Web Security in the age of AI

September 2026

Account Manager

Charles Penny

FALCON DIGITAL | CLIENT SECURITY BRIEFING | SEPTEMBER 2026

FALCON DIGITAL

Web Security in the Age of AI

Why website hosting and maintenance must change

CLIENT REPORT | RESEARCH CUT-OFF: 7 SEPTEMBER 2026

A clear, practical guide for Falcon Digital clients

This report explains how artificial intelligence is accelerating familiar cyber threats, why modern websites need continuous protection, and how Falcon Digital is upgrading its management and security approach.

Prepared by Integral Digital Technologies Ltd trading as Falcon Digital

Company number 13682575 | Registered in England and Wales

Suite 6, 6 St Paul's Road, Newton Abbot, Devon, TQ12 2HP

falcondigital.co.uk

> **IMPORTANT CONTEXT**
> Security statistics measure different things. A blocked request, a vulnerability, an attack and a confirmed data breach are not interchangeable. This report labels them carefully so that the figures inform rather than alarm.

Contents

OUR CORE MESSAGE

AI is an amplifier. It is helping attackers work faster and at greater scale, but most successful intrusions still depend on familiar weaknesses: vulnerable software, stolen credentials, poor configuration, weak access controls and slow detection. [5]

1. Executive summary

The web has always been scanned by automated systems. What is changing is the speed, volume and quality of that automation. The UK National Cyber Security Centre (NCSC) assesses that AI will almost certainly make parts of cyber intrusion more effective and efficient, increasing the frequency and intensity of threats through 2027. It also expects AI to improve existing attack methods rather than create entirely new ones. [1]

That matters for websites because they are permanently connected, publicly discoverable and built from many moving parts: the hosting operating system, web server, content-management system, theme, plugins, APIs, forms, payment services and user accounts. A weakness in any one of those parts can create an entry point.

THE PRACTICAL CONCLUSION
Traditional hosting kept a website online. Modern managed hosting must also know what software is present, identify urgent vulnerabilities, apply or shield critical fixes quickly, filter hostile automation, detect unusual change, preserve recoverable backups and support a disciplined incident response.

Five things clients should take from this report

1. **Your website is being tested continually.** Most activity is automated and most is blocked; it is not evidence that somebody is personally targeting your organisation.
2. **AI shortens the attacker's working time.** It can speed up reconnaissance, vulnerability research, phishing, coding and analysis of stolen data. [1]
3. **The patch window is shrinking.** Industry telemetry found a weighted median of five hours to mass exploitation for heavily exploited WordPress vulnerabilities disclosed in 2025. [6]
4. **Security is now a continuous service.** Monthly or ad-hoc updates alone cannot provide the speed, visibility or recovery capability that modern websites require.
5. **No system can promise zero risk.** Good security reduces the likelihood of compromise, limits the damage, improves detection and makes recovery faster and more reliable.

Falcon Digital's operational context

MORE THAN ONE MILLION SUSPICIOUS REQUESTS IN AN HOUR
Recent Falcon Digital monitoring has recorded periods in which the wider server group received more than one million suspicious or hostile automated requests and probes within an hour. This does not mean one million successful compromises or one million individual attackers. It reflects repeated, machine-generated activity across multiple websites and defensive layers. Counts depend on how each tool classifies and aggregates requests.

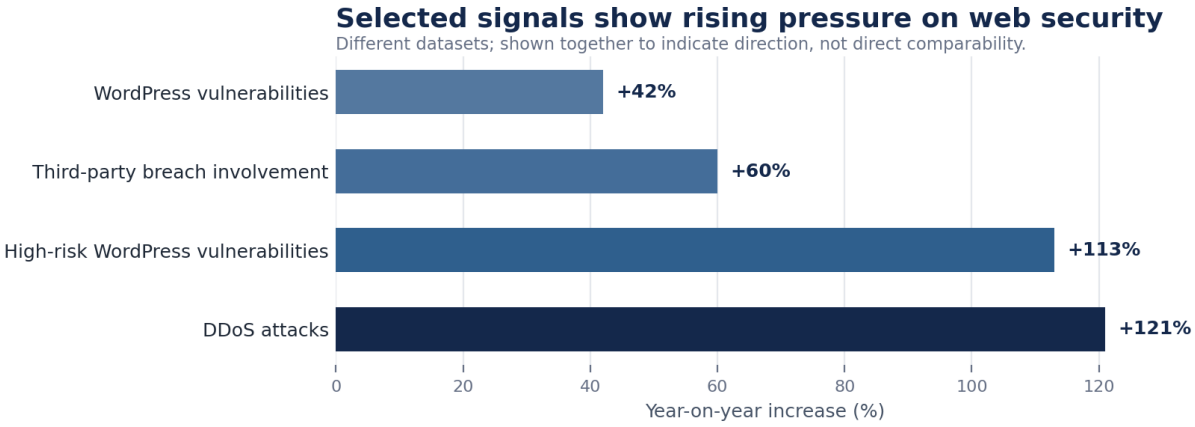
The wider internet data is consistent with this high-volume environment. Cloudflare reported 47.1 million DDoS attacks during 2025, a 121% rise from the prior year, and an average of 5,376 DDoS attacks mitigated every hour across its network. In the final quarter of 2025, the UK rose to sixth among the locations most targeted by DDoS activity in that dataset. [7]

2. The evidence at a glance

The following figures come from current government, threat-intelligence and web-security research. Each source has a different scope and methodology, so the figures should be read as complementary signals rather than added together.

FIGURE	WHAT IT SHOWS	FIGURE	WHAT IT SHOWS
43%	of UK businesses identified a breach or attack in the previous 12 months *DSIT 2025/26 [3]*	**5 hours**	weighted median to first mass exploitation among heavily exploited WordPress flaws *Patchstack [6]*
31%	of breaches in Verizon's 2026 DBIR began with exploitation of a software vulnerability *Verizon [4]*	**47.1m**	DDoS attacks were mitigated by Cloudflare during 2025 *Cloudflare [7]*
11,334	new WordPress ecosystem vulnerabilities were reported for 2025 *Patchstack [6]*	**48%**	of breaches involved a third party in Verizon's 2026 dataset *Verizon [4]*

The UK government's 2025/26 survey estimates that 43% of businesses and 28% of charities experienced an identifiable cyber breach or attack in the previous year - approximately 612,000 businesses and 57,000 charities. Medium and large businesses reported higher prevalence at 65% and 69%. The survey also warns that unidentified attacks mean the true level may be higher. [3]



Sources: Patchstack State of WordPress Security 2026; Verizon 2026 DBIR; Cloudflare DDoS Threat Report 2025 Q4. Different datasets and populations; not directly comparable. [4, 6, 7]

HOW TO READ THESE FIGURES

Attack volume is not the same as compromise, and a vulnerability is not automatically exploitable on every site. Risk depends on the affected version, configuration, privileges, exposure and active exploitation. Vendor telemetry reflects each source's own customers and definitions; no single dataset represents the whole internet.

3. What AI changes

The NCSC's assessment to 2027 is unusually clear: AI is expected to make existing cyber intrusion methods more effective and efficient. It identifies reconnaissance, vulnerability research, exploit development, social engineering, basic malware generation and processing stolen data as areas where threat actors are already gaining assistance. [1]

Six ways AI can accelerate an attack

6. **Faster reconnaissance.** AI can summarise public information about an organisation, its people, technology and suppliers, helping an attacker decide where to focus.
7. **More convincing deception.** Generative tools can improve spelling, tone, translation and personalisation, making fake emails, password-reset requests, invoices and support messages harder to spot.
8. **Quicker vulnerability work.** AI can help skilled operators review code, adapt proof-of-concept exploits and search for common configuration errors. The NCSC expects the time between disclosure and exploitation to shrink further.
9. **Cheaper automation.** Tasks that previously required more time or specialist skill can be repeated across thousands of domains, accounts or software versions.
10. **Faster evasion and adaptation.** Attackers can modify scripts, infrastructure and malicious code more quickly. This makes static blocklists and occasional manual reviews less effective on their own.
11. **Quicker use of stolen data.** AI can classify and summarise exfiltrated information, helping criminals identify valuable personal data, credentials or commercial material.

> **WHAT AI DOES NOT MEAN**
> It does not mean that ChatGPT, Claude or another well-known assistant is personally attacking a website. These are general-purpose technologies. The threat comes from misuse of commercial, open-source or purpose-built tools by people and criminal groups. Google Mandiant also cautions that it did not consider 2025 a year in which breaches were directly caused by AI; most successful intrusions still arose from human and systemic failures. [5]

AI also helps defenders

The same pattern-recognition and automation capabilities can help defenders triage alerts, identify suspicious behaviour, prioritise vulnerabilities and respond consistently across large groups of websites. IBM's 2025 UK study of breached organisations found that those using security AI and automation extensively reported average breach costs of £3.11 million, compared with £3.78 million among those not using those technologies. Those enterprise figures should not be treated as a forecast for an individual small business, but they do demonstrate the value of faster detection and containment. [11]

> **THE REAL CONTEST IS SPEED AND VISIBILITY**
> The practical challenge is not 'humans versus AI'. It is whether defenders have enough visibility and automation to keep pace with automated hostile activity while retaining experienced people to make risk decisions, investigate anomalies and manage recovery.

4. The main threats to websites

A modern website can be attacked through its code, its users, its hosting environment or a connected supplier. The most important risks are familiar, but automation allows them to be tested more frequently and at greater scale.

THREAT	WHAT IT CAN MEAN FOR A WEBSITE
Stolen or guessed credentials	Bots test leaked username and password combinations against administrator logins. Phishing and fake support requests can also persuade a genuine user to approve access.
Vulnerable plugins, themes and libraries	An attacker scans for a known affected version and attempts the same exploit across many websites. A popular component can create a large, attractive target.
Broken access control	A user or unauthenticated visitor is able to do something the website should not permit, such as viewing private data, installing a plugin or elevating privileges.
Injection and malicious input	Crafted input sent through a form, API, URL or database query may be used to change data, run code or expose information.
Malware, backdoors and persistence	After entry, attackers may inject code into legitimate files, create hidden administrator accounts or leave mechanisms that restore the infection after a superficial cleanup.
SEO spam, redirects and payment skimming	A compromised website may silently serve spam to search engines, redirect selected visitors, capture card details or damage the organisation's reputation.
DDoS and resource exhaustion	Large volumes of requests can make a site slow or unavailable. Smaller application-level floods can target expensive pages, searches, logins or APIs.
Third-party and supply-chain compromise	A breach at a software vendor, hosting service, analytics tool, email account, payment platform or developer can create a route into downstream websites.
Misconfiguration and exposed secrets	Public backups, weak file permissions, forgotten staging sites, exposed API keys and unnecessary services can reveal data or provide access.
Unmonitored change	If nobody is watching for unexpected files, new users, altered DNS, expired certificates or sudden traffic patterns, an incident may remain hidden for longer.

The 2025 OWASP Top 10 for web applications places broken access control, security misconfiguration and software supply-chain failures in its top three categories. [8]

WHY A SMALL WEBSITE IS STILL USEFUL TO AN ATTACKER

Attackers do not always want the client's own data. A compromised site can be used to send spam, host phishing pages, redirect visitors, mine cryptocurrency, attack other systems, manipulate search results or become part of a botnet. Automation makes low-profile websites economical to target.

5. Why WordPress needs active management

WordPress remains the world's largest content-management ecosystem. W3Techs reported on 7 September 2026 that it powered 40.7% of all websites it measured and held 58.9% of the CMS market. Its popularity, flexibility and enormous extension ecosystem are strengths, but they also give attackers a large pool of sites on which the same automated technique may work. [12]

The 2025 WordPress vulnerability picture

FIGURE	WHAT PATCHSTACK REPORTED	WHY IT MATTERS
11,334	new vulnerabilities reported in the WordPress ecosystem	+42% year on year
91%	of reported vulnerabilities were in plugins	9% in themes; only six low-priority core issues
4,124	were assessed by Patchstack as representing a real threat	36% of the total
1,966	were rated high priority for likely automated mass exploitation	17% of the total; +113% year on year
46%	did not have a developer fix by public disclosure	updates alone cannot cover an unpatched disclosure
5 hours	weighted median to exploitation for the most heavily targeted flaws	roughly half of high-impact flaws were exploited within 24 hours

Source: Patchstack, State of WordPress Security in 2026, using vulnerability and exploitation telemetry from 2025. Vendor research; definitions and customer coverage should be considered when interpreting the figures. [6]

Why 'just run the updates' is no longer enough

12. **A fix may not exist when a vulnerability becomes public.** A temporary protection rule or removal of the affected component may be required.
13. **An update can introduce compatibility problems.** Critical updates still need monitoring, backup, verification and a rollback route.
14. **Old flaws remain useful to attackers.** Automated scans continue to test for vulnerable versions long after the original disclosure.
15. **A site may already be compromised.** Updating the vulnerable plugin does not automatically remove injected code, hidden accounts or stolen credentials.
16. **Traditional network rules may miss application-specific abuse.** Patchstack's own 2025 testing reported materially different and often low block rates against WordPress-specific exploits, reinforcing the case for vulnerability-aware protection. [6]

> **THE FIVE-HOUR PROBLEM**
> The operational lesson is not that every disclosed flaw must be installed blindly within five hours. It is that a managed service needs live vulnerability intelligence, an accurate software inventory, risk prioritisation, temporary shielding where possible, backups, controlled updating and post-update verification.

6. How hosting and maintenance are changing

The old model separated hosting from maintenance: the server kept the site online, while somebody occasionally logged in and applied updates. The modern model treats availability, security, software health and recovery as one continuous system.

AREA	TRADITIONAL APPROACH	MODERN MANAGED APPROACH
Software inventory	A list created when the site launches	Continuously updated visibility of core, themes, plugins, versions, licences and exposed services
Updates	Monthly, quarterly or when remembered	Risk-led updates with urgent handling for active exploitation, plus testing, verification and rollback
Firewall	Generic server firewall	Layered edge, network and application controls with rate limits, bot filtering and vulnerability-specific rules
Malware	Scan after a complaint	Server-level and application monitoring, file-integrity checks and investigation of persistence
Access	One administrator password	Unique accounts, least privilege, MFA, account reviews and rapid removal of leavers
Monitoring	A simple 'is the homepage up?' check	Uptime, SSL, domain/DNS, performance, resource, change and security alerting
Backups	A backup exists somewhere	Frequent, isolated, retained and periodically tested restore points
Response	Clean the site when it breaks	Prepared containment, evidence capture, credential reset, recovery, communication and lessons learned
Management	Each site handled separately	Central fleet management so urgent action can be coordinated across every affected website

The NCSC's May 2026 'patch wave' guidance tells organisations to prioritise internet-facing attack surfaces and prepare to deploy security updates quickly, more frequently and at scale. It recommends an 'update by default' policy, ideally using secure hot patching or automatic updates where suitable, while recognising that patching alone will not resolve unsupported or end-of-life technology. [2]

> **SHARED RESPONSIBILITY STILL MATTERS**
> A hosting provider can secure infrastructure and provide managed controls, but the website owner still controls many risk decisions: who has access, what data is collected, which third-party services are requested, whether suspicious requests are reported, and whether the organisation maintains its own cyber and data-protection procedures.

A modern website protection model

17. **Know the estate.** Maintain an accurate inventory of websites, components, versions, users, domains, certificates, integrations and data flows.
18. **Reduce exposure.** Remove unused plugins and accounts, close unnecessary services, harden configuration and put protective controls in front of public endpoints.
19. **Move quickly on vulnerabilities.** Use live intelligence, prioritise active exploitation, apply tested updates and use compensating controls or virtual patching when no safe fix is available.
20. **Protect identity.** Use MFA, unique accounts, least privilege, credential monitoring and prompt removal of access that is no longer required.
21. **Detect unexpected behaviour.** Monitor files, administrators, traffic, errors, resources, DNS, SSL and logs so suspicious change is visible before a customer reports it.
22. **Design for recovery.** Keep frequent, isolated backups; protect backup access; test restores; and retain enough history to recover from delayed discovery or reinfection.
23. **Prepare the response.** Define who investigates, who decides, how the site is contained, what records are kept, how clients are told and when legal or regulatory reporting is considered.

These layers align with current NCSC Cyber Essentials themes: firewalls, secure configuration, security update management, user access control and malware protection. The 2026 requirements also emphasise asset management and strongly recommend regular backups. [10]

> **DEFENCE IN DEPTH**
> Every control can fail. A layered model assumes that one update may be late, one password may be stolen or one rule may miss an attack. The remaining layers should still prevent, detect, contain or recover from the event.

7. Falcon Digital's response

Falcon Digital is moving its managed websites onto a more centralised protection and management approach. The purpose is to give our team faster visibility across the whole website group and to reduce the time between an emerging issue, a decision and protective action.

What the new approach is designed to provide

CAPABILITY	CLIENT BENEFIT
Centralised website oversight	A consistent view of site status, software, alerts and required actions across the websites we manage.
Vulnerability-aware protection	Faster identification and prioritisation of relevant security issues, with protective action based on the software actually present.
Automated critical maintenance	Quicker handling of suitable critical security updates, supported by monitoring and recovery controls.
Improved uptime monitoring	Stronger availability checks and clearer alerting when a website or critical service cannot be reached.
Layered hostile-traffic controls	Better filtering, rate controls and protective rules to reduce automated probing and abusive requests before they reach the website.
Deeper malware and change visibility	Monitoring intended to identify suspicious files, changes or behaviour that a simple homepage check cannot see.
Coordinated incident handling	A repeatable route to investigate, contain, restore, communicate and document serious events.

WHAT ONBOARDING MEANS

Websites will be added to the new management system in phases. Falcon Digital will confirm completion individually. The exact controls available can vary by website, hosting arrangement, software stack and maintenance package; any site-specific issue or required client decision will be communicated directly.

What we will not claim

24. **That any website is 'unhackable'.** No responsible provider can guarantee that.
25. **That every automated request is an AI attack** or a determined human adversary.
26. **That automation removes the need for skilled people.** Monitoring, investigation and risk decisions still require human judgement.
27. **That a security tool replaces the client's own responsibility** for users, content, data protection and third-party accounts.

OUR COMMITMENT

We will continue to improve the layers around the websites we manage, communicate material issues clearly and use evidence-led controls to reduce risk, disruption and recovery time.

8. What clients can do

Most clients do not need to become cyber-security specialists. A handful of practical behaviours materially improve the protection Falcon Digital can provide.

28. **Use MFA wherever it is offered.** Prioritise website administrators, domain registrar, DNS, email, payment, booking and cloud accounts.
29. **Use unique passwords.** Do not reuse the website password for email or another service. A password manager makes this manageable.
30. **Keep access current.** Tell Falcon promptly when a staff member, volunteer, trustee or supplier leaves or no longer needs access.
31. **Do not install unapproved software.** Ask before adding plugins, themes, tracking scripts or external integrations. Every component adds code, permissions and a supplier relationship.
32. **Treat urgent requests with care.** Verify unexpected requests to reset passwords, approve MFA prompts, change payment details, transfer a domain or disclose access.
33. **Keep ownership details current.** Maintain access to the registered domain, billing method and administrative email so security or expiry notices are not missed.
34. **Report unusual behaviour quickly.** Unexpected redirects, new users, strange emails, browser warnings, missing orders or altered content may be early indicators.
35. **Maintain your own important records.** Keep copies of essential content, customer or member data and business records in line with your retention and legal obligations.
36. **Plan who decides during an incident.** Know who in your organisation can authorise containment, password resets, customer communication and regulatory decisions.

> **PLEASE COORDINATE CHANGES**
> Unauthorised changes can bypass controls, introduce incompatible software or overwrite forensic evidence. If you need a new administrator, plugin, integration, migration or DNS change, contact Falcon Digital first so it can be handled safely.

A simple internal client checklist

37. We know who is authorised to request website changes.
38. Every administrator has their own account and uses MFA where available.
39. Leavers and old suppliers have had access removed.
40. Our domain and billing contacts are current.
41. Staff know how to report a suspicious website or account event.
42. We know who will lead a personal-data breach assessment.

9. Incidents and UK data protection

A website security incident and a personal data breach are related but not identical. A personal data breach occurs where security failure causes personal data to be destroyed, lost, changed, disclosed without authorisation, accessed without authorisation or made unavailable in a way that significantly affects people.

What the ICO expects

43. **Assess whether personal data was affected** and the likely risk to people's rights and freedoms.
44. **Notify the ICO of a notifiable breach** without undue delay and, where feasible, within 72 hours of becoming aware of it. [9]
45. **Tell affected people without undue delay** when the breach is likely to create a high risk to their rights and freedoms. [9]
46. **Keep a record of every personal data breach**, including incidents that are assessed as not reportable. [9]
47. **Maintain robust detection, investigation and internal reporting procedures** so decisions can be made in time. [9]

> **NOT EVERY EVENT MUST BE REPORTED**
> The ICO's test is risk-based. If a personal data breach is unlikely to result in a risk to people's rights and freedoms, it may not need to be reported to the ICO, but the decision and reasoning should still be documented. Clients remain responsible for their own legal assessment as data controller, with Falcon providing relevant technical information in line with the applicable contract. [9]

Why monitoring matters to compliance

The 72-hour period runs from awareness, not from the end of a complete forensic investigation. Better monitoring and clearer escalation help an organisation establish what happened, contain it and make a defensible reporting decision. The ICO allows information to be supplied in phases where a full investigation cannot be completed within the initial window. [9]

A sensible first-response sequence

48. **Contain.** Protect visitors and data: restrict access, isolate the affected site or component, and preserve backups.
49. **Preserve.** Keep relevant logs, alerts, files, timestamps and communications. Avoid unnecessary changes that erase evidence.
50. **Investigate.** Identify the entry point, affected systems, users, data and the period of exposure.
51. **Recover.** Remove persistence, reset access, patch or replace the cause, restore safely and verify integrity.
52. **Assess and communicate.** Decide whether clients, individuals, insurers, banks, regulators or law enforcement need to be informed.
53. **Improve.** Record lessons and change controls so the same route is less likely to succeed again.

This section provides general information, not legal advice. Reporting duties depend on the facts, the data affected, contractual roles and the law applying to the organisation.

10. Client questions

Is AI attacking my website?

AI may assist a person or criminal service with parts of an attack, but routine logs rarely prove that a particular request was AI-generated. It is more accurate to say that websites face growing automated activity and that AI is increasing the capability and speed available to some attackers.

Does a million attack attempts mean our websites were breached?

No. High figures usually count requests, probes, scans or login attempts, often repeated by the same automated infrastructure. They describe pressure on defensive systems, not successful access.

Why was occasional maintenance enough before?

It was never risk-free, but slower disclosure and exploitation cycles gave teams more time. Modern automation, larger software supply chains and five-hour exploitation windows for some WordPress flaws make continuous visibility and prioritisation much more important.

Will automatic updates break the website?

Any software change can create a compatibility problem. A managed approach combines risk-based automation with monitoring, backups, verification and rollback. The alternative - delaying a critical fix without compensating protection - can carry a greater risk.

Can Falcon guarantee that our website will never be hacked?

No reputable provider can make that guarantee. Falcon's role is to reduce exposure, respond quickly, detect abnormal activity, limit impact and maintain recovery capability.

Will the new protection affect genuine visitors or search engines?

Protective rules are designed to distinguish legitimate traffic from abuse, but false positives are possible. Monitoring and tuning are part of the service, and clients should report any genuine user who is unexpectedly blocked.

Do we need to do anything during onboarding?

Usually very little. Falcon will contact each client after onboarding or if access, a software decision, account change or other action is required.

Does the new system make our organisation ICO compliant?

It supports important security and incident-response obligations, but ICO and UK GDPR compliance is broader. Your organisation remains responsible for lawful processing, privacy information, retention, contracts, cookies, staff practices and risk-based breach decisions.

What should we report to Falcon?

Unexpected redirects, browser warnings, new administrators, suspicious password-reset emails, missing orders, altered pages, unusual payment behaviour, domain notices and any loss of access to a connected account.

THE SHORT VERSION

Your website is part of a living software supply chain. The safest approach is active management: know what is running, reduce unnecessary exposure, move quickly when credible risk appears, watch for unexpected change and be ready to restore and respond.

Looking ahead

The NCSC expects a growing divide between systems that keep pace with AI-enabled threats and those that do not. It also expects a wave of software patches as AI-assisted research exposes more of the technical debt built up across open-source, commercial and cloud software. [1, 2]

That forecast does not call for panic. It calls for a better operating model. Websites should be managed as continuously changing services rather than static files that are launched and forgotten.

> **FALCON DIGITAL'S POSITION**
> We are investing in centralised management, faster critical maintenance, improved monitoring and stronger protective controls because the threat environment has changed. Our objective is simple: reduce risk, preserve trust, keep services available and give clients a clear, experienced response when something unusual happens.

For support or further information

Falcon Digital

Telephone: 01392 908804

Office hours: 9:00am to 5:00pm, Monday to Friday

Suite 6, 6 St Paul's Road, Newton Abbot, Devon, TQ12 2HP

Website: falcondigital.co.uk

Report prepared September 2026. Threat intelligence changes quickly; Falcon Digital will continue to review its controls and client guidance as new evidence and vulnerabilities emerge.

11. Sources and methodology

Research cut-off: 7 September 2026. The report prioritises UK government guidance, recognised security frameworks and first-party threat-intelligence publications. Commercial telemetry is clearly attributed. Statistics are not combined where their definitions, populations or measurement methods differ.

[1] National Cyber Security Centre. Impact of AI on cyber threat from now to 2027. 7 May 2025.

[2] National Cyber Security Centre. Preparing for a 'vulnerability patch wave'. 1 May 2026.

[3] Department for Science, Innovation and Technology / Home Office. Cyber Security Breaches Survey 2025/2026. 30 April 2026.

[4] Verizon. 2026 Data Breach Investigations Report - publication summary. 19 May 2026.

[5] Google Cloud / Mandiant. M-Trends 2026: Data, Insights, and Strategies From the Frontlines. 23 March 2026.

[6] Patchstack. State of WordPress Security in 2026. data updated 25 February 2026.

[7] Cloudflare Radar. DDoS Threat Report for 2025 Q4. 5 February 2026.

[8] OWASP Foundation. OWASP Top 10:2025. 2025.

[9] Information Commissioner's Office. Personal data breaches: a guide. updated 20 August 2025.

[10] National Cyber Security Centre. Cyber Essentials: Requirements for IT Infrastructure v3.3. April 2026.

[11] IBM UK / Ponemon Institute. Cost of a Data Breach Report 2025 - UK findings. 30 July 2025.

[12] W3Techs. Usage statistics and market shares of content management systems. accessed 7 September 2026.

Falcon Digital operational data

The Falcon Digital server-group request figure is based on internal monitoring described by Falcon Digital. It has not been independently audited and will vary by time window, systems included, defensive layer and classification rules. It should be described as suspicious or hostile automated requests/probes, not as confirmed breaches or unique attackers.

Limitations

54. Threat reports reflect their own customers, investigations and definitions; no single dataset represents the whole internet.
55. Some statistics describe observed attacks, while others describe reported incidents, vulnerabilities or confirmed breaches.
56. AI attribution is difficult. A suspicious request rarely proves which tool, model or level of human involvement produced it.
57. This report explains risk and operational good practice; it is not a penetration test, security certification, insurance assessment or legal opinion.