IBM UK Newsroom

IBM Security Report: Energy Sector Becomes UK’s Top Target for Cyberattacks as Adversaries Take Aim at Nation’s Critical Industries

• Energy sector saw 24% of all UK cyberattacks in 2021, followed by manufacturing and financial services with 19% each, increasing pressure on supply chain challenges and energy costs

• UK was one of the top three most-attacked countries in Europe in 2021, along with Germany and Italy

• Data theft was the most common attack type in the UK during 2021, making up 31% of incidents – though ransomware was top globally, with 21% of attacks (UK: 15%)

ARMONK, N.Y. and LONDON, UK, 23 February 2022 – IBM Security (NYSE: IBM) today released its 2022 X Force Threat Intelligence Index, which reveals the UK’s energy industry was the country’s top target for cyberattacks, accounting for 24% of all incidents, followed by manufacturing and financial services, which each received 19% of attacks. The UK became one of the top three most attacked countries in Europe in 2021, along with Germany and Italy, according to the report.

The study comes amid intense pressure on the UK’s energy and manufacturing sectors, with the energy regulator preparing to increase its cap on prices by over 50% in April, and ongoing supply chain challenges. With the cost of cyberattacks trickling down to consumers, the findings highlight the urgent need for robust cyber resiliency in the nation’s critical industries.

The UK has been stepping up its efforts to meet the security challenge, with the government recently publishing the National Cyber Strategy and Government Cyber Security Strategy 2022-2030, as well as proposing amendments to the Network and Information Systems (NIS) Regulations to improve the cyber resilience of UK businesses. The Government’s latest Annual Cyber Sector Report also showed record investment in the cybersecurity sector last year, with revenues exceeding £10 billion.

Laurance Dine, Global Partner, X-Force Incident Response, IBM, said: “Cybercriminals worldwide are becoming increasingly resilient, resourceful, and stealthy in their pursuit of critical data. In Europe, we saw adversaries overwhelmingly exploiting unpatched vulnerabilities to infiltrate victim environments in 2021, highlighting the importance of adopting a Zero Trust approach to security. Businesses must start operating under the assumption of compromise, putting the proper controls in place to defend their environment and protect critical data.

“In the UK, critical industries such as energy, manufacturing and finance are key targets for cybercriminals, underlining the importance of the government’s National Cyber Security Strategy to ensure the economy remains resilient in our fast-moving digital world.”

The 2022 IBM Security X Force Threat Intelligence Index found:

Ransomware’s Reign is Far from Over

This notorious attack, which typically “locks” a computer system until a sum of money is paid, has accounted for more than one in five cyberattacks worldwide (15% in the UK). Other findings include:

- The REvil ransomware group was responsible for 37% of all ransomware attacks X-Force observed in 2021.
- Data theft was the most common attack type in the UK during 2021, making up 31% of incidents.
- Phishing was overwhelmingly the top infection method used against UK businesses in 2021, leading to 63% of incidents.

Businesses Remain Vulnerable to Attacks

Vulnerability exploitation, a term used to describe a threat actor taking advantage of an unpatched flaw or weakness in an IT system, remains a top challenge for– in fact:

- The number of network compromises caused by vulnerability exploitation rose 33% in a year.
- Vulnerability exploitation was the cause of 44% of ransomware attacks
- In Europe, 46% of cyberattacks were caused by vulnerability exploitation.

“Manu-fractured” Supply Chains

- Manufacturing was the most attacked industry globally in 2021, with ransomware persisting as the main culprit, representing 23% of attacks.
- In the UK, energy was the top-attacked industry, with 24% of incidents, followed by manufacturing and finance and insurance, each receiving 19% of attacks.

Commenting on the findings, Simon Hepburn, CEO, UK Cyber Security Council said: “IBM Security’s latest research highlights the constantly evolving nature of the global cyber threat, as adversaries seize on new vulnerabilities created by digital transformation. With the UK’s critical industries under constant threat, it’s imperative that the UK rapidly expands its professional cyber security workforce by investing in training and professional development opportunities. Providing pathways for people to enter the profession as career changers or graduates, as well as ensuring people from all backgrounds have access to opportunities, will be key to achieving this.”

Julian David, **Chief Executive Officer, techUK said:** “The IBM Security X-Force Threat Intelligence Index highlights the developing cyber threats we face globally, with Ransomware continuing to grow as the go-to attack method for cyber-criminals. Clear growth in attacks across all sectors – notably Manufacturing and Energy – and the fact the UK is now one of the most targeted countries in Europe, the second-most targeted region globally, should harden all organisations’ resolve to strengthen their cyber resilience. Fortunately, the UK has a world-leading cyber industry and a clear longstanding National Strategy which stands ready to offer further support across the country. At techUK we have 250 member companies working to address this threat and reports such as this are important in highlighting where we need to direct our efforts.”

The Charter Of Trust, a global initiative aimed at advancing security standards and cross-sector collaboration in cybersecurity, welcomed the report, stating: "With IBM revealing that nearly half of cyberattacks observed in Europe were caused by vulnerability exploitation last year, it's more important than ever that industry and policy strengthen their threat information sharing ecosystem, increase standardisation, and combine know-how to evolve and enhance organisations' defences against new cyber threats."

The annual report from IBM Security X-Force, which maps the latest security trends and attack patterns, analysed global data ranging from network and endpoint detection devices, incident response (IR) engagements, and phishing kit tracking, from January to December 2021.

To read the full report, please visit: https://www.ibm.com/security/data-breach/threat-intelligence/

Notes to Editors

About IBM

IBM is a leading global hybrid cloud and AI, and business services provider. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. Nearly 3,000 government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM’s hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM’s breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and business services deliver open and flexible options to our clients. All of this is backed by IBM’s legendary commitment to trust, transparency, responsibility, inclusivity and service.

Visit www.ibm.com for more information.

IBM Contact
Gregor Hastings
UKI External Relations
Gregor.Hastings@IBM.com
