UK businesses faced record cyberattack attempts in Q3 2026

- **Beaming's latest Cyber Threat Analysis recorded an average of 203,585 detected attempts per monitored business, up 7.0% on Q3 2025.**
- **Businesses faced an average of 2,213 attempts a day, with remote control services the most targeted of the eight service categories tracked.**
- **Beaming encourages business leaders to use Cyber Security Awareness Month to review security settings, access permissions and recovery plans.**

8 October 2026, Hastings, UK: UK businesses monitored by business internet service provider Beaming faced an average of 203,585 detected cyberattack attempts each between July and September 2026, the highest quarterly figure recorded since Beaming began its analysis.

The total was 7.0% higher than in the same period last year and 6.7% above the previous quarter, equivalent to an average of 2,213 attempts per business every day.

Published during October's Cyber Security Awareness Month, the findings reinforce the value of regular checks on the systems businesses depend on to work, communicate and serve customers.

Beaming is encouraging business owners, directors and IT teams to review whether their security arrangements still reflect how their business operates, particularly where staff, suppliers or systems have changed.

Connected devices and web services were the most targeted categories

Remote control services, used to manage internet-connected devices such as networked security cameras and building control systems, were the most heavily targeted of the eight service categories tracked by Beaming. They attracted an average of approximately 193 detected attempts per business each day.

Web services were the second most targeted category, reinforcing the importance of protecting the online systems businesses use to serve customers and manage operations. Web services can include websites, customer portals and browser-based interfaces for managing equipment.

Businesses should work with their IT team or provider to check which devices and online services need to be accessible from the internet, review staff and supplier permissions, and remove remote access that is no longer needed. Access to administration functions should be restricted and software kept supported and updated, with

clear responsibility for security updates, monitoring and recovery where an external provider manages the service.

Increase in attack traffic from infrastructure in Brazil

Beaming also recorded an increase in source IP addresses associated with infrastructure in Brazil. The sum of monthly unique source IP addresses rose from 19,849 in Q2 to 29,312 in Q3, an increase of 47.7%.

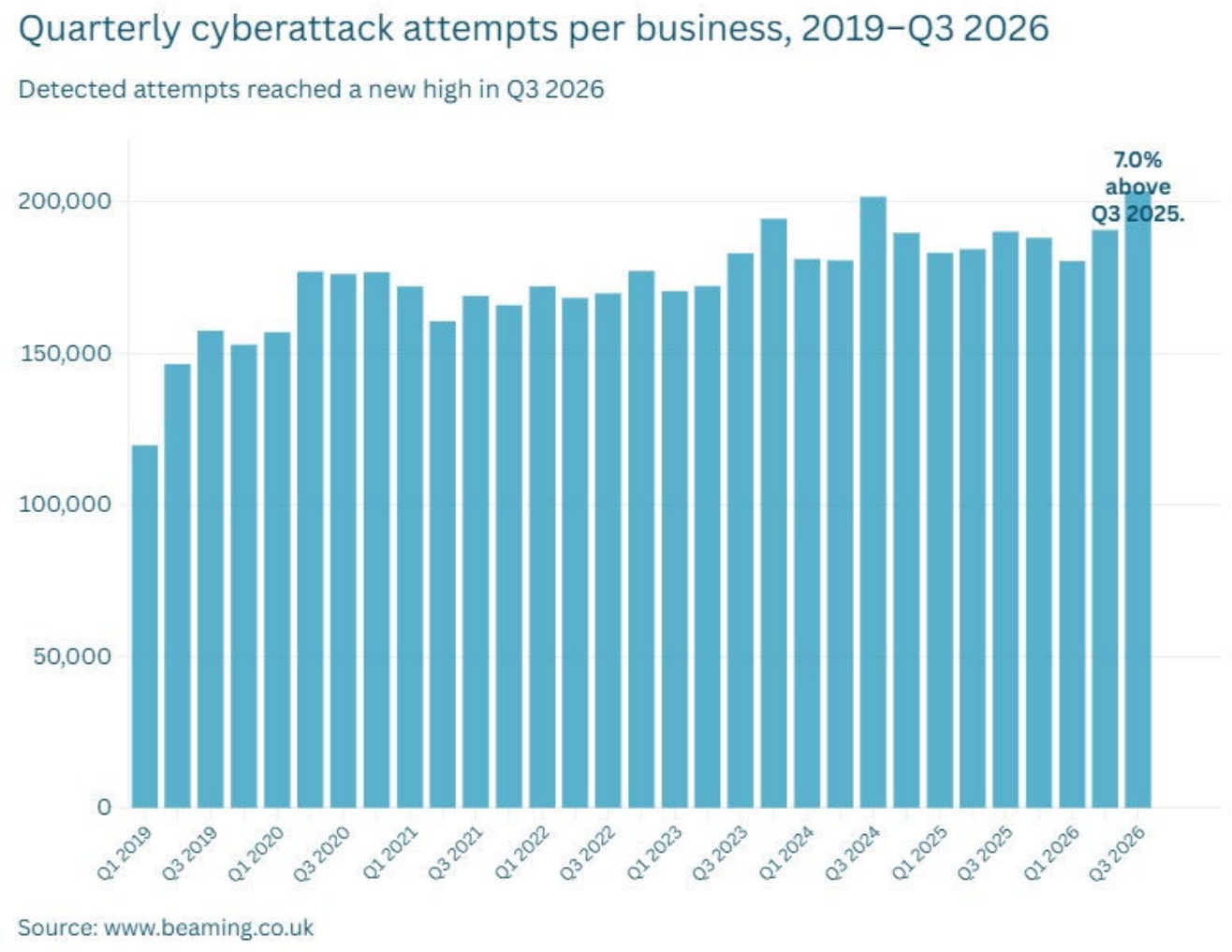
Within the ten-country comparison group tracked by Beaming, China and the USA remained above Brazil. Source IP locations indicate where the infrastructure used for an attack is located, rather than necessarily identifying where the attacker is based.

Sonia Blizzard, Managing Director of Beaming, commented:
"Good cyber security needs to keep pace with the way your business works. When people join or leave, suppliers need access, or new systems are introduced, it is worth checking that permissions and protection still fit. These figures are a useful prompt to have that conversation with your IT team or provider. Keeping systems up to date, reviewing access, and testing recovery arrangements helps businesses prepare, while allowing their people to get on with their work."

Practical checks to support business resilience

Beaming recommends that business leaders work with their IT team or provider to:

- Keep systems supported and updated: Check that operating systems, applications, routers and firewalls receive security updates, and replace or upgrade unsupported technology.
- Review firewall settings and remote access: Remove unnecessary access, check permissions for staff and suppliers, and use multi-factor authentication (MFA) to strengthen protection for remote access and other business accounts.
- Check incident and recovery arrangements: Agree who reviews security alerts and coordinates a response, keep escalation contacts current, and test that backups can be restored.



ENDS

Notes to editors

- Beaming has analysed cyberattacks in real-time targeting thousands of UK-based businesses since the beginning of 2016 to better understand their nature and origin. From this, it can calculate the average number of attacks businesses receive and use the analysis results to help organisations improve their cyber security. Detected attempts do not necessarily represent successful breaches.
- To download a picture of Sonia Blizzard or charts to accompany this press release please visit https://www.beaming.co.uk/media-resources/

For more information please contact:
Rachael White – Marketing Manager
press@beaming,biz
01424 462613

About Beaming: www.beaming.co.uk

Established in 2004, with offices in Sussex and Kent, Beaming is a specialist internet service provider (ISP) for businesses, supplying thousands of organisations across the UK with fast, reliable, and secure voice and data connectivity. Beaming works with businesses across the UK that rely on the internet and need an ISP partner to ensure they are always connected and protected online. Follow Beaming online and on LinkedIn to get regular updates on its cyber threat analysis and new IT insights.