybersecurity in Industry and IoT**

- **ID 7:** A Signal Processing Approach for Cyber Data Classification with Deep Neural Networks
- **ID 15:** Cyber risk cost and management in IoT devices-linked health insurance
- **ID 19:** Using Risk Assessments to Assess Insurability in the Context of Cyber Insurance
- **ID 20:** Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective
- **ID 23:** A framework for effective corporate communication after cyber security incidents
- **ID 24:** What are the actual costs of cyber risk events?
- **ID 25:** An insurance theory based optimal cyber-insurance contract against moral hazard
- **ID 28:** Cyber risk and insurance for transportation infrastructure
- **ID 29:** Cyber Insurance Market in Israel – What is the Official Policy?
- **ID 33:** A framework for incorporating insurance in critical infrastructure cyber risk strategies
- **ID 34:** Preventing the Drop in Security Investments for Non-competitive Cyber-Insurance Market
- **ID 35:** Optimal Security Configuration for Cyber Insurance
- **ID 36:** The evolution of the cyber-insurance industry and market: An institutional analysis

#### **Group 4: Cybersecurity in Medical Devices and Healthcare**

- **ID 12:** Clinical Cybersecurity Training Through Novel High-Fidelity Simulations
- **ID 13:** Risk management-based security evaluation model for telemedicine systems
- **ID 14:** Evaluation of Mobile Health Applications: Is Regulatory Policy Up to the Challenge?
- **ID 17:** Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem

#### **Group 5: Information Security in Healthcare and External Threats**

- **ID 9:** Information security climate and the assessment of information security risk among healthcare employees
- **ID 10:** Infotech. Cyber Security. Health Care Learns to Share Scares and Solutions
- **ID 11:** Phishing in healthcare organisations: threats, mitigation and approaches
- **ID 18:** RiskWriter: Predicting Cyber Risk of an Enterprise

The categorization reflects the varying focuses and methodologies in the field of cyber risk, from technological advancements in detection and intrusion prevention to the management of cyber risk in specific industries like healthcare and IoT. Each group represents a distinct aspect of cyber risk research, unified by common themes and perspectives. [7]