Hungarian Association of Agricultural Informatics
European Federation for Information Technology in Agriculture, Food and the Environment

Journal of Agricultural Informatics. Vol. 16, No. 2
journal.magisz.org

Cybersecurity Risks in Critical Infrastructures: Insights from CISA and ENISA Data

Zsanett Angyalos-Porkoláb, Róbert Szilágyi

I N F O
Received: 23/07/2025
Accepted: 29/05/2025
Available on-line 29/09/2025
Responsible Editor: László Várallyai

Keywords:
maximum 5 keywords, separated by commas. Securuty, risk, data, ENISA, CISA

A B S T R A C T

Cyberattacks on critical infrastructures have escalated in frequency and complexity over the past decade, posing systemic risks to national security, public safety, and economic stability. This study analyzes cybersecurity risks across key infrastructure sectors including energy, healthcare, finance, transportation, and others, drawing on threat intelligence from the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the EU Agency for Cybersecurity (ENISA), and industry sources such as IBM X-Force and Verizon DBIR. We compare U.S. and EU regulatory approaches, identifying strengths and limitations in frameworks like the NIS2 Directive and the NIST Cybersecurity Framework. Our findings show that while the EU favors centralized and mandatory compliance, the U.S. has leaned toward voluntary and sector-specific standards, although this is gradually changing. We also examine the most frequently targeted sectors, highlight trends in attack types such as ransomware, and discuss how smaller organizations, particularly SMEs and minority-owned businesses, often serve as vulnerable entry points for attackers. The results emphasize the urgent need for integrated and forward-looking cybersecurity strategies that combine regulation, collaboration, and continuous adaptation to an evolving threat landscape.

1. Introduction

Critical infrastructure refers to the key systems and services, both physical and digital, that a country depends on for its security, economy, public health, and safety. This includes areas like energy (such as power grids and pipelines), finance (banking systems), healthcare (hospitals and medical records), transportation (airports and railways), water supply, food distribution, and communication networks. As these sectors increasingly rely on digital technologies and interconnected networks, their vulnerability to cyber threats has grown significantly (Khan, 2025). Because of this, protecting critical infrastructure from cyberattacks has become a top security concern in both the United States and Europe.

In the past decade, cyberattacks targeting critical infrastructure have become more frequent and more severe. In the U.S., for example, the number of reported data breaches rose from just 447 in 2012 to over 3,200 by 2023.

Around the world, cyber threats have grown far more sophisticated. What used to be the work of lone hackers has evolved into coordinated operations led by well-organized groups, including state-sponsored teams and cybercrime networks, constantly developing new methods of attack. As a result, major cyber incidents that were once seen as rare exceptions have now become disturbingly common. Ransomware attacks, massive data breaches, and disruptive malware are regularly affecting organizations across all industries, including those responsible for critical infrastructure (Zaid & Garai, 2024). The risks are serious: a successful cyberattack on a power grid, transport network, or healthcare system could endanger public safety and disrupt the lives of millions.

Several high-profile cases show just how serious the impact of cyberattacks on critical infrastructure can be. In 2015, a cyberattack on Ukraine's power grid caused a massive blackout, cutting electricity to hundreds of thousands of homes. (CISA, 2021) In May 2021, the Colonial Pipeline ransomware attack forced one of the largest fuel pipelines in the U.S. to shut down, leading to gas shortages and prompting a federal emergency response. (CISA, 2023)

That same year, the world's largest meat processor (JBS Foods) suffered a ransomware incident that halted meat production, highlighting threats to the food supply. Hospitals and healthcare providers have been hit with ransomware that crippled medical services, even during the COVID-19 pandemic. These examples illustrate that cyber incidents can cascade into physical disruptions of energy supplies, transportation, food distribution, and healthcare delivery. In summary, critical infrastructures constitute highly attractive targets for adversaries, yet many operators have historically lacked the resources or maturity to implement adequate security measures (Sentinelone, 2021).

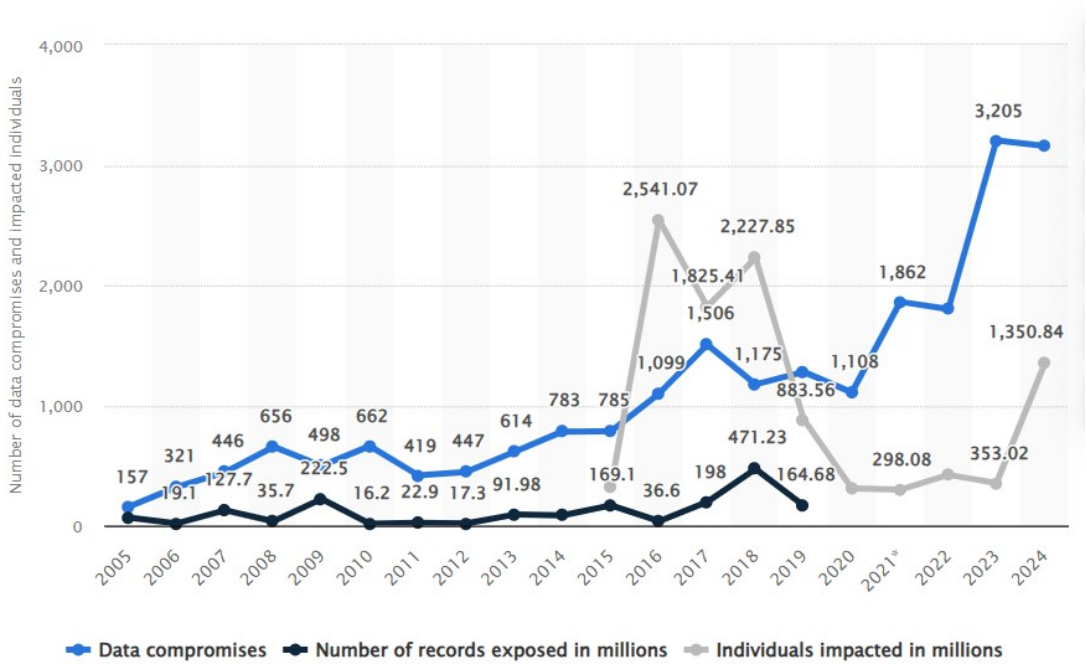

Figure 1. Annual number of data compromises and individuals impacted in the United States from 2005 to 2024

Source: Statista

This article aims to provide a comprehensive analysis of cybersecurity risks in critical infrastructure sectors, drawing on data and reports from leading authorities. In doing so, it bridges both policy and technical dimensions, examining real-world threats and systemic responses.

The research is guided by three main questions:

1. What are the differences between U.S. and European approaches to regulating and protecting critical infrastructures, and how might these regimes be harmonized or improved?
2. Which critical infrastructure sectors are most frequently targeted by cyber attacks, according to recent data?
3. How have the prevalence and types of cyber threats to critical infrastructure evolved over the past decade?

Addressing these questions will enable a structured examination of cybersecurity threats, regulatory approaches, and threat evolution across the U.S. and the EU.

2. Methodology

To address the research questions, this study applied an interdisciplinary methodology that integrates cybersecurity analytics, regulatory policy analysis, and organizational risk perspectives. The research design combined qualitative policy review, incident trend analysis, and content-based interpretation of technical reports.

The study began with a comparative review of cybersecurity governance frameworks in the United States and the European Union. Key documents including the NIS1 and NIS2 Directives, the GDPR, the NIST Cybersecurity Framework, and sector-specific standards such as NERC CIP were examined to identify differences in scope, enforcement, incident reporting obligations, and institutional roles.

To map trends in cyber threats, the study then reviewed incident data from 2013 to 2023, using publicly available reports and datasets from ENISA, CISA, IBM X-Force, and Verizon DBIR. The focus was on the frequency and typology of attacks (particularly ransomware, data breaches, and DDoS incidents) across various critical infrastructure sectors. The data were used to highlight evolving attack patterns and differences between the U.S. and EU threat landscapes.

Finally, to enrich the analysis, qualitative content review was performed on official reports, policy alerts, and threat assessments published by national and sectoral agencies. The goal was to identify how risks are described, which vulnerabilities are prioritized, and what defensive strategies are emphasized in both regions.

3. Results

3.1 Regulatory Differences: EU vs. US Approaches to Critical Infrastructure Cybersecurity

Governing the cybersecurity of critical infrastructures requires a complex mix of policy, regulation, and public-private collaboration. The United States and the European Union have developed different approaches over time, reflecting their distinct legal systems and threat perceptions. Here, We compare the two regimes across several dimensions – scope of coverage, prescriptiveness of requirements, incident reporting mandates, and enforcement – focusing on key frameworks like the EU's NIS2 Directive and GDPR, versus U.S. guidelines from CISA, sector-specific standards (e.g. NERC CIP for energy), and federal programs like FedRAMP.

Scope and Strategy: The European Union's approach to critical infrastructure cybersecurity has been characterized by comprehensive, binding legislation that imposes baseline requirements across member states. The first major EU-wide law was the Network and Information Security Directive of 2016 (known as NIS1), which required essential service operators in sectors like energy, transport, banking, health, water, and digital infrastructure to implement security measures and report incidents. However, NIS1 gave member states some leeway in implementation, leading to fragmentation. Learning from that, the EU adopted an updated NIS2 Directive in 2022, which significantly broadens the scope of regulation and tightens requirements. NIS2 applies to an even wider set of sectors – including some that were not in NIS1, such as waste management, space, food production, manufacturing, and public administration effectively covering "all sectors of the economy" that are either critical or considered important providers of services NIS2 is less voluntary than NIS1 and is designed to reduce divergence by being more prescriptive (European Commission, 2022). It requires each EU member state to translate its provisions into national law (by October 2024) and ensure that both public and private entities in the covered sectors comply. (ENISA)

As highlighted by recent research, ENISA's role has evolved from a technical advisory body into a strategic regulatory actor, shaping accountability frameworks across data protection, ePrivacy, and cybersecurity domains (Dunn Cavelty & Smeets, 2023). This reflects a broader trend within the EU toward embedding legal responsibility and oversight into cybersecurity governance structures (Voss, 2021).

In contrast to the EU's centralized and binding regulatory model, the United States has historically taken a more decentralized and sector-specific approach to critical infrastructure cybersecurity. Rather than imposing comprehensive federal mandates, the U.S. strategy has emphasized voluntary frameworks, industry collaboration, and incentives, except in certain high-risk sectors. The federal government designates 16 critical infrastructure sectors, such as energy, finance, healthcare, and defense, each overseen by a Sector Risk Management Agency (SRMA) responsible for sector-specific guidance and coordination.

However, this governance model remains fragmented, with overlapping and sometimes competing responsibilities among federal agencies. As Folio, Ross, Wolfe, and Weigel (2025) note,

such decentralization can create ambiguity over which authority is responsible during a cyber incident, thereby hindering timely and coordinated responses.

Some sectors have mandatory cybersecurity standards (often in response to past incidents or clear risks), while others rely on voluntary frameworks. For example, the electric power grid is subject to federally enforceable NERC CIP standards (Critical Infrastructure Protection standards) which set detailed technical controls for bulk power system operators. Similarly, the nuclear sector has strict NRC cybersecurity regulations, and the transportation sector has some regulations. In finance, banks must follow FFIEC cybersecurity guidance and the NYDFS cyber regulations if in New York, etc.

One notable U.S. initiative was the development of the NIST Cybersecurity Framework (CSF), first released in 2014, which provides a voluntary set of best practices (Identify, Protect, Detect, Respond, Recover) widely adopted by companies as a baseline.

In essence, the U.S. approach has been more decentralized and flexible, whereas the EU approach has been more centralized and standardized.

Security Requirements and Controls: Under EU's NIS2, organizations in scope must implement a comprehensive set of cybersecurity measures. These include risk analysis and mitigation policies, incident handling processes, business continuity/disaster recovery plans, supply chain security measures, secure system development practices, vulnerability disclosure policies, cyber hygiene and training, access control (including use of multi-factor authentication), and encryption of data. NIS2 explicitly enumerates these as obligations. Management bodies of companies can be held accountable if they fail to ensure compliance. Additionally, NIS2 mandates incident reporting: significant incidents must be reported to the national CSIRT within 24 hours and a detailed report within 72 hours, and a final report within one month.

Another EU law, the General Data Protection Regulation (GDPR) of 2018, while focused on data privacy, also indirectly improved cybersecurity: it requires any organization (including critical infrastructure entities) that handles personal data to implement appropriate security and to report personal data breaches within 72 hours. GDPR's penalties incentivized companies to strengthen controls to avoid breaches. In the context of critical infrastructure, consider a hospital or energy utility - if a cyber attack leads to exposure of personal data (patient records or customer info), GDPR can come into play with severe consequences. Thus, GDPR and NIS2 together impose both technical duties and breach disclosure duties on EU critical infrastructure operators, backed by significant fines.

The U.S. currently lacks a single overarching equivalent. Instead, security requirements are scattered: sectoral regulations (like NERC CIP standards which include ~12 detailed standards covering baseline cybersecurity for the electric grid, such as CIP-007 on system security management, CIP-010 on configuration change management, etc.), federal guidelines, and contractual requirements. For instance, water utilities until recently had no mandatory federal cyber standards; in 2021 Congress considered legislation to empower the EPA to enforce cybersecurity in water systems. Healthcare entities must follow the HIPAA Security Rule (which sets general requirements like risk assessment and access controls for protecting electronic health records), a legal requirement but less technically detailed than NIS2's catalog. Pipeline operators got new requirements from TSA in 2021-2022 (after Colonial) that mandate specific measures like having an incident response plan and conducting vulnerability assessments. Many of the "requirements" in U.S. critical sectors have historically been voluntary best practices promoted by agencies like CISA or sector coordinating councils. For example, in 2018 the DoE launched a voluntary Cybersecurity Capability Maturity Model (C2M2) for energy companies. The CISA Cybersecurity Performance Goals (CPGs) released in 2022 are another voluntary tool – essentially a prioritized subset of practices from the NIST CSF aimed at critical infrastructure small/medium enterprises. While highly useful, these are not enforceable.

One area where the U.S. has a well-defined program is cloud security for government: the FedRAMP (Federal Risk and Authorization Management Program), established in 2011, provides a

standardized security assessment framework for cloud service providers used by federal agencies. Cloud providers must implement rigorous controls (based on NIST 800-53) and undergo audits to become FedRAMP authorized. (GSA)

Although FedRAMP is not specific to critical infrastructure sectors, many critical infrastructure organizations rely on cloud services, so FedRAMP indirectly raises the security baseline of widely used cloud offerings (AWS, Azure, Google Cloud are all FedRAMP compliant at high levels, meaning they meet strong encryption, access control, monitoring, and testing standards).

Incident Reporting and Information Sharing: One of the biggest practical differences is how incidents are reported and shared. The EU's NIS2 makes reporting mandatory as described (within 24 hours for notice, etc.) to national authorities/CSIRTs. These reports are intended to enable a cooperative response and to feed into EU-level awareness. The U.S. historically relied on voluntary reporting, which meant many incidents were not brought to the government's attention unless the victim chose to disclose or needed help. However, this is changing: the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022 will require many critical infrastructure entities in the U.S. to report significant cyber incidents to CISA within 72 hours, and any ransomware payments within 24 hours.

Enforcement and Accountability: In the EU, failure to comply with NIS2 can result in fines. GDPR fines for data breaches have already been enforced in multiple cases (e.g. a €10 million fine to a German telecom for security failings). The EU's philosophy is that cybersecurity is a regulated compliance issue akin to financial auditing or environmental regulation.

The culture of enforcement is less uniform in the U.S. because many critical infrastructure entities are privately owned and regulated by different bodies. The result is that EU operators face a more clear-cut obligation to invest in cybersecurity or face penalties, whereas U.S. operators may face market and reputational pressure, but not always legal penalties unless they fall under specific regulations or are found grossly negligent. However this is changing gradually as critical infrastructure cyber incidents get more attention.

Public-Private Collaboration vs. Regulation: The U.S. has placed a big emphasis on voluntary public-private partnerships for critical infrastructure protection. Organizations like the National Infrastructure Advisory Council (NIAC) and sector coordinating councils bring industry and government together to develop best practices. The logic has been that industry often owns the assets, so cooperation is better than heavy regulation that might be inflexible. Indeed, many improvements in sectors have come from these collaborations and the sharing of threat information by agencies like CISA with companies. In the EU, while collaboration also exists, the framework leans more toward regulatory compliance, industry must meet certain standards and authorities can assist but ultimately will enforce if needed. Neither approach in pure form is perfect: a purely voluntary regime can leave gaps, whereas an overly rigid regulation can become outdated given fast technology changes or create a compliance mentality over security mindset.

Comparative Summary: In simple terms, EU cybersecurity laws for critical infrastructure are more stringent and centralized, requiring broad compliance and reporting, whereas U.S. policies have been more fragmented and voluntary, until recently. However, the trajectories are converging somewhat. The U.S. is introducing more mandatory elements (incident reporting, sector-specific regulations) as the threat level demands it. U.S. lawmakers may be waiting to see NIS2's impact in Europe before deciding on a similar comprehensive framework. At the same time, organizational investment in cybersecurity is influenced not just by regulation, but also by internal capabilities and past cyber incidents (Fernandez De Arroyabe et al., 2023).

3.2 Most Affected Sectors

Frequency of attacks by sector

Recent industry analyses indicate that all critical infrastructure sectors are exposed to cyber threats, although the distribution of incidents is not uniform. According to the IBM X-Force Threat

Intelligence Index, the manufacturing sector accounted for the largest proportion of observed cyberattacks in both 2021 and 2022, representing approximately 24.8% of incidents in the latter year. The financial and insurance sector followed, with 18.9% of reported cases (IBM, 2023). This trend suggests a sustained targeting pattern, likely attributable to the operational impact of disruptions in manufacturing environments and the presence of valuable intellectual property. Ransomware and industrial espionage have been identified as primary vectors, with attackers exploiting the high cost of downtime and the strategic importance of proprietary technologies (Spanning, 2022).

IBM's findings are consistent with those of other industry analyses. For instance, research by Security Intelligence has identified manufacturing, finance, and professional services as high-risk sectors, primarily due to their low tolerance for operational disruptions and relatively high capacity to meet extortion demands (PGIM, 2023).

Complementing this, the 2023 Verizon Data Breach Investigations Report (DBIR) provides insight into confirmed breach incidents rather than general attack attempts. According to the DBIR, the financial services sector experienced the highest number of confirmed data breaches within the reporting period (Verizon, 2023). Financial institutions, including banks, insurance companies, and investment firms, remain consistent targets for both financially motivated cybercriminals and state-sponsored actors, due to the direct exploitation potential of financial assets and sensitive data. Significant breach activity has also been reported in the public sector. ENISA's Threat Landscape 2023 identifies public administration as the most frequently targeted sector in Europe, accounting for approximately 19% of all documented incidents. This trend likely reflects the critical role of government agencies in maintaining essential services and managing large-scale citizen data repositories. Additionally, many public institutions operate on constrained budgets and rely on outdated digital infrastructures, which further increases their exposure to cyber threats.

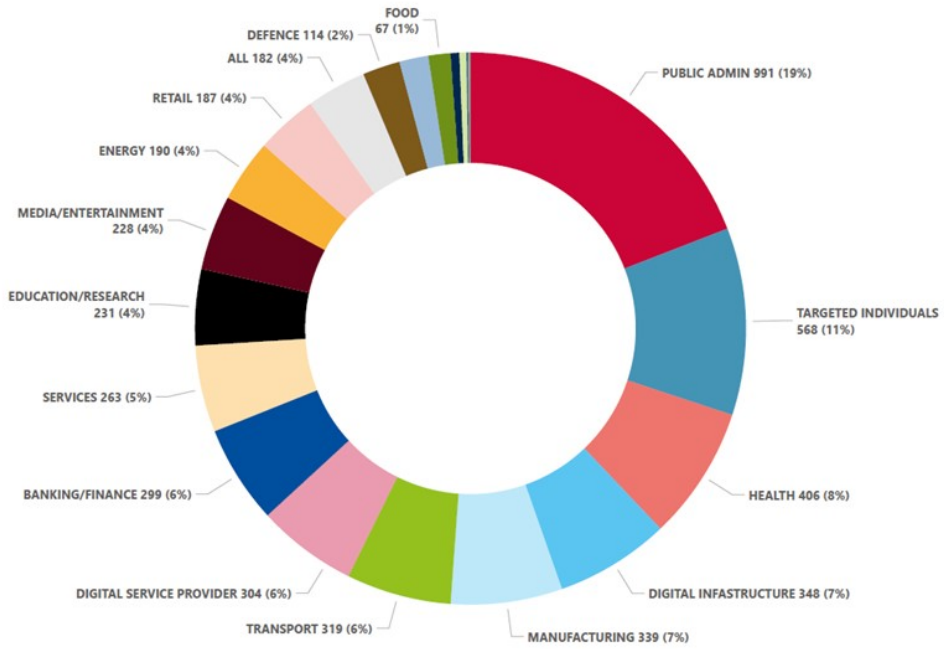

Figure 2. Targeted sectors per number of incidents (July 2022 - June 2023)

Source: ENISA's Threat Landscape 2023

The healthcare and public health sectors have also experienced a notable increase in cyberattacks in recent years. A fundamental vulnerability in smart hospital environments stems

from the exceptionally high value of personal health information, which is often regarded as more lucrative than financial data. In addition to compromising sensitive patient records, cybercriminals may target healthcare systems to gain access to prescription medications or disrupt medical services (Mayol et al., 2016).

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), healthcare represents a "target-rich, cyber-poor" area, frequently attacked, yet chronically underfunded in terms of cybersecurity investment. The 2023 Verizon DBIR identified healthcare as one of the sectors most affected by ransomware incidents in the preceding year. In the European context, ENISA similarly reported that the healthcare sector accounted for approximately 8% of all documented cyber incidents, underscoring its continued position among the most targeted critical infrastructure domains (ENISA, 2023).

While traditionally recognized sectors such as finance, healthcare, and public administration continue to dominate cybersecurity risk assessments, emerging domains are increasingly exhibiting significant vulnerabilities. One such domain is agriculture, where the integration of digital technologies has introduced a range of complex cyber risks. In particular, the rise of smart farming systems, which depend on interconnected IoT devices, automation, and cloud-based infrastructures, has created new attack surfaces and operational dependencies that are not yet fully addressed by existing security frameworks (Bui et al., 2024).

Small and medium-sized businesses (SMBs), which are often part of critical infrastructure supply chains, frequently lack the cybersecurity resources or expertise to defend against sophisticated threats. It is observed that the digital maturity of small and medium-sized enterprises (SMEs) lags considerably behind that of large enterprises. This disparity substantially elevates cybersecurity risks for all stakeholders, as SMEs often represent numerous potential points of vulnerability within interconnected systems. (Péntek, Anita, & Tamás, 2025) As Saha and Anwar highlight, despite leveraging modern technologies, many entrepreneurs remain unprepared for cybersecurity challenges, and the absence of a tailored governance framework puts their operations, and by extension, the broader infrastructure they support, at significant risk

Beyond the commonly highlighted areas, several additional sectors have emerged as critical focal points due to their strategic importance and evolving cyber threat exposure.

Energy systems continue to represent high-value targets, particularly for state-sponsored threat actors. High-profile incidents such as the 2015 cyberattack on Ukraine’s power grid and the 2021 ransomware attack on the Colonial Pipeline illustrate the potential for major operational and societal disruption. While the sector may not experience the highest volume of attacks, the potential impact of successful intrusions makes it a persistent focus for sophisticated adversaries. Regulatory frameworks such as the North American Electric Reliability Corporation’s Critical Infrastructure Protection (NERC CIP) standards reflect the strategic necessity of maintaining robust cybersecurity in this domain (Allianz, 2016).

Transportation infrastructure (including airports, railways, and maritime ports) has likewise become an increasingly prominent target. ENISA’s assessments consistently rank transportation among the top affected sectors, with attacks frequently driven by extortion or aimed at causing cascading operational delays. The inherent interconnectivity of transportation networks renders them particularly vulnerable to disruptions that can ripple across entire supply chains (CybersecurityDive, 2022).

Water and food supply systems, while historically considered less susceptible, have recently been subject to increased scrutiny following a series of targeted incidents. For example, the Florida water treatment facility breach and ransomware attacks on food producers have exposed significant cybersecurity gaps. According to CISA, the combination of aging infrastructure and limited cybersecurity investment leaves these sectors acutely vulnerable, prompting their elevation within recent U.S. critical infrastructure protection efforts.

In summary, the finance, government, and manufacturing sectors consistently appear as the most targeted domains across multiple sources, with healthcare, energy, and transportation also demonstrating elevated levels of exposure. ENISA data from Europe identifies public administration as the most frequently targeted sector, while IBM and Verizon's global data rank manufacturing and finance at the top. These discrepancies may be attributed to differences in threat environments and reporting practices, for example, a higher incidence of data breaches in the U.S. private financial sector, contrasted with politically motivated attacks on European governmental institutions. Despite these regional and sectoral variations, a recurring pattern emerges: threat actors tend to focus on sectors where disruptions generate significant operational or financial impact. Financially motivated attackers often prioritize industries with low tolerance for downtime, such as manufacturing, healthcare, and food production. In contrast, state-sponsored actors and ideologically driven groups are more likely to target government agencies, energy systems, and transportation infrastructure due to their strategic and societal relevance. The financial sector represents a convergence point, serving both as a lucrative target for cybercriminals and a critical node of interest for geopolitical adversaries.

It is also important to emphasize that smaller entities within critical infrastructure sectors frequently serve as vulnerable points within larger systems. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has noted that numerous recent cyber incidents, particularly those involving ransomware, have affected small and medium-sized organizations operating within critical supply chains, including rural healthcare facilities, municipal water treatment plants, and local government offices.

In many cases, these entities lack the cybersecurity maturity, financial resources, or strategic planning capacity to implement adequate protection. This issue is particularly pronounced in developing economies, where small businesses often underestimate cyber risks and remain underprepared, as illustrated in the Indonesian case study by Yudhiyati et al. (2023).

Adversaries frequently exploit these gaps, recognizing that while smaller operators may appear less consequential, successful compromises can yield significant consequences, either directly or by serving as pivot points to larger, interconnected systems. This underscores the necessity of raising baseline cybersecurity standards across the full spectrum of infrastructure providers, not only among large-scale operators. The risks are even more acute for minority-owned small businesses, which often encounter structural disadvantages, including limited access to technical expertise and security resources (Thompson, 2023).

The following section examines how threat patterns affecting critical infrastructure have evolved over the past decade, with particular attention to the increasing prevalence of ransomware and the growing technical sophistication of threat actors.

4. Time Trends in Threats (2013–2023)

Over the past decade, the landscape of cyber threats to critical infrastructure has shifted dramatically. What began with relatively rudimentary attacks in the early 2010s has morphed into highly advanced, multi-stage campaigns by the 2020s.

Perhaps the clearest trend is the sheer growth in the volume of cyber incidents. The number of reported data breaches in the U.S. (across all sectors, including critical infrastructure) climbed year over year, from under 500 in 2012 to over 1,000 by 2016, and then to more than 1,800 in 2021 and 3,200+ in 2023. This reflects both improved reporting and an actual increase in malicious activity. In particular, ransomware has become a dominant threat since the mid-2010s. Around 2013, ransomware was an emerging issue primarily known within cybersecurity circles; by the early 2020s it had grown into a societal menace affecting hospitals, pipelines, city governments, and businesses worldwide. Verizon's data show ransomware usage in breaches rose by 13% from 2020 to 2022 alone (Verizon, 2022), and by 2023 ransomware was present in 23–24% of all breaches analyzed. IBM X-Force similarly notes that ransomware and extortion attacks have risen markedly, constituting roughly one-third of attacks in recent years. The years 2016–2017 were a turning point: WannaCry (2017) and NotPetya (2017) were two ransomware/wiper outbreaks that caused

global damage to critical systems (WannaCry hit healthcare in the UK, among others, and NotPetya crippled logistics and government networks in Ukraine and beyond).

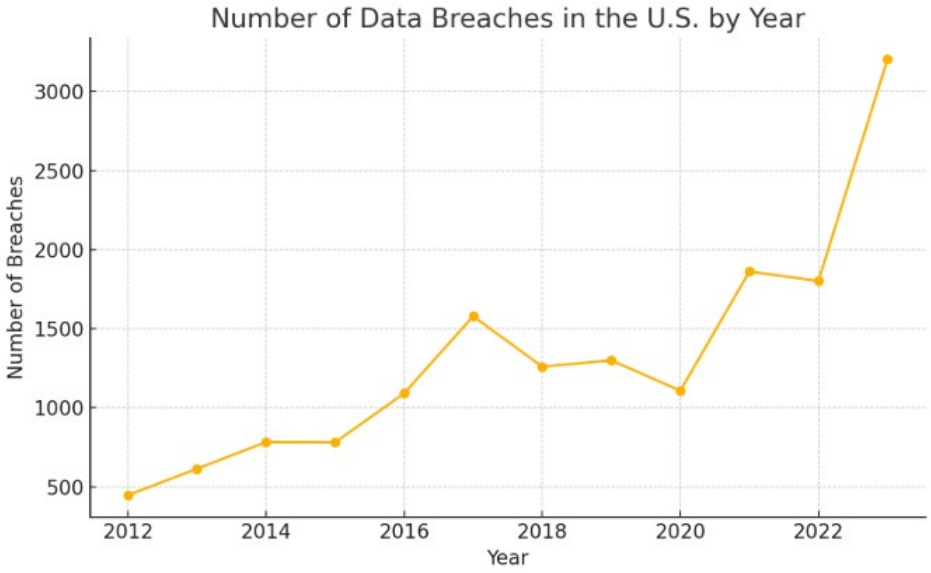

Figure 3. Number of data breaches in the United States per year (2012–2023)

Source: Statista

As the threat landscape continues to evolve, future cybersecurity strategies for critical infrastructure must adapt to emerging challenges. Recent research highlights several key trends, including the adoption of AI-driven threat detection, the shift toward zero-trust architectures, and the increasing use of stealthy, targeted attacks. (Daniel and Victor, 2024) emphasize that these developments demand a proactive, adaptive defense posture, as traditional perimeter-based models become increasingly inadequate.

Conclusion

Cybersecurity in critical infrastructure is no longer a purely technical concern. It is a systemic issue with societal, economic, and political dimensions. This article has shown that while cyber threats have become more sophisticated and widespread, the capacity to defend against them remains uneven across sectors and regions. Regulatory approaches vary: the EU has embraced a unified and mandatory framework, while the U.S. has historically favored sectoral autonomy and voluntary standards, although this is gradually shifting.

The real fault line, however, lies not only between continents but also between large, well-resourced entities and smaller, underfunded organizations embedded within critical systems. As threat actors increasingly exploit these weak links, protecting infrastructure requires more than just legal compliance. It calls for coordinated action, threat intelligence sharing, and an inclusive approach to security. The evolution of threats, from isolated breaches to large-scale ransomware campaigns, shows that we need ongoing investment, stronger cooperation across sectors, and a shift in mindset: instead of reacting to attacks, we must be prepared for them in advance.

References

Please use the Harvard Referencing System http://guides.is.uwa.edu.au/harvard (some examples are below). The Digital Object Identifier (DOI) have to use to cite and link to electronic documents (eg.doi: 10.4018/ijaeis.2015010101).

……

Allianz, 2016 - Cyber attacks on critical infrastructure. Download: 2025.05.28 https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html

Arroyabe, I., F.A. Arranz, C., Arroyabe, M., & Arroyabe, J. (2022). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers & Security, 124, 102954. doi:10.1016/j.cose.2022.102954

Bui, H. T., Aboutorab, H., Mahboubi, A., Gao, Y., Sultan, N. H., Chauhan, A., et al. (2024). Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems. Computers & Security, 140, 103754. doi:10.1016/j.cose.2024.103754

CISA, 2021 - Cyber-Attack Against Ukrainian Critical Infrastructure. Download: 2025.05.28 https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA, 2023 - The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. Download: 2025.05.28 https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

CybersecurityDive, 2022 - Food supplier cyber risk spreads 1 year after JBS attack. Download: 2025.05.28 https://www.cybersecuritydive.com/news/food-supplier-cyber-risk-spreads-jbs/624800/

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy, 30*, 1–23. doi:10.1080/13501763.2023.2173274

Folio, J., Ross, A., Wolfe, I., & Weigel, N. (2025). Seeking harmony: CISA's proposed cyber reporting rules for critical infrastructure are an ambitious work in progress. Cyber Security: A Peer-Reviewed Journal, 8, 255. doi:10.69554/JHEV8231

GSA – FedRAMP Download: 2025.05.28 https://www.gsa.gov/technology/government-it-initiatives/fedramp

Khan, M. (2025). Cybersecurity in critical infrastructure: Challenges and future directions

Mayol, J., Manzoni, A., Calcavecchia, F., Iliev, Y., Kabisch, B., et al. (2016). Smart hospitals security and resilience for smart health service and infrastructures NOVEMBER 2016 smart hospitals about ENISA doi:10.2824/28801

Péntek, A., Anita, P., & Tamás, K. (2025). How to increase workflow efficiency for micro and small businesses with a custom-built mobile app in hungary - a case study for a language learning school. Applied Studies in Agribusiness and Commerce, 18 doi:10.19041/APSTRACT/2024/2/3

PGIM, 2023 - Cybersecurity: How it Affects ESG Impact and Credit Quality Download: 2025.05.28 https://www.pgim.com/fixed-income/blog/cybersecurity-how-it-affects-esg-impact-and-credit-quality

Saha, B., & Anwar, Z. (2024). A review of cybersecurity challenges in small business: The imperative for a future governance framework. Journal of Information Security, 15, 24–39. doi:10.4236/jis.2024.151003

Sentinelone, 2021 - JBS Ransomware Attack – A Comprehensive Guide 101 https://www.sentinelone.com/blog/when-jbs-met-revil-ransomware-why-we-need-to-beef-up-critical-infrastructure-security

Sontan, A., & Samuel, S. (2024). Emerging trends in cybersecurity for critical infrastructure protection: A comprehensive review. Computer Science & IT Research Journal, 5, 576–593. doi:10.51594/csitrj.v5i3.872

Spanning, 2022 - Cyberattacks 2022: Phishing, Ransomware & Data Breach Statistics. Download: 2025.05.28 https://www.spanning.com/blog/cyberattacks-2022-phishing-ransomware-data-breach-statistics/

Thompson, J. (2023). Factors Influencing Cybersecurity Risk Among Minority-Owned Small Businesses. Reviews of Contemporary Business Analytics, 6(1), 29–42. Retrieved from https://researchberg.com/index.php/rcba/article/view/114

Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. Journal of Information, Communication and Ethics in Society, ahead-of-print doi:10.1108/JICES-03-2021-0035

Voss, W. Gregory, The Concept of Accountability in the Context of the Evolving Role of ENISA in Data Protection, ePrivacy and Cybersecurity (May 28, 2021). in Technocracy and the Law: Accountability, Governance and Expertise 247-284 (Alessandra Arcuri and Florin Coman-Kund, eds, Routledge, 2021)., Available at SSRN: https://ssrn.com/abstract=4290558 or http://dx.doi.org/10.2139/ssrn.4290558

Zaid, T., & Garai, S. (2024). Emerging trends in cybersecurity: A holistic view on current threats, assessing solutions, and pioneering new frontiers. Blockchain in Healthcare Today, 7, 10.30953/bhty.v7.302. eCollection 2024. doi:10.30953/bhty.v7.302