ZEROFOX INTELLIGENCE

Flash

Series of UK Cyberattacks Inspires New Cybersecurity Law

F-2025-11-14b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Ransomware, European Critical Infrastructure

November 14, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 10:00 AM (EST) on November 13, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Series of UK Cyberattacks Inspires New Cybersecurity Law

| Key Findings

- On November 12, 2025, the Labour Party proposed a Cyber Security and Resilience Bill to the UK Parliament to enhance the United Kingdom's existing cybersecurity law and improve defenses against cyberattacks that are increasingly targeting European Union (EU) critical infrastructure.
- A series of recent cyberattacks against UK-based organizations and critical infrastructure underpin how captive the UK economy is to its industry leaders and the depth of vulnerabilities stemming from cybersecurity gaps impacting them.
- Western political priorities have demonstrated an increased focus on protecting critical infrastructure, as evidenced by U.S. and UK policies targeting the intersection of cybersecurity and national security vulnerabilities.
- ZeroFox has projected ransomware and digital extortion (R&DE) incidents targeting European critical infrastructure in 2025 will increase at least 1.7 percent year-over-year. There were at least 286 attacks in all of 2024 and at least 243 so far in 2025; if trends continue, there will likely be at least 291 incidents by the end of this year.

Details

On November 12, 2025, the Labour Party proposed a Cyber Security and Resilience Bill to the UK Parliament to enhance the United Kingdom's existing cybersecurity law, Network and Information Systems (NIS) Regulations of 2018, and improve cyber defenses against increasingly targeted EU critical infrastructure. The reform bill proposal follows a series of prominent cyberattacks in 2025 that caused major disruptions to Britain's critical infrastructure and retail sectors, including to Marks & Spencer (M&S), the Co-op, Harrods, and Jaguar Land Rover (JLR).[1]

- In April 2025, M&S, the Co-op, and Harrods reported multiple separate cyber incidents, including network intrusion attempts, personally identifiable information (PII) breaches, and impacted web domains that effectively disrupted the retail brands over the course of several weeks.
- In August 2025, UK-based automotive manufacturer JLR experienced a cyberattack and was forced to shut down its factories for over five weeks as part of efforts to contain it; the fallout from this attack is expected to be the most economically damaging cyber incident in UK history.[2]

The new bill is designed to reform the UK's singular cybersecurity law to expand protections across additional digital services and supply chains, add provisions for resources and investigative powers to ensure cyber safety measures are followed, and mandate proper reporting.[3] Notably, UK public and private sector IT and cybersecurity companies will be under mandated security regulations for the first time if the new bill passes.[4]

A series of recent cyberattacks against UK-based organizations and critical infrastructure underpin how captive the UK economy is to its industry leaders and the depth of vulnerabilities stemming from cybersecurity gaps impacting them, both of which ultimately impact the wider economy. While political and ideological targeting of the UK government and organizations is likely to continue despite the bill, the economic

[1] hXXps://www.reuters[.]com/world/uk/uk-plans-tougher-laws-protect-public-services-cyberattacks-2025-11-12/
[2] hXXps://www.bbc[.]com/news/articles/cy9pdld4y81o
[3] hXXps://www.gov[.]uk/government/collections/cyber-security-and-resilience-bill
[4] hXXps://www.helpnetsecurity[.]com/2025/11/12/uk-cyber-security-and-resilience-bill/

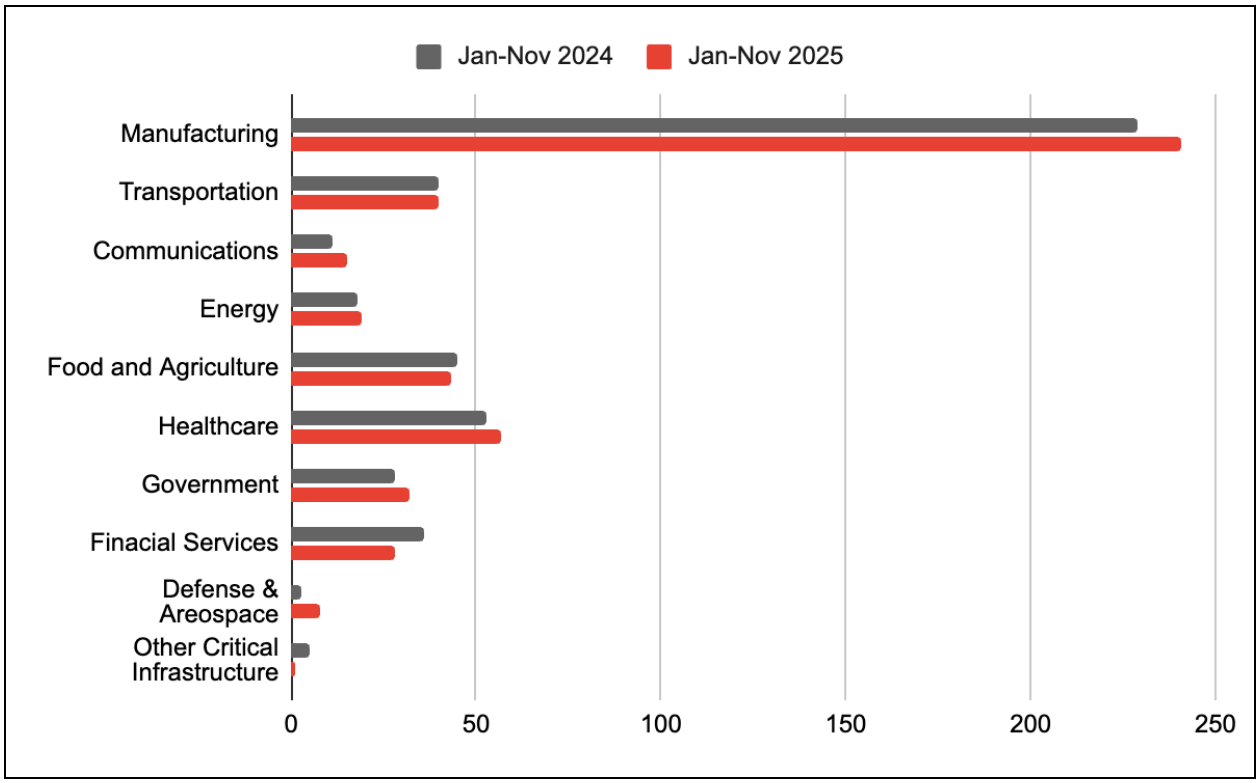
strain and severity of incidents will likely dampen as a result of reinforced cybersecurity policies.

- If the updated cybersecurity legislation is implemented, there is a roughly even chance that threat actors will shift their targeting patterns to other sectors or regions and prioritize lower-effort and higher-payoff targets.
- With strengthened legislation and continued European-led law enforcement efforts to combat cybercrime in the region, low-skilled actors are very likely to be deterred from targeting the United Kingdom.

In the past year, Western political priorities have demonstrated an increased focus on protecting critical infrastructure—especially manufacturing—as evidenced by U.S. and UK policies targeting the intersection of cybersecurity and national security vulnerabilities. It is unclear whether these measures are driving cyber threat actors to target these sectors, but it is apparent that Western governments have determined that protecting industrial jobs and profitability are long-term priorities.

European R&DE Targeting Trends

ZeroFox has projected R&DE incidents targeting European critical infrastructure in 2025 will increase at least 1.7 percent year-over-year. There were at least 286 attacks in all of 2024 and at least 243 attacks so far in 2025; if similar trends persist to the end of this year, the projected 2025 total will likely reach approximately 291 attacks.



R&DE Incidents Targeting European Critical Infrastructure (January 2024–November 2025)

Source: ZeroFox Intelligence

Attacks targeting the European Healthcare, Government, and Communications sectors have all increased in 2025. The EU Defense & Aerospace sector had the largest proportional jump—an approximate 167 percent increase from 2024. Financial Services has experienced a slight decline of incidents so far this year. Incidents impacting European Manufacturing—one of the highest-targeted critical infrastructure sectors—have risen at least 5.2 percent year-to-date in 2025; if trends remain consistent, the sector is on pace to likely meet or exceed 2024's total by year-end.

The total attacks in 2025 will likely increase slightly by 1–3 percent, hovering near at least 290–295 incidents. However, industry targeting is shifting, with a more significant focus on government, healthcare, and defense-related industries, which is likely tied to geopolitical activity. While overall volume appears stable, the sectoral distribution demonstrates notable shifts, suggesting evolving threat priorities against EU critical infrastructure.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%