Article

Not peer-reviewed version

Understanding Cyber Incident Dynamics in the European Union: A Study of Actor Types and Sector Vulnerabilities

Thanasis Pseftelis * and Gregory Chondrokoukis

Posted Date: 25 April 2025

doi: 10.20944/preprints202504.2169.v1

Keywords: cybersecurity; data; policy

 doi:10.20944/preprints202504.2169.v1

Article

Understanding Cyber Incident Dynamics in the European Union: A Study of Actor Types and Sector Vulnerabilities

Thanasis Pseftelis * and Gregory Chondrokoukis

University of Piraeus
* Correspondence: psesftelis@unipi.gr

Abstract: As cyber threats have increased in both frequency and complexity, the European Union (EU) has taken measures to enhance its cybersecurity framework. This has included the implementation of directives such as NIS1 and NIS2, as well as the establishment of databases such as the European Repository of Cyber Incidents (EuRepoC) and the Cyber Events Database from the University of Maryland. This research investigates the relationships between different types of cyber actors and the corresponding incidents, as well as the correlation between industry sectors and types of cyber incidents. Utilizing chi-square testing on a dataset comprising over 14,000 cyberattack incidents, we identified statistically significant correlations that substantiate the hypotheses proposed. The results of the study indicated that specific actor types, such as nation-states and criminals, were more likely to be associated with particular incident types. In contrast, industry sectors like healthcare and public administration exhibited distinct vulnerabilities. The findings underscore the imperative for data-driven and sector-specific cybersecurity policies within the EU, underscoring the role of comprehensive data repositories in informing effective governance against cyber threats. It is imperative that member states continue to collaborate in order to leverage these insights and enhance resilience and safeguard critical services across Europe.

Keywords: cybersecurity; data; policy

1. Introduction

The European Union has historically prioritized cybersecurity concerns, with the objective of safeguarding its member states and extending this protection beyond its borders. This commitment is evidenced by the issuance of directives such as NIS 1 [1] and NIS 2 [2], and the establishment of a specialized agency, the European Union Agency for Cybersecurity (ENISA [3]), which was created to address cybersecurity concerns within the European Union.

In December 2024, the Cybersecurity Agency published the inaugural report [4] assessing the state of cybersecurity in the different member states. This report was intended to provide reliable information for policy making by the competent bodies of each member state. It is evident that reliable sources of information capable of contributing to their further protection are scarce.

The availability of public datasets that comprehensively document cyberattacks experienced over time remains constrained. Notable exceptions are represented by the datasets from the Center for International and Security Studies at Maryland [5] and the European Repository of Cyber Incidents (EuRepoC [6]).

This research utilizes research hypotheses to examine the existence of relationships between the collected data and the conclusions that can be drawn from it, with the objective of further contributing to the formulation of security policies in the future.

The utilization of the chi-square test [7] is deemed appropriate, as it is a widely used statistical method for examining the relationships between categorical variables.

 doi:10.20944/preprints202504.2169.v1

The objective of the present research study is to examine the existence, or absence, of relationships between the type of actors and the type of cyber incidents, as well as between industry sectors and type of cyber incidents.

2. Materials and Methods

2.1. Basic Terms

The ENISA Directive [8] (2019/881) delineates its objectives, tasks, and organizational arrangements. The NIS1 Directive (2016/1148) and the NIS2 Directive (2022/2555) further elaborate various definitions. Among these directives, the following definitions merit particular attention:

Cybersecurity: "means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"

Incident: "means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems"

Cyber threat: "means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons"

2.2. NIS360 [9]

In March of 2025, the European Union's (EU) Agency for Cybersecurity (ENISA) published a report that detailed the findings of the NIS360 methodology. This methodology employs data from National Authorities, companies (in accordance with the NIS2 Directive), and EUROSTAT. The report's primary objective is to enhance cybersecurity resilience within the following sectors:

- Energy
- Transport
- Finance
- Health
- Drinking and waste water
- Digital infrastructure
- ICT service management
- Public administrations
- Space

The NIS360 methodology is a systematic approach to evaluating the maturity and criticality of various sectors and their sub-sectors. According to the data assessment, the following sectors and sub-sectors fall within the critical risk zone:

- ICT Service Management
- Space
- Public Administration
- Maritime
- Health
- Gas

2.3. NIS2

The NIS2 Directive, a cybersecurity framework, aims to ensure a high level of cybersecurity for Member States. A central tenet of the directive is the facilitation of optimal functionality in networks and information systems. In comparison to its predecessor, the directive has expanded the scope to encompass a more extensive array of sectors.

The directive establishes the following key objectives:

- The manage cybersecurity-related risks.
- The reporting of cyber incidents
- The minimum compliance with cybersecurity standards

 doi:10.20944/preprints202504.2169.v1

In the event of noncompliance by the implicated parties, the directive empowers national cybersecurity authorities to proceed with the imposition of sanctions.

A distinguishing feature of the directive is its comprehensive approach to addressing diverse cyber risks, with a primary objective being the uninterrupted delivery of services to citizens of the European Union.

2.4. Cyber Events Database - European Repository of Cyber Incidents (EuRepoC) [10]

The European Repository of Cyber Incidents (EuRepoC) is a comprehensive database designed to document and analyze security incidents affecting entities across various sectors in Europe. The objective of this study is to provide a comprehensive overview of the database's structure, the types of data it encompasses, and its significance within the broader context of cybersecurity in Europe.

The increasing frequency and sophistication of cyber incidents necessitate meticulous tracking for informed decision-making and policy formation. EuRepoC is an initiative that aims to catalog cyber events to support research and enhance the collective cyber resilience of European nations. The repository's objective is to compile data encompassing a diversity of attacks, their impact, and the responses instituted.

The database is structured to facilitate efficient data retrieval and analysis through relational processes. The system incorporates numerous fields intended to provide a thorough synopsis of incidents, encompassing, but not limited to, the following:

- Incident Description: The text provides a detailed account of the event, offering a comprehensive narrative that captures the essence of the occurrence.
- Type of Incident: These threats are classified into various subtypes, including data breaches, ransomware, denial-of-service attacks, and phishing attempts.
- Sector Affected: The following sectors have been identified as being impacted by the incident: public, healthcare, finance, and information technology.
- Geographical Location: The region or country in which the incident was registered is specified, thereby enabling geographically focused analysis of cyber threats.
- Date and Time of Incident: The documentation of the incident is imperative for conducting a trend analysis.
- Impact Assessment: The evaluation process is intended to ascertain the consequences of the incident on affected entities. Such consequences may include financial losses and operational disruption.
- Mitigation Efforts: The following information is provided for the purpose of elucidating the responses to the incident: updates to security measures, public disclosures, and alterations to policy.

EuRepoC encompasses a wide array of incidents, structured to reflect the evolving threat landscape. The following categories of incidents have been documented:

- Malware Attacks: This encompasses a range of malicious software, including viruses, worms, and Trojan horses, which are designed to compromise the integrity of the system.
- Phishing Attacks: In the realm of cybersecurity, incidents involving the masquerade of attackers as legitimate entities to obtain sensitive information are of particular concern.
- Data Breaches: The phenomenon of events involving unauthorized access to confidential data, which frequently encompasses sensitive personal data, is of particular concern.
- Denial-of-Service: The phenomenon of service unavailability, often characterized by an excessive influx of requests directed towards a particular system, is a salient example of this phenomenon.
- Insider Threats: Incidents stemming from actions taken by individuals within the organization, whether intentionally or not, that result in harm.

The repository fulfills several pivotal functions, including:

- Data-Driven Insights: EuRepoC plays a pivotal role in this endeavor by aggregating diverse incident data, thereby facilitating research into patterns and trends within the cybersecurity landscape in Europe.
- Policy Formulation: is the process of establishing guidelines and regulations for the governance of an organization, institution, or system. It is evident that policymakers have the capacity to employ the

 doi:10.20944/preprints202504.2169.v1

findings from EuRepoC in order to formulate regulations that are intended to fortify cyber defenses on a sector-wide basis.

- Security Awareness: Organizations can utilize this database to assess their vulnerability to prevalent cyber threats, facilitating the implementation of proactive rather than reactive strategies.
- International Collaboration: EuRepoC, a European-centered initiative, fosters collaboration and information sharing among member states, ultimately enhancing collective cybersecurity measures.

The European Repository of Cyber Incidents signifies a substantial advancement in the realm of understanding and responding to cyber threats within the European continent. EuRepoC facilitates this process by consolidating extensive data on incidents across various sectors and countries. This consolidation enables individual organizations to enhance their cybersecurity postures and contributes to the development of strategies at the national and European levels. The continued evolution of this repository is imperative, as it must align with the rapidly changing cybersecurity landscape and emerging technologies.

2.5. Cyber Events Database - University of Maryland [11–13]

The Cyber Events Database, which is hosted on the Critical Infrastructure Security and Resilience (CISR) website operated by the University of Maryland, functions as a comprehensive repository of notable cyber incidents. This database has been developed for the use of researchers, policymakers, and cybersecurity professionals, providing detailed information on major cyber events and attacks that have occurred on a global scale. The subsequent discussion will elucidate the salient features and insights derived from this database.

This dataset provides a detailed account of a structured framework for logging incidents of cybersecurity breaches, employing a consistent categorical format. The employment of variables that delineate event dates, actors, organization types, tactics, motives, and the impacts of such breaches engenders a robust reporting mechanism to track these incidents comprehensively.

In an era of increasing digitalization, cybersecurity breaches have the potential to have far-reaching consequences. A comprehensive understanding of the nature of these incidents, the actors involved, and their motives is imperative for the development of effective strategies for prevention and response. This dataset delineates the specific variables indispensable for reporting and analyzing cybersecurity events, emphasizing the significance of standardization in data collection.

The structure of the dataset can be described as follows:

Event Date and Year

Event Date (event_date): This variable captures the specific date of the event occurrence in the DD-MM-YYYY format. For estimated dates, the first day of the month is recorded.

Year (year): This captures the year the event occurred in the YYYY format.

Actors Involved

Actor (actor): An identification string representing the individual or organization responsible for the event. If unknown, the entry shall be noted as “undetermined.”

Actor Type (actor_type): This variable indicates the nature of the actor:

- Criminal: Organizations engaging in illicit activities for financial profit.
- Nation-State: Entities affiliated with government bodies or militaries.
- Terrorist: Non-state actors employing violence or intimidation for political objectives.
- Hacktivist: Groups or individuals conducting cyber-attacks for political or social causes.
- Hobbyist: Individuals acting out of curiosity or interest rather than for financial gain.

Target Organization Details

Organization (organization): This string variable specifies the name of the organization affected by the breach.

North American Industry Classification System (NAICS) Code (industry_code): A two-digit code categorizing the industry of the impacted organization.

Industry Name (industry): This field presents the name correlating to the NAICS category.

 doi:10.20944/preprints202504.2169.v1

Motives of the Actors

Motive (motive): This categorical variable defines the objectives of the attacking agent:

- Protest: Activities aimed at causing service disruptions to convey political messages.
- Sabotage: Actions leading to the irreversible destruction of information or networks.
- Espionage: The act of improperly accessing networks to acquire intelligence.
- Financial: The exfiltration of sensitive data for economic gain.

Event Type Classification

Event Type (event_type): Indicating the primary end effects of the incident, this can be:

- Disruptive: Events that disrupt normal operations.
- Exploitive: Events that entail stealing sensitive information.
- Mixed: Uniting both disruptive and exploitative elements, exemplified by ransomware attacks.

Event Sub-Types

The classification of events can be further detailed into specific sub-types, categorized as either disruptive or exploitive incidents:

Disruptive Events:

- Message Manipulation: Tampering with organizational messages, affecting communication accuracy.
- External Denial of Services: Attacks executed from external networks to halt communication.
- Internal Denial of Services: Disruptions instigated from within the organization's infrastructure.
- Data Attack: Actions aimed at damaging, encrypting, or manipulating data.
- Physical Attack: Direct manipulation of IT components affecting physical systems.

Exploitive Events:

- Exploitation of Sensors: Data theft from peripheral devices.
- Exploitation of End Host: Information theft from individual user devices.
- Exploitation of Network Infrastructure: Theft accomplished via direct access to network devices.
- Exploitation of Application Server: Gaining access to data through application vulnerabilities.
- Exploitation of Data in Transit: Theft of information while in transit between devices.

Additional Information

- Event Description (description): A concise narrative detailing the event, typically ranging from one to three sentences.
- Source URL (source_url): A direct link to the information source utilized in compiling the data.
- Target Country (targeted_country): An ISO three-letter code identifying the country where the target organization is located.
- Actor Country (actor_country): A corresponding ISO three-letter code for the location of the actor.

The utilization of the Cyber Events Database has the potential to yield valuable insights into the cybersecurity landscape :

- Trend Analysis: It is imperative for users to engage in the analysis of data to identify trends in cyber incidents. Such trends may include the increasing prevalence of ransomware attacks or targeted attacks against critical infrastructure, which have escalated in recent years.
- Sector Vulnerabilities: By examining the database's categorization of incidents, researchers can identify sectors that are particularly vulnerable to cyber threats. This information can then inform risk assessments and resource allocation.
- Impact Assessment: The database facilitates the evaluation of the impact of specific incidents on organizations and broader societal implications, including economic repercussions and effects on national security.

 doi:10.20944/preprints202504.2169.v1

- Policy Development: It is imperative that policymakers take advantage of the findings from the database in order to formulate cybersecurity legislation and frameworks that are informed and take into account the most prevalent threats and vulnerabilities present in various sectors.
- Historical Context: The historical documentation of cyber incidents provides a context for understanding contemporary threats and the evolution of cybersecurity strategies from both organizational and governmental perspectives.

The Cyber Events Database, a resource provided by the Critical Infrastructure Security and Resilience team at the University of Maryland, is instrumental in comprehending the substantial trends and ramifications of cyber security incidents. Its structured, comprehensive approach facilitates detailed analysis and understanding of the current cybersecurity landscape. By leveraging this database, researchers and professionals can formulate effective strategies for mitigating risks and enhancing cybersecurity resilience.

2.6. Methodology

As previously stated, the present research study investigates the presence or absence of relationships between:

- The Actors and the Cyber incidents
- The Industry sectors and the Cyber incidents

Research Questions:

RQ1 A correlation has been observed between the type of actor and the type of cyber incident.

RQ2 The industry sector has been found to be correlated with the type of cyber incident.

The University of Maryland's Cyber Events database is a suitable dataset for this investigation, as it is capable of contributing to the study of our research questions. The database under consideration contains more than 14,000 cyberattack incidents, spanning the period from 2014 to 2024. Among the variables examined, three were identified as the most pertinent to the research interests under investigation. In the context of this study, the following variables are of particular relevance:

Actor Type (actor_type):

- Criminal
- Nation-State
- Terrorist
- Hacktivist
- Hobbyist

Event Type (event_type):

- Disruptive
- Exploitive
- Mixed

Industry Name (industry)

3. Results

Based on the above, the results are as follows:

RQ1: A correlation has been observed between the type of actor and the type of cyber incident

The null hypothesis (H0) and the alternative hypothesis (H1) of the chi-square independence test are formulated as follows for the pair of variables (actor_type, event_type):

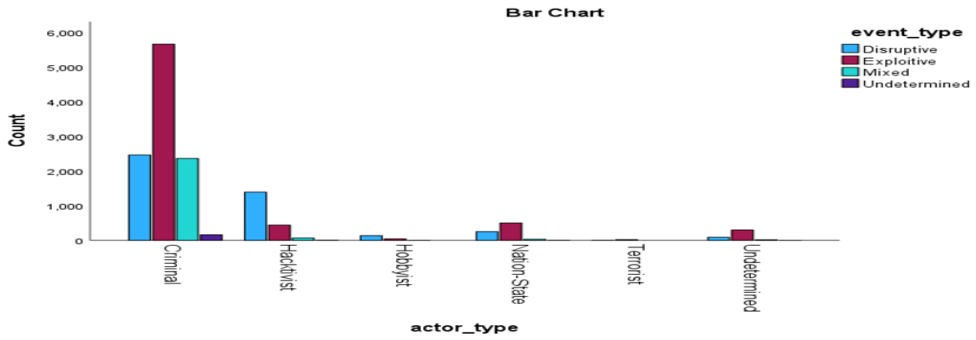
- H0: The null hypothesis posits that "Actor Type is independent of Event Type."
- H1: The alternative hypothesis posits that "Actor Type is not independent of Event Type."

Our first research question was examined using the chi-square test. The categorical variables employed in this study included actor type and event type. Both are nominal variables and include the categories presented above. The following contingency table enumerates the observations that fall into each combination.

 doi:10.20944/preprints202504.2169.v1

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
actor_type * event_type	14041	100.0%	0	0.0%	14041	100.0%



actor_type * event_type Crosstabulation

			event_type				
			Disruptive	Exploitive	Mixed	Undetermined	Total
actor_type	Criminal	Count	2470	5671	2369	166	10676
		Expected Count	3315.1	5322.4	1900.9	137.6	10676.0
		% within actor_type	23.1%	53.1%	22.2%	1.6%	100.0%
		Adjusted Residual	-36.1	13.8	24.2	5.0	
	Hacktivist	Count	1397	447	73	9	1926
		Expected Count	598.1	960.2	342.9	24.8	1926.0
		% within actor_type	72.5%	23.2%	3.8%	0.5%	100.0%
		Adjusted Residual	42.4	-25.2	-17.3	-3.4	
	Hobbyist	Count	139	48	4	0	191
		Expected Count	59.3	95.2	34.0	2.5	191.0
		% within actor_type	72.8%	25.1%	2.1%	0.0%	100.0%
		Adjusted Residual	12.5	-6.9	-5.7	-1.6	
	Nation-State	Count	256	507	35	5	803
		Expected Count	249.3	400.3	143.0	10.4	803.0
		% within actor_type	31.9%	63.1%	4.4%	0.6%	100.0%
		Adjusted Residual	.5	7.8	-10.3	-1.7	
	Terrorist	Count	5	25	0	0	30
		Expected Count	9.3	15.0	5.3	.4	30.0
		% within actor_type	16.7%	83.3%	0.0%	0.0%	100.0%
		Adjusted Residual	-1.7	3.7	-2.6	-.6	
	Undetermined	Count	93	302	19	1	415
		Expected Count	128.9	206.9	73.9	5.3	415.0
		% within actor_type	22.4%	72.8%	4.6%	0.2%	100.0%
		Adjusted Residual	-3.9	9.5	-7.1	-1.9	
Total		Count	4360	7000	2500	181	14041
		Expected Count	4360.0	7000.0	2500.0	181.0	14041.0
		% within actor_type	31.1%	49.9%	17.8%	1.3%	100.0%

The chi-square test yielded a statistic of $\chi^2 = 2308.371$ with 15 degrees of freedom (df = 15), $p < 0.001$. This finding suggests the presence of a statistically significant correlation between the variables under study.

 doi:10.20944/preprints202504.2169.v1

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2308.371[a]	15	<.001
Likelihood Ratio	2247.332	15	<.001
N of Valid Cases	14041		

a. 2 cells (8.3%) have expected count less than 5. The minimum expected count is .39.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	.405	<.001
	Cramer's V	.234	<.001
N of Valid Cases		14041	

Furthermore, all of the test criteria were met. Specifically, the following conditions were satisfied:

- The expected cell frequencies all met the required conditions (80% of the cells are greater than or equal to 5).
- The categories of the categorical variables are more than two.
- The sample size is large.

RQ2: The industry sector has been found to be correlated with the type of cyber incident

The null hypothesis (H0) and the alternative hypothesis (H1) of the chi-square independence test are formulated as follows for the pair of variables (industry, event_type):

- H0: The null hypothesis posits that " Industry is independent of Event Type."
- H1: The alternative hypothesis posits that " Industry is not independent of Event Type."

Our second research question was examined using the chi-square test. The categorical variables employed in this study included industry and event type. Both are nominal variables and include the categories presented above. The following contingency table enumerates the observations that fall into each combination.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
industry * event_type	14041	100.0%	0	0.0%	14041	100.0%

 doi:10.20944/preprints202504.2169.v1

industry * event_type Crosstabulation

			event_type				
			Disruptive	Exploitive	Mixed	Undetermined	Total
industry	Accommodation and Food Services	Count	38	221	43	4	306
		Expected Count	95.0	152.6	54.5	3.9	306.0
		% within industry	12.4%	72.2%	14.1%	1.3%	100.0%
		Adjusted Residual	-7.1	7.9	-1.7	.0	
	Administrative and Support and Waste Management and Remediation Services	Count	45	96	35	3	179
		Expected Count	55.6	89.2	31.9	2.3	179.0
		% within industry	25.1%	53.6%	19.6%	1.7%	100.0%
		Adjusted Residual	-1.7	1.0	.6	.5	
	Agriculture, Forestry, Fishing and Hunting	Count	6	3	9	0	18
		Expected Count	5.6	9.0	3.2	.2	18.0
		% within industry	33.3%	16.7%	50.0%	0.0%	100.0%
		Adjusted Residual	.2	-2.8	3.6	-.5	
	Arts, Entertainment, and Recreation	Count	163	213	40	4	420
		Expected Count	130.4	209.4	74.8	5.4	420.0
		% within industry	38.8%	50.7%	9.5%	1.0%	100.0%
		Adjusted Residual	3.5	4	-4.5	-.6	
	Construction	Count	9	10	27	1	47
		Expected Count	14.6	23.4	8.4	.6	47.0
		% within industry	19.1%	21.3%	57.4%	2.1%	100.0%
		Adjusted Residual	-1.8	-3.9	7.1	.5	
	Educational Services	Count	438	583	276	25	1322
		Expected Count	410.5	659.1	235.4	17.0	1322.0
		% within industry	33.1%	44.1%	20.9%	1.9%	100.0%
		Adjusted Residual	1.7	-4.4	3.1	2.0	
	Finance and Insurance	Count	300	855	173	12	1340
		Expected Count	416.1	668.0	238.6	17.3	1340.0
		% within industry	22.4%	63.8%	12.9%	0.9%	100.0%
		Adjusted Residual	-7.2	10.7	-4.9	-1.3	
	Health Care and Social Assistance	Count	334	1070	436	25	1865
		Expected Count	579.1	929.8	332.1	24.0	1865.0
		% within industry	17.9%	57.4%	23.4%	1.3%	100.0%
		Adjusted Residual	-13.2	7.0	6.8	.2	
	Health Care and Social Services	Count	4	11	11	1	27
		Expected Count	8.4	13.5	4.8	.3	27.0
		% within industry	14.8%	40.7%	40.7%	3.7%	100.0%
		Adjusted Residual	-1.8	-.9	3.1	1.1	
	Information	Count	585	709	138	9	1441
		Expected Count	447.5	718.4	256.6	18.6	1441.0
		% within industry	40.6%	49.2%	9.6%	0.6%	100.0%
		Adjusted Residual	8.3	-.5	-8.6	-2.4	
	Management of Companies and Enterprises	Count	5	8	7	0	20
		Expected Count	6.2	10.0	3.6	.3	20.0
		% within industry	25.0%	40.0%	35.0%	0.0%	100.0%
		Adjusted Residual	-.6	-.9	2.0	-.5	
	Manufacturing	Count	168	204	264	9	645
		Expected Count	200.3	321.6	114.8	8.3	645.0
		% within industry	26.0%	31.6%	40.9%	1.4%	100.0%
		Adjusted Residual	-2.8	-9.5	15.7	.2	
	Mining, Quarrying, and Oil and Gas Extraction	Count	32	30	10	1	73
		Expected Count	22.7	36.4	13.0	.9	73.0
		% within industry	43.8%	41.1%	13.7%	1.4%	100.0%
		Adjusted Residual	2.4	-1.5	-.9	.1	
	Other Services (except Public Administration)	Count	291	555	86	5	937
		Expected Count	291.0	467.1	166.8	12.1	937.0
		% within industry	31.1%	59.2%	9.2%	0.5%	100.0%
		Adjusted Residual	0	5.9	-7.1	-2.1	
	Professional, Scientific, and Technical Services	Count	188	649	324	9	1170
		Expected Count	363.3	583.3	208.3	15.1	1170.0
		% within industry	16.1%	55.5%	27.7%	0.8%	100.0%
		Adjusted Residual	-11.6	4.0	9.2	-1.6	
	Public Administration	Count	1253	1041	310	44	2648
		Expected Count	822.3	1320.1	471.5	34.1	2648.0
		% within industry	47.3%	39.3%	11.7%	1.7%	100.0%
		Adjusted Residual	20.1	-12.0	-9.1	1.9	
	Real Estate and Rental and Leasing	Count	16	40	28	0	84
		Expected Count	26.1	41.9	15.0	1.1	84.0
		% within industry	19.0%	47.6%	33.3%	0.0%	100.0%
		Adjusted Residual	-2.4	-.4	3.7	-1.1	
	Retail Trade	Count	57	321	84	7	469
		Expected Count	145.6	233.8	83.5	6.0	469.0
		% within industry	12.2%	68.4%	17.9%	1.5%	100.0%
		Adjusted Residual	-9.0	8.2	.1	.4	
	Transportation and Warehousing	Count	229	136	70	8	443
		Expected Count	137.6	220.9	78.9	5.7	443.0
		% within industry	51.7%	30.7%	15.8%	1.8%	100.0%
		Adjusted Residual	9.5	-8.2	-1.1	1.0	
	Undetermined	Count	56	112	40	2	210
		Expected Count	65.2	104.7	37.4	2.7	210.0
		% within industry	26.7%	53.3%	19.0%	1.0%	100.0%
		Adjusted Residual	-1.4	1.0	.5	-.4	
	Utilities	Count	119	81	60	10	270
		Expected Count	83.8	134.6	48.1	3.5	270.0
		% within industry	44.1%	30.0%	22.2%	3.7%	100.0%
		Adjusted Residual	4.7	-6.6	1.9	3.6	
	Wholesale Trade	Count	24	52	29	2	107
		Expected Count	33.2	53.3	19.1	1.4	107.0
		% within industry	22.4%	48.6%	27.1%	1.9%	100.0%
		Adjusted Residual	-1.9	-.3	2.5	.5	
Total		Count	4360	7000	2500	181	14041
		Expected Count	4360.0	7000.0	2500.0	181.0	14041.0
		% within industry	31.1%	49.9%	17.8%	1.3%	100.0%

The chi-square test yielded a statistic of $\chi^2 = 1631.719$ with 63 degrees of freedom (df = 63), $p < 0.001$. This finding suggests the presence of a statistically significant correlation between the variables under study.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1631.719[a]	63	<.001
Likelihood Ratio	1604.880	63	<.001
N of Valid Cases	14041		

a. 14 cells (15.9%) have expected count less than 5. The minimum expected count is .23.

 doi:10.20944/preprints202504.2169.v1

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	.341	<.001
	Cramer's V	.197	<.001
N of Valid Cases		14041	

Furthermore, all of the test criteria were met. Specifically, the following conditions were satisfied:

- The expected cell frequencies all met the required conditions (80% of the cells are greater than or equal to 5).
- The categories of the categorical variables are more than two.
- The sample size is large.

4. Discussion

The cybersecurity landscape in the European Union is marked by a mounting cognizance of the perils engendered by cyber incidents, as substantiated by the establishment of comprehensive frameworks by directives such as NIS1 and NIS2, in conjunction with the inauguration of pivotal data repositories including the European Repository of Cyber Incidents (EuRepoC) and the Cyber Events Database from the University of Maryland. These frameworks and databases serve as pivotal tools for understanding the dynamics between the types of actors engaged in cyber activities and the nature of incidents they perpetrate, as noted through research findings. Specifically, the results of the chi-square tests indicated robust correlations between the types of actors and cyber incidents (RQ1) and between industry sectors and the incidents (RQ2). These findings served to validate the initial research hypotheses [14].

The substantial correlation between actor types and incident types corroborates extant literature suggesting that particular actors are more prone to perpetrate specific types of cyber incidents. For instance, nation-state actors are typically attributed to sophisticated espionage-related cyber incidents, while criminal actors often exploit financial vulnerabilities [15]. The aforementioned patterns underscore the considerable heterogeneity within the actor landscape. Consequently, it is imperative that tailored cybersecurity strategies be formulated that account for the motives and capabilities of these different actors [16].

Furthermore, an analysis of the relationships between various industry sectors and their susceptibility to distinct types of cyber incidents reveals that critical sectors, such as healthcare and public administration, are especially vulnerable [17,18]. The implications of these findings are significant, as they underscore the necessity of conducting sector-specific risk assessments. Reports have emphasized the increasing sophistication of cyberattacks on healthcare infrastructures, necessitating a focused approach to the development of cybersecurity policy. Such an approach would need to incorporate lessons learned from the trends observed in the Cyber Events Database and other states' cybersecurity strategies [19,20].

Data-driven insights from repositories such as EuRepoC play a significant role in identifying and analyzing trends within the cybersecurity landscape [21,22]. By facilitating the examination of incident contexts—including categorical classifications such as incident type, actor motivations, and operational impacts—these databases enable researchers and policymakers to tailor their responses more effectively. Evidently, data repositories are indispensable for the procurement of immediate operational insights. Moreover, they are integral to the broader formulation of preventive and reactive cybersecurity policies across European sectors.

5. Conclusions

The findings of this research underscore the critical importance of cultivating an informed understanding of the relationships between actor types, incident types, and industry sectors in the evolving realm of cybersecurity. The statistical evidence from the chi-square tests corroborates our hypotheses and supports the narrative that a nuanced understanding of actor motivations and sector

 doi:10.20944/preprints202504.2169.v1

vulnerabilities is essential for formulating effective cybersecurity governance mechanisms within the European Union.

In the face of escalating cyber threats, both in terms of frequency and complexity, the importance of comprehensive data repositories such as EuRepoC and the Cyber Events Database cannot be overstated. These tools offer two primary benefits. First, they provide essential insight into the nature of cyber incidents. Second, they enable the creation of targeted, evidence-based policies that can enhance resilience against cyber threats. In the future, the incorporation of empirical data into policy discussions will be essential for ensuring a proactive and adaptable cybersecurity posture across the EU.

The cornerstone of a robust European cybersecurity environment is ultimately formed by continued collaboration among member states, leveraging insights from incident data, and fostering sector-specific security awareness. This will safeguard essential services and public trust across the continent.

References

1. https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng
2. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
3. https://www.enisa.europa.eu/
4. https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union
5. https://cissm.umd.edu/research-impact/publications/cyber-events-database-home
6. https://eurepoc.eu/database/
7. https://libguides.library.kent.edu/spss/chisquare
8. https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
9. https://www.enisa.europa.eu/publications/enisa-nis360-2024
10. https://eurepoc.eu/
11. https://cissm.umd.edu/cyber-events-database
12. Harry, C., & Gallagher, N. (2018). Classifying Cyber Events. Journal of Information Warfare, 17(3), 17-31 https://cissm.umd.edu/sites/default/files/2019-07/Cyber-Taxonomy-101918.pdf
13. https://doi.org/10.4337/9781839109362.00007
14. Saalman, L., Su, F., & Dovgal, L. (2023). Cyber crossover and its escalatory risks for europe.. https://doi.org/10.55163/siep1930
15. Stergiopoulos, G., Gritzalis, D., & Limnaios, E. (2020). Cyber-attacks on the oil & gas sector: a survey on incident assessment and attack patterns. Ieee Access, 8, 128440-128475. https://doi.org/10.1109/access.2020.3007960
16. Renaud, K. and Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by smes. Organizational Cybersecurity Journal Practice Process and People, 1(1), 24-46. https://doi.org/10.1108/ocj-03-2021-0004
17. Raizada, N. and Biswal, M. (2024). An evidence-based investigation of cert-in's reporting on cyber-threats in healthcare sector. Conhecimento & Diversidade, 16(42), 219-246. https://doi.org/10.18316/rcd.v16i42.11694
18. Alade, O., Amusan, E., & Ojo, O. (2024). Strategic assessment of intricacies in healthcare cyber security: analyzing distinctive challenges, evaluating their ramifications on healthcare delivery, and proposing advanced mitigation strategies. Asian Journal of Research in Computer Science, 17(5), 238-248. https://doi.org/10.9734/ajrcos/2024/v17i5452
19. Nasser, M., Ahmad, R., Yassin, W., Hassan, A., Zainal, Z., Salih, N., … & Hameed, K. (2018). Cyber-security incidents: a review cases in cyber-physical systems. International Journal of Advanced Computer Science and Applications, 9(1). https://doi.org/10.14569/ijacsa.2018.090169
20. Hugyik, A. (2020). Best practices in the application of the concept of resilience: building hybrid warfare and cybersecurity capabilities in the hungarian defense forces. Connections the Quarterly Journal, 19(4), 25-38. https://doi.org/10.11610/connections.19.4.02
21. Wang, K., Guo, X., & Yang, D. (2022). Research on the effectiveness of cyber security awareness in ics risk assessment frameworks. Electronics, 11(10), 1659. https://doi.org/10.3390/electronics11101659

 doi:10.20944/preprints202504.2169.v1

22. Shevchenko, P., Jang, J., Malavasi, M., Peters, G., Sofronov, G., & Trück, S. (2022). The nature of losses from cyber-related events: risk categories and business sectors.. https://doi.org/10.48550/arxiv.2202.10189