Categorizing Differences in Cyber Incident Reporting Definitions and The Impact on Regulatory Compliance

Dr. Angelica Marotta & Dr. Stuart Madnick
Cybersecurity at MIT Sloan (CAMS)

ICIS 2024 BANGKOK - THAILAND December 15-18, 2024

Background

Problem

- **Rising Cyber Incidents**
  - **Cybercrime is projected to cost** the global economy **$10.5 trillion annually by 2025**
  - **Cyber-attacks** t increasing across all industries.
  - **Regulations often require Incident Reporting**
- **Inconsistent Definitions**
  - **Variations in regulatory definitions** complicate incident identification and response.
  - **Some definitions** focus on critical infrastructure (e.g., power grids, transportation), while others, like the **US SEC**, focus on whether the incident has a **"material impact"** on organizations.
- **Challenges**
  - Inconsistent definitions create confusion, making it difficult for organizations to **identify, report, and respond** to cyber incidents.
  - **84% of companies** report difficulty in aligning their cybersecurity practices with varying regulatory definitions.

Objectives

1.Analyze cyber incident definitions across major regulations.

2.Assess consistency and discrepancies within these definitions.

3.Explore implications of these differences on cybersecurity practices and compliance.

4.Recommend standardized definitions to enhance response and risk management

Methodology

To explore cyber incident definitions, this study employed a systematic methodology focused on regulatory bodies from **the United States** and **Europe**. Our research included the following steps:

Phase	Description	Details
Initial Data Collection	Assembled a database of almost 200 enacted or proposed regulations from the US and Europe.	Identified distinct regulatory components, categories, legal bodies, regions, and objectives.
Qualitative Validation	Conducted interviews with executives.	Validated insights from regulatory materials and grounded findings in industry experience.
Comparative Analysis	Analyzed cyber incident definitions across collected data.	Identified keywords, themes, similarities, limitations, and discrepancies among definitions.
Synthesis	Synthesized findings from data analysis.	Emphasized importance of harmonizing cybersecurity regulations and definitions.

Analysis: Agencies' and Regulations' Definitions Of Cyber Incident

Agencies' definitions
Agencies in the US and Europe provide varying definitions of a "cyber incident," which influence their respective cybersecurity strategies. Examples:

Region	Agency	Definition
USA	NIST (National Institute of Standards and Technology)	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system
USA	CISA (Cybersecurity and Infrastructure Security Agency)	Includes attempts to gain unauthorized access, unwanted disruption or denial of service
EU	ENISA (European Union Agency for Cybersecurity)	An event with an actual or potentially adverse effect on the security or performance of a system

Cybersecurity Regulations' Definitions
US cybersecurity regulations define cyber incidents to guide compliance, while EU regulations focus more on personal data and system security. Examples:

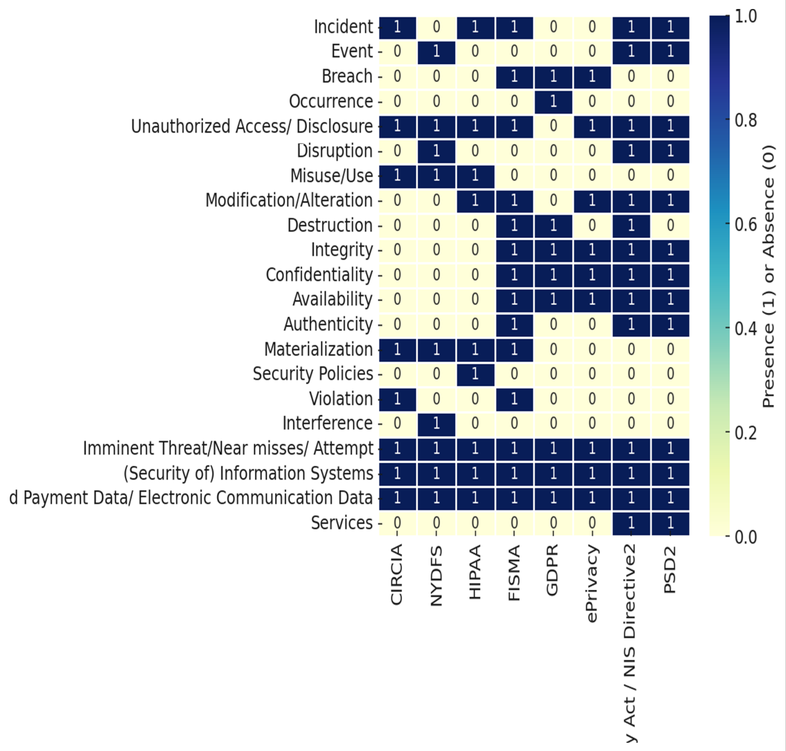
Region	Regulations	Key Points
US	CIRCIA, NYDFS, HIPAA, FISMA	Focus on actual jeopardy, unauthorized access, and policy violations
EU	GDPR, ePrivacy, NIS2, PSD2	Emphasis on data protection, **introduces 'near miss' concept**

Key Observations from the Analysis

- **Agencies' definitions** influence various regulations in their regions:
  - Regulations often **adopt or adapt** agency definitions to suit specific sectors or contexts
  - Some regulations, like NIS2, expand on agencies' definitions by including new concepts like **"near misses"**
  - **While agency definitions are influential, there are still significant variations in how different regulations define cyber incidents!**

Comparative Analysis

Regulations' definitions highlight specific **keywords** that can **impact** the comprehension of the cyber incident concept. The heatmap below (Figure 1) showcases the inclusion of these terms across some key regulations described:



Discussion

The comparative analysis highlights both **similarities** and **differences** in various cybersecurity regulations .

Key Similarities

- **Common Focus: Protection of personal and healthcare information** from unauthorized access, reduction of the **impact of cybersecurity incidents**, such as damage and alterations, emphasis on **Confidentiality, Integrity, Availability**
- **Primary Assets: Personal data** and **information systems** are commonly defined as primary assets in these regulations.

Key Differences

- **Terminology Variations:** Definition, such as **"incident," "event," "breach,"** and **"occurrence"** are interpreted differently across regulations.
- **Scope & Applicability:** Varies by **sector** and **jurisdiction.**
- **Reporting Timelines:** Multiple **thresholds** (typically, **24-72 hours)**.
- **Cross-border Data:** Different **restrictions** and **safeguards**.
- **Cybersecurity Standards:** Varying **technical requirements**.
- **Critical Terms:** Terms like **authenticity**, **materialization**, and **near misses** are inconsistently covered, hindering proactive risk management.

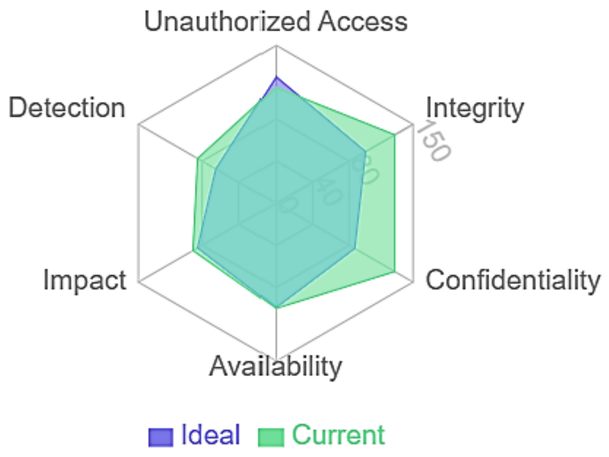
Takeaways

Challenges of the Fragmented Regulatory Landscape

- **Varying Standards**: Differences in **what constitutes a "cyber incident"** across regions and sectors.
- **Conflicting Interpretations:** Diverse interpretations of incidents, causing **confusion across countries and industries.**
- **Inconsistent Reporting:** Varied approaches to reporting incidents, leading to **gaps in data and response.**
- **Difficulty in International Collaboration:** Challenges in working across borders due to **regulatory and legal differences.**
- **Complex Compliance Requirements:** Complex and often **conflicting compliance obligations** add to the burden.

Recommendation:

- Developing a **standardized definition** of a "cyber incident, focusing on **common keywords/themes** identified in the research (**unauthorized access, integrity breaches, confidentiality**



Thought Experiment

Which of these should be reported? … As a Near Miss? … and why?

1. Someone tries to login to your systems, but fails due to bad password?
2. A Phishing email is reported in your company?
3. A Spear Phishing email targeted specifically for your company?
4. Someone searching for evidence of a common vulnerability in your system (e.g., log4j)?
5. Someone got into your system, but expelled before doing damage?
6. Someone got into your system, but not realized until after they left, and no obvious damage done or data copied (e.g., cryptominer)?

Action Items

Regulatory Pluralism: The **coexistence and interplay** of various cybersecurity regulations and definitions across local, federal, and international levels demands a more dynamic approach from both private and public sectors .

Call to Action:

***Companies*: Adopt modular policies for flexibility and agility in compliance.**

***Policy-makers*: Develop proactive, harmonized regulations to address cyber threats before they occur, rather than responding after incidents**

Contact information

How can you help with this project?

Please share your thoughts, experiences, and insights with us.

Dr. Angelica Marotta
amarotta@mit.edu

Dr. Stuart Madnick
smadnick@mit.edu